



UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE INGENIERÍA EN SISTEMAS
ELECTRÓNICA E INDUSTRIAL

Carrera de Ingeniería en Electrónica y Comunicaciones

TEMA:

“CALIDAD DE SERVICIO (QoS) EN LA RED MAN DE LA EMPRESA ELÉCTRICA AMBATO REGIONAL CENTRO NORTE S.A (E.E.A.S.A) Y SUS SUCURSALES”

Proyecto de Trabajo de Graduación. Modalidad: TEMI. Trabajo Estructurado de Manera Independiente, presentado previo la obtención del título de Ingeniero en Electrónica y Comunicaciones.

SUBLÍNEAS DE INVESTIGACIÓN: Programación de Dispositivos de Comunicación

AUTOR: Luis Cristóbal Azogue Talahua

PROFESOR REVISOR: Ing. Msc. Carlos Alberto Serra Jiménez

Ambato - Ecuador

Enero 2015

APROBACIÓN DEL TUTOR

En mi calidad de tutor del trabajo de investigación sobre el tema: **“CALIDAD DE SERVICIO (QoS) EN LA RED MAN DE LA EMPRESA ELÉCTRICA AMBATO REGIONAL CENTRO NORTE S.A (E.E.A.S.A) Y SUS SUCURSALES”**, del señor Luis Cristóbal Azogue Talahua, estudiante de la Carrera de Ingeniería en Electrónica y Comunicaciones, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad con el Art. 16 del Capítulo II, del Reglamento de Graduación para obtener el título terminal de tercer nivel de la Universidad Técnica de Ambato.

Ambato, Enero del 2015

EL TUTOR

Ing. Msc. Carlos Alberto Serra Jiménez

AUTORÍA

El presente trabajo de graduación titulado: **“CALIDAD DE SERVICIO (QoS) EN LA RED MAN DE LA EMPRESA ELÉCTRICA AMBATO REGIONAL CENTRO NORTE S.A (E.E.A.S.A) Y SUS SUCURSALES”**. Es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, Enero del 2015

Luis Cristóbal Azogue Talahua

C.C:180426181-4

APROBACIÓN DEL TRIBUNAL DE GRADO

La Comisión Calificadora del presente trabajo conformada por los señores docentes Ing. Mg. Patricio Córdova e Ing. Mg. Santiago Altamirano, revisó y aprobó el Informe Final del trabajo de graduación titulado: “**CALIDAD DE SERVICIO (QoS) EN LA RED MAN DE LA EMPRESA ELÉCTRICA AMBATO REGIONAL CENTRO NORTE S.A (E.E.A.S.A) Y SUS SUCURSALES**”, presentado por el señor Luis Cristóbal Azogue Talahua de acuerdo al Art. 24 del Reglamento de Graduación para obtener el Título Terminal de Tercer Nivel de la Universidad Técnica de Ambato.

Ing. Mg. Vicente Morales Lozada.
PRESIDENTE DEL TRIBUNAL

Ing. Mg. Patricio Córdova
DOCENTE CALIFICADOR

Ing. Mg. Santiago Altamirano
DOCENTE CALIFICADOR

DEDICATORIA

El presente proyecto de titulación está dedicado primeramente a Dios, por darme la fortaleza necesaria para superar los momentos difíciles; a mis padres; Luz Teresa y Manuel que siempre me han brindándome sus consejos, enseñanzas y amor, para hacer de mí una persona mejor, ya que gracias a ellos he logrado llegar hasta aquí y convertirme en lo que soy, a mis hermanos Jessica, Marco, Evelyn y Jennifer que son mis pilares para seguir adelante y que siempre me han estado apoyando en todo momento.

A toda mi familia que siempre me han brindado su apoyo y comprensión, que con consejos me han mostrado el camino correcto y motivado a seguir adelante para conseguir mis metas.

Luis Cristóbal Azogue

AGRADECIMIENTO

A Dios por darme la fuerza necesaria para luchar día a día y seguir adelante e iluminar mi camino para obrar con sabiduría y responsabilidad.

Agradezco de manera especial a mi madre Luz Teresa por apoyarme a culminar mis estudios, por su apoyo incondicional y ser el ejemplo de lucha y esfuerzo que inculco en mí.

De igual manera un agradecimiento al Ing. Msc. Carlos Serra, por ser guía en la elaboración y desarrollo de este proyecto, y por compartir sus experiencias profesional para la culminación del presente proyecto.

Un sincero agradecimiento a EEASA por brindarme la confianza para la elaboración del proyecto, al Ing. Rene Terán por su confianza, colaboración y tiempo, ayudándome a solventar dudas durante la elaboración de este proyecto y por su interés y apoyo para que este proyecto de titulación saliera adelante.

Luis Cristóbal Azogue

ÍNDICE DE CONTENIDOS

| | |
|---|----------|
| APROBACIÓN DEL TUTOR | ii |
| AUTORÍA | iii |
| APROBACIÓN DEL TRIBUNAL DE GRADO | iv |
| DEDICATORIA | v |
| AGRADECIMIENTO | vi |
| RESUMEN EJECUTIVO..... | xvii |
| ABSTRACT | xviii |
| GLOSARIO DE TÉRMINOS | xix |
| INTRODUCCIÓN | xxi |
| CAPÍTULO 1: | 1 |
| EL PROBLEMA | 1 |
| 1.1 Tema..... | 1 |
| 1.2 Planteamiento del Problema | 1 |
| 1.3 Delimitación del Problema | 2 |
| 1.4 Justificación..... | 3 |
| 1.5 Objetivos | 4 |
| 1.5.1 Objetivo General | 4 |
| 1.5.2 Objetivos Específicos | 4 |
| CAPÍTULO 2 | 5 |
| MARCO TEÓRICO | 5 |
| 2.1 Antecedentes Investigativos | 5 |
| 2.2 Fundamentación Teórica | 6 |
| 2.2.1 Redes de Datos | 7 |
| 2.2.2 Medios de Transmisión | 8 |
| 2.2.3 Redes Inalámbricas..... | 10 |
| 2.2.4 Estándares de las redes Inalámbricas (IEEE 802.11)..... | 11 |
| 2.2.5 Calidad de Servicio (QoS)..... | 12 |

| | |
|--|-----------|
| 2.2.6 Técnicas de Priorización de Tráfico | 14 |
| 2.2.7 Modelos de Priorización QoS | 16 |
| 2.2.8 Ventajas y desventajas que presenta el método IntServ y DiffServ. | 20 |
| 2.2.9 Mecanismos para Administrar Calidad de Servicio (QoS) | 21 |
| 2.2.10 Clasificación del Tráfico | 25 |
| 2.2.11 Calidad de Servicio (QoS) en Redes Inalámbricas | 26 |
| 2.2.12 Multi-Protocol Label Switching (MPLS) | 29 |
| 2.3 Propuesta de Solución | 31 |
| CAPÍTULO III..... | 32 |
| METODOLOGÍA..... | 32 |
| 3.1 Modalidad de la investigación | 32 |
| 3.1.1 Investigación Bibliográfica..... | 32 |
| 3.1.2 Investigación de Campo | 32 |
| 3.1.3 Investigación Experimental | 33 |
| 3.2 Recolección de la información | 33 |
| 3.3 Procesamiento y Análisis de la Información | 33 |
| 3.4 Desarrollo del proyecto | 33 |
| CAPÍTULO IV..... | 35 |
| DESARROLLO DE LA PROPUESTA | 35 |
| 4.1 Análisis de la topología física y lógica implementada en la red MAN de EEASA. | 35 |
| 4.1.1 Topología Física de la Red..... | 35 |
| 4.1.2 Análisis de la Topología Lógica | 37 |
| 4.1.3 Equipos de la red MAN de EEASA | 40 |
| 4.1.4 Modelos y versiones del sistema operativo de interconexión (IOS) de los routers y switches de la red MAN de EEASA..... | 41 |
| 4.1.5 Análisis de equipos de la red MAN de EEASA que soportan QoS | 44 |
| 4.2 Herramienta de Monitoreo de la red MAN..... | 50 |
| 4.2.1 SolarWinds Orion NPM..... | 50 |
| 4.3 Análisis de la red MAN de EEASA | 51 |
| 4.3.1 Tipo de Tráfico que circula en los enlaces de la Red MAN | 52 |

| | | |
|-------|---|----|
| 4.3.2 | Tiempo de Respuesta en los enlaces de la red MAN de EEASA | 53 |
| 4.3.3 | Diagnóstico de los Dispositivos de red en los enlaces de EEASA..... | 61 |
| 4.3.4 | Análisis de requerimientos en la red MAN de EEASA | 61 |
| 4.4 | Proceso de servicios aplicables para brindar QoS en la red MAN de EEASA | 63 |
| 4.4.1 | Elección del Modelo de QoS a implementarse en la red MAN de EEASA | 63 |
| 4.4.2 | Método de Clasificación y Marcado de tráfico para la red MAN de EEASA..... | 64 |
| 4.4.3 | Manejo de Congestión de Colas..... | 66 |
| 4.4.4 | Método de Evasión de Congestión..... | 67 |
| 4.5 | Elaboración de Prototipo Basado en simuladores de redes para la implementación de Calidad de servicio QoS. | 68 |
| 4.5.1 | Simulador OPNET Modeler..... | 69 |
| 4.5.2 | GNS3 (Graphical Network Simulator)..... | 70 |
| 4.5.3 | Requerimientos de Calidad de Servicio QoS en simulación. | 72 |
| 4.5.4 | Características de Simulación en GNS3 y OPNET..... | 74 |
| 4.6 | Simulación de Calidad de Servicio QoS en OPNET Modeler..... | 75 |
| 4.6.1 | Esquema de Simulación en OPNET Modeler | 75 |
| 4.6.2 | Configuración de Aplicaciones | 76 |
| 4.6.3 | Configuración de Perfiles..... | 78 |
| 4.6.4 | Configuración de Servidores de aplicaciones | 79 |
| 4.6.5 | Configuración de Estaciones Suscriptoras SS..... | 80 |
| 4.6.6 | Configuración de Wimax y entornos Inalámbricos..... | 81 |
| 4.6.7 | Configuración de Estación Base BS..... | 83 |
| 4.6.8 | Implementación de Calidad de Servicio (QoS) en OPNET Modeler | 85 |
| 4.7 | Simulación de la red MAN en GNS3 | 87 |
| 4.7.1 | Configuración de Equipos..... | 89 |
| 4.7.2 | Instalación y configuración de servidor VoIP | 90 |
| 4.7.3 | Configuración de <i>Call Manager</i> en Router Matriz | 91 |
| 4.7.4 | Servidor Video | 91 |
| 4.7.5 | Configuración de Lista de Acceso ACLs | 92 |
| 4.7.6 | Marcado y clasificación del tráfico en el router | 93 |

| | |
|--|------------|
| 4.7.7 Creación de la política..... | 94 |
| 4.7.8 Asignación de la política a la interfaz de entrada..... | 96 |
| 4.8 Análisis de Resultados en simulador GNS3 | 99 |
| 4.8.1 Clasificación y marcado de paquetes en el router Matriz de la red MAN de EEASA | 101 |
| 4.8.2 Análisis de rendimiento de la red simulado en GNS3..... | 103 |
| 4.9 Análisis de Resultados OPNET | 112 |
| 4.10 Análisis de Factibilidad de QoS en la red MAN de EEASA. | 122 |
| CAPÍTULO 5 | 124 |
| CONCLUSIONES Y RECOMENDACIONES | 124 |
| 5.1 Conclusiones | 124 |
| 5.2 Recomendaciones..... | 126 |
| 6. REFERENCIAS BIBLIOGRÁFICAS..... | 127 |
| ANEXO 1 | 133 |
| Análisis y monitoreo de los nodos pertenecientes al enlace de fibra óptica e inalámbrica de la red MAN de EEASA..... | 133 |
| ANEXO 2 | 146 |
| Configuraciones desarrolladas en OPNET MODELER..... | 146 |
| ANEXO 3 | 150 |
| Configuración de Servidores Simulados en GNS3 | 150 |
| ANEXO 4 | 155 |
| Configuración de Routers realizado En Gns3 | 155 |
| ANEXO 5 | 162 |
| Monitoreo de Equipos de La red MAN de EEASA y sus direcciones Ip de administración | 162 |
| ANEXO 6 | 163 |
| Características de los equipos pertenecientes a la red de EEASA | 163 |

Índice de Figuras

| | |
|---|----|
| Figura 2.1. Red de Datos | 7 |
| Figura 2.2. Redes Inalámbricas..... | 10 |
| Figura 2.3: Tipo de Servicio | 16 |
| Figura 2.4: Esquema de Funciones de Modelo IntServ | 18 |
| Figura 2.5: Esquema que conforma el Modelo DiffServ..... | 19 |
| Figura 2.6. Campo DS y DSCP PHBs | 19 |
| Figura 2.7: Esquema para análisis de QoS | 27 |
| Figura 2.8: Distintos tipos de servicio | 28 |
| Figura 2.9: Intercambio de paquetes en una red MPLS..... | 29 |
| Figura 2.10: Ejemplo de arquitectura MPLS | 30 |
| Figura 4.1: Topología Física de la Red MAN Fibra Óptica. | 36 |
| Figura 4.2: Topología Física de la Red MAN Enlace Inalámbrico. | 36 |
| Figura 4.3: Topología Lógica de la Red MAN Fibra Óptica..... | 38 |
| Figura 4.4: Topología Lógica de la red MAN enlace Inalámbrica..... | 39 |
| Figura 4.5: Diferencias QoS de imágenes software Catalyst 2960..... | 45 |
| Figura 4.6: Diagrama de Flujo de Paquetes | 48 |
| Figura 4.7: Interfaz de SolarWinds para el monitoreo de la red MAN | 51 |
| Figura 4.8: Análisis de Tráfico generado en la red MAN | 53 |
| Figura 4.9: Tráfico capturado por SolarWinds MATRIZ..... | 56 |
| Figura 4.10: Bytes transmitidos en Int. Giga Ethernet 0/27. | 56 |
| Figura 4.11: Tráfico capturado por SolarWinds LORETO | 58 |
| Figura 4.12 Bytes transmitidos en Interfaz Giga Ethernet 0/27, /25 Loreto..... | 58 |
| Figura 4.13: Tráfico capturado por SolarWinds Router NITON..... | 59 |
| Figura 4.14: Monitoreo de Router Nitón | 60 |
| Figura 4.15: Bytes transmitidos en Router Nitón | 60 |
| Figura 4.16: Requerimientos de Aplicaciones | 63 |
| Figura 4.17: Tipo de Servicio (ToS) y DSCP..... | 65 |
| Figura 4.18: Funcionamiento de CBWFQ..... | 66 |
| Figura 4.19: Funcionamiento Low Latency Queue (LLQ) para el manejo de congestión | 67 |
| Figura 4.20: Opnet Modeler 14.5..... | 69 |

| | |
|--|-----|
| Figura 4.21: Eslogan de GNS3 (Graphical Network Simulator) | 70 |
| Figura 4.22 Escenario de prueba Wimax en OPNET | 76 |
| Figura 4.23 <i>Application Definition</i> en OPNET | 77 |
| Figura 4.24: Configuración de Aplicación de VoIP | 77 |
| Figura 4.25: <i>Profile Definition</i> en OPNET | 78 |
| Figura 4.26 Configuración de Perfiles | 79 |
| Figura 4.27 Configuración de Servidores de Aplicación..... | 80 |
| Figura 4.28: Estaciones Suscriptoras. | 80 |
| Figura 4.29 Configuración de Estaciones Suscriptoras y clientes. | 81 |
| Figura 4.30 <i>Wimax Config</i> | 82 |
| Figura 4.31 Configuración Parámetros de <i>WiMAX</i> | 82 |
| Figura 4.32: Configuración Parámetros de <i>WiMAX</i> | 83 |
| Figura 4.33 Estación Base | 83 |
| Figura 4.34: Configuración de Downlink/Uplink Service Flows..... | 84 |
| Figura 4.35 Configuración Parámetros de <i>WiMAX</i> | 85 |
| Figura 4.36 Ejecución de Simulador para redes Inalámbricas..... | 86 |
| Figura 4.37 Red MAN de EEASA en GNS3..... | 88 |
| Figura 4.38: Inicio del Cisco IP Communicator | 90 |
| Figura 4.39 Teléfonos instalados en nodo Matriz, EDPuyo y Tena. | 90 |
| Figura 4.40 VLC actúa como servidor de Video | 92 |
| Figura 4.41 Configuración de ACLs..... | 92 |
| Figura 4.42 Configuración de Clases..... | 94 |
| Figura 4.43 Verificación de Clases creadas..... | 94 |
| Figura 4.44 Configuración de Políticas | 95 |
| Figura 4.45 Verificación de Políticas Creadas..... | 95 |
| Figura 4.46 Verificación de Políticas output e input | 96 |
| Figura 4.47 Asignación de políticas a interfaces | 96 |
| Figura 4.48: Prototipo basado en simuladores de red y generador de trafico real..... | 99 |
| Figura 4.49 Esquema utilizado para sección de Pruebas | 100 |
| Figura 4.50 Verificación de tráfico marcado | 101 |
| Figura 4.51 Verificación de trafico marcado en Multimedia..... | 102 |
| Figura 4.52 Verificación de tráfico marcado en Dato | 102 |

| | |
|---|-----|
| Figura 4.53 Ejecución de tráfico de video | 104 |
| Figura 4.54: Verificación de Tráfico generado con Wireshark | 104 |
| Figura 4.55 Verificación de Tráfico generado en VoIP..... | 105 |
| Figura 4.56 Tráfico generado al enviar información | 106 |
| Figura 4.57 Tráfico generado por pin extendido | 106 |
| Figura 4.58 Tráfico generado por Video con QoS..... | 107 |
| Figura 4.59: Tráfico generado por VoIP con QoS..... | 109 |
| Figura 4.60: Tráfico generado por transferencia de archivo con QoS..... | 110 |
| Figura 4.61 Tráfico generado por ping extendido con QoS | 111 |
| Figura 4.62 Verificación de Estadísticas y marcado de tráfico en router matriz..... | 112 |
| Figura 4.63 Carga y Throughput generado en AGBaños | 113 |
| Figura 4.64 a) Retardo de extremo a extremo, b) <i>Jitter</i> generado en AGBaños | 114 |
| Figura 4.65 Tráfico rechazado en el nodo AGBaños..... | 115 |
| Figura 4.66 Configuración de Ancho de banda para aplicación de voz | 115 |
| Figura4.67 Carga y Throughput generado en AGBaños, aplicación de voz | 116 |
| Figura 4.68 <i>Jitter</i> en nuevo mapeo en aplicación de voz..... | 116 |
| Figura 4.69 Retardo nuevo mapeo en aplicación de voz | 117 |
| Figura 4.70 Carga y Throughput generado en AGBaños, aplicación de video | 117 |
| Figura 4.71 Retardo presente en aplicación de video | 118 |
| Figura 4.72 Carga generado en aplicación FTP en cada nodo SS | 119 |
| Figura 4.73 Carga generado en la aplicación Oracle | 119 |
| Figura 4.74 Retardo generado en aplicación FTP..... | 120 |
| Figura 4.75 Tráfico Recibido y <i>Throughput</i> en aplicación Http..... | 120 |
| Figura 4.76 Tiempo de respuesta en aplicación Http..... | 121 |
| Figura 4.77 Carga y tráfico enviado en aplicación Http | 121 |
| Figura 4.78 Delay en aplicación Http | 122 |

ANEXO1

| | |
|--|-----|
| Figura 1. Tráfico Generado en Switch Pelileo..... | 133 |
| Figura 2. Bytes transmitidos en Switch Pelileo | 133 |
| Figura 3. Tráfico Generado en Switch Baños..... | 134 |
| Figura 4. Bytes transmitidos en Switch Baños | 134 |

| | |
|---|-----|
| Figura 5. Tiempo de respuesta en Nodo Router SubPuyo..... | 135 |
| Figura 6. Bytes transmitidos en Router SubPuyo | 135 |
| Figura 7. Tiempo de respuesta en Nodo Switch SubPuyo..... | 136 |
| Figura 8. Bytes transmitidos en Switch SubPuyo..... | 136 |
| Figura 9. Tiempo de respuesta en Nodo Router Puyo 1 | 137 |
| Figura 10. Bytes transmitidos en Nodo Router Puyo 1 | 137 |
| Figura 11. Tiempo de respuesta en Nodo Switch SubTena..... | 138 |
| Figura 12. Bytes transmitidos en Nodo Switch SubTena | 138 |
| Figura 13. Tiempo de respuesta en Nodo Router SubTena | 139 |
| Figura 14. Bytes transmitidos en Nodo Router SubTena | 139 |
| Figura 15. Tiempo de respuesta en Nodo Router Tena 1 | 140 |
| Figura 16. Bytes transmitidos en Nodo Router Tena 1..... | 140 |
| Figura 17. Tiempo de respuesta en Nodo Router Tena 2 | 141 |
| Figura 18. Bytes transmitidos en Nodo Router Tena 2..... | 141 |
| Figura 19. Tiempo de respuesta en Nodo Nitón-Santa Rosa..... | 142 |
| Figura 20. Tiempo de respuesta en Nodo Loma Grande-Baños..... | 142 |
| Figura 21. Tiempo de respuesta en Nodo Router Tena 2 | 143 |
| Figura 22. Tiempo de respuesta en Nodo Router Tena 2 | 143 |
| Figura 23. Tiempo de respuesta en Nodo Router Tena 2 | 144 |
| Figura 24. Tiempo de respuesta en Nodo Router Tena 2 | 144 |
| Figura 25. Tiempo de respuesta en Nodo Router Tena 2 | 145 |
| Figura 26. Tiempo de respuesta en Nodo Router Tena 2 | 145 |

ANEXO 2

| | |
|--|-----|
| Figura 1. Configuración de Aplicación de FTP | 146 |
| Figura 2. Configuración de Aplicación de Video | 147 |
| Figura 3. Configuración de Aplicación HTTP..... | 148 |
| Figura 4. Configuración de Aplicación de E-MAIL..... | 148 |
| Figura 5. Configuración de Perfiles | 149 |

ANEXO 3

| | |
|---|-----|
| Figura 1 Reconocimiento de los dispositivos de audio..... | 150 |
|---|-----|

| | |
|---|-----|
| Figura 2 Mensaje informativo..... | 151 |
| Figura 3. Configuración del servidor TFTP é Interfaz a utilizar | 151 |
| Figura 4. Presentación VLC..... | 152 |
| Figura 5. Esquema de Emisión de Video..... | 152 |
| Figura 6. Esquema de Emisión de Video..... | 153 |
| Figura 7. Fuente de emisión y destino | 154 |
| Figura 8. Emisor de Video Streaming | 154 |

ANEXO 6

| | |
|---|-----|
| Figura 1. Mainboard Mikrotik Wireles | 163 |
| Figura 2. Características de Equipo Proxim Modelo | 164 |
| Figura 3. Características técnicas de Ubiquiti Wireeles | 165 |

Índice de Tablas

| | |
|--|----|
| Tabla 2.1 Valores de Prioridades CoS | 15 |
| Tabla 2.2 Ventajas y desventajas de IntServ-DiffServ | 20 |
| Tabla 2.3 Ventaja y desventaja de manejo de tráfico RED | 23 |
| Tabla 2.4 Ventaja y desventaja de manejo de tráfico RED | 24 |
| Tabla 4.1 Routers Utilizados en la red MAN de EEASA..... | 40 |
| Tabla 4.2 Switches utilizados en la red MAN de EEASA..... | 40 |
| Tabla 4.3 Routers utilizados para los enlaces inalámbricos. | 41 |
| Tabla 4.4 IOS y Versión de switches de la red MAN..... | 42 |
| Tabla 4.5 IOS y Versión de routers de la red MAN | 43 |
| Tabla 4.6 Datasheet Cisco 2901 | 46 |
| Tabla 4.7 Tiempos de respuesta presentes en los switches principales de la red MAN de EEASA..... | 54 |
| Tabla 4.8 Tiempos de respuesta presentes en los routers principales de la red MAN de EEASA..... | 54 |
| Tabla 4.9 Tiempos de respuesta entre los enlaces inalámbricos de la red MAN de EEASA..... | 55 |
| Tabla 4.10 Clase DSCP | 65 |
| Tabla 4.11 Valores del campo DSCP | 65 |
| Tabla 4.12 Algoritmos para la implementar QoS | 68 |
| Tabla 4.13 Características de Simuladores | 72 |
| Tabla 4.14 Clasificación de Servicios, Valores de DSCP y Ancho de Banda para QoS..... | 75 |
| Tabla 4.15 Algoritmos para la implementar QoS | 87 |
| Tabla 4.16 Estadísticas a medir en la simulación de redes inalámbricas | 87 |

RESUMEN EJECUTIVO

La Empresa Eléctrica Ambato Regional Centro Norte S.A (EEASA), es una institución que presta el servicio de suministrar energía eléctrica, a clientes en su área de concesión. EEASA cuenta con una infraestructura de telecomunicaciones implementada con fibra óptica y enlaces inalámbricos, los cuales juegan un papel importante para monitorear y operar tanto el sistema eléctrico como el sistema de comunicaciones. El problema que presentaba EEASA es que no se contaba con una acción preventiva, regularización y un estudio de la real capacidad de aprovechamiento la red de datos transmitidos a través de los enlaces de fibra óptica e inalámbrica, limitando a ofrecer una optimización en la transmisión de ciertas aplicaciones en tiempo real como VoIP, Videoconferencia, SCADA y otros. Esto dio paso al desarrollo de un estudio de factibilidad para implementar calidad de servicio (QoS) en la red de área metropolitana (MAN) de EEASA y sus sucursales, el propósito es establecer experimentalmente la implementación de QoS en la red MAN, que incluyó el estudio de la situación actual de la red, compuesta por enlaces de fibra óptica e inalámbrica, así como los mecanismos de Calidad de Servicio (QoS) que se adaptan a condiciones de hardware y software de la red. La investigación permitió realizar la elaboración de un prototipo basado en simuladores de red, donde las pruebas realizadas se basan en las características que posee la red MAN de EEASA. Así los resultados obtenidos permitieron evaluar las ventajas y desventajas que trae consigo el uso de Calidad de Servicio (QoS) y determinar la optimización del tráfico que puede tomar la red MAN tanto en los enlaces de fibra óptica e inalámbrica.

ABSTRACT

The Empresa Eléctrica Ambato Regional Centro Norte S.A (EEASA), is an institution that provides the service of supply electricity to customers in its concession area. EEASA has a telecommunications infrastructure implemented with optical fiber and wireless links, which play an important role to monitor and operate both electrical and communications system. The problem presented EEASA is that he is it did not have a preventive action, regularization, and a study of the actual ability to use network data transmitted over fiber optic and wireless links, limiting to offer an optimization in the transmission of certain applications in real-time such as VoIP, videoconferencing, SCADA and others. Giving way to the development of a feasibility study to implement quality of service (QoS) in the network of metropolitan area (MAN) EEASA and its branches, the purpose is experimentally set the implementation of QoS on the network MAN, which included the study of the current situation of the network, composed of fiber optic and wireless links, as well as mechanisms for quality of service (QoS) adapted to conditions of the network hardware and software. The research allowed for the elaboration of a prototype based on network simulators, where tests are based on characteristics that possess the EEASA MAN network. Thus the results allowed evaluate the advantages and disadvantages it brings with it the use of quality of service (QoS) and determine the optimization of traffic that can take the black MAN both fiber optic and wireless links.

GLOSARIO DE TÉRMINOS

ACL: Access control List, lista de control de acceso.

AP: Access Point, punto de acceso inalámbrico

ATM: Asynchronous Transfer Mode, Modo de Transferencia Asíncrona.

BACKBONE: La columna vertebral de la red.

BANDWIDTH: Ancho de banda,

BE: Best Effort, Mejor Esfuerzo

BTS: Base Transceiver Station, estación base.

CoS: Class of Service, Clases de Servicio.

CBWFQ: Class Based Weighted Fair Queuing, Encolamiento equitativo ponderado basado en clase.

CSMA/CD: Acceso Múltiple por Detección de Portadora con Detección de Colisiones.

Diff-Serv: Differentiated Services, Servicios Diferenciados

DSCP: DiffServ Code Point, Punto Código DiffServ.

EDCA: Enhanced Distributed Channel Access, Función Mejorada de Distribución de Acceso al Canal.

ECN: Explicit Congestion Notification, Notificación Explícita de Congestión

Estándar 802.1p: Valor de tres bits que pueden aplicarse dentro de una etiqueta de trama 802.1Q. Generalmente es convertido a IP precedente o DSCP cuando el paquete alcanza el primer router.

FIFO: First in, first out, Primero en Entrar-Primero en Salir.

FTP: File Transfer Protocol, Protocolo de transferencia de Archivos.

HCF: Función de Coordinación Híbrida

HCCA: HCF Controlled Channel Acces, Función HCF de Control de Acceso al Canal

IEEE: Institute of Electrical and Electronics Engineers, Instituto de Ingenieros Eléctricos Electronicos.

Int-Serv: Integrated Services, Servicios Integrados.

IOS: Internetwork Operating System, Sistema operativo de Internetwork.

LER: Label Edge Router, son dispositivos que operan en los extremos de la red MPLS

LSR: Label Switching Router, son routers de gran velocidad en el núcleo de la red MPLS, encargados de dirigir el tráfico en el interior de la red.

MAC: Media Access Control, Control de Acceso al Medio, es un identificador de 48 bits que corresponde de forma única a una tarjeta o dispositivo de red.

MPLS: Multi-Protocol Label Switching,

OSPF: Open Shortest Path First, un protocolo de enrutamiento jerárquico de pasarela interior, para calcular la ruta más idónea.

PRTG: Paessler Router Traffic Grapher, herramienta de monitorear de tráfico en una red.

QoS: Quality of Service, Calidad de Servicio.

RSVP: Resource Reservation Protocol, Protocolo de Reserva de Recursos.

RIP: Routing Information Protocol, Protocolo de Información de Enrutamiento.

TCP: Transmission Control Protocol, Protocolo de Control de Transmisión

ToS: Type of Service, Tipo de Servicio.

INTRODUCCIÓN

Como consecuencia del crecimiento continuo de servicios de tiempo real que actualmente EEASA posee, como es el caso VoIP, videoconferencia, SCADA (Supervisión, Control y Adquisición de Datos) y datos, dependiendo de las necesidades de la empresa, y para que estos servicios funcionen de manera adecuada es necesario que parámetros como el retardo, jitter, ancho de banda y pérdida de paquetes, tengan un excelente control para la comunicación, sin afectar el rendimiento de la red.

Debido al tráfico simultáneo que presentan las diferentes aplicaciones que circulan a través de red de datos, hace que generen congestión en determinado canal, lo que conlleva a no tener el mejor rendimiento a la hora de transmitir información, ocasionando que los datos ocupen un largo período en alcanzar su destino o estos se pierdan. Por tanto el proyecto de investigación permitió determinar qué tan factible es la implementación de QoS en la red MAN de EEASA, compuesta por enlaces de fibra óptica e inalámbrica, evaluando el estado actual de la red MAN, analizando la aplicabilidad de QoS en base al entorno de la red determinado por su topología y equipos que conforman la red MAN como cisco, Proxim, Ubiquiti y Mikrotik, para posteriormente aplicar el método QoS que mejores características de priorización provean a la red, el cual permita la escalabilidad y convergencia con tecnologías como MPLS implementado en EEASA e incluso para otras aplicaciones que no operan en tiempo real, de manera que permite mejorar los procesos internos de la institución y mejorar la comunicación con cada una de las agencias.

Por último se implementó un prototipo basado en simuladores de red como GNS3 y OPNET Modeler, así pues se ejecutaron pruebas en diferentes escenarios con características de QoS y se determinó el comportamiento de la red basada en un entorno real como la de EEASA, de manera que permitió determinar el mejor método de priorización de QoS, que puede ser implementada en área operativa de la red MAN de EEASA.

El presente trabajo consta de 5 capítulos, los cuales se detallan a continuación:

En el Capítulo I: Se realizó el análisis del planteamiento del problema, que indica las necesidades y problemáticas a responder del proyecto de investigación; así como la justificación que indica los beneficios que implica implementar QoS en la red MAN de EEASA.

En el Capítulo II: Comprende los antecedentes investigativos, es decir se recopila información que ayuda a comprender los modelos y mecanismos de QoS, que permita analizar el método de priorización de tráfico en redes cableadas e inalámbricas para aclarar una propuesta de solución que se ejecutará en la investigación.

En el Capítulo III: Este capítulo muestra los diferentes métodos que se utilizaron para la realización del proyecto, el enfoque que se dio al proceso de investigación, las técnicas e instrumentos de investigación, y detalles del desarrollo del proyecto tomando en cuenta los pasos a realizarse en un tiempo determinado.

En el Capítulo IV: En este capítulo se detalla el desarrollo de la propuesta donde se analiza la situación actual de la red MAN de EEASA. Elaboración de prototipo basado en simuladores de red y el análisis de resultados que determina el mejor método de priorización de QoS en la red MAN de EEASA.

En el Capítulo V: En este capítulo se tomó como base la investigación y simulación realizada permitiendo obtener conclusiones y recomendaciones sobre la implantación de QoS en la red MAN de EEASA.

CAPÍTULO 1:

EL PROBLEMA

1.1 Tema:

“Calidad de Servicio (QoS) en la Red MAN de la Empresa Eléctrica Ambato Regional Centro Norte S.A (EEASA) y sus Sucursales”.

1.2 Planteamiento del Problema

A nivel mundial uno de los aspectos claves es la convergencia de las redes, permitiendo transportar todos los servicios de voz, datos y video sobre una única infraestructura, así estos servicios generan distintos tipos de tráfico, cada uno de ellos con requerimientos muy diversos, en consecuencia se da la necesidad de satisfacer una serie de requisitos o parámetros aplicando calidad de servicio (QoS) es prioritario, para poder transportar múltiples servicios con requisitos diferentes y soportar futuros servicios con requerimientos todavía desconocidos [1][2].

Hoy en día el número de aplicaciones que introducen datos a la red ha crecido, de modo que existe la obligación de dar un tratamiento específico a cada tipo de tráfico, proporcionando los mejores servicios y gestionando las aplicaciones tales como VoIP, Videoconferencia, comercio electrónico, base de datos compartidos y otras aplicaciones en tiempo real [2][3].

En la actualidad las empresas del país requieren de servicios en tiempo real, como son las aplicaciones telemáticas, por tal motivo la demanda de ancho de banda es mayor lo cual implica un incremento económico, además a esto se tiene que los enlaces no siempre son de calidad por lo que se genera un problema al transmitir información en las empresas. Sin embargo, no basta con aumentar el ancho de banda, es necesario gestionar de manera más eficiente la capacidad para transmitir los datos [2]. Es por ello que el aplicar calidad de servicio en enlaces de datos asegurara la correcta transmisión en servicios de tiempo real [4].

En la actualidad la Empresa Eléctrica Ambato Regional Centro Norte S.A (EEASA) y sucursales no cuentan con un estudio que indique la real capacidad de aprovechamiento de la red de área metropolitana (MAN), por consiguiente la posibilidad de tener una mejora continua es nula, generando una deficiente optimización de servicios requeridos en el futuro, lo cual afectaría su crecimiento y rendimiento en forma significativa.

El no contar con una acción preventiva para el control de tráfico en la red MAN de EEASA, genera una deficiente administración de los recursos de la red ante situaciones de congestión, lo que conlleva a no tener el mejor rendimiento a la hora de transmitir información, ocasionando que los datos ocupen un largo período en alcanzar su destino, dentro de la red MAN de EEASA y sus sucursales.

Actualmente EEASA cuenta con enlaces de radio punto a punto, basado en los estándares IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) 802.11b WLAN (*Wireless Area Network*, Red de área local inalámbrica) y 802.16 WiMAX (*Worldwide Interoperability for Microwave Access*, Interoperabilidad Mundial para Acceso por Microondas) por tal motivo, la falta de regularización en los servicios transmitidos en el enlace inalámbrico, provoca que el ancho de banda se sature, generando deficiente optimización en la transmisión de ciertas aplicaciones provocando un alto índice de pérdida de paquetes.

1.3 Delimitación del Problema

- ❖ **Área Académica:** Programación y Redes
- ❖ **Línea de Investigación:** Programación y Redes
- ❖ **Sublineas de Investigación:** Programación de Dispositivos de Comunicación

- ❖ **Delimitación Espacial:** La investigación se realizó en la Empresa Eléctrica Ambato Regional Centro Norte S.A de la ciudad de Ambato.
- ❖ **Delimitación Temporal:** La investigación se desarrolló en un periodo de seis meses a partir de ser aprobada por el Honorable Consejo Directivo de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

1.4 Justificación

La presente investigación es de importancia porque se basa en realizar un estudio de factibilidad de implementación de Calidad de Servicio (QoS) en la red de área metropolitana (MAN), el cual permitió analizar el estatus de congestión y retardos generados en una topología física basada en GigaEthernet, y enlace inalámbrico, así como la asignación de ancho de banda según los requerimientos solicitados por EEASA y sus sucursales, permitiendo tener un panorama para una optimización de los servicios requeridos a futuro sin interrupciones o pérdida de datos.

Al contar con una Red inalámbrica de área metropolitana (WMAN) basada en el estándar 802.11 (WLAN) y 802.16 (WiMAX) se presenta la necesidad de que este soporte las mismas aplicaciones que una red cableada, por tal motivo el estudio para implementar calidad de servicio es fundamental para establecer métodos y parámetros de calidad de servicio (QoS), garantizando prioridades sin la necesidad de implementar o adoptar infraestructuras de redes más rápidas.

La implementación de QoS en EEASA asegura una correcta entrega de información, de manera que permite aprovechar toda la capacidad que brinda la red de área metropolitana (MAN), dando preferencias a aplicaciones necesarias y generando un uso eficiente de recursos ante situaciones de congestión generadas en enlaces de fibra óptica, enlace inalámbrico y de línea dedicada las. Así pues el estudio determino como garantizar QoS de extremo a extremo para enlaces con tecnología GigaEthernet e inalámbricas implementados en EEASA con el plan de llegar a la convergencia de redes y servicios basados en IP.

El proyecto de investigación es factible realizarlo porque se cuenta con datos e información necesaria, en particular información online de índole académico, científico, además de libros referentes a calidad de servicio (QoS), así los resultados obtenidos al realizar el estudio permiten evaluar la ventaja y desventaja que trae implementar calidad de servicio (QoS) en la red MAN, determinando si la ejecución es aplicable a la red basado en la tecnología de GigaEthernet e inalámbrica implementada con WLAN y WiMAX.

El presente trabajo, beneficia a las autoridades y trabajadores de la institución ya que permite que el tráfico de datos sea óptimo, eficiente y sin pérdidas de información, además también ayudará a que los usuarios puedan realizar consultas de panillas u otros servicios de manera más rápida.

1.5 Objetivos

1.5.1 Objetivo General

Desarrollar un estudio de factibilidad de implementación de calidad de servicio (QoS) en la Red de Área Metropolitana (MAN) de la Empresa Eléctrica Ambato Regional Centro Norte S.A y sus sucursales.

1.5.2 Objetivos Específicos

- ❖ Analizar el estado actual de la red y determinar el tráfico circulante en la red MAN de la Empresa Eléctrica Ambato Regional S.A.
- ❖ Determinar la factibilidad de implementar calidad de servicio (QoS) en los diferentes tipos de enlaces de la red MAN de EEASA.
- ❖ Establecer el tipo de modelo de calidad de servicio (QoS) para la red de área metropolitana (MAN).
- ❖ Diseñar un prototipo para determinar la optimización de servicios en los enlaces de la red MAN de EEASA.

CAPÍTULO 2

MARCO TEÓRICO

2.1 Antecedentes Investigativos

En el presente proyecto de investigación se propone realizar un estudio de factibilidad de calidad de servicio (QoS) en la red MAN de EEASA, para lo que se investigó en las tesis de la biblioteca de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato, donde se encontró que Hugo Gabriel Fonseca Romero propone en su trabajo de titulación “Calidad de Servicio (QoS) para el Mejoramiento de la Red de Datos en la Fábrica de Calzado LIWI” con el objetivo de implementar protocolos y estándares de QoS para solucionar problemas de congestión y retardos que existen en la red de datos [5].

Diego Llerena plantea en su tesis de grado “Algoritmos de Calidad de Servicio (Qos) y la congestión en los enlaces de comunicación de los usuarios de la empresa Uniplex Systems de la Ciudad de Quito”. En este trabajo propone la utilización de sistemas complejos para la aplicación de Calidad de Servicio en enlaces de transmisión de datos, dando prioridad a las aplicaciones críticas en tiempo real [6].

Se investigó también en los repositorios de la Escuela Politécnica Nacional en la Facultad de Ingeniería Eléctrica y Electrónica donde Darwin Quevedo y Paulina Vaca realizaron el proyecto de titulación denominado “Diseño e Implementación de Calidad de Servicio (Qos) en la Red del Transporte de Datos del Municipio del Distrito Metropolitano de Quito (MDMG)” el cual ayuda a mejorar el rendimiento de la red de transporte de datos del MDMQ y obtengan una adecuada asignación de recursos de acuerdo a sus requerimientos [7].

En la Escuela de Ingeniería Electrónica y Telecomunicaciones de la Universidad Particular de Loja, Arrobo Jimmy Daniel y Sarmiento María del Cisne proponen en su trabajo de titulación la “Implementación de QoS en la red LAN de La UTPL” el cual establece la implementación de QoS en un área operativa de la red LAN de la UTPL con el objetivo de verificar la priorización de tráfico en un ambiente real. Una conclusión importante se tomó de este proyecto de investigación.

“Existen dos modelos de QoS (IntServ y DiffServ) que realizan diferentes operaciones para ofrecer priorización de tráfico, la elección para la aplicación de cualquiera de estos dos métodos dependerá de requerimientos como ancho de banda, retardo, jitter, y demás variables a la que está sometida la red.” [8].

Realizando una búsqueda a nivel global se logró encontrar que Eduardo de la Cruz Gámez y Félix F. Álvarez Paliza propone en su artículo científico realizar la “Evaluación de la calidad de los servicios en redes E-MAN” el cual analiza el comportamiento y desempeño de un modelo de simulación basado en el núcleo de backbone de una red metropolitana [9].

En el Instituto Superior Politécnico José Antonio Echeverría, Habana, Cuba. El Msc. Omar Álvarez y Msc. Margarita Mayoral desarrollan el trabajo de investigación basado en la “Contribución para QoS en Redes Metropolitanas Ethernet” enfocado para enlaces de 1 Gbps y 10 Gbps para sesiones de voz y video permiten garantizar los requerimientos de QoS de extremo a extremo de la red [2].

2.2 Fundamentación Teórica

En la actualidad la aparición de nuevos medios de transmisión más rápidos y fiables, como la fibra óptica y enlaces inalámbricos tienen requerimientos de tráfico en tiempo real, como aplicaciones de voz y video que han hecho posible que el volumen de datos haya incrementado considerablemente, por tal motivo se hace indispensable contar con la disponibilidad de que los datos transmitidos tengan un retardo mínimo hasta llegar a su destino, así como el de obtener bajos porcentajes de pérdida de paquetes que no representen daños en una comunicación multimedia.

Debido a este incremento en el intercambio de archivos multimedia, en la actualidad las empresas ya ven la necesidad de priorizar el tráfico con el fin de otorgar preferencias a cierto tipo de datos.

2.2.1 Redes de Datos

Las redes de datos permiten compartir recursos, equipos, información y programas que se encuentran localmente o dispersos geográficamente, cuya finalidad es transmitir información entre usuarios distantes de la manera más rápida y eficiente, brindando confiabilidad a la información y disponiendo de alternativas de almacenamiento. En la figura 1 se muestra el sistema de una red de datos que enlaza dos o más puntos ya sea por un medio físico o inalámbrico, de manera que permita enviar o recibir un determinado flujo de información [10].

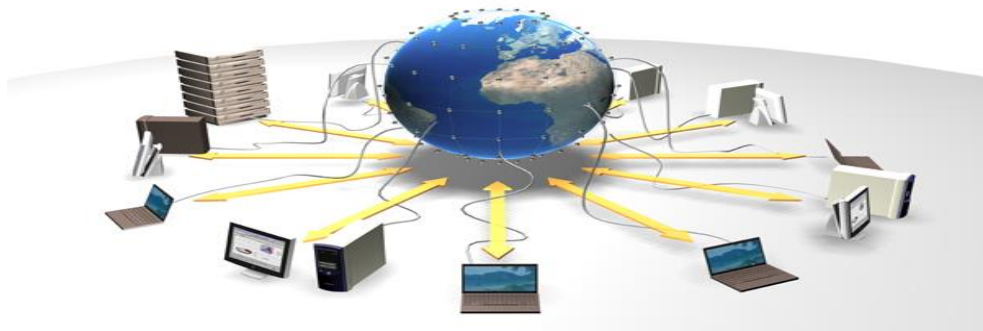


Figura 2.1. Red de Datos [10]

Hoy en día existen redes de Fibra Óptica e inalámbricas que permite la comunicación a larga distancia, con mayor capacidad debido a que los anchos de banda son más grandes, de manera que en forma independiente de la tecnología utilizada, las redes de datos pueden ser clasificadas según el alcance o tamaño de las mismas:

Red de Área Local (LAN)

Las redes de áreas locales son comunicaciones que interconectan varios dispositivos y proporcionan un medio para el intercambio de información entre ellos. La cobertura de una LAN son de alcance limitado, generalmente son redes privadas que están instaladas dentro de un mismo edificio, oficina o campus [10] [11].

Red de Área Metropolitana (MAN)

Una red MAN es una red que se interconecta con varios dispositivos que se expande por pueblos o ciudades y se interconecta mediante instalaciones públicas o privadas. La implementación de redes MAN requieren de dispositivos de interconexión, como Bridge, routers y switches de capa3, la MAN es una red cuyo diámetro pueden extenderse hasta un máximo de 50 km [6] [12].

Red de Área Extensa (WAN)

Una red WAN es aquella que cubren una extensa área geográfica, requieren atravesar rutas de acceso público, y utilizan parcialmente circuitos proporcionados por una entidad proveedora de servicios de telecomunicaciones. Las funciones típicas de las redes WAN es la interconexión de dos o varias redes LAN, además la topología de la redes de área extensa pueden ser de tipo estrella, anillo, árbol o malla [10] [11].

2.2.2 Medios de Transmisión

Se denomina a un medio de transmisión al camino físico entre el transmisor y el receptor mediante el cual se establece la comunicación. Este medio físico puede transportar información en forma eléctrica, óptica o radiofrecuencia. Entre los principales medios de transmisión se tiene a los medios guiados y no guiados, en ambos casos la comunicación se lleva a cabo con ondas electromagnéticas [11].

Medios Guiados

Los medios guiados conducen las ondas a través de un camino físico, la capacidad de transmisión, en términos de velocidad de transmisión o ancho de banda, depende drásticamente de la distancia [10]. Los tres medios guiados más utilizados para la transmisión de datos son:

- ❖ Par Trenzado
- ❖ Cable Coaxial
- ❖ Fibra Óptica

Medios no Guiados

Los medios de transmisión no guiados utilizan el aire o espacio para enviar la información de un punto a otro en forma de señales electromagnéticas, tanto la transmisión como la recepción se lleva a cabo mediante antenas que radian energía electromagnética en el medio [11]. Los medios no guiados son los normalmente utilizados para llegar a lugares remotos de difícil acceso estos medios los podemos clasificar en:

- ❖ Ondas de Radio
- ❖ Microondas
- ❖ Infrarrojos

A continuación se realiza la revisión de conceptos teóricos de medios de transmisión por microondas y ondas de radio debido a que es prioritario para el presente trabajo de investigación.

Ondas de Radio

Las ondas de radio se utilizan para transmitir información a grandes distancias a través del aire, su radiación es omnidireccional, mientras que las microondas son mucho más direccional, la banda de frecuencia va desde 3 kHz a 300GHz. Este rango cubre la radio comercial FM así como televisión UHF y VHF a igual que se utiliza para aplicaciones de redes de datos. El alcance y ancho de banda dependerá de la frecuencia utilizada. Por regla general a mayor frecuencia más ancho de banda pero menos alcance y viceversa. Se utilizan en sistemas de televisión y radio [11].

Microondas

Los sistemas de microondas son los servicios de telecomunicaciones de larga distancia, como alternativa al cable coaxial o a la fibra óptica, el uso de las microondas es frecuente en la transmisión de voz, datos y video en enlaces punto a punto entre edificios para la interconexión de redes locales. La banda de frecuencias está comprendida entre 2 y 40 GHz, por cuanto mayor sea la frecuencia utilizada, mayor es el ancho de banda potencial, y por tanto, mayor es la posible velocidad de transmisión [11].

En esta sección se realiza la revisión de concepto teórico de la tecnología Gigabit Ethernet que se emplearse como troncal para conectar diversas redes que actualmente se encuentra implementada dentro de la red MAN de EEASA.

Gigabit Ethernet

Gigabit Ethernet es la evolución de la tecnología Ethernet, diseñada originalmente como una tecnología conmutada que permite garantizar no sólo el envío de datos y tráfico multimedia, sino de voz, ya que el medio de transmisión para el que fue diseñado es la fibra óptica. Además el ancho de banda puede escalar desde 10 Mbps a 10 Gbps, sin inhabilitar ninguno de los servicios de red inteligentes [13].

Asimismo Gigabit Ethernet admite las técnicas de gestión de tráfico existentes que ofrecen calidad de servicio en Ethernet, como priorización del tráfico IEEE 802.1p en la cabecera 802.1q, clases de tráfico en, conmutación de etiquetas multiprotocolo (MPLS) y protocolo de reserva de recursos (RSVP) [14].

2.2.3 Redes Inalámbricas

Las redes inalámbricas permiten comunicar dos o más dispositivos sin la necesidad de conectarse con cable como portátiles, celulares, etc. Este tipo de redes utilizan el término movilidad debido a que los usuarios pueden mantenerse conectados a la red cuando se desplazan dentro de una determinada área geográfica [15]. Existen diferentes tipos de redes inalámbricas como se puede observar en la figura 2.2



Figura 2.2. Redes Inalámbricas [15]

Existe una clasificación de redes de acuerdo al tamaño entre estas tenemos a WPAN (Wireless Personal Area Network), con un alcance de 5 a 10 m, WLAN (Wireless Local Area Network) esta red cubre distancias mayores de 100m, WMAN (Wireless Metropolitan Area Network) con alcances de 50 Km y WWAN (Wireless Wide Area Network) el cual permite la comunicación entre países. Estos tipos de redes utilizan ondas de radio o luz infrarroja para transmitir los datos permitiendo acceso inalámbrico de banda ancha, proporcionando a los usuarios acceso de alta velocidad.

2.2.4 Estándares de las redes Inalámbricas (IEEE 802.11)

IEEE 802.11

Primero de los estándares definidos por la IEEE para aplicaciones WLAN, con velocidades de transmisión de 1 y 2 Mbps que se transmiten por señales de Radiofrecuencias e infrarrojos. Funciona sobre la banda de 2.4 GHz, y debido a la aparición de una serie de variantes que mejoran la velocidad de transferencia este estándar está en desuso [15].

IEEE 802.11a

Estándar de conexión inalámbrica que tiene como velocidad de transmisión de 54 Mbps que trabajan en la banda de 5 GHz. La distancia de cobertura alcanza entre 30m (a 54Mbps) y 300m (a 6 Mbps) en exteriores. Este estándar es también conocido como “Wifi5”, su mayor desventaja es que sus ondas son más fácilmente absorbidas, esto implica que los equipos deben quedar en línea de vista y es necesario un mayor número de AP [15].

IEEE 802.11b

Estándar de conexión inalámbrica que tiene una velocidad de transmisión que varían entre 1, 2, 5.5 y 11Mbps, trabaja en la banda de 2,4 GHz y la distancia de cobertura depende de las velocidades aplicadas, número de usuarios conectados y antenas que se pueden utilizar, pero se podría dar una cifra de entre 120m y 460m con velocidades de 11 y 1 Mbps respectivamente [15].

IEEE 802.11e

Estándar de conexión inalámbrica que tiene como objetivo introducir mecanismos a nivel de capa MAC para soportar los servicios de que requieran de Calidad de Servicio (QoS), introduciendo un elemento llamado HCF (Función de Coordinación Híbrida) con dos tipos de acceso [15]:

- ❖ EDCA (Enhanced Distributed Channel Access, Función Mejorada de Distribución de Acceso al Canal)
- ❖ HCCA (HCF Controlled Channel Access, Función HCF de Control de Acceso al Canal)

IEEE 802.11g

Estándar de conexión inalámbrica que suministra una velocidad de transmisión de 54 Mbps en una banda de frecuencia de 2.4 GHz, este estándar es compatible con el 802.11b y cubre de 50 a 100m de distancia en interiores y establece comunicaciones de hasta 50Km con antenas parabólicas [15].

IEEE 802.11n

Estándar de conexión inalámbrica con velocidad real estimada de 600Mbps, y debería ser hasta 10 veces más rápida que una red bajo los estándares 802.11a y 802.11g, y 40 veces más rápida que una red bajo el estándar 802.11b. Este estándar trabaja en las bandas de 5 GHz, y se puede usar en 2.4 GHz si las frecuencias están libres [15].

2.2.5 Calidad de Servicio (QoS)

La Calidad de Servicio (QoS) hace referencia a la capacidad de una red para proporcionar mejores servicios al tráfico que generan las aplicaciones de la red y que funcionan bajo distintas tecnologías [8]. QoS reduce la pérdida de paquetes, evita y gestiona las congestiones, permitiendo y fijando prioridades del tráfico a través de la red. Es necesario tomar en cuenta de que QoS no es aumentar ancho de banda sino distribuirlo de acuerdo a las necesidades de la empresa [7].

Existen parámetros que definen la QoS en una red y que varían según la aplicación y la identificación de los mismos, estos permiten clasificar o determinar la prioridad de

algunas aplicaciones sobre otras. A continuación se muestra los parámetros que intervienen en la medición de QoS en una red.

Ancho de Banda (Bandwith)

El término de ancho de banda es una medida de la capacidad de transmisión de datos y se refiere al número de bits por segundo que puede viajar a través del medio. Aumentar el ancho de banda significa poder transmitir mayor transferencia de datos por unidad de tiempo (mayor velocidad), pero también implica un aumento económico. El ancho de banda es expresado en Hertzios (Hz) o en Mega hertzios (MHz) [8].

El Caudal (Throuhgput)

El caudal o throughput es un término genérico que describe la capacidad de un sistema para transferir datos. En redes TCP/IP se define y se mide la tasa de bytes o paquetes que va por el circuito, de una aplicación específica, de un nodo a otro o de una red a otra. Un parámetro directo en que un router puede configurar y controlar el throughput es la cantidad de ancho de banda reservado para los diferentes tipos de paquetes [16].

Retardo (Delay)

El retardo es el tiempo de retraso en la llegada de los paquetes hasta su destino. Al transmitir paquetes de un punto a otro se genera una variación temporal o retraso de flujos de datos a su destino, hoy en día varios factores influyen en el retardo de un paquete que atraviesa la red, dependiendo de las aplicaciones que se estén orientando las telecomunicaciones se presentan retardos de enrutamiento (router), retardo en colas, retardo de propagación y retardo de serialización, que se producen en cada nodo y enlaces en la red [16].

Variación del Retardo (Jitter)

La Variación del retardo se produce cuando los paquetes transmitidos en una red no llegan, debido a una distorsión en los tiempos de llegada de los paquetes. En si es el efecto del retardo en la comunicación ya que se producen fluctuación en el canal por la diferencia entre varios retardos de paquetes en un mismo flujo. Una fuente potencial de Jitter es que los paquetes consecutivos de un mismo flujo sigan caminos físicos diferentes [8].

Además, el *Jitter* crece exponencialmente con el aumento de la utilización del ancho de banda al igual que el retardo. Según el estudio de mecanismo de calidad de servicio el *Jitter* lo puede medir usando diferentes técnicas, incluyendo la media, desviación típica, máximo o mínimo del tiempo de llegada entre los paquetes, consecutivos de un mismo flujo. Por todo ello, el *Jitter* influye en la calidad de servicio percibida, sobre todo en aplicaciones de voz o vídeo [16].

Pérdida de Paquetes

La pérdida de paquetes o Packet Loss indica el número de paquetes perdidos durante la transmisión que normalmente se miden en tanto por ciento, hay tres fuentes de pérdidas de paquetes en una red IP estas son, rotura en un enlace físico que evita la transmisión de un paquete, un paquete corrupto debido al ruido detectado por un sistema de *checksum* y desbordamiento de las memorias producidas por la congestión de la red [16].

2.2.6 Técnicas de Priorización de Tráfico

Calidad de Servicio (QoS) engloba dos técnicas en la priorización de tráfico que son la Clase de servicio (CoS) que permite a los administradores de red solicitar prioridad para un tráfico, mientras que los Tipos de Servicio (ToS) equivale a una ruta de uso compartido donde el ancho de banda es reservado para asignar tráfico de prioridad [7].

A continuación se presenta la descripción de como la calidad de servicio engloba las técnicas de CoS y ToS.

Clases de Servicio (CoS)

Clase de Servicio (CoS) es un esquema de clasificación con que son agrupados los tráficos, se basa en diferenciar los tipos de tráfico y por ende poder priorizarlos. En primer lugar la priorización de los distintos tipos de tráfico claramente definidos a través de la red y, en segundo lugar, la definición de un pequeño número de clases de servicio a las que se aplica [7].

Priorizar es importante en los puntos de congestión de la red, donde las decisiones de priorización pueden ser realizadas por routers y switches. A diferencia de QoS, CoS no garantiza ancho de banda o latencia, en cambio permite a los administradores de red solicitar prioridad para el tráfico [17].

La Clase de Servicio es el esquema de prioridad 802.1p, donde se establece ocho niveles de priorización con su respectiva cola como se puede visualizar en la tabla 1.

Tabla 2.1: Valores de Prioridades CoS

| Valor de CoS | Valores de las colas de reenvío | Aplicación |
|--------------|---------------------------------|----------------------------------|
| 0 | Q2 (Routine) | Datos |
| 1 | Q1(Priority) | Datos de media prioridad |
| 2 | Q1(Inmediate) | Datos de alta prioridad |
| 3 | Q2 (Flash) | Señal de llamada |
| 4 | Q3 (Flash-Override) | Videoconferencia |
| 5 | Q3(Critical) | Voz |
| 6 | Q4(Internet) | Reservado (internetwork control) |
| 7 | Q4(Network) | Reservado (network control) |

Fuente: Implementación de QoS en la red LAN, pág. 24 [8]

La prioridad más alta es siete que será el tráfico más crítico, se generaría en las actualizaciones de la tabla cuando se use RIP (Protocolo de Información de Enrutamiento) y OSPF (*Open Shortest Path First*). Los valores de cinco y seis podrían ser tráfico sensibles al retardo como video interactivo y de voz; mientras que los cuatro últimos valores se destinaria para clases de datos a través de una gama de aplicaciones de carga controlada, como el tráfico de streaming multimedia. El priorizar el tráfico con CoS únicamente será una clasificación en capa 2 y será renviado directamente al usuario, pues no establece reserva del ancho de banda [8].

Tipo de Servicio (ToS)

El Tipo de Servicio proporciona una indicación de la calidad de servicio deseada al transmitir un datagrama de un paquete IP. Algunas redes ofrecen prioridad de servicio, la cual trata de algún modo el tráfico de alta prioridad como la más importante que el resto del tráfico, a través de parámetros que determinan la prioridad de un servicio como precedencia, máxima throughput, mínimo retardo y máximo fiabilidad [7][8].

Se debe considerar los requerimientos fundamentales que se deben reunir para lograrla tomando en cuenta que CoS y ToS son técnicas que permiten obtener QoS [7].

Los tres primeros campos representan una prioridad, el cual permite marcar los datagramas según su importancia este tiene ocho niveles ordenados como se muestra en la figura 2.3.

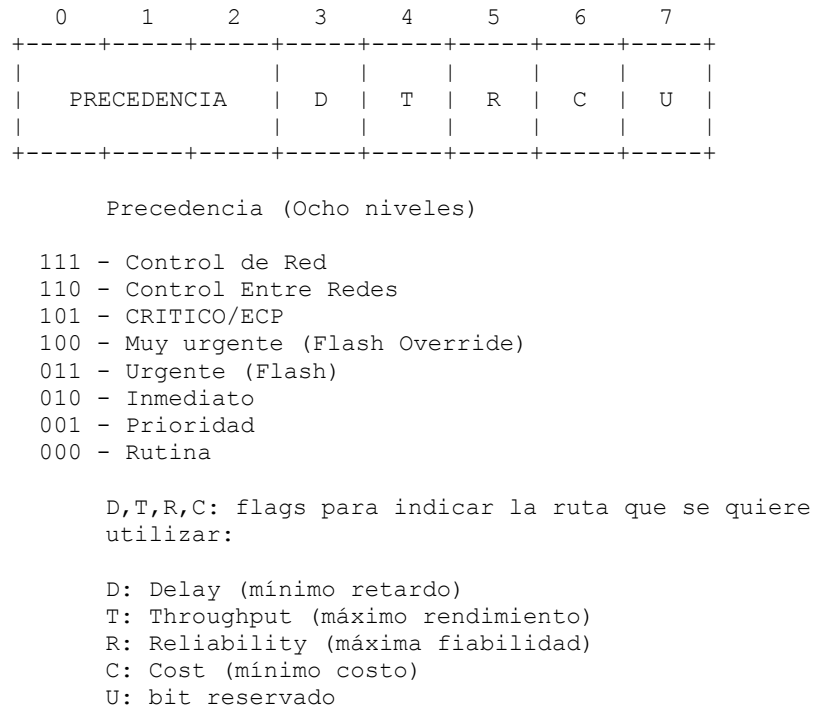


Figura 2.3: Tipo de Servicio [17]

2.2.7 Modelos de Priorización QoS

Considerando los parámetros que debe permitir la calidad de servicio en la red, es necesario indicar el tipo de métodos a utilizados actualmente en la transmisión de paquetes que permiten priorizar un tráfico. A continuación se hace una descripción de los tres modelos para implementar QoS en una red, los cuales son: Mejor Esfuerzo (Best Effort), Servicios Integrados (IntServ) y Servicios Diferenciados (DiffServ) [7] [8].

Mejor esfuerzo (Best Effort)

El servicio de mejor esfuerzo provee la red cuando hace todo lo posible para entregar un paquete a su destino sin garantía de su recepción. El principal problema de este tipo de algoritmos es que, si tenemos varios flujos de datos, una ráfaga de paquetes en uno de ellos va a afectar a todos los demás flujos, retardando su transmisión. Es decir, que el tiempo de llegada de los paquetes de un flujo puede verse afectado por otros flujos [17].

Modelo utilizado por aplicaciones FTP y HTTP, este modelo no es apropiado para aplicaciones sensibles al retardo, variación de ancho de banda que necesitan de un tratamiento como aplicaciones de VoIP y video conferencia, su desventaja es que no es posible garantizar ningún tipo de servicio a ninguna aplicación.

Servicios Integrados (InstServ)

Se trata del primer modelo que proporciona QoS de extremo a extremo basado en la señalización explícita y reserva de recursos de red, sirve a aplicaciones de tiempo real y el control de ancho de banda compartido entre diferentes clases de tráfico [7].

El protocolo usado es el RSVP (*Resource Reservation Protocol*), actúa al momento que una aplicación tiene el requerimiento de ancho de banda, RSVP va salto por salto a lo largo del camino intentando hacer la reserva solicitada en cada uno de los routers que se encuentran en la ruta [18]. La aplicación solicita un nivel de servicio necesario, para que opere apropiadamente, y se base en QoS para reservar recursos de red necesarios antes de que la aplicación comience a transmitir [8].

Características de RSVP

- ❖ Está diseñado para trabajar con cualquier método de QoS
- ❖ No transporta datos de Usuario
- ❖ Permite Unicast y Multicast
- ❖ No es un protocolo de ruteo, sino que está pensando para trabajar conjuntamente con estos, los protocolos de ruteo determinan donde se reenvía los paquetes mientras que RSVP se preocupa por los QoS de los paquetes reenviados de acuerdo con el ruteo [7].
- ❖ Permite diferentes tipos de reservas.
- ❖ Soporta IPV4 e IPV6 aunque no sea un protocolo de transporte.

Para implementar Servicios Integrados además de RSVP se debería habilitar lo siguiente:

- ❖ Control de Admisión
- ❖ Clasificación de tráfico
- ❖ Políticas
- ❖ Encolamiento
- ❖ Programación

La desventaja a mencionar es que cada flujo activo necesita señalización continua, usando así recursos extra y haciendo que no sea un modelo altamente escalable.

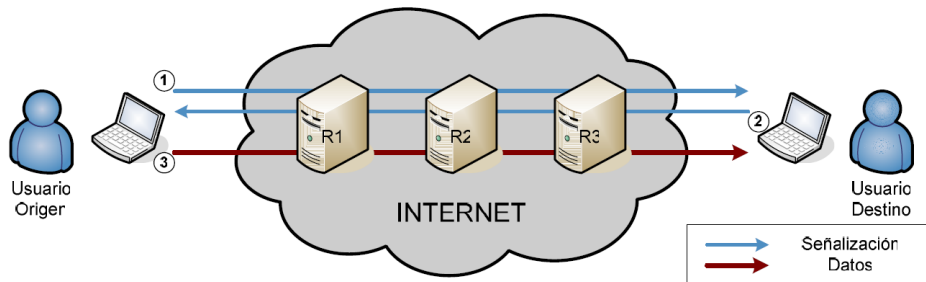


Figura 2.4: Esquema de Funciones de Modelo IntServ [19]

Servicios Diferenciados (DiffServ)

El servicio diferenciado es un conjunto de tecnologías por las cuales los proveedores de servicio de red ofrecen distintos niveles de QoS para diferentes clientes y tráfico de información [16]. Este modelo se basa en marcar los paquetes IP y los routers los tratarán en base a esa marca, de tal forma que se da un tratamiento diferenciado a los paquetes.

DiffServ satisface requisitos de altas prestaciones, escalabilidad, permitir el crecimiento sostenido del tamaño de las redes y su ancho de banda, entre otros. Esta arquitectura propone un tratamiento diferenciado en los nodos para un conjunto reducido de flujos o clases, de forma que todos los paquetes que pertenezcan a una misma clase recibirán un mismo tratamiento por parte de la red. [19]

En los servicios diferenciados hay que tener en cuenta que:

- ❖ El tráfico es clasificado
- ❖ Las políticas de QoS son aplicadas dependiendo de la clase.
- ❖ Se debe elegir el nivel de servicio para cada tipo de clase que corresponde a unas necesidades determinadas.

El punto negativo de servicio diferenciado es que no es absolutamente garantizado y es más complejo de implementar [18].

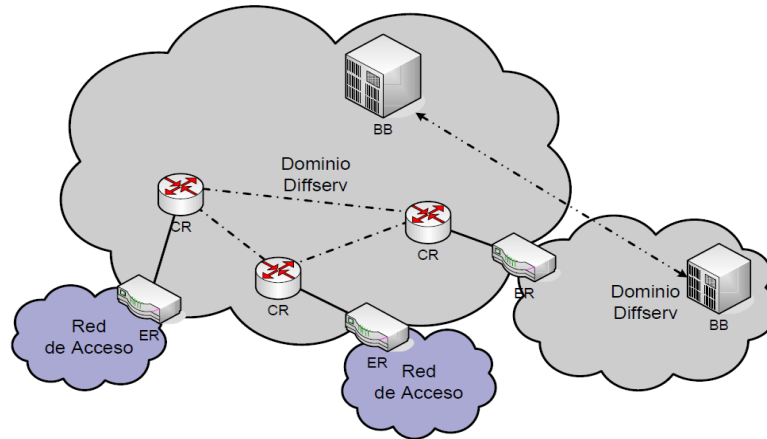


Figura 2.5: Esquema que conforma el Modelo DiffServ [19]

El modelo DiffServ está basado en la redefinición del significado del campo tipo de servicio en la cabecera IP. Donde 6 bits son correspondientes al DSCP (DiffServ Code Point, Punto Código DiffServ) y dos bits para ECN (Explicit Congestion Notification, Notificación Explícita de Congestión) [7].

| DS Field | | | | | | | | |
|-------------|---|---|---|---|---|---|-----------------------------|-----|
| 6 DSCP Bits | | | | | | 0 | ECN | ECN |
| | | | | | | | | |
| - | - | - | 0 | 0 | 0 | } | Class Selector PHB | |
| 0 | 0 | 0 | - | - | 0 | | | } |
| 0 | 0 | 1 | - | - | 0 | } | Assured Forwarding (AF) PHB | |
| 0 | 1 | 0 | - | - | 0 | | | } |
| 1 | 0 | 0 | - | - | 0 | } | | |
| 1 | 0 | 1 | 1 | 1 | 0 | | | |

Figura 2.6. Campo DS y DSCP PHBs [7]

El tratamiento de retransmisión de un paquete es llamado PHB y es representado por uno de los 32 valores DSCP de uso estándar en la cabecera del paquete. Los PHBs se describen perfectamente como distribución de ancho de banda, prioridad de descarte, entre otros. Existen cuatro servicios disponibles de PHBs.

- ❖ Best-Effort
- ❖ Class-Selector (CS)
- ❖ Assured Forwarding (AF)

❖ Expedited Forwarding o Premium (EF)

2.2.8 Ventajas y desventajas que presenta el método IntServ y DiffServ.

Tabla 2.2: Ventajas y desventajas de IntServ-DiffServ

| | IntServ (Integrated Services) | DiffServ (Differentiated Services) |
|-------------------|---|---|
| Ventajas | <p>Este modelo permite crear reglas de QoS para flujos discretos, esto permite conocer a los nodos extremos sobre la disponibilidad de ancho de banda.</p> <p>Los paquetes no necesitan llevar ninguna marca que indique como han de ser tratados, la información la tienen los routers.</p> <p>Facilita que toda la red mantenga una política de red integrada</p> <p>Cada router mantiene información de estado por cada flujo.</p> | <p>No hay reservación del canal</p> <p>Reduce la carga de la red</p> <p>Se basa en el marcado de paquetes. No hay reserva de recursos por flujo, no hay información de estado en los routers.</p> <p>La escalabilidad en los routers frontera se mantiene información para cada flujo o agregados de flujos, en los routers del núcleo se mantiene información por cada clase</p> <p>En vez de distinguir flujos individuales clasifica los paquetes en categorías según el tipo de servicios solicitados.</p> <p>Los routers no necesitan conservar información de estado.</p> |
| Desventaja | <p>Los routers intermedios deben tener RSVP en sus funciones.</p> <p>Requiere de mensajes periódicos de refresco para mantener la sesión, aumentando el tráfico en la red.</p> <p>Presenta problemas de escalabilidad debidos a la necesidad de mantener información de estado en cada router de cada flujo.</p> <p>No es escalable en grandes redes o implementaciones muy complejas</p> | <p>Los servicios no están garantizados debido a que no hay reserva</p> <p>Algún router intermedio puede cambiar la marca</p> <p>Las garantías de QoS no son tan severas como en IntServ pero en muchas cosas se consideran suficientes.</p> |

Fuente: Implementación de QoS en red de transporte de datos del MDMQ [7]

2.2.9 Mecanismos para Administrar Calidad de Servicio (QoS)

Para la correcta implementación de calidad de servicio es necesario tomar en cuenta que existen varios mecanismos para administrar QoS, que se aplican a los modelos mencionados anteriormente, en donde se hace referencia al manejo de congestión y manejo de tráfico [8].

Manejo de Congestión

El manejo de congestión hace referencia a los mecanismos de administración de encolamiento en una interfaz, la principal causa de la congestión en las interfaces es la diferencia de velocidades que existen entre ellas. En función de la clasificación del tráfico se da diferente tratamiento a cada flujo de datos para asegurar que el tráfico perteneciente a aquellas clases que requieran menor retardo sea reenviado antes que el tráfico que no es sensible al retardo. Las implementaciones propietarias de cisco están basadas de los siguientes algoritmos de manejo de colas [7] [8].

Primero en ingresar, primero en salir (FIFO)

- ❖ En su forma más sencilla, el mecanismo de cola FIFO, se encarga de almacenar paquetes cuando hay congestión en la red, y a enviarlos cuando tiene la posibilidad, manteniendo el orden de llegada, es decir, que no ofrece ninguna prioridad de unos paquetes sobre otros.
- ❖ Cisco lo utiliza por defecto en enlaces superiores a T1 (1.5 Mbps)
- ❖ Este algoritmo, al igual que ocurre con el resto de mecanismo de cola, tiene como limitación la capacidad de su búfer en momentos de congestión.
- ❖ Hoy en día se necesitan algoritmos más sofisticados, que permiten diferenciar entre distintos tipos de paquete, por lo que este método está cayendo en desuso.

Colas de Prioridad (PQ)

- ❖ Asegura que el tráfico importante reciba un servicio rápido en cada punto de la red, donde el mecanismo este presente.
- ❖ En el mecanismo PQ, cada uno de los paquetes debe de ser colocado en una de las cuatro posibles colas (alta, media, normal, baja prioridad), servidas en riguroso orden de prioridad, lo cual puede crear inanición.

- ❖ La prioridad de los paquetes puede diferenciarse por diversos medios, como: el protocolo de red, el interfaz del router por el que llegue el paquete, el tamaño del paquete y la dirección de origen o destino.
- ❖ Los paquetes que no se puedan clasificar serán asignados a la cola de prioridad normal.

Encolamiento Balanceado justo (WFQ)

- ❖ Los mecanismos vistos anteriormente son estáticos, y por lo tanto no se adaptan a los cambios producidos en la red
- ❖ WFQ es adecuado para situaciones donde se necesite un buen tiempo de respuesta, para usuarios que hagan tanto un uso elevado de la red, tanto como para los que hagan un uso más leve, sin añadir ancho de banda adicional [7].
- ❖ Cisco lo utiliza por defecto en enlaces inferiores a T1 (1,5 Mbps)
- ❖ WFQ es un algoritmo de cola basado en flujos (o sesiones), que realiza dos tareas simultáneamente y de forma automática [8]:
 - Organiza el tráfico (de tiempo real), poniéndolo al principio de la cola, reduciendo así el tiempo de respuesta.
 - Comparte equitativamente el resto del ancho de banda, entre el resto de tráfico de alta prioridad
- ❖ WFQ asegura que las diferentes colas no se queden privadas de un mínimo ancho de banda, de modo que el servicio proporcionado al tráfico es más predecible.
- ❖ Considera flujos de poco caudal con flujos sensibles al retardo, por ej. VOIP
- ❖ No es escalable dentro de una gran red

Manejo de tráfico

El manejo de tráfico tiene como objetivo evadir la congestión, un método para reducir la congestión, es descartar paquetes de clases de menor precedencia cuando el sistema está cerca a la saturación, para preservar el tráfico de las clases de alta prioridad. A continuación se describen los principales métodos que se utilizan para el manejo de tráfico [7] [8].

- ❖ Descarte de cola (DT)
- ❖ Detección temprana aleatoria (RED)

A continuación se puede visualizar en la tabla las ventajas y desventajas que presenta este tipo de manejo de tráfico.

Tabla 2.3: Ventaja y desventaja de manejo de tráfico RED

| Ventajas | Desventaja |
|---|---|
| <ul style="list-style-type: none"> ❖ RED identifica las etapas tempranas de congestión y responde con descartes aleatorios de paquetes. ❖ Si la cantidad de congestión se sigue incrementando, RED descarta paquetes de manera más agresiva para evitar que la cola alcance el 100% de su capacidad. ❖ Debido a que RED no espera hasta que la cola se llene para comenzar a descartar paquetes, RED permite a la cola aceptar todos los paquetes de una ráfaga. ❖ Como resultado, RED trata bien al tráfico TCP y ayuda a evitar la sincronización ❖ RED permite mantener la cantidad de tráfico en una cola en un nivel moderado. ❖ RED permite mantener la profundidad de la cola en un nivel que produce la mejor utilización del ancho de banda de salida. | <ul style="list-style-type: none"> ❖ RED puede ser difícil de configurar si se quiere alcanzar una ejecución predecible. ❖ Si no se ponen los parámetros de configuración adecuados de RED puede que la utilización del ancho de banda de salida sea peor que si se usa Trail Drop. ❖ Cuando se descarga un paquete que no es de TCP con RED la fuente no sabe que el paquete se ha descartado y no altera su tasa de transmisión. Por esta razón se recomienda no usar RED con tráfico basado en UDP. También se recomienda utilizar tamaños de cola pequeños para este tipo de tráfico para evitar grandes retardos. |

Fuente: Implementación de QoS en red de transporte de datos del MDMQ [7]

- ❖ Detección temprana aleatoria balanceada (WRED).

En la tabla se puede determinar las ventajas y desventajas que presenta la detección temprana aleatoria balanceada (WRED), para el buen manejo de tráfico.

Tabla 2.4: Ventaja y desventaja de manejo de tráfico RED

| Ventajas | Desventajas |
|--|--|
| <ul style="list-style-type: none"> ❖ Es una extensión de RED que permite asignar diferentes perfiles de descarte a diferentes tipos de tráfico. ❖ La habilidad para definir diferentes colas o a diferentes tipos de tráfico en la misma cola proporciona una precisión mayor de control que el RED clásico. Por ejemplo suponiendo que la gestión de la memoria de la cola permitiese definir dos niveles de precedencia de descarte dentro de una misma cola. Esto permitiría asignar un perfil de descarte de RED menos agresivo para ciertos paquetes y más agresivo para otros dado un mismo nivel de congestión. | <ul style="list-style-type: none"> ❖ Si el valor de n alcanza valores demasiado altos, WRED no reacciona a la congestión. Donde n es el factor de peso exponencial (exponential weight factor), configurable por el usuario. ❖ Si el valor de n llega a ser demasiado bajo, WRED reacciona muy fuerte a ráfagas temporales muy fuertes y descarta paquetes innecesariamente |

Fuente: Implementación de QoS en la red LAN de la UTPL [8]

Por otro lado el modelamiento de tráfico general (GTS) detalla los métodos que se emplean para prevenir congestión, mediante la reducción de flujo de paquetes a la salida para evitar la congestión. El modelo se aplica sobre cada interfaz mediante la utilización de listas de acceso para seleccionar el tráfico a modelar [8]. El modelamiento de tráfico funciona con tecnologías de la capa 2 como SMDS, ATM, Frame Relay y Ethernet, compatible con medios de comunicaciones y tipos de encapsulación en el router [8].

2.2.10 Clasificación del Tráfico

Proceso que permite dividir el tráfico de la red en diferentes categorías, cada una de las cuales requiere un tratamiento diferente, se utiliza procedimientos básicos de clasificación y asignación de prioridad, denominado mapas de clases y mapas de política.

Un mapa de clase es un mecanismo para nombrar y asilar un flujo de tráfico específico, este compara el tráfico para más tarde clasificarlo, el cual puede incluir herramientas ACL (Listas de Control de Acceso) estándar o extendido, a una lista específica de DSCP (Punto de Código de Servicios Diferenciados), o valores de precedencia IP, para posteriormente clasificarlo mediante el uso de mapas de políticas [8].

Un mapa de política específica en qué clase de tráfico actúa, estas pueden ser:

- ❖ Confiar en los valores de CoS, DSCP o Precedencia IP de la clase de tráfico
- ❖ Establecer un valor específico o especificar limitaciones de ancho de banda y la acción a tomar cuando el tráfico cae fuera del perfil definido en el mapa de política [8].

Es posible clasificar desde unas pocas a cientos de variación de tráfico dentro de diferentes clases, estas han de ir de acuerdo a las necesidades y objetivos empresariales. Las siguientes clases son el resultado de varios estudios las cuales aparecen en cualquier red empresarial [18].

- ❖ **Clase de VoIP**, como su propio nombre indica corresponde al tráfico de VoIP
- ❖ **Clase de aplicaciones de misión crítica**, corresponde a aplicaciones de alta importancia.
- ❖ **Clase de tráfico de señalización**, pertenece al tráfico de señalización de VoIP, video, etc.
- ❖ **Clase Best-effort**, esta clase engloba el tráfico no estipulado en las anteriores y se le proporciona al ancho de banda que sobre.
- ❖ **Clase sin importancia**, corresponde a servicios o aplicaciones que se consideran inferiores a las Best-effort. Podrían ser e-mail personal, aplicaciones P2P, juegos online, etc.
- ❖ Mecanismo de regulación de tráfico

Traffic Policing

2.2.11 Calidad de Servicio (QoS) en Redes Inalámbricas

La demanda de aplicaciones sobre redes que presentan limitaciones de ancho de banda como es el caso de las inalámbricas se impone la necesidad de brindar Calidad de Servicio (QoS) en entornos inalámbricos haciendo énfasis al estudio en tecnologías fundamentales como la wifi, 802.11 y la 802.16 y el análisis que describen los parámetros de calidad de servicios, en entornos inalámbricos así como los métodos que se emplean en las tecnologías mencionadas para obtener dicha Calidad de Servicio [15].

Calidad de servicio (QoS) en Wimax

La calidad de servicio en Wimax o estándar IEEE 802.16, se logra por medio de un mecanismo de programación de servicio en la estación base (BTS). Esta programación es diseñada para mejorar la eficiencia de acceso al medio. Mediante un servicio programado y los parámetros asociados de QoS, la estación base podrá anticiparse a las necesidades del rendimiento, *jitter* u otro parámetro del tráfico de subida y además proveer de los métodos adecuados de sondeo y peticiones de concesión de ancho de banda en tiempos apropiados. En redes inalámbrica el estándar 802.16, integra QoS en la capa MAC coordina la comunicación en el medio inalámbrico compartido, protocolo orientado a conexión por lo cual cuando una estación suscriptora (SS) ingresa a la red, éste crea conexiones donde sus datos son transmitidos desde y hacia la estación base (BS). Los parámetros de calidad de servicio son definidos por los denominados flujos de servicio que no es más que el envío MAC que provee un transporte unidireccional de paquetes [15].

Wimax soporta QoS diferenciado para distintos usuarios y para distintos flujos, empleando estos flujos de servicio para llevar a cabo las dos tareas necesarias de cualquier mecanismo de QoS: Clasificación del tráfico y Asignación de recursos. En la figura representa un modelo simplificado pero útil para comprender cómo funcionan los mecanismos de QoS [20].

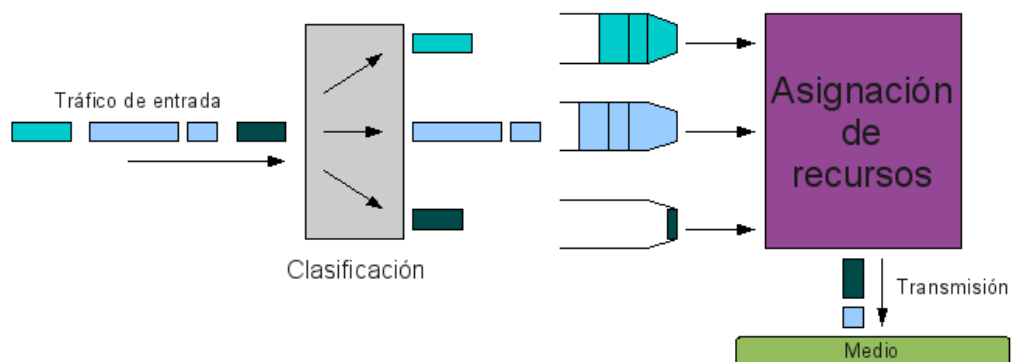


Figura 2.7: Esquema para análisis de QoS [20]

La Calidad de Servicio (QoS) en Wimax se apoya en los siguientes puntos:

- **Capa MAC:** El nivel de Acceso al Medio es la piedra angular de esta tecnología. Con una estructura entramada, una gran eficiencia espectral, y una estación base que ejerce en todo momento de árbitro y gestiona el espectro, Wimax permite implementar de forma determinista cualquier mecanismo de QoS.
- **Layer2QoS:** Uno de los puntos fuertes de la tecnología Wimax es que implementa mecanismos de QoS hasta nivel 2 que le permiten ofrecer servicios diferenciados de forma determinista, ya que la BS conoce las modulaciones hacia todos los usuarios y por lo tanto es capaz de asignar los recursos en cada momento.
- **Flujos de servicio:** Los datos que fluyen por el aire deben ser transportados por flujos de servicio, estos flujos son unidireccionales e independientes por cada usuario, la tecnología Wimax se basa en diferenciar aplicaciones utilizando la diferenciación de flujos.
- **Tipos de servicio:** Los flujos de datos en Wimax pueden ser de cinco tipos distintos en función del tipo de priorización que se quiera realizar entre ellos tenemos.
 - ❖ **BE (Best Effort):** Empleados muy habitualmente para servicios de datos, que no suelen requerir niveles mínimos de servicio.
 - ❖ **RTPS (Real Time Polling Service):** Son ideales para productos como VoIP, y tienen una tasa binaria mínima garantizada.
 - ❖ **NRTPS (Non Real Time Polling Service):** Extensión de rtPS
 - ❖ **eRTPS (Extended Real Time Polling Service):** Extensión de rtPS

- ❖ **UGS** (*Unsolicited Grant Service*): son ideales para aplicaciones de tráfico constante como transmisión de vídeo ininterrumpido o tramas E1/T1

Los servicios de Wimax mencionados anteriormente permiten ofrecer al operador un modelo de datos equivalente al de un acceso cableado de última milla como QoS, separación voz de y datos, además de tener todas las ventajas del acceso al enlace de radio como inmediatez, reducción de costos y escalabilidad [20].

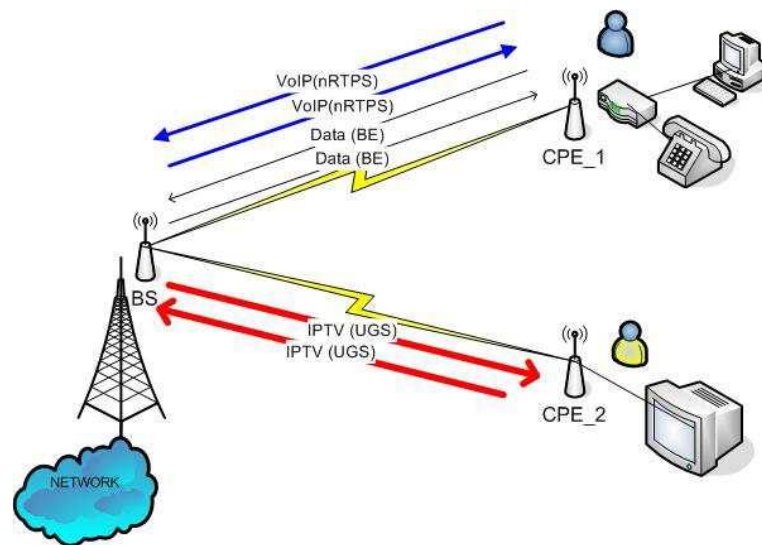


Figura 2.8: Distintos tipos de servicio [20]

Calidad de servicio (QoS) en Redes WI-FI

En la tecnología WiFi se definió el protocolo IEEE 802.11e para la implementación de QoS el cual agrega un campo al protocolo 802.11 para el control de la QoS, permitiendo diferenciar los tipos de tráfico para darle un trato diferenciado a estos [15].

Los estándares de QoS para redes inalámbricas están definidas como 802.11e y Wi-fi Multimedia (WMN), en este tipo de red es importante analizar como enlazar los campos de prioridad en las cabeceras 802.1p o DSCP con 802.11e. Para mantener QoS de extremo a extremo el controlador inalámbrico y la arquitectura centralizada de AP tienen que llevar a cabo ciertas asociaciones entre las marcas de los datos de tráfico que reciben y el que deben enviar, para proporcionar un campo equivalente tanto de CoS como al DSCP. La tecnología WiFi y WiMAX permiten implementaciones de QoS, de manera que la tecnología WiMAX se garantiza la QoS a nivel MAC [20].

2.2.12 Multi-Protocol Label Switching (MPLS)

MPLS Multi Protocol Label Switching, es creado con el fin de mejorar la compatibilidad entre la Capa de Red, protocolo IP, y la capa de enlace, en tecnologías como ATM, Frame Relay, PPP, entre otros. Posee nuevas características tanto de capa de red como de capa de Enlace, lo cual lo hace atractivo para la Internet de la Nueva generación. Además de estas facilidades, nos provee de Calidad de Servicio (QoS) y de Ingeniería de Tráfico tanto para la generación del camino como para la restauración de este [21] [22].

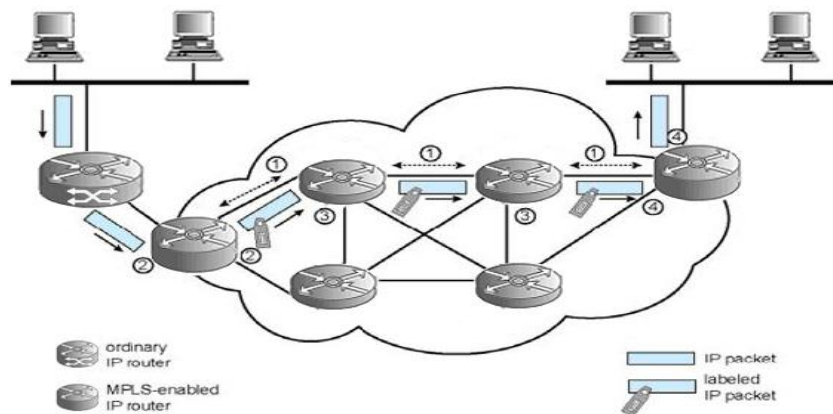


Figura 2.9: Intercambio de paquetes en una red MPLS [22]

Terminología MPLS. Nodos: LER y LSR.

Los dispositivos que básicamente forman parte de una red MPLS son dos tipos específicos de routers que pueden clasificarse en LER y LSR. Los LER son dispositivos que operan en los extremos de la red MPLS, son los responsables de enviar el tráfico entrante a la red MPLS y distribuir el tráfico saliente hacia las distintas redes destino. Funcionan como el punto de interconexión entre la red MPLS y la red de acceso.

Los LSRs son los encargados de dirigir el tráfico en el interior de la red, de acuerdo con las etiquetas asignadas. Cuando un paquete arriba a un LSR, éste examina su etiqueta y la utiliza como un índice en una tabla propia que especifica el siguiente "salto" y una nueva etiqueta. Los LSR son routers de gran velocidad en el núcleo de la red MPLS.

Sus principales funciones son: participar en el establecimiento de los circuitos extremo-extremo dentro de la red usando un protocolo de señalización apropiado y conmutar rápidamente el tráfico de datos entre los caminos establecidos [22].

De este modo los LER constituyen la interfaz entre la red MPLS y otras redes, y los LSR representan el cuerpo de la red MPLS tal y cómo se muestra en la figura 2.10.

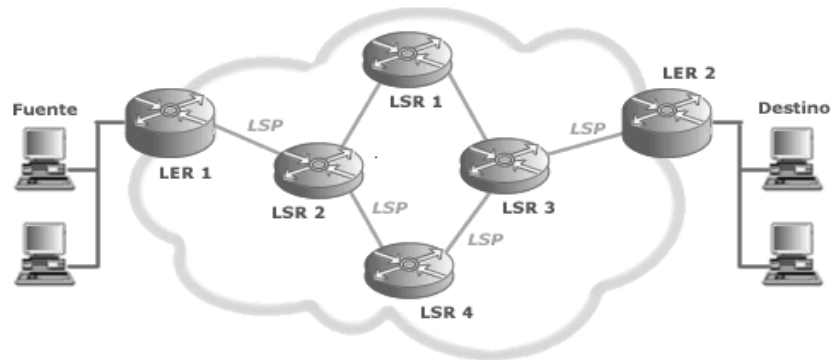


Figura 2.10: Ejemplo de arquitectura MPLS [22]

La ruta que sigue un paquete entre dos nodos (LSRs) de la red MPLS se conoce como LSP. Cada LSP es unidireccional, por lo que el tráfico de regreso deberá utilizar un LSP diferente [22].

Arquitectura MPLS y Calidad de Servicio QoS en una red IP

La arquitectura MPLS nos provee de un circuito virtual o LSP a través de los diferentes nodos que conforman la red MPLS. Gracias a este tipo de funcionamiento, el circuito virtual creado provee de un trato igualitario a los diferentes tráficos que se envían bajo a un mismo túnel LSP bajo una etiqueta FEC en particular. Estudios relacionados a la Calidad de Servicio en diferentes escenarios son de interés actualmente debido a la comparación con las demás arquitecturas, MPLS ofrece escalabilidad, simplicidad, velocidad, entre otros [21]. Las facilidades que ofrece esta arquitectura para la implementación de Calidad de Servicio son las que se explicarán a continuación:

- ❖ Se ha descrito los algoritmos y las diferentes opciones que se pueden utilizar para implementar Calidad de Servicio en la Red de Datos y algunas características sobre redes que ayudaran a comprender mejor el diagnóstico del estado de la red [21].
- ❖ Se acomoda a los modelos de Calidad de Servicio (QoS). Gracias al campo experimental EXP el cual cuenta con 3 bits, que puede priorizar los diferentes tipos de tráficos cursados en el mismo túnel LSP. Nótese que con 3 bits podemos

obtener 8 tipos de prioridades, lo cual coincide con el número de clases de Servicio [21].

- ❖ Esta característica se suma al hecho de que MPLS es capaz de reservar recursos a través de un mismo dominio. Puede entenderse que una Clase de Servicio pueda ser implementada bajo una reserva de recursos para ciertos tipos de tráfico provenientes de un cliente y dentro de esta reserva de recursos se daría prioridad a los tráfico que la necesiten.
- ❖ Garantía de Calidad de servicio sobre el esquema IP. A diferencia del esquema actual de Internet Best Effort y de DiffServ, los cuales no dan una garantía total sobre el envío del tráfico que se inserta a la red IP. MPLS, por su parte, antes del envío construye un túnel LSP, donde el comportamiento es igual en todos los nodos que constituyen este túnel LSP, es decir, los recursos que se destinan para este tráfico serán destinados para este tráfico exclusivamente hasta que el tráfico acabe y se liberen los recursos asignados y sean tomados por otro requerimiento [21].
- ❖ Aunque IntServ tiene un comportamiento muy parecido en lo que respecta a asignación de recursos, MPLS lo hace de red a red, es decir, crea un túnel LSP desde el router origen al router destino pero no de host a host como lo hace IntServ; otra diferencia entre estas arquitecturas es el hecho que IntServ crea un comportamiento de recursos dedicados por cada flujo en la red, MPLS crea el mismo comportamiento de recursos dedicados pero con la gran diferencia que los mismos recursos pueden ser usados por diferentes tráfico según los requerimientos especificados en el LSA [21].

2.3 Propuesta de Solución

El estudio de factibilidad de implementar QoS en la red MAN, permite determinar que equipos soportan el método de priorización para QoS a implementarse en la red MAN para una adecuada gestión y priorización del tráfico generado, como es el de voz, datos y video información primordial para la Empresa Eléctrica Ambato Regional Centro Norte S. A (EEASA) optimizando así los recursos de la institución.

CAPÍTULO III

METODOLOGÍA

3.1 Modalidad de la investigación

La presente investigación tendrá una modalidad aplicada, ya que se pondrá en práctica los conocimientos científicos adquiridos como también la información sobre la tecnología actual relacionada al tema, permitiendo conocer el problema, analizarlo y contextualizar la información obtenida, con la cual servirán para dar solución al problema planteado.

3.1.1 Investigación Bibliográfica

El presente proyecto de investigación fue de modalidad bibliográfica, debido a que el sustento científico del tema planteado se lo realizó consultando en libros, revistas y publicaciones de la web, para respaldar científicamente las soluciones técnicas referentes a la priorización de calidad de servicio (QoS) en la red MAN de EEASA, siendo esta la mejor manera de obtener información.

3.1.2 Investigación de Campo

La investigación de campo, permitirá estudiar sistemáticamente los hechos en el lugar donde se producen los acontecimientos, en este caso las instalaciones de la Empresa Eléctrica Ambato Regional Centro Norte S.A y sus sucursales. Con esta modalidad se dará contacto en forma directa con la realidad, para tener información de acuerdo con los objetivos del proyecto.

3.1.3. Investigación Experimental

Para la solución del problema propuesto se utilizarán herramientas de software específicas como: SolarWind, GNS3 (Graphical Network Simulator) y Packet Tracer, permitiendo realizar simulaciones de la red, así como el monitoreo de la red MAN de EEASA, el cual ayudara en las pruebas necesarias, para la factibilidad de aplicar calidad de servicio (QoS) en la red de enlace de fibra óptica e inalámbrica.

3.2 Recolección de la información

La recolección de información se realizó a través de visitas al departamento de planificación e información, y se aplicó la entrevista al ingeniero encargado del funcionamiento y administración de la red de EEASA, además se efectuó la observación participativa el cual implica la visita al trayecto del enlace, con estos datos se realizó el análisis de la información para determinar la factibilidad de la propuesta, el cual permitió conocer varios parámetros relacionados al tema.

3.3 Procesamiento y Análisis de la Información

Una vez que se ha obtenido la información necesaria de la investigación, la misma será parte de un proceso estadístico como es la tabulación de datos en forma sistemática y ordenada, para facilitar su análisis y encontrar solución al problema.

3.4 Desarrollo del proyecto

- Análisis y recopilación de información de la topología física y lógica implementada en la red MAN de EEASA y sus sucursales.
- Monitoreo de la red de datos para establecer los niveles de congestión y retardos mediante software.
- Organización de datos obtenidos para el respectivo análisis del tráfico circulante en la red MAN de EEASA para determinar su factibilidad.
- Análisis de dispositivos comunicación y aplicaciones implementados en la red MAN de EEASA para el respectivo trato de prioridad.

- Análisis de los tipos de modelos de servicios aplicables para brindar QoS en la red MAN de EEASA.
- Determinar los parámetros de clasificación, marcado de tráfico, manejo y evasión de congestión a implementar en los equipos de comunicación de EEASA.
- Elaboración del prototipo basado en simuladores de redes para el diseño e implementación de calidad de servicio (QoS).
- Análisis de resultados para determinar la mejora de servicios en la red MAN de EEASA y sus sucursales.

CAPÍTULO IV

DESARROLLO DE LA PROPUESTA

4.1 Análisis de la topología física y lógica implementada en la red MAN de EEASA.

Se realiza el estudio de la infraestructura física y lógica de la red MAN de EEASA y sus respectivas sucursales, con la finalidad de verificar la compatibilidad de equipos para que soporten parámetros de calidad de servicio (QoS), de acuerdo a los recursos que presenta la red en su inventario.

4.1.1 Topología Física de la Red

Gracias a la información facilitada por el departamento de planificación e información se puede conocer que la topología de la red MAN de EEASA es de tipo punto a punto, que mediante la conexión de switches puede extender su alcance y cobertura. Actualmente la red cuenta con 8 nodos de comunicación pertenecientes a la red de área metropolitana, interconectados mediante fibra óptica, cable Ethernet y enlaces inalámbricos para el transporte de información.

En la figura 4.1 se muestra la ubicación física de los nodos de la red MAN, cada uno de los cuales tiene un sistema de red de fibra óptica que está conformada con un router o switch de capa 3 y un switch de distribución. Los enlaces de la red MAN están conformados por fibra óptica monomodo utilizada para largas distancias, y que en contrato con TRANSELECTRIC, permite el tendido de dos pares fibra óptica a través

de torres para la interconexión sus agencias, llegando así al usuario final con cable UTP categoría 5 y 6.

Esta topología de red distingue niveles de acceso, distribución y Core como esquema principal para la red MAN, donde el router de Core está ubicada en el edificio principal de EEASA como eje inicial de la red y posterior mente se manejan switches de distribución y acceso por cada área operativa de la red MAN de EEASA.

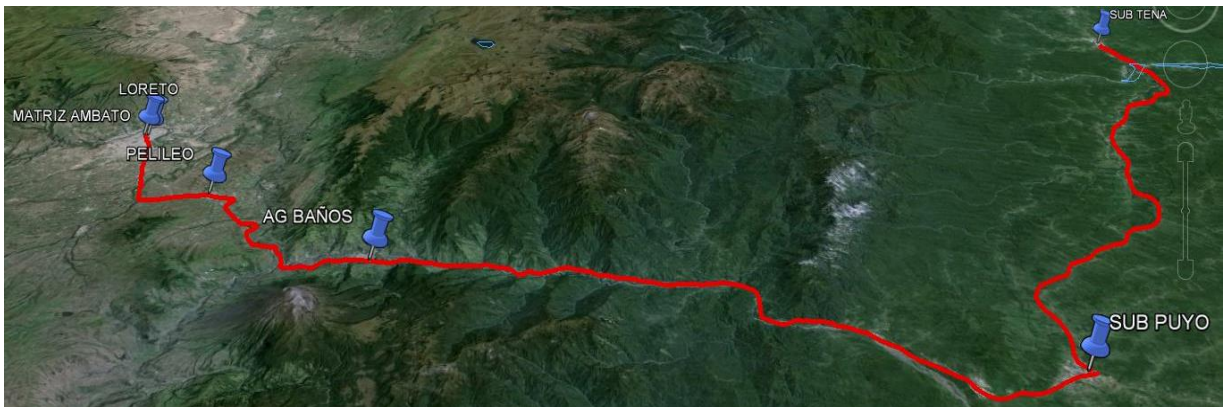


Figura 4.1: Topología Física de la Red MAN Fibra Óptica.

Elaborado por: Investigador.

En la figura 4.2, se puede apreciar la topología física del que está compuesta el enlace inalámbrico de EEASA, cada uno de estos nodos están conectados a un router y este a su vez a los switches de distribución para la respectiva transferencia de información. El sistema inalámbrico tiene una topología punto a punto y cuenta con la implementación del estándar IEEE 802.11b en cada enlace.

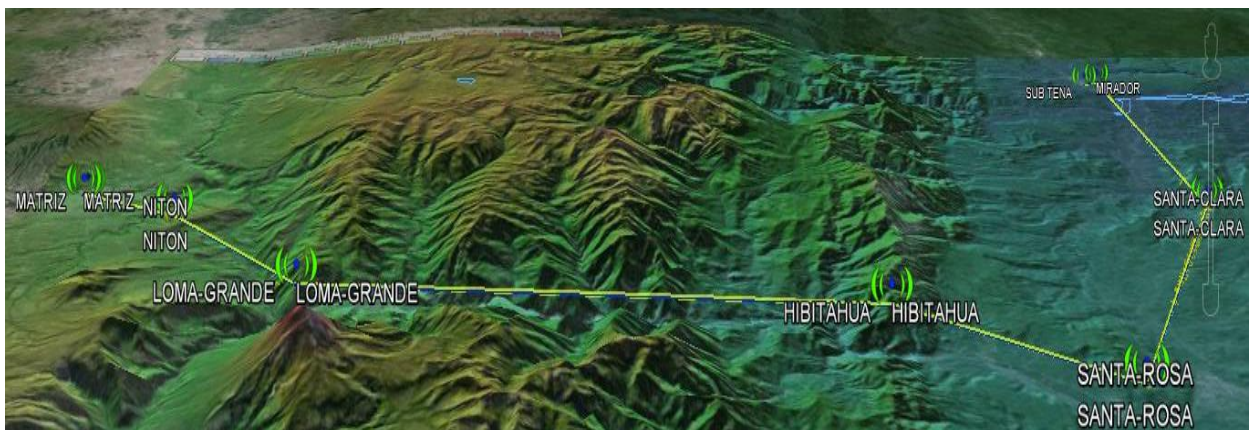


Figura 4.2: Topología Física de la Red MAN Enlace Inalámbrico.

Elaborado por: Investigador.

4.1.2 Análisis de la Topología Lógica

La red MAN de EEASA cuenta con un anillo de fibra óptica, el cual está interconectado entre cada sub estación, del cual se desprende 8 nodos que forman enlaces punto a punto entre cada terminal de la red.

El sistema de red de fibra óptica, está conectado a través de switches con tecnología Gigabit Ethernet 1000Base-LX, que puede alcanzar una longitud del enlace de hasta 30 km sobre fibra monomodo en 1Gbps, utilizado para largas distancias.

La distribución lógica de la red de área metropolitana, del enlace de comunicaciones de fibra óptica de la Empresa Eléctrica Ambato, se detalla en la figura 4.3.

En la figura 4.4 se puede observar la distribución lógica de la Red MAN, que está compuesto por enlaces inalámbricos, que cuentan con 7 nodos principales que ayudan a la interconexión entre sus agencias utilizando la topología punto a punto, este sistema inalámbrico está conformado por switches Cisco Catalyst 2960s Stack, routers Cisco 2901K9, Cisco 3845, Cisco 2821 y equipos para radio enlace como Mikrotik, Ubiquiti, Orinoco y Proxim que en su mayoría presenta características muy importantes mencionadas a continuación.

- ❖ Soporta comunicaciones inalámbricas, que permiten instalar una red con necesidades de comunicaciones avanzadas.
- ❖ Permite la aplicación de parámetros de calidad de servicio (QoS) para proporcionar un tratamiento prioritario a las aplicaciones críticas de negocio, además en modelos como Ubiquiti permite dar prioridad QoS inteligente para voz / video streaming sin problemas.
- ❖ Cuentan con interfaces de FastEthernet con transferencia de datos de 100 megabits por segundo y Gigabit Ethernet con transferencia de datos de 1000 megabits por segundo, en función del precio y sus necesidades de rendimiento.
- ❖ Tienen la capacidad de configurar LAN virtuales de forma que los empleados estén conectados a través de funciones de organización, equipos de proyecto o aplicaciones en lugar de criterios físicos o geográficos [23] [8] [24].

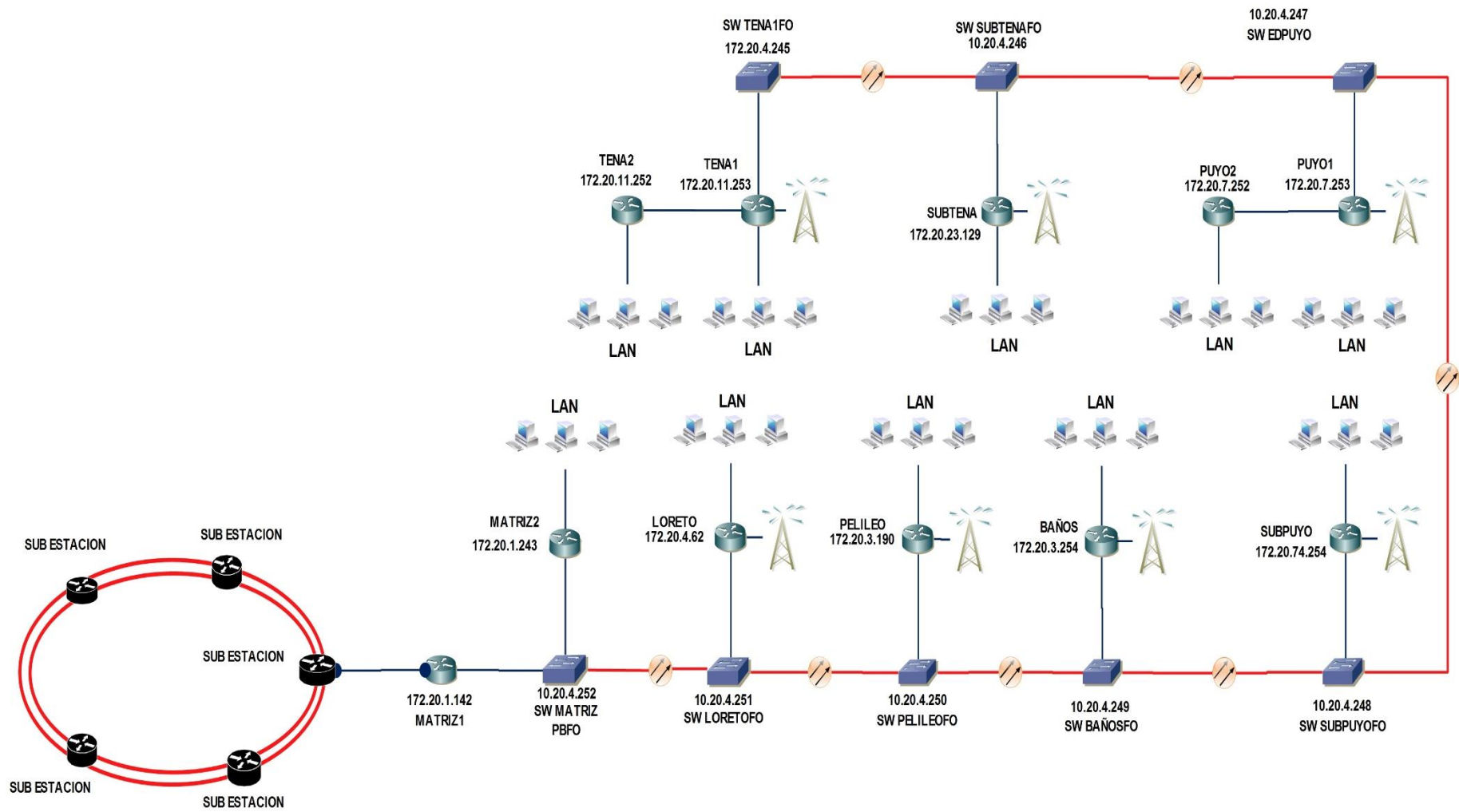


Figura 4.3: Topología Lógica de la Red MAN Fibra Óptica.

Elaborado por: Investigador.

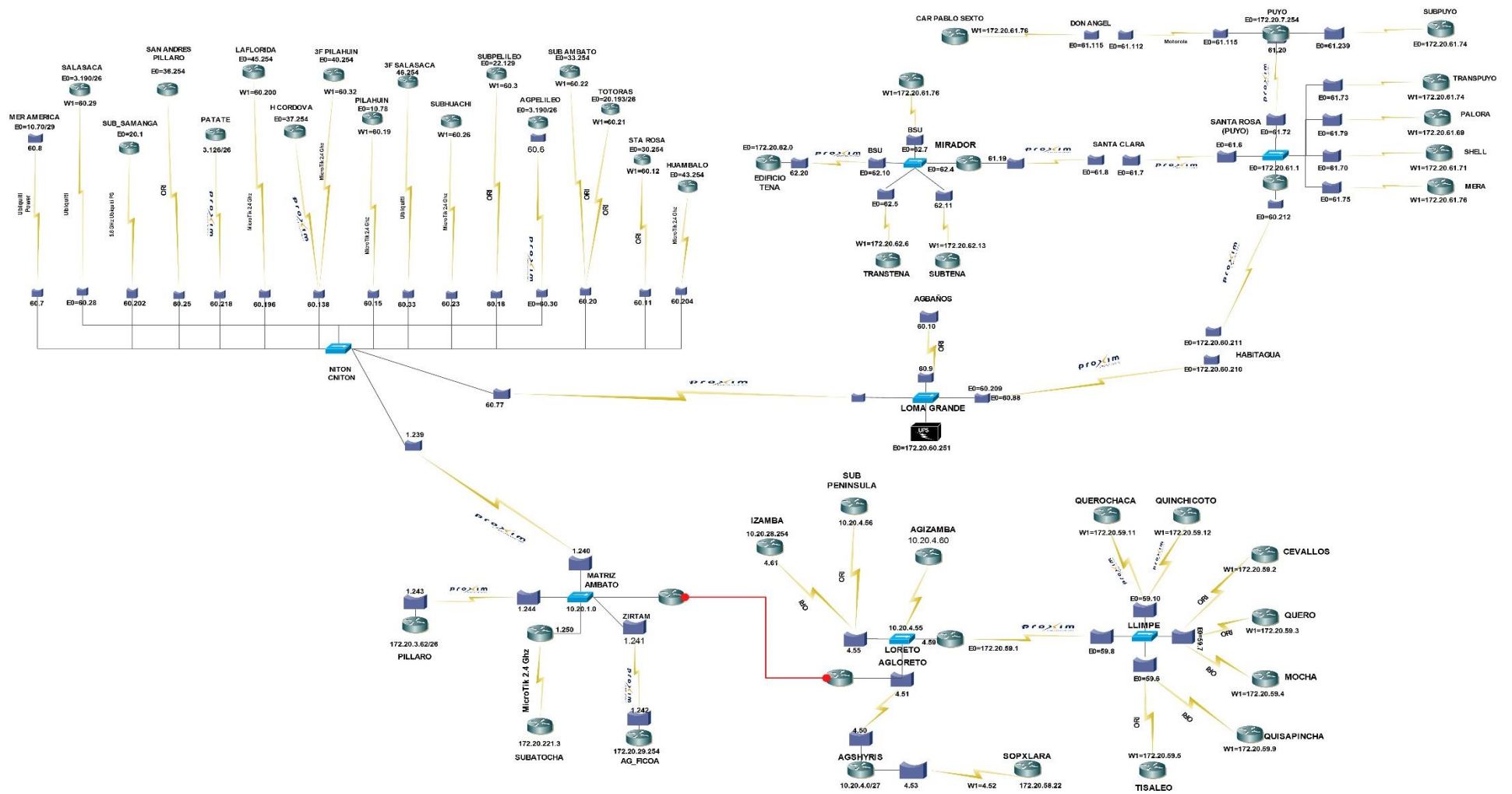


Figura 4.4: Topología Lógica de la red MAN enlace Inalámbrica.

Elaborado por: Investigador.

4.1.3 Equipos de la red MAN de EEASA

Basado en el inventario realizado en la red de EEASA, los equipos que componen esta red son switches Cisco con diferentes modelos o series, la red MAN posee 4 series de switches: Cisco Catalyst 29xxStack, Cisco Catalyst 2960S-24TS-S, Cisco WS-C2960-24PC-L y Cisco Catalyst 2960-24TC-S. También la red cuenta con routers cisco con diferentes modelos, la red posee 5 routers: Cisco 2821, Cisco 2921K9, Cisco 2901K9, Cisco 2911K9 y Cisco 3845, adicionalmente los equipos utilizados para los enlaces inalámbricos son: MICROTIK, UBIQUITI, PROXIM y ORINOCO.

Analizando el diagrama lógico de la red de EEASA, tanto el enlace de fibra óptica como el inalámbrico, se pudo verificar los equipos que componen actualmente en la red MAN de EEASA, así pues se detallan los equipos utilizados en las tablas 4.1, 4.2, y 4.3.

Serie de Routers utilizados en la red MAN de EEASA

Tabla 4.1: Routers Utilizados en la red MAN de EEASA

| MODELO ROUTER | # ROUTERS |
|---------------|-----------|
| Cisco 2821 | 4 |
| Cisco 2921K9 | 5 |
| Cisco 2901K9 | 12 |
| Cisco 2911K9 | 1 |
| Cisco 3845 | 2 |
| TOTAL | 24 |

Elaborado por: Investigador

Serie de Switches utilizados en la red MAN de EEASA

Tabla 4.2: Switches utilizados en la red MAN de EEASA

| MODELO SWITCH | # SWITCH |
|-----------------------------|-----------|
| Cisco Catalyst 2960S-24TS-S | 3 |
| Cisco Catalyst 29xxStack | 11 |
| Cisco WS-C2960-24PC-L | 1 |
| Cisco Catalyst 2960-24TC-S | 1 |
| TOTAL | 16 |

Elaborado por: Investigador

Series de routers utilizados en los enlaces inalámbricos de la red MAN de EEASA

Tabla 4.3: Routers utilizados para los enlaces inalámbricos.

| MODELO EQUIPO | # Equipos |
|--------------------------|-----------|
| MICROTIK 411 | 11 |
| UBIQUITI AIGIRD M2 | 2 |
| UBIQUITI AIGIRD M5 | 2 |
| UBIQUITI POWER STATION | 2 |
| UBIQUITI NANO BRIDGE M2 | 4 |
| UBIQUITI NANO BRIDGE M5 | 1 |
| UBIQUITI NANO STATION M2 | 4 |
| UBIQUITI NANO STATION M5 | 7 |
| UBIQUITI ROQUET M5 | 2 |
| PROXIM 2454R | 5 |
| PROXIM 5054R | 4 |
| PROXIM 5012SUR | 7 |
| PROXIM QB8100 | 2 |
| MOTOROLA | 1 |
| ORINOCO | 15 |
| TOTAL | 69 |

Elaborado por: Investigador

4.1.4 Modelos y versiones del sistema operativo de interconexión (IOS) de los routers y switches de la red MAN de EEASA

La red cuenta con 8 switches principales Cisco Catalyst 2960S Stack con IOS C2960S-UNIVERSALK9-M, Versión 15.0 (2) SE5 y 1 switch Cisco Catalyst 2960S-24TS-S con IOS C2960S-UNIVERSALK9-M, Versión 15.0 (2) SE4 para interconexión de la red de fibra óptica e inalámbrica.

Versiones de IOS disponibles en switches y routers de EEASA

Las versiones del Cisco IOS están compuestas de números y letras que denotan diferentes características según como se agrupan. Cada versión optimiza las redes IP y otorga funciones más avanzadas de enrutamiento, Calidad de Servicio (QoS) y seguridad. Las imágenes de software Cisco tiene una nomenclatura específica para distinguir entre las diferentes versiones de productos, a continuación se detalla uno de estas versiones del IOS según la referencia [8].

C2960S-UNIVERSALK9-M, Versión 15.0 (2) SE5

UNIVERSAL: Significa el tipo de software que contiene el IOS de Cisco

K9: Significa que esta versión soporta una seguridad encriptada.

15.0 (2): Significa la versión del IOS junto al número de lanzamiento o desarrollo

SE: Significa el identificador de la serie para la que fue producida, en este caso es para proveedores de servicios (S) y ambientes empresariales (E).

5: Significa la revisión del lanzamiento, en este caso la revisión 5.

Switches de la red MAN de EEASA.

A continuación en la tabla 4.4 se presenta los switches con su determinada imagen de software, así como la ubicación y las direcciones lógicas de cada uno de los switches según los diagramas de la red MAN.

Tabla 4.4: IOS y Versión de switches de la red MAN

| SWITCHES RED MAN | | | |
|-------------------------|-----------------------------|--------------------------------|--|
| LUGAR | EQUIPOS | DIRECCION IP DE ADMINISTRACION | IOS Y Versión |
| MATRIZ | Cisco Catalyst 29xxStack | 10.20.4.252 | C2960S-UNIVERSALK9-M, Versión 15.0(2)SE5 |
| LORETO | Cisco Catalyst 29xxStack | 10.20.4.251 | C2960S-UNIVERSALK9-M, Versión 15.0(2)SE5 |
| PELILEO | Cisco Catalyst 29xxStack | 10.20.4.250 | C2960S-UNIVERSALK9-M, Versión 15.0(2)SE5 |
| BAÑOS | Cisco Catalyst 29xxStack | 10.20.4.249 | C2960S-UNIVERSALK9-M, Versión 15.0(2)SE5 |
| SUBESTACION PUYO | Cisco Catalyst 29xxStack | 10.20.4.248 | C2960S-UNIVERSALK9-M, Versión 15.0(2)SE5 |
| EDIFICIO PUYO | Cisco Catalyst 29xxStack | 10.20.4.247 | C2960S-UNIVERSALK9-M, Versión 15.0(2)SE5 |
| SUBESTACION TENA | Cisco Catalyst 29xxStack | 10.20.4.246 | C2960S-UNIVERSALK9-M, Versión 15.0(2)SE5 |
| EDIFICIO TENA | Cisco Catalyst 2960S-24TS-S | 10.20.4.245 | C2960S-UNIVERSALK9-M, Versión 15.0(2)SE4 |

Elaborado por: Investigador

Routers de la red MAN de EEASA.

La red cuenta con 11 routers principales conectados a los switches de fibra óptica y a los enlaces del sistema inalámbrico, la red cuenta con 4 routers Cisco 2901K9 con IOS C2900-UNIVERSALK9-M, Versión 15.1(4)M6, 4 routers Cisco 2821 con IOS C2800NM-ADVENTERPRISEK9-M, Versión 15.1(4)M6, 2 routers Cisco 3845 con IOS C3845-ADVENTERPRISEK9-M, Versión 15.1(4)M6 y 1 router Cisco 2921K9 con IOS C2900-UNIVERSALK9-M, Versión 15.1(4)M6 y cuentan con las direcciones IP mostradas en la tabla 4.5.

Tabla 4.5: IOS y Versión de routers de la red MAN

| ROUTERS RED MAN | | | |
|-------------------------|----------------|---------------------------------------|---|
| LUGAR | EQUIPOS | DIRECCION IP DE ADMINISTRACION | IOS Y Versión |
| MATRIZ 1 | Cisco 3845 | 172.20.1.242 | C3845-ADVENTERPRISEK9-M, Version 15.1(4)M6 |
| MATRIZ 2 | Cisco 3845 | 172.20.1.243 | C3845-ADVENTERPRISEK9-M, Version 15.1(4)M6 |
| LORETO | Cisco 2921K9 | 172.20.4.62 | C2900-UNIVERSALK9-M, Versión 15.1(4)M6 |
| PELILEO | Cisco 2901K9 | 172.20.3.190 | C2900-UNIVERSALK9-M, Versión 15.1(4)M6 |
| BAÑOS | Cisco 2901K9 | 172.20.3.254 | C2900-UNIVERSALK9-M, Versión 15.1(4)M6 |
| SUBESTACION PUYO | Cisco 2901K9 | 172.20.74.254 | C2900-UNIVERSALK9-M, Versión 15.1(4)M6 |
| PUYO 1 | Cisco 2821 | 172.20.7.253 | C2800NM-ADVENTERPRISEK9-M, Version 15.1(4)M6 |
| PUYO 2 | Cisco 2821 | 172.20.7.252 | C2800NM-ADVENTERPRISEK9-M, Version 15.1(4)M6 |
| SUBESTACION TENA | Cisco 2901K9 | 172.20.23.129 | C2900-UNIVERSALK9-M, Versión 15.1(4)M6 |
| TENA 1 | Cisco 2821 | 172.20.11.253 | C2800NM-ADVENTERPRISEK9-M, Version 15.1(4)M6 |
| TENA 2 | Cisco 2821 | 172.20.11.252 | C2800NM-ADVENTERPRISEK9-M, Version 15.1(4)M6 |

Elaborado por: Investigador

4.1.5 Análisis de equipos de la red MAN de EEASA que soportan QoS

Con los equipos existentes actualmente en la red MAN de EEASA los cuales son de la serie Cisco Catalyst 29xxStack, Cisco Catalyst 2960S-24TS-S, Cisco WS-C2960-2 4PC-L y Cisco Catalyst 2960-24TC-S, a continuación se detalla las diferentes imágenes de Cisco para estos equipos y sus características en cuanto a QoS.

Switch Cisco Series Catalyst 2960 Stack

Los switches Cisco Catalyst 2960S son una familia de dispositivos que proporcionan rápida conectividad tanto para Ethernet como para Giga Ethernet, lo que permite mejorar los servicios de la red MAN y el nivel de operación de la institución (EEASA) con sus dependencias. A continuación se menciona las características que tiene este equipo.

- ❖ Presenta flexibilidad para Ethernet y GigaEthernet permitiendo el uso de cable de cobre o de fibra, cada enlace tiene un puerto 10/100/1000/ Ethernet y con la opción de conectar un transceiver (SFP).
- ❖ Permite el control de redes y optimización de ancho de banda con QoS, ACL's, y servicios de multidifusión es decir aplicación de VTP.
- ❖ También permite la configuración de la red de seguridad a través de una amplia gama de métodos de autenticación, el cifrado de tecnologías de datos y control de administración de red basada en los usuario, puertos y direcciones MAC.[23]
- ❖ El switch Catalyst 2960 ofrece seguridad integrada, incluyendo la admisión de control de la red (NAC), calidad de servicio (QoS), y la entrega de servicios inteligentes de extremo a extremo de la red [23].

Calidad de servicio (QoS) que ofrece el Switch Cisco Catalyst 2960-S Stack

Ofrece características de calidad de servicio de múltiples capas, es decir que utiliza información tanto de capa 3 como de capa 4 para ayudar a asegurar que el tráfico de la red está siendo clasificado y se está tomando en cuenta sus prioridades para evitar la congestión. La configuración de calidad de servicio se simplifica a través de Auto QoS, que es una característica que detecta y configura automáticamente QoS en el Switch, para la adecuada clasificación y gestión de colas generando la optimización de tráfico, priorización y disponibilidad de la red sin una configuración compleja [23].

Imágenes del software de Cisco Catalyst 2960-S

La serie de Catalyst 2960 según el modelo de switch puede traer dos tipos de Imagen de Cisco las cuales son:

- ❖ Catalyst 2960 LAN Lite Series: Soporta QoS estándar
- ❖ Catalyst 2960 LAN Base Series: Soporta QoS avanzado

En la figura 4.5 se visualiza la diferencia entre estos dos tipos de imagen de Cisco, en la que se detalla las características de QoS.

| | Cisco® Catalyst® 2960 LAN Lite | Cisco Catalyst 2960 LAN Base |
|----------------------------------|--------------------------------|------------------------------|
| Port CoS Trust and Override | Yes | Yes |
| Trusted Boundary | No | Yes |
| ACL Classification | No | Yes |
| Ingress Policing (1MB incr.) | No | Yes |
| Auto QoS | No | Yes |
| 802.1p queues | 4 | 4 |
| Scheduling | SRR | SRR |
| Priority Queuing | Yes | Yes |
| Configure CoS Priority Queues | Yes | Yes |
| Configure Queue Weights | No | Yes |
| Configure Buffers and Thresholds | No | Yes |
| Class & Policy Maps | No | Yes |
| Modify CoS and DSCP Mapping | No | Yes |
| DSCP Transparency | Yes | Yes |
| Weighted Tail Drop | Yes | Yes |

Figura 4.5: Diferencias QoS de imágenes software Catalyst 2960 [23]

Como se puede visualizar en la figura 4.5 la comparación nos permite saber qué tipo de QoS se puede implementar en los switches de la Serie Catalyst 2960 [23].

Router Cisco Serie 2901/K9

Los routers de la serie cisco 2900 de servicios integrados incluyen los routers Cisco ISR 2901, 2911, 2921 y 2951. Todos los routers Cisco 2900 Series ofrecen aceleración de cifrado integrada en hardware, ranuras para procesamiento digital de señales (DSP) con capacidades de voz y video, firewall opcional, prevención de intrusiones, procesamiento de llamadas, correo de voz y servicios de aplicaciones. Las plataformas también admiten la más amplia variedad de opciones de conectividad cableada e inalámbrica dentro del sector, entre ellas T1/E1, T3/E3, xDSL y GE en cobre y fibra óptica [23].

Calidad de servicio (QoS) que ofrece Router Cisco serie 2901/K9

La serie de los Router Cisco 2901/K9 permite la administración del tráfico con QoS, basado en CBWFQ (mecanismo de cola de espera equitativo y ponderado basado en clases), WRED (detección temprana aleatoria y ponderada), QoS jerárquica, PBR (routing basado en políticas), PFR (routing de alto rendimiento) y NBAR (routing avanzado con base en la red) [8].

Imagen del software IOS Cisco Serie 2901/K9

Los routers Cisco ISR 2900 Series ofrecen versiones 15 M y T del software Cisco IOS. En la versión 15.0 (1) M está disponible de inmediato y es compatible con una amplia cartera de tecnologías de Cisco, que incluye las funcionalidades y características de las versiones 12.4 y 12.4T. Las innovaciones que ofrece la versión 15.0(1)M abarcan diversas áreas tecnológicas, tales como seguridad, voz, alta disponibilidad, routing y multidifusión IP, calidad de servicio (QoS), movilidad IP, switching por etiquetas multiprotocolo (MPLS), redes VPN y administración integrada. En la tabla 4.6 se puede detallar las características generales de este router

Tabla 4.6: Datasheet Cisco 2901

| Cisco 2901 Router Details | |
|-----------------------------------|---|
| Product Description | Cisco 2901 Integrated Services Router - router |
| Manufacturer | Cisco Systems, Inc |
| Manufacturer Part Number | CISCO2901/K9 |
| Product Type | Router |
| Form Factor | External - modular - 1U |
| Dimensions (WxDxH) | 43.9 cm x 43.8 cm x 4.5 cm |
| Weight | 6.1 kg |
| DRAM Memory | 512 MB (installed) / 2 GB (max) |
| Flash Memory | 256 MB (installed) / 8 GB (max) |
| Routing Protocol | OSPF, IS-IS, BGP, EIGRP, DVMRP, PIM-SM, IGMPv3, GRE, PIM-SSM, static IPv4 routing, static IPv6 routing |
| Data Link Protocol | Ethernet, Fast Ethernet, Gigabit Ethernet |
| Remote Management Protocol | SNMP, RMON |
| Features | Cisco IOS IP Base , MPLS support, Syslog support, IPv6 support, Class-Based Weighted Fair Queuing (CBWFQ), Weighted Random Early Detection (WRED) |
| Compliant Standards | IEEE 802.1Q, IEEE 802.3af, IEEE 802.3ah, IEEE 802.1ah, IEEE 802.1ag |
| Power | AC 120/230 V (50/60 Hz) |

Fuente: CISCO Integrated Services Routers 2900 Series [23].

Las características técnicas de todos los equipos de la red MAN se encuentran en el Anexo 6.

Como se puede observar en las tablas 4.4 y 4.5 en la red MAN de EEASA los equipos cuentan con diferentes tipos de IOS Cisco instalados permitiendo que las características de QoS varíen, pese a esta diferencia todos los equipos que ahora están funcionando en la red MAN, tanto en el enlace de fibra óptico como el inalámbrico soportan QoS, ya sea estándar o avanzado.

Calidad de Servicio que ofrece Router Mikrotik 411

La tecnología Mikrotik, al igual que Cisco, posee calidad de servicio con modelos de priorización de tráfico: modelo IntServ y modelo DiffServ.

RouterOS pueden implementar QoS (802.11Q) aplicando mecanismos de control que usa Mikrotik citados a continuación:

- ❖ Limitar la tasa de datos en direcciones IP determinadas, subredes, protocolos, puertos y otros parámetros como cabeceras ToS.
- ❖ Limitar el tráfico peer-to-peer
- ❖ Dar prioridad a algunos flujos de paquetes sobre los demás.
- ❖ Utilizar encolamiento por ráfagas para la navegación web más rápida.
- ❖ Aplicar las colas en los intervalos de tiempo fijos.

En la figura se puede apreciar el diagrama de flujo de paquetes que es la base para que el Routerboard de Mikrotik provea QoS en la red.

Este diagrama hace uso de marcado y modelamiento conocidas como mangle y HTB (Hierarchical Token Bucket, Árbol de Colas) [24].

La técnica mangle permite el marcado especial del paquete IP, mientras que la técnica HTB tiene funciones de manejo de colas a través de varios algoritmos de encolamiento [25].

QoS Packet Flow

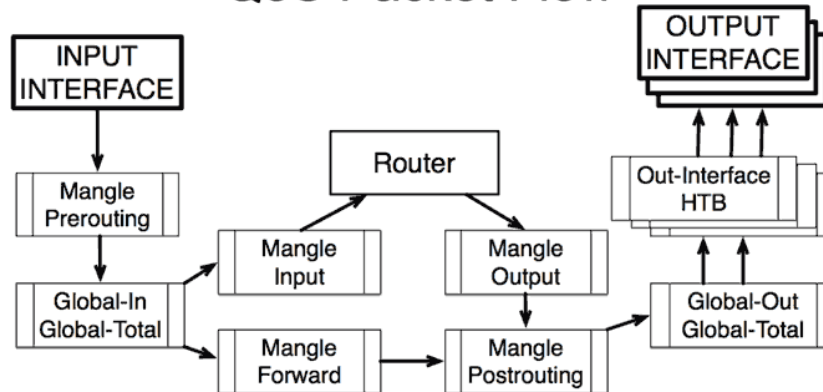


Figura 4.6: Diagrama de Flujo de Paquetes [25].

Algoritmos de encolamiento.

Tipos de colas

- ❖ RED (Random Early Detection).
- ❖ BFIFO (Byte limited First-In, First-Out queue).
- ❖ PFIFO (Packet limited First-In, First-Out Queue).
- ❖ PCQ (Packet Classification and Queuing)

Colas simples

- ❖ Por origen/destino de red.
- ❖ Dirección IP de cliente.
- ❖ Por interface

Árboles de colas

- ❖ Por protocolo
- ❖ Por puerto
- ❖ Por tipo de conexión.

Control de Ancho de Banda

RouterOS para el control de ancho de banda y QoS, utiliza HTB (Hierarchical Token Bucket), este sistema se basa en un algoritmo el cual controla la cantidad de datos que es inyectado dentro de una red, permitiendo una ráfaga de datos en un tiempo determinado, además de crear una estructura jerárquica que determina relaciones de colas de datos entre padres e hijos, para una mejor distribución y priorización de los datos [24] [25].

Calidad de Servicio (QoS) en Proxim Modelo 5054-R y 2454-R

Para el modelo 5054/2454 –R la calidad de servicio (QoS) se basa en el estándar 802.16 que mediante el software incorporado en el equipo permite crear, editar y eliminar las clases de servicio especificados para la siguiente jerarquía de los parámetros: [26][27]

- ❖ Regla de paquetes de identificación (PIR): Es una combinación de parámetros que especifica qué tipo de tráfico es permitido o denegado
- ❖ Clase de flujo de servicio (SFC): Es un conjunto de parámetros que determina cómo un flujo de datos de una aplicación será manejada
- ❖ Prioridad para cada regla dentro de cada clase SF de 0 a 255, donde 0 es la prioridad más baja
- ❖ Clase de QoS: Es un conjunto de parámetros que incluye los PIR y SFCs que se han configurado previamente.

Parámetros de QoS en Proxim

Varias clases de calidad de servicio predefinidas, SFC y PIRs disponibles que se puede elegir para que cubra la mayoría de los tipos de tráfico [26]. Al realizar la configuración se inicia la construcción de la jerarquía de una clase QoS las cuales son:

- ❖ Definir PIR (Definir Dirección PIR MAC, direcciones IP y entradas de puerto TCP / UDP)
- ❖ Definir PIRs y especificar reglas de clarificación de paquetes, asociado Dirección MAC Dirección / IP / TCP-UDP entradas de puerto si es necesario
- ❖ A continuación se asocia algunas de esas PIRs a clases específicas de flujo de servicio (SFC);
- ❖ Asignar prioridades a cada PIR dentro de cada SFC.
- ❖ Se define la clase de QoS mediante la asociación de SFC correspondientes a cada clase de QoS [26] [27].

En el Anexo 4 se visualiza la configuración de calidad de servicio (QoS) en equipos Proxim pertenecientes a los modelos QB8100 y 5054/2454 –R.

4.2 Herramienta de Monitoreo de la red MAN

Consiste en el monitoreo de tráfico mediante herramientas como, Solarwinds, y Wiresharke, cuya finalidad es obtener histogramas sobre el comportamiento de la red MAN de EEASA. Esto es necesario en la administración de toda la red ya que brinda la información necesaria que ayuda a detectar los problemas en la red de EEASA. A continuación se detalla cada una de las herramientas de monitoreo que permitirá detectar el tráfico circulante en la red MAN de EEASA tanto en el enlace de fibra óptica el inalámbrica.

4.2.1 SolarWinds Orion NPM

SolarWinds Orion NPM (Network Performance Monitor) es un sistema de gestión que permite administrar ancho de banda y fallos en la red en tiempo real directamente desde el navegador. Esta herramienta monitoriza y recoge datos de routers, switches, servidores, y cualquier dispositivo de red con capacidad SNMP. SolarWind Orion NPM es altamente escalable capaz de monitorizar desde 10 hasta más de 10.000 nodos.

La herramienta de Solarwinds Orion, permite al administrador ver el tráfico y comportamiento de la red. Aprovechando el protocolo NetFlow de Cisco para extraer datos de equipos CISCO. Y así saber que usuarios y que aplicaciones están consumiendo el mayor ancho de banda. Además Solarwinds Orion cuenta con un módulo adicional para monitoreo a las redes inalámbricas [28].

SolarWinds NPM es generador de informes, el motor de generación avanzada de informes de SolarWinds NPM permite generar rápidamente informes personalizados de red que pueden exportarse a PDF, imprimirse o visualizarse en Internet. Al incluir numerosos informes incorporados, SolarWinds NPM facilita la generación de informes sobre datos de rendimiento en períodos específicos de tiempo o por segmento de red [28].

En la figura 4.7 se puede observar el monitoreo de procesos con SolarWinds Orion NPM, en el que se puede observar todos los nodos que se monitorea, además se puede observar un esquema de los enlaces que actualmente existen en la red MAN de EEASA.

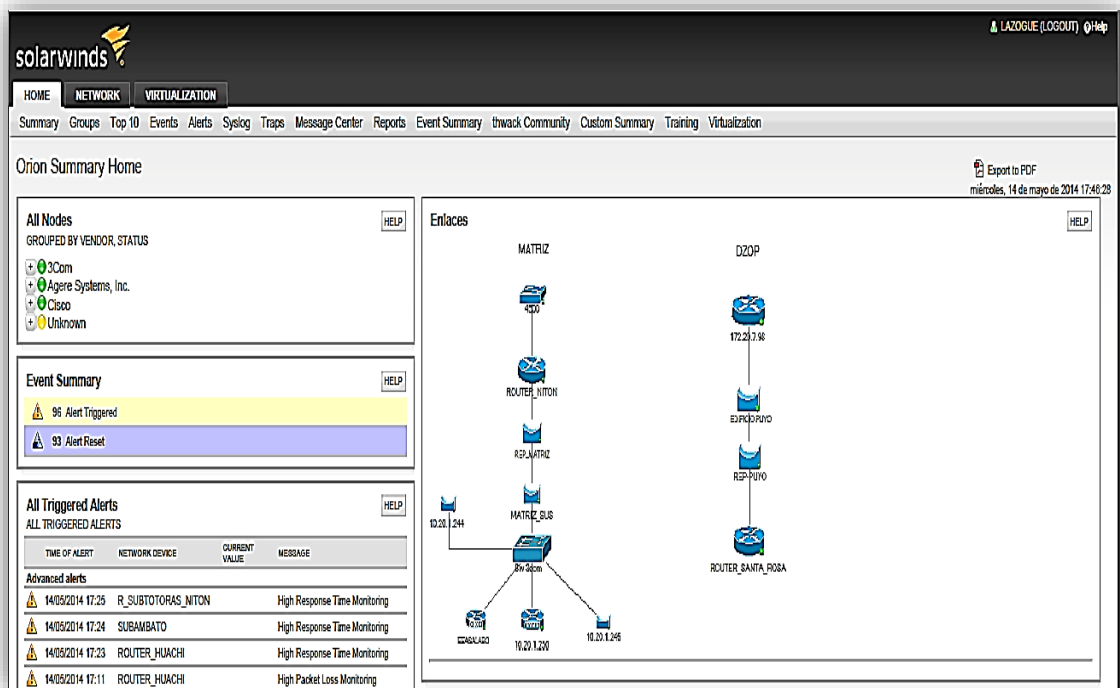


Figura 4.7: Interfaz de SolarWinds para el monitoreo de la red MAN

Elaborado por: Investigador

Para el monitoreo en la red de EEASA, se han instalado 2 tipos de software muy eficientes para cumplir con los objetivos antes mencionados estos son SolarWinds y PRTG Network Monitor, para el estudio se centra en el uso del Solarwind porque este muestra en forma más didáctica el uso del ancho de banda [7] [8].

4.3 Análisis de la red MAN de EEASA

Al realizar el monitoreo de tráfico, se obtuvo parámetros de cómo se generaba el tráfico en la red cada cierto periodo de tiempo, además se determinó las configuraciones que presentan cada uno de los equipos al transmitir la información, así como las características de cada uno de ellos. El análisis se lo realizó tanto para el enlace de fibra óptica como para el enlace inalámbrico. Se realizó un continuo análisis del ancho de banda, así como del tráfico circulante en la red para poder determinar los siguientes parámetros.

- ❖ Tiempos de respuesta.
- ❖ Desempeño de los dispositivos de red.
- ❖ Tipo de tráfico y puertos utilizados
- ❖ Ancho de Banda utilizando en cada uno de los enlaces de la red MAN

Para la medición de estos parámetros se ha utilizado la herramienta SolarWinds, que permite mediante gráficos verificar el tiempo de respuesta, total de bytes transmitidos y el consumo de ancho de banda en cada uno de los puertos, pertenecientes a los routers y switches ubicados en cada uno de los nodos antes mencionados. Todas las lecturas del tráfico circulante están tomadas en los puertos Gigabit Ethernet de cada switch, que conforman la red de distribución tanto para el enlace de fibra como para el inalámbrico.

Mientras se realiza el monitoreo con esta herramienta también se captura tráfico en los picos obtenidos con las herramientas Wireshark para clasificar el tipo de tráfico que circula en la red. Se tomaron muestras durante un mes, las cuales nos permiten ver el comportamiento del consumo de ancho de banda; debido a la gran cantidad de información obtenida durante el proceso se procedió a la tabulación de datos para su respectivo análisis, para después tomar muestras y proceder a comparálas por días, para determinar los picos de utilización; una vez obtenidos los picos se procede a clasificar el tráfico capturado con SolarWinds para determinar el porcentaje de utilización por IP, por puerto, por protocolo, etc.

Todo este proceso ayudara en el diseño e implementación de QoS. A continuación se visualizara el proceso realizado con muestras tomadas aleatoriamente de tres semanas como se muestra en las siguientes figuras, el resto de información se presenta en el Anexo 1.

4.3.1 Tipo de Tráfico que circula en los enlaces de la Red MAN

En la figura 4.8 se muestra el tipo de tráfico que circula en la red MAN, este grafico se obtiene utilizando la herramienta de monitoreo wireshark.

Se puedo determinar qué porcentaje de paquetes pertenece a un determinado tipo de tráfico, así se tiene que el tráfico TCP tiene un mayor tráfico, el cual es el mayor de todos e indica que la mayoría de servicios que se usa son aplicaciones basadas en TCP/IP, también se tiene aplicaciones con UDP, dcerpc, arp, etc. Como se sabe, una aplicación puede usar varios protocolos al momento de transmitir paquetes de información.

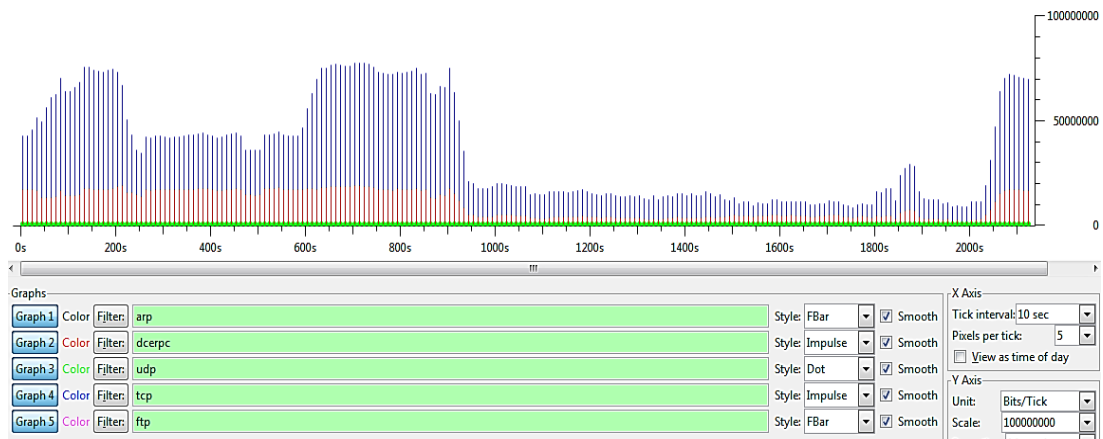


Figura 4.8: Análisis de Tráfico generado en la red MAN

Elaborado por: Investigador

4.3.2 Tiempo de Respuesta en los enlaces de la red MAN de EEASA

Se presentan los resultados obtenidos durante la transferencia de información y monitoreo en todos los nodos que comunican al sistema de fibra óptica y enlaces inalámbricos. También con la utilización del ping y de las estadísticas del SolarWinds se puede verificar los tiempos de respuesta y el porcentaje de paquetes perdidos

Esto nos permite conocer que tan eficiente es el traspaso de información en cada nodo conformado por routers con series Cisco 2901K9, Cisco 2821, Cisco 3845 y Cisco 2921K9; switches series Cisco Catalyst 2960S Stack, Cisco Catalyst 2960S-24TS-S; y equipos de radio enlace como: Ubiquiti Nano Bridge M2/M5, Proxim 2054/5054r, Orinoco 8100 y Mikrotik-411 que interconectan la red MAN de EEASA, además se verifica si existe algún tipo de degradación en las comunicaciones debido a que no se maneja QoS, y se analiza si la red da el mismo trato a todo el tráfico.

El análisis de los tiempos de respuesta permitió verificar los niveles máximos de transferencia del canal, esto permitió indicar si se producen pérdidas en paquetes por tiempos de respuesta muy altos, además se pudo verificar las variaciones de los tiempos de respuesta presentes en la red, con el cual ayudo a determinar qué tan eficiente resulta la implementación de QoS sin la necesidad de aumentar la capacidad del canal.

La especificación de la ITU G.114 recomienda menos de 150 ms de retraso máximo entre los nodos extremos (bordes de la red), para tráfico en tiempo real.

Tabla 4.7: Tiempos de respuesta presentes en los switches principales de la red MAN de EEASA

| NODOS | PAQUETES | | | | | TIEMPO DE IDA Y VUELTA | | |
|------------------|--------------------------------|---------|-----------|---------|------------|------------------------|--------|-------|
| | DIRECCION IP DE ADMINISTRACION | ENIADOS | RECIBIDOS | PÉRDIDA | % PÉRDIDAS | MAXIMO | MINIMO | MEDIA |
| SWITCH MATRIZ FO | 10.20.4.252 | 720 | 718 | 2 | 0,5 | 27 | 1 | 0,93 |
| SWITCH LORETO | 10.20.4.251 | 360 | 360 | 0 | 0 | 19 | 1 | 2,2 |
| SWITCH PELILEO | 10.20.4.250 | 361 | 358 | 2 | 0,5 | 14 | 1 | 1,14 |
| SWITCH BAÑOS | 10.20.4.249 | 360 | 360 | 0 | 0 | 15 | 1 | 1,64 |
| SWITCH SUB PUYO | 10.20.4.248 | 360 | 357 | 3 | 1 | 13 | 2 | 2,39 |
| SWITCH ED PUYO | 10.20.4.247 | 121 | 121 | 0 | 0 | 4 | 2 | 2,42 |
| SWITCH SUB TENA | 10.20.4.246 | 360 | 358 | 0 | 0,5 | 16 | 2 | 2,59 |
| SWITCH TENA | 10.20.4.245 | 360 | 360 | 0 | 0 | 13 | 2 | 2,55 |

Tabla 4.8: Tiempos de respuesta presentes en los routers principales de la red MAN de EEASA

| NODOS | PAQUETES | | | | | TIEMPO DE IDA Y VUELTA | | |
|-----------------|--------------------------------|---------|-----------|---------|------------|------------------------|--------|-------|
| | DIRECCION IP DE ADMINISTRACION | ENIADOS | RECIBIDOS | PÉRDIDA | % PÉRDIDAS | MAXIMO | MINIMO | MEDIA |
| ROUTER MATRIZ1 | 172.20.1.242 | 362 | 362 | 0 | 0 | 4 | 0 | 0,07 |
| ROUTER MATRIZ2 | 172.20.1.243 | 360 | 360 | 0 | 0 | 3 | 0 | 0,06 |
| ROUTER LORETO | 172.20.4.62 | 360 | 360 | 0 | 0 | 5 | 0 | 0,11 |
| ROUTER PELILEO | 172.20.3.190 | 362 | 362 | 0 | 0 | 3 | 1 | 0,18 |
| ROUTER BAÑOS | 172.20.3.254 | 360 | 360 | 0 | 0 | 4 | 1 | 0,99 |
| ROUTER SUB PUYO | 172.20.74.254 | 365 | 365 | 0 | 0 | 3 | 1 | 1,1 |
| ROUTER PUYO 1 | 172.20.7.253 | 372 | 372 | 0 | 0 | 4 | 2 | 2,01 |
| ROUTER PUYO 2 | 172.20.7.252 | 300 | 300 | 0 | 0 | 3 | 2 | 2 |
| ROUTER SUB TENA | 172.20.23.129 | 372 | 372 | 0 | 0 | 3 | 2 | 2,03 |
| ROUTER TENA 1 | 172.20.11.253 | 120 | 120 | 0 | 0 | 4 | 2 | 2,06 |
| ROUTER TENA 2 | 172.20.11.252 | 169 | 169 | 0 | 0 | 4 | 2 | 2,59 |

Elaborado por: Investigador

Tabla 4.9: Tiempos de respuesta entre los enlaces inalámbricos de la red MAN de EEASA.

| NODOS | PAQUETES | | | | | TIEMPO DE IDA Y VUELTA | | |
|------------------------|--------------------------------|---------|-----------|---------|------------|------------------------|--------|-------|
| | DIRECCION IP DE ADMINISTRACION | ENIADOS | RECIBIDOS | PÉRDIDA | % PÉRDIDAS | MAXIMO | MINIMO | MEDIA |
| MATRIZ-NITON | 10.20.1.240 | 420 | 417 | 3 | 1 | 29 | 7 | 11,2 |
| NITON - LOMA GRANDE | 172.20.60.1 | 420 | 418 | 0 | 0,5 | 85 | 14 | 20,8 |
| NITON - AGPELILEO | 172.20.60.6 | 432 | 432 | 0 | 0 | 98 | 21 | 26,34 |
| NITON – SAN ANDRES | 172.20.60.25 | 420 | 417 | 3 | 1 | 14 | 4 | 7,29 |
| NITON – SUB HUACHI | 172.20.60.23 | 420 | 420 | 0 | 0 | 11 | 4 | 7,83 |
| NITON – SUB AMBATO | 172.20.60.22 | 420 | 412 | 8 | 2 | 171 | 41 | 96,39 |
| LOMA GRANDE-HABITAHUA | 172.20.60.209 | 360 | 357 | 2 | 1 | 109 | 11 | 23,67 |
| LOMA GRANDE-BAÑOS | 172.20.60.10 | 420 | 420 | 0 | 0 | 152 | 15 | 29,63 |
| HABITAHUA-SANTA ROSA | 172.20.60.212 | 360 | 349 | 11 | 3,5 | 177 | 20 | 45,75 |
| SANTA ROSA-SANTA CLARA | 172.20.61.7 | 361 | 333 | 28 | 8 | 181 | 34 | 66,08 |
| SANTA CLARA-MIRADOR | 172.20.61.19 | 720 | 664 | 56 | 8 | 237 | 33 | 51,46 |
| MIRADOR-EDIFICIO TENA | 172.20.13.30 | 720 | 720 | 0 | 0 | 111 | 16 | 23,8 |
| RADIOENLACE NITON | 10.20.1.254 | 721 | 719 | 2 | 1 | 14 | 3 | 6,84 |
| RADIOENLACE MIRADOR | 172.20.62.4 | 360 | 273 | 87 | 24 | 29 | 8 | 9,28 |
| RADIOENLACE SANTA ROSA | 172.20.61.1 | 361 | 355 | 6 | 2 | 160 | 11 | 38,44 |
| R_EDIFICIO PRINCIPAL | 10.20.1.247 | 361 | 361 | 0 | 0 | 16 | 5 | 8,7 |

Elaborado por: Investigador

En las tablas 4.7, 4.8, 4.9 se puede observar los tiempos de respuesta generados en cada nodo de la red MAN compuesta por routers, switches y equipos para enlace inalámbrico, los datos fueron tomados gracias al software de monitoreo SolarWinds que está constantemente verificando el estado de la red.

Nodo Switch Matriz

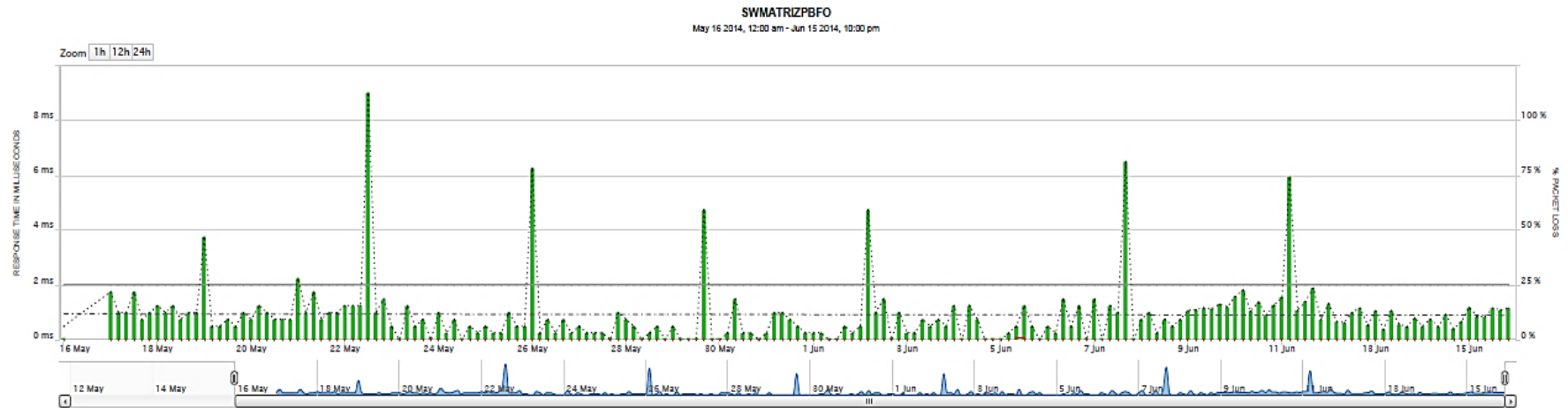


Figura 4.9: Tráfico capturado por SolarWinds MATRIZ
Elaborado por: Investigador

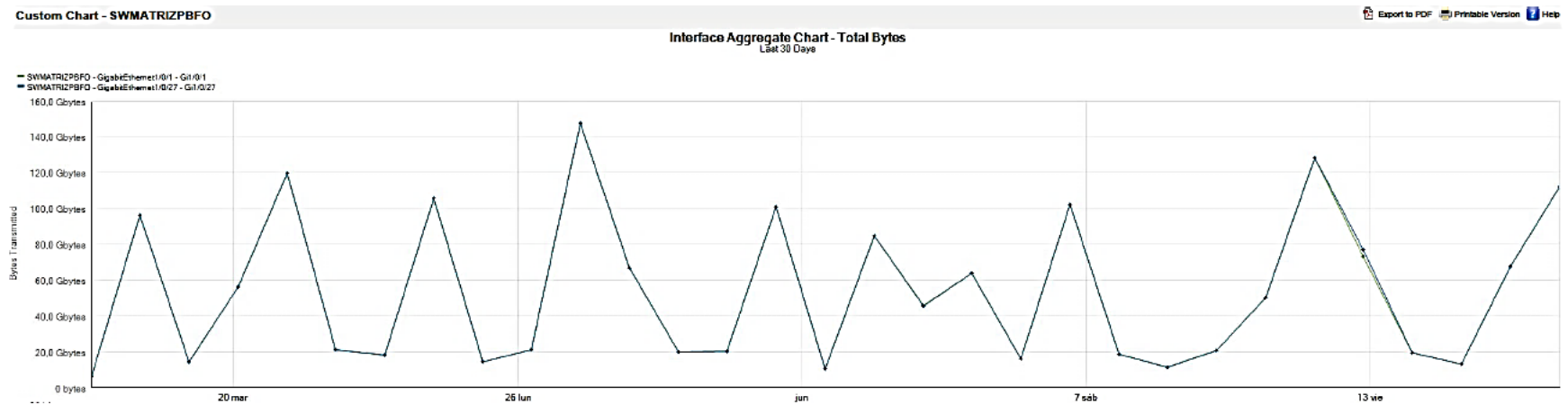


Figura 4.10: Bytes transmitidos en Int. Giga Ethernet 0/27.
Elaborado por: Investigador

A continuación se presenta los resultados obtenidos durante la transferencia de información en el nodo principal (MATRIZ1), en el cual se determina que durante el periodo establecido para el monitoreo este no presenta pérdida de paquetes una prueba de congestión del canal en la cual se procedió al envío de paquetes ICMP.

En la figura 4.10 se detalla los Bytes transmitidos durante el monitoreo, en el cual se puede apreciar que el promedio de transferencia de información está entre los 80 Gbytes por día, esto indica que el nodo de la matriz no presenta conflictos al momento de la transferencia de información.

En esta prueba se pudo determinar que los niveles picos máximos de respuesta llegan a los 9ms en la transferencia de información como se puede observar en la figura 4.9, se puede determinar que al realizar el monitoreo este no presenta saturaciones y variaciones de los tiempos de respuesta que sean críticas, este proceso ayuda a determinar qué tan eficiente resulta la implementación de calidad de servicio en el enlace de fibra óptica.

Nodo Switch Loreto

De la misma manera se presenta el monitoreo del switch de Loreto perteneciente al enlace de fibra óptica, según el gráfico 4.11 se determina que este equipo presenta pérdida de paquetes en un promedio de 0,2 %, el cual es bajo, así también se determinó un tiempo de respuesta promedio de 2,2ms al transmitir información, se realiza pruebas de congestión del canal en la cual se procedió al envío de paquetes ICMP.

Además se verifica en el gráfico 4.12 que el switch Loreto presenta un promedio en la transmisión de información que está entre los 75 Gbytes por día.

Al realizar la tabulación de los datos obtenidos en el monitoreo del switch de Loreto, se pudo determinar que el tráfico generado en el equipo no presenta conflictos al momento de transmitir información, además se determinó que el ancho de banda consumido no sobrepasa los picos críticos que generen congestión en los dispositivos conectados al switch.

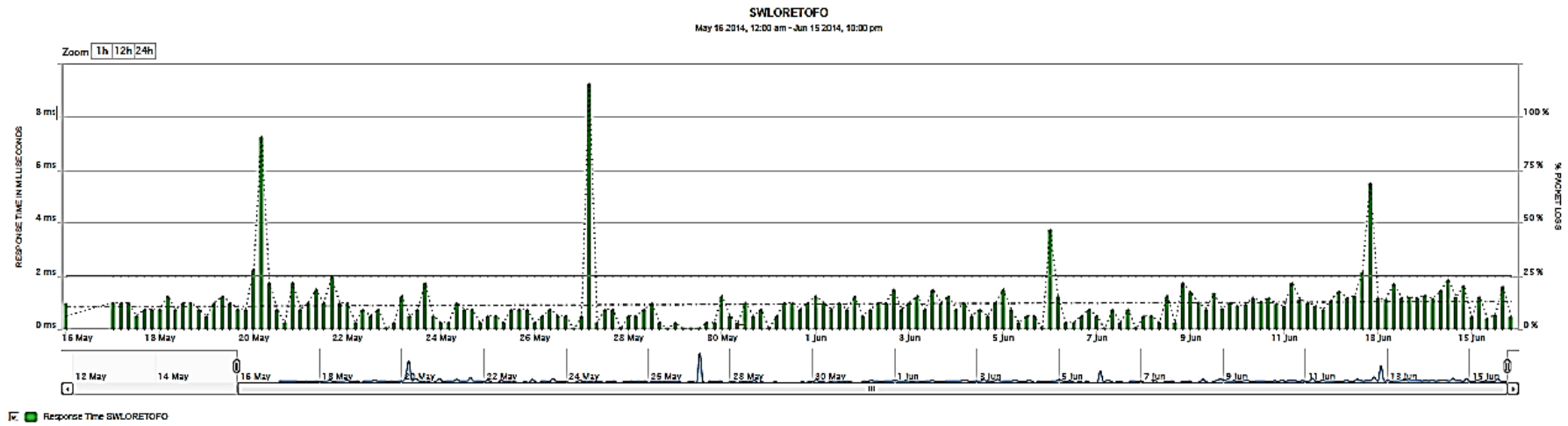


Figura 4.11: Tráfico capturado por SolarWinds LORETO
Fuente: Elaborado por el investigador

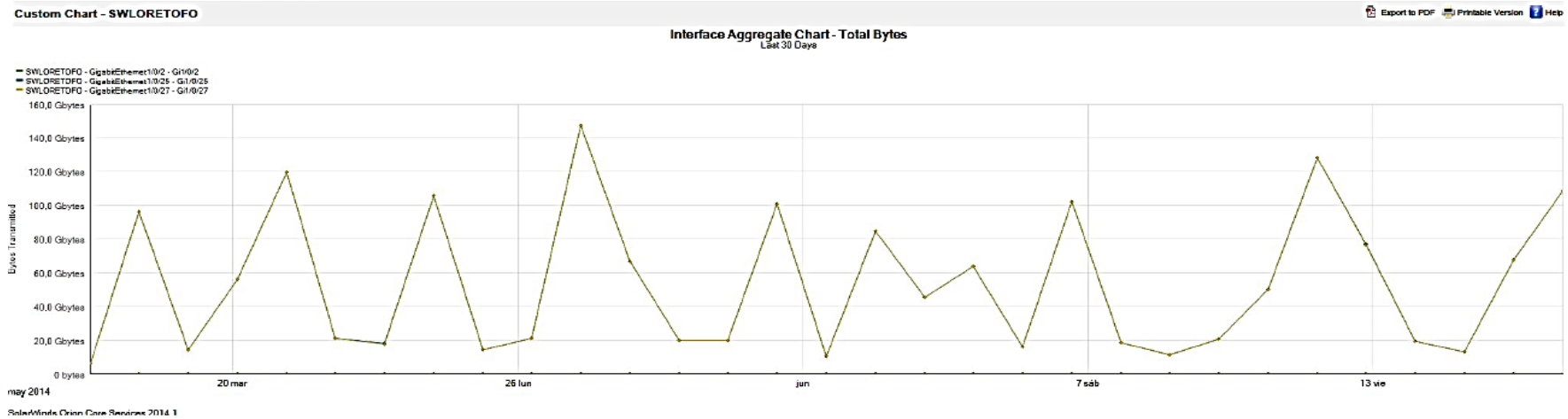


Figura 4.12 Bytes transmitidos en Interfaz Giga Ethernet 0/27, /25 Loreto
Fuente: Elaborado por el investigador

A continuación se presenta el tiempo de respuesta generado en el router Nitón, el cual permite la interconexión hacia los enlaces inalámbricos de la red MAN de EEASA.

Monitoreo de Router Nitón

En la figura 4.14 se puede apreciar el tiempo de respuesta generado al transmitir datos en el router de nitón hacia sus distintas agencias, se realizó la tabulación de los datos obtenidos en el monitoreo del equipo y se determinó que el tiempo de respuesta promedio es de 6,84ms.

También se analizó y tabulo los datos de la grafico 4.13 de manera que se obtuvo un trazo percentil el cual es de 95%, esto permite el seguimiento de ancho de banda en la utilización máxima de cantidad de bytes transmitidos por el router, a cada uno de los enlaces inalámbrico establecidos en la configuración del nodo de Nitón.

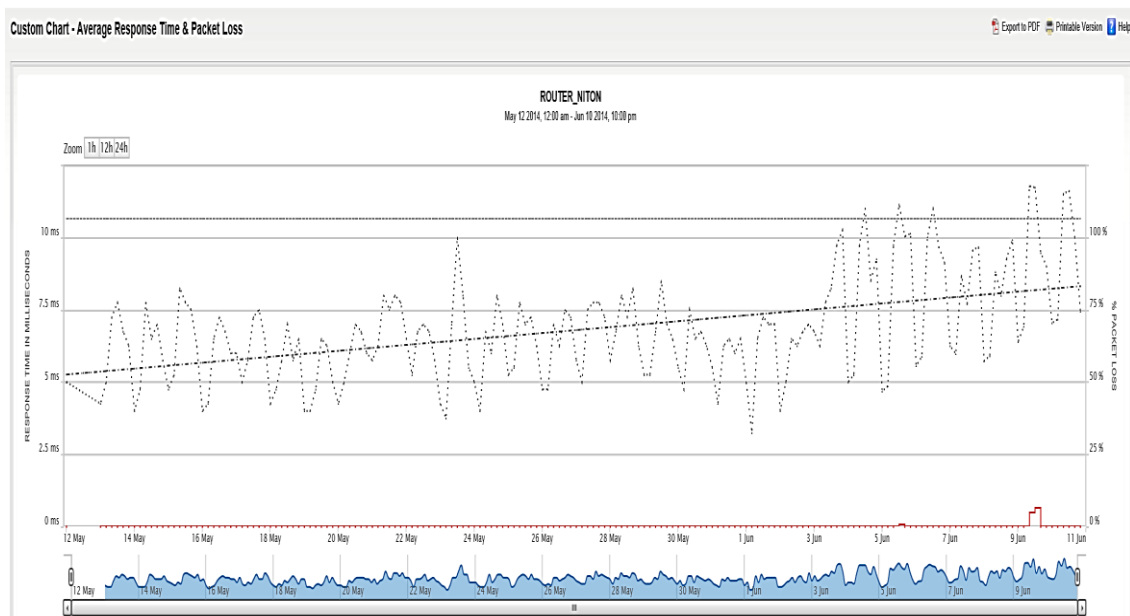


Figura 4.13: Tráfico capturado por SolarWinds Router NITON

Fuente: Elaborado por el investigador

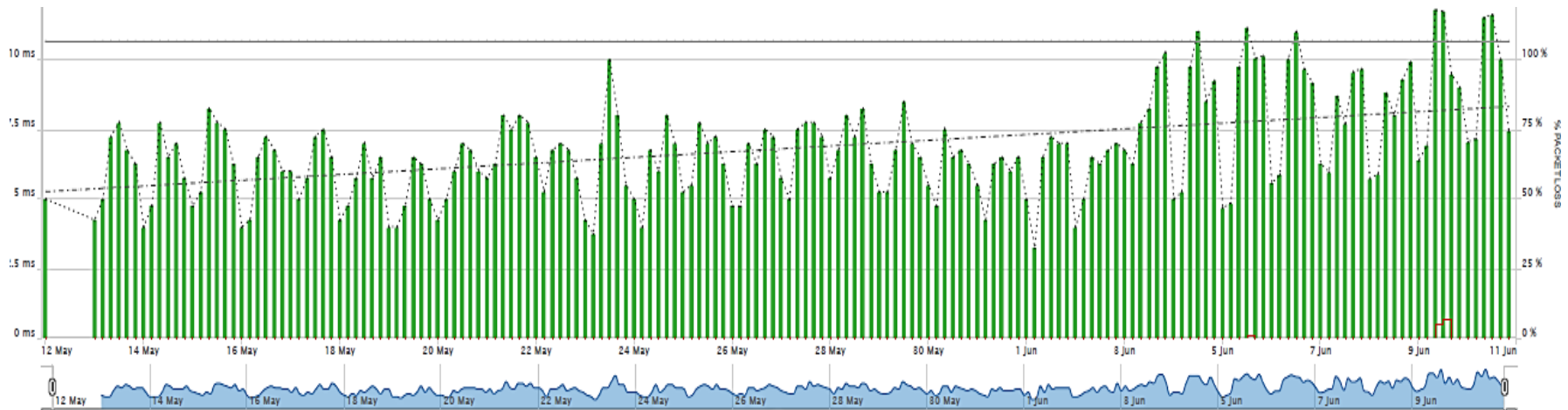


Figura 4.14: Monitoreo de Router Nitón
Elaborado por: Investigador

Custom Chart - ROUTER_NITON

Export to PDF Printable Version Help

Interface Aggregate Chart - Total Bytes
 Last 30 Days

- ROUTER_NITON - FastEthernet0/0 - Fa00/0
- ROUTER_NITON - FastEthernet0/1 - Fa00/1
- ROUTER_NITON - GigabitEthernet0 TO_AP
- ROUTER_NITON - GigabitEthernet1 TO_SWITCH

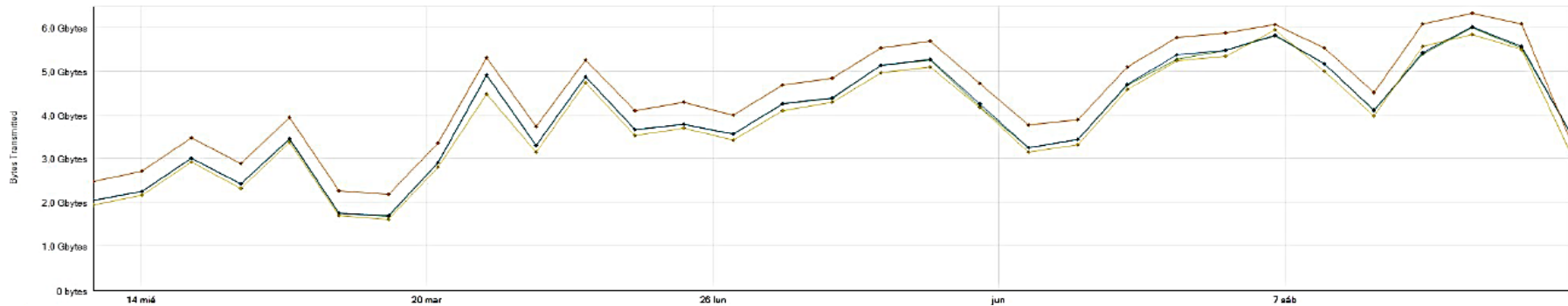


Figura 4.15: Bytes transmitidos en Router Nitón
Elaborado por: Investigador

En la figura 4.15 se detalla los Bytes transmitidos durante el monitoreo, al realizar el análisis y tabulación de los datos se obtuvo un promedio de transferencia de información está entre los 5 Gbytes por día, presentando una pérdida de paquetes de un promedio de 2,13%, esto indica que el nodo niton presenta pequeños conflictos al momento de la transferencia de información pero que no son críticos.

El resto de información de los nodos pertenecientes a la red de MAN del enlace de fibra óptica como el enlace inalámbrico se presenta en el Anexo 1.

4.3.3 Diagnóstico de los Dispositivos de red en los enlaces de EEASA

Después del análisis de las características de todos los dispositivos de comunicación con los que cuenta la red de EEASA se determinó que se cuenta con la tecnología necesaria para la implementación de calidad de servicio QoS, el cual facilitara la convergencia de aplicaciones, como videoconferencia, streaming de video y telefonía IP, logrando una optimización en la transferencia de información tanto en el enlace de fibra óptica como el inalámbrico.

EEASA cuenta con gran cantidad de aplicaciones que se transportan a través del enlace de fibra óptica e inalámbrica, por tal motivo el presente estudio determinara la factibilidad, de que con la implementación de parámetros de calidad de servicio (QoS) en los equipos de enlace de fibra óptica e inalámbrica, estos sean más eficientes y ofrecerán mayores garantías al tráfico más relevante de la institución.

Cabe indicar que la implementación de Calidad de Servicio (QoS) se realiza a través de simulación por software con características de equipos de comunicación similares que forman la red MAN de EEASA, y que para ello se tomara en cuenta todos los datos recogidos a lo largo del desarrollo de este capítulo

4.3.4 Análisis de requerimientos en la red MAN de EEASA

El análisis de requerimientos y prioridad de aplicaciones, se lo realizo en base a la importancia de los servicios y aplicaciones que son utilizadas en la red MAN de EEASA. En el presente estudio se realizó la identificación de aplicaciones de prioridad crítica, alta y baja presentes en la red.

Las aplicaciones de prioridad crítica son aquellas que posibilitan el funcionamiento de la empresa, en estas aplicaciones se encuentran los servicios de voz sobre IP y video conferencia, el objetivo es mantener siempre comunicado a las distintas sucursales con la matriz, debido a que la institución tiene como función principal la prestación y manejo de facturación de consumo de energía eléctrica como una de las aplicación principal y además de las dependencias que tienen EEASA dentro y fuera de la ciudad, se ve la necesidad tener una determinada prioridad con este tipo de tráfico ya que operan en tiempo real y por su importancia en la red de EEASA es fundamental.

Las aplicaciones de prioridad alta son aquellas que están presentes diariamente en el funcionamiento de la red de EEASA, pero no necesitan de gran ancho de banda como las base de datos y aplicaciones con las que trabajan los servidores pero que sigue siendo sensibles al tiempo y tiene impacto directo al rendimiento de la red.

Aplicaciones de prioridad media permite que todos los recursos de la red se identifiquen entre si y estén accesibles al usuario según su nivel de servicio que requieran como DNS, DHCP o de directorio activo [7] [8].

El análisis se basa en que si estas aplicaciones no operan correctamente los usuarios no reciben los parámetros de red adecuados y no podrán acceder a los recursos de red que dispone la Empresa Eléctrica Ambato S.A, el análisis se basa en que el tiempo que debe tomar esta asignación de recursos no debe ser muy alta, el máximo es de 4 segundos, porque el usuario requiere acceder a los recursos compartidos de manera inmediata.

Aplicaciones de prioridad baja son utilices para EEASA pero estas aplicaciones tienen mayor resistencia al retardo y que en caso de falla no afectan al correcto funcionamiento de la misma.

Se procede a especificar el trato que se le da a cada tipo de tráfico a través del monitoreo a dichas aplicaciones con el fin de determinar que puertos usan, y así poder manejar adecuadamente una clasificación de tráfico más específica. En la figura se puede apreciar los requisitos con las que opera cada aplicación, así como el retardo admisible para cada uno de estas aplicaciones.

| Tipo de servicio | Ejemplo de aplicación | Velocidad binaria requerida | Retraso admisible (s) | Entorno de uso |
|----------------------|----------------------------------|-----------------------------|---------------------------------|--|
| Voz | Conversación (telefonía) | 8 - 32 kB/s | Tiempo real | Todos |
| Voz / sonido | Grabación (correo de voz, etc.) | 8-32 kB/s | (1 s) | Todos |
| Datos | Archivos informáticos | 1,6 MB/archivo | < 10 < 120 | Interiores, Microceldas Todos |
| Texto | Teletexto | 40 kB/página | < 2 s/página | Todos |
| Foto fija | Imagen alta calidad (color) | 5 MB/página | < 10 s/página < 180 s/página | Interiores, Microceldas Todos |
| Imagen en movimiento | Fax (G4) | 500 kB/página | < 10 s/página | Todos |
| | Videoteléfono | 64 kB/s | Tiempo real | Interiores, Microceldas y algunas Macrocelas |
| Portadores RDSI | Videokonferencia de alta calidad | < 384 kB/s | Tiempo real | Interiores |
| | 2B + D 1B + D | 144 kB/s 80 kB/s | Tiempo real deseable | Interiores, Microceldas Todos |

Figura 4.16: Requerimientos de Aplicaciones [8]

4.4 Proceso de servicios aplicables para brindar QoS en la red MAN de EEASA

Para la implementación de calidad de servicio (QoS) en la red MAN de EEASA se procede a trabajar sobre el parámetro de ancho de banda, para esto se procede a realizar la elección del modelo de QoS.

4.4.1 Elección del Modelo de QoS a implementarse en la red MAN de EEASA

Como se mencionó en el capítulo 2 se tiene dos modelos que permiten obtener calidad de servicio (QoS) en una red, esta son los Servicios Integrados (IntServ) y Servicios Diferenciados (DiffServ), cada una con su modo de operación y soporte de tecnología IP. En la arquitectura de QoS no todas las técnicas son apropiadas para todos los routers o switches de la red, hay que seleccionar las características apropiadas de QoS en cada sitio. Para encontrar el modelo adecuado para la implementación de QoS en la red de EEASA se realizó una comparación entre estos modelos que permiten trabajar con QoS [8] [29]. La elección para aplicar cualquiera de estos dos métodos dependerá de requerimientos como el ancho de banda, retardo, jitter y demás variables a la que está sometida la red [7]. Por tales razones se concluye que el mejor modelo a aplicarse en la red MAN de EEASSA es el DiffServ ya que ofrece varias ventajas sobre IntServ, como su escalabilidad, flexibilidad, distinción de diferentes clases de servicios mediante el marcado de paquetes, entre otras. De esta manera se tomó la decisión de escoger el modelo DiffServ para el desarrollo de la implementación de QoS en la red.

4.4.2 Método de Clasificación y Marcado de tráfico para la red MAN de EEASA.

La clasificación y marcado es el proceso de identificar el tráfico generado para luego manipularlos y añadirles QoS, utilizando procedimientos de clasificación y asignación de priorización, conforme atraviesa cada nivel de red. Al dar una preferencia a un tipo de tráfico, primero hay que identificarlo, para después marcar o no el paquete [7]. Para realizar la identificación de los flujos hay que aplicar métodos comunes como las listas de control de acceso (ACL) y DiffServ Code Point (DSCP)

ACLs (Listas de control de acceso)

Se usan para aplicar una política de seguridad que permite o niega el acceso de cierta parte de la red a otra, además los ACL permite realizar el filtrado de paquetes en función de diversas opciones como son; dirección origen, dirección destino, tipo de paquete, cualquier combinación de los elementos anteriores [7].

Ventajas

- ❖ Proporciona control de flujo del tráfico que debe pasar por el router
- ❖ Proporciona un nivel de seguridad básico de acceso a la red en función de distintos parámetros.
- ❖ El administrador decide qué tipo de tráfico se envía o se bloquea en los interfaces del router
- ❖ Se categorizan como cortafuegos de filtrado de paquetes en capa 3 y 4.

Desventajas

- ❖ Al aplicar ACLs se debe realizar un análisis de tráfico que hay una condición implícita que deniega o permite todo lo que no se haya configurado en las ACL

DSCP (DiffServ Code Point)

El marcado de tráfico será mediante DSCP debido a que en el análisis y elección del modelo de QoS se eligió trabajar con servicios diferenciados (DiffServ) y por ende está especificado por este modelo de servicio.

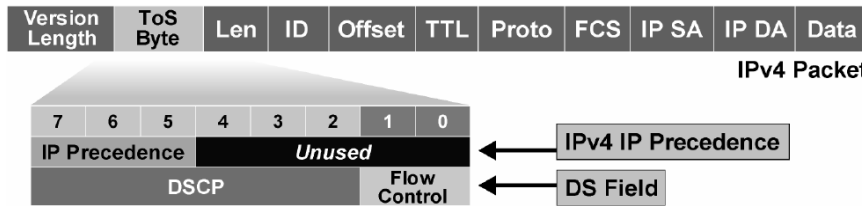


Figura 4.17: Tipo de Servicio (ToS) y DSCP [23].

Una vez que existe la capacidad de marcar los paquetes utilizando DSCP, es necesario proveer del tratamiento apropiado para cada una de estas clases. Para realizar el marcado de los paquetes se puede utilizar varias técnicas, pero la más extendida y estandarizada es utilizar DSCP con la asignación de valores como se muestran en las tablas 4.9 y 4.10, donde el marcado se puede extender a IPv6, MPLS, etc. [7] [29]

Tabla 4.10: Clase DSCP

| Rango (decimal) | Valor (binario) | Significado | Equivalente precedencia |
|-----------------|-----------------|----------------------------|-------------------------|
| 56-63 | 111xxx | Control de la red | 7 |
| 48-55 | 110xxx | Control de la red | 6 |
| 40-47 | 101xxx | Expedited Forwarding | 5 |
| 32-39 | 100xxx | Assured Forwarding clase 4 | 4 |
| 24-31 | 011xxx | Assured Forwarding clase 3 | 3 |
| 16-23 | 010xxx | Assured Forwarding clase 2 | 2 |
| 8-15 | 001xxx | Assured Forwarding clase 1 | 1 |
| 0-7 | 000xxx | Best effort (default) | 0 |

Fuente: Implementación de QoS en red de transporte de datos del MDMQ [7]

Tabla 4.11: Valores del campo DSCP

| Dec. | Binario | Significado |
|------|---------|----------------------------------|
| 62 | 111110 | Reserv. |
| 60 | 111100 | Reserv. |
| 58 | 111010 | Reserv. |
| 56 | 111000 | Preced. 7 (routing y control) |
| 54 | 110110 | Reserv. |
| 52 | 110100 | Reserv. |
| 50 | 110010 | Reserv. |
| 48 | 110000 | Preced. 6 (routing y control) |
| 46 | 101110 | EF (Premium) |
| 44 | 101100 | Config. Usuario |
| 42 | 101010 | Config. Usuario |
| 40 | 101000 | Preced. 5 |
| 38 | 100110 | AF43 |
| 36 | 100100 | AF42 |
| 34 | 100010 | AF41 |
| 32 | 100000 | Preced. 4 |
| 30 | 011110 | AF33 |
| 28 | 011100 | AF32 |
| 26 | 011010 | AF31 |
| 24 | 011000 | Preced. 3 |
| 22 | 010110 | AF23 |
| 20 | 010100 | AF22 |
| 18 | 010010 | AF21 |
| 16 | 010000 | Preced. 2 |
| 14 | 001110 | AF13 |
| 12 | 001100 | AF12 |
| 10 | 001010 | AF11 |
| 8 | 001000 | Preced. 1 |
| 6 | 000110 | Config. usuario |
| 4 | 000100 | Config. Usuario |
| 2 | 000010 | Config. Usuario |
| 0 | 000000 | Preced. 0 (Best Effort, default) |

Fuente: Implementación de QoS en red de transporte de datos del MDMQ [7]

Después de haber detallado los mecanismos de marcado y clasificación, se procede a analizar el proceso de priorización y gestión de colas, el cual se detalla a continuación

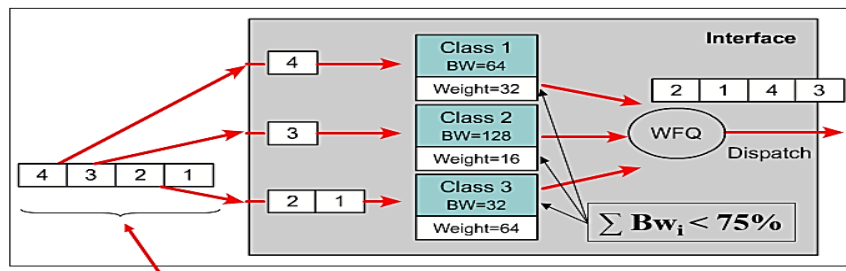
4.4.3 Manejo de Congestión de Colas

Custom Queueing (CQ)

- ❖ CQ fue diseñado para permitir que varias aplicaciones compartieran la red, y que además tuvieran asignado un ancho de banda mínimo garantizado, y unas garantías aceptables en cuanto a los retrasos [29].
- ❖ En este método el ancho de banda debe de ser compartido proporcionalmente entre las aplicaciones o usuarios en forma de Round Robin o quantos de tiempo, sin dejar tráfico fuera de servicio [29].
- ❖ No da garantías estrictas.

Funcionamiento de CBWFQ

Permite al sistema tener un número limitado de colas que llevan un conjunto de flujos de tráfico. Para esta configuración el sistema utiliza políticas de QoS o los tres bits de IP Precedence.



Los paquetes llegan clasificados, ya no tenemos en cuenta los flujos independientes, **solo la clase.**

Figura 4.18: Funcionamiento de CBWFQ [29]

La falta de escalabilidad WFQ se soluciona con Class Based WFQ. Donde las clases utilizadas en CBWFQ pueden asociarse a:

- ❖ Flujos (direcciones origen-destino, protocolo, puertos)
- ❖ Prioridades (campo DS differentiated service, otras etiquetas)
- ❖ Interfaces de entrada/salida
- ❖ VLAN

Estas clases se implementan filtrando el tráfico con filtros en los routers. Este proceso se llama clasificación de tráfico, que puede ir acompañado a su vez con proceso de marcado de paquetes. El servicio recibido en función de esta clasificación se asocia a la política de servicio [29].

Low Latency Queue (LLQ)

Es actualmente el método de encolamiento recomendado para aplicaciones en tiempo real LLQ se comporta como una Priority Queue

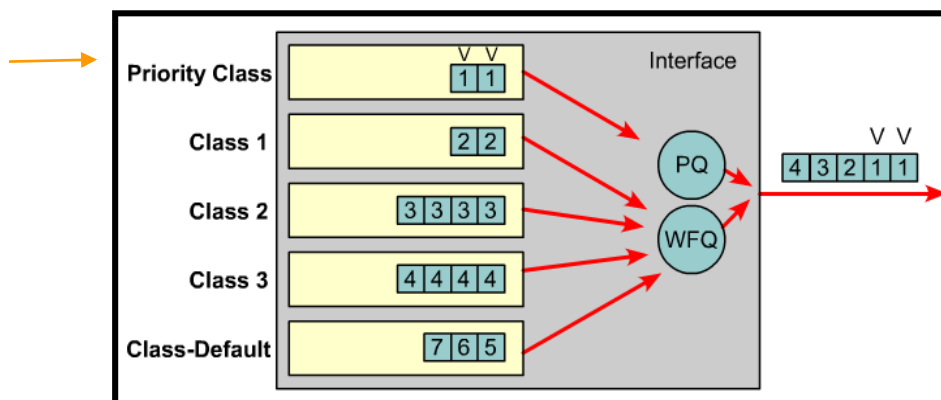


Figura 4.19: Funcionamiento Low Latency Queue (LLQ) para el manejo de congestión [29].

LLQ es recomendable para tráfico multimedia (VoIP) que requiere de unas características muy especiales: bajo retardo y jitter. Se puede configurar junto al resto de colas CBWFQ como una cola más asociada a una clase determinada. Los tipos de encolamiento que se escogieron para la implementación de QoS son CBWFQ complementado con LLQ [7] [8] [29].

4.4.4 Método de Evasión de Congestión

Existen controles de congestión que se basan en la manera en que el protocolo TCP opera, con el fin de no llegar a la congestión de la red.

Las técnicas de RED (*Random Early Detection*) y WRED (*Weighted Random Early Detection*) evitan el efecto conocido como sincronización global. Si no se configura ninguno de los dos, el router usa el mecanismo de descarte de paquetes por defecto llamado *tail drop* [29].

RED (*Random Early Detection*)

Provee a los operadores de la red, la posibilidad de aplicar normas para el manejo del tráfico y maximizar el throughput bajo condiciones de congestión [29].

WRED (*Weighted Random Early Detection*)

Combina las capacidades de RED y de IP Precedence, para proveer diferentes clases de servicio en función de las características de la información.

Después de realizar el análisis de las características de cada uno de los métodos y servicios para la implantación de QoS, se muestra en la tabla el método que se eligieron para el proceso de implantación de QoS en la red MAN de EEASA. [7][29]

Tabla 4.12: Algoritmos para la implementar QoS

| Parámetros a Aplicar | Método Seccionado | Detalle de Requerimiento |
|--|---|--|
| Clasificación del tráfico | <ul style="list-style-type: none">• ACL | Ancho de banda en forma dedicada |
| Marcado de tráfico | <ul style="list-style-type: none">• DSCP | Asignación de ancho de banda dedicada |
| Administración de Congestión del tráfico | <ul style="list-style-type: none">• CBWFQ• LLQ | Administrar la congestión |
| Control de congestión | <ul style="list-style-type: none">• WRED | Control de la congestión de la red MAN de EEASA. |

Elaborado por: Investigador

4.5 Elaboración de Prototipo Basado en simuladores de redes para la implementación de Calidad de servicio QoS.

Una técnica que imita el comportamiento de un sistema del mundo real, son los simuladores, que permite analizar y observar características, sin la necesidad de acudir al sistema real. Actualmente existen varios tipos de simuladores de red disponibles, muchos de libre distribución y otros bajo licencias.

A continuación se procede a realizar el análisis de cada uno de los simuladores de red, que se utilizaron para que soporten los protocolos de Calidad de Servicio QoS necesarios para la simulación de la red MAN de EEASA.

4.5.1 Simulador OPNET Modeler

OPNET Modeler es un programa ampliamente utilizado en la industria para modelar y simular sistemas de comunicaciones. El nombre corresponde a las siglas de Optimized Network Engineering Tool. Permite diseñar y estudiar redes, dispositivos, protocolos y aplicaciones. Está basado en la teoría de redes de colas e incorpora las librerías para facilitar el modelado de las topologías de red. Soporta un amplio rango de tecnologías tipo LAN, MAN y WAN [30].

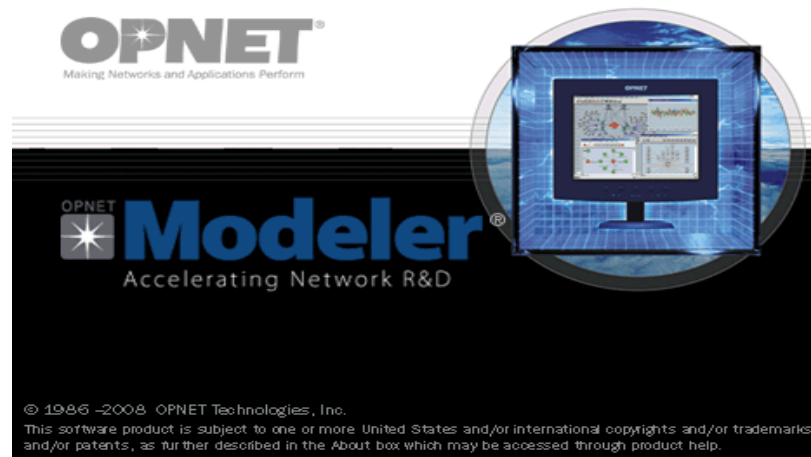


Figura 4.20: Opnet Modeler 14.5

OPNET Modeler utiliza distintos niveles de modelado o paradigmas para representar los diferentes componentes de una red. Cada nivel está asociado a un dominio y a un editor. Para hacer el desarrollo más intuitivo al usuario, los editores se organizan jerárquicamente, de forma que los modelos desarrollados en el Editor de Proyectos (Project Editor) dependen de elementos desarrollados en el Editor de Nodos (Node Editor). Éste a su vez usa modelos definidos Editor de Procesos (Process Editor).

Estos son los tres principales editores de OPNET, pero existen también otros complementarios como son Link Model Editor (para crear, editar y ver modelos de link), Packet Format Editor (sirve para desarrollar paquetes con un formato determinado) o Probe Editor (para configuración de las estadísticas que se quieren obtener durante una simulación) [30] [31] [32].

Ventajas

- ❖ Tiene un realismo alto
- ❖ Abarca miles de modelos y enlaces para poder generar nuestra topología
- ❖ Extensa biblioteca de modelos y protocolos.

Desventaja

- ❖ Licencia muy costosa
- ❖ La versión disponible no puede generar nodos con ISIS ni MPLS, es necesario hacer un análisis para equipo por equipo para definir estos parámetros [32].
- ❖ Simulación lenta
- ❖ No hace un análisis detallado a nivel de paquetes.

4.5.2 GNS3 (Graphical Network Simulator)

GNS3 es un simulador de red gráfico que permite la emulación de redes complejas, al igual que un emulador como VMWare, VirtualBox o Virtual PC que se utilizan para emular varios sistemas operativos en un entorno virtual; GNS3 utiliza los IOS de los equipos de Cisco y los ejecuta en un entorno virtual en el ordenador, la emulación se lo puede realizar en computadoras basadas en Windows, Linux y Mac OS X [33].



Figura 4.21: Eslogan de GNS3 (Graphical Network Simulator)

Debido a que el emulador posee una larga lista de plataformas de routers y otros dispositivos, es más fácil para que el administrador pueda interactuar con los equipos, agregando todas las características y potencialidades de un router real, sin tener el problema de comandos no reconocidos o no funcionales, probando de esta forma todas las configuraciones posibles y necesarias [33] [34].

Características de GNS3

Las principales características que tiene el emulador GNS3 son las siguientes:

- ❖ Diseño de topologías de redes de alta calidad y complejidad.
- ❖ Emulación de muchas plataformas de IOS de routers Cisco IOS, switch firewalls y otros.
- ❖ Emulación de Ethernet simple, ATM, switches Frame Relay, etc.
- ❖ Conexión de redes simuladas al mundo real.
- ❖ Captura de paquetes utilizando Wireshark.
- ❖ Es de fácil instalación debido a que todos los programas que se necesita para que funcione se encuentra en un solo paquete de instalación.
- ❖ Está en constante actualización y periódicamente se puede encontrar versiones de la aplicación más robustas y con nuevas funcionalidades.

Cabe mencionar que GNS3 es un programa de código abierto gratuito para su uso. Sin embargo, debido a restricciones de licencia en lo que se refiere a los IOS de los equipos (routers) de Cisco es necesario adquirirlos bajo una cierta cantidad de dinero para poder usarlos en GNS3 [35].

Al poder interactuar directamente con los IOS de Cisco, se puede observar la potencia del Software ya que es la mejor manera de ver su comportamiento y probar configuraciones debido a que se está ejecutando las imágenes reales de los equipos, dando incluso la alternativa de conectar los esquemas creados en GNS3 con Hardware real [33][35].

Descripción Técnica de GNS3

Para permitir simulaciones completas, el emulador GNS3 utiliza 3 componentes importantes:

- **Dynamips**, el programa básico que permite la emulación de Cisco IOS.
- **Dynagen**, un texto basado en front-end para Dynamips.
- **Qemu**, máquina emuladora y virtualizadora de código abierto.

Desventajas:

- ❖ Depende de la capacidad de memoria RAM del CPU donde está ejecutándose el programa

- ❖ Alto consumo de recursos de CPU y RAM en redes complejas.
- ❖ Solo se puede emular hasta la serie Cisco 7200. [35]

A continuación se detalla en la tabla las características de los simuladores analizados.

Tabla 4.13: Características de Simuladores

| SIMULADOR | LICENCIA | EQUIPOS SOPORTADOS | PROTOCOLOS SOPORTADOS | OBSERVACIONES |
|------------------|-----------------|--|--|---|
| OPNET | Pagada | Soporta casi todas los routers y switches CISCO | VoIP, TCP, OSPFv3, MPLS, IPV6, Otros. | Licencia pagada, complejo manejo y simulación |
| GNS3 | Gratis | 1710, 1720, 1750, 1751, 1760 2610, 2611, 2610XM, 2620, 2620XM, 2650XM 2611XM, 2621, 2621XM 3620, 3640, 3660 2691, 3725, 3745 7206 | Todos los soportados por el IOS cargado. | Soporta Wireshark, más adecuado para la simulación. |

Elaborado por: Investigador

4.5.3 Requerimientos de Calidad de Servicio QoS en simulación.

Una vez elegido el método y algoritmos que se van a utilizar para la implementación de calidad de servicio (QoS) en la red MAN de EEASA, se procede a realizar la simulación para implementación de QoS. La simulación tiene como objetivo determinar qué tan eficaz y eficiente resulta aplicar QoS tanto en la red cableada como la inalámbrica, así determinar el mejoramiento de servicios internos de la red MAN de EEASA.

Para objetivos de nuestra investigación se usa aplicaciones para su priorización como la de VoIP, videoconferencia, datos (FTP), Http y Correo Electrónico, aplicaciones más utilizadas dentro de la red de EEASA. A continuación describa cada una de estas aplicaciones con sus parámetros establecidos para realizar la simulación.

Aplicaciones VoIP

Para las aplicaciones de VoIP la gestión del tráfico para proveer la calidad de servicio, se requiere de fiabilidad o disponibilidad media del servicio, retardo bajo, jitter bajo y ancho de banda bajo.

El parámetro más importante que se debe tomar para la transmisión de VoIP es el retardo definido por el estándar ITU.G. 114, el cual considera un retardo de 0-150 ms de extremo a extremo como aceptable, de 150-400ms se degrada el servicio y mayor a 400ms es inaceptable. Para equipos terminales que permitan usar los servicios telefónicos IP Cisco, usa 20 ms de retardo en voz con paquetes RTP (Código G.11 y G729)

La aplicación utiliza poco ancho de banda para realizar el envío de paquetes, donde este valor ya está definido en su códec [7]:

- ❖ G711 PCM: 64Kbps
- ❖ G726 ADPCM: 32Kbps
- ❖ G729: 8Kbps
- ❖ G723.1: 5.3 Kbps

Aplicación de Video

Para la aplicación de video conferencia, el proveer de calidad de servicio requiere de fiabilidad, jitter bajo, retardo bajo y ancho de banda alto para que la aplicación pueda funcionar correctamente, esta aplicación está formada por cuatro flujos, dos en cada sentido, uno para el audio y otro para video y se puede agruparse en una misma clase para recibir QoS.

El ancho de banda para video toma en cuenta el códec que usa para transmitir los paquetes con calidad de servicio [7]:

- ❖ MPEG-1: 500-1500 Kbps
- ❖ MPEG-2: 5 a 10 Mbps
- ❖ MPEG-4: 28.8 a 400 Kbps
- ❖ H.261: 100 a 400 Kbps
- ❖ Donde el video de alta calidad requiere aproximadamente 768 Kbps.

Aplicación con datos

En toda empresa existen áreas que son críticas por el flujo de tráfico que generan y los recursos que estos requieren de la red, por tal motivo se debe realizar una administración dando prioridades de tráfico, esto permitirá que tales datos que son más importantes que otros en la red se las pueda clasificar en cinco modelos de clases de datos [7].

- ❖ Aplicación de misión Crítica
- ❖ Aplicación interactiva
- ❖ Aplicación masiva de datos
- ❖ Aplicaciones de mejor esfuerzo

Herramientas de Monitoreo en la Simulación

Servidor de monitoreo

Este servidor de monitoreo fue el más importante en la elaboración de la simulación ya que permite proporcionar datos del consumo de tráfico y pérdida de paquetes provenientes desde la interfaz del router cuyo resultado es el análisis de cada segmento de la red en parámetros de velocidad de transmisión, puertos de aplicación, tipo de tráfico saliente y entrante (UDP o TCP). Para esto se realizó la configuración de NetFlow dentro de los routers simulado en GNS3.

Analizador de tráfico Wireshark

Esta herramienta permite capturar y analizar el tráfico mediante el software Wireshark o conocido como Ethereal, este software viene incluido en el paquete de instalación de GNS3, lo cual facilita la captura de tráfico y analizar que contiene los flujos de paquetes provenientes de todos los puntos que generan tráfico en la red simulada tanto en GNS3 como OPNET.

4.5.4 Características de Simulación en GNS3 y OPNET

La primera parte de la prueba, es el análisis de tráfico no priorizado sin aplicar la configurar de QoS en la red, generalmente los equipos switch fueron configurados en esquema de VLAN de acceso y VLAN modo trunk, para permitir la comunicación entre los niveles de acceso y distribución, los equipos fueron configurados a través de CLI, y sus comandos se detallan en el anexo 4. El análisis de la red sin QoS, en cada switch, router y enlace inalámbrico, tiene la función de únicamente dejar pasar los flujos provenientes de las aplicaciones, todos ellos sin características de priorización de tráfico de red. La segunda parte de simulación de la red MAN de EEASA es aplicar QoS agregando nuevas configuraciones de políticas de calidad de servicio en los equipos (routers, switches y enlaces inalámbricos), los resultados que presente la red con el

mecanismo de priorización de tráfico, permitirá analizar la optimización de la red y determinar mecanismos de manejo y congestión del tráfico que toma la red tanto en los enlaces por cableados como los enlaces inalámbricos. A continuación se describe las políticas y parámetros que se aplicara al configurar calidad de servicio (QoS) en OPNET Modeler y GNS3.

Los parámetros aplicados en los routers y switches simulados en GNS3 permiten la oferta de calidad de servicio, planteando la clasificación de tráfico para distribuir las aplicaciones de voz, datos, video y otras aplicaciones de acuerdo a la prioridad. En la tabla 4.14 se muestra los valores DSCP que se utiliza para marcarlos a cada clase, en este caso AF (Assured Forwarding) y sus variantes, el tipo de tráfico de cada clase y además la cantidad de ancho de banda requerido, así también se asigna los nivel de prioridad del tráfico a lo largo del trayecto en la red [35].

Tabla 4.14: Clasificación de Servicios, Valores de DSCP y Ancho de Banda para QoS

| PRIORIDAD | ENLACE INALÁMBRICO | TRÁFICO | DIFFSERV (DSCP) | TIPO | ANCHO DE BANDA |
|-----------|--------------------|----------------------------------|-----------------|-------------------|----------------|
| Critica | Premium | VoIP | EF | TCP, UDP | 14% |
| | | Videoconferencia | AF31 | TCP | 14% |
| Alta | Oro | Streaming | AF42 | HTTP | 12% |
| Media | Plata | Aplicaciones Empresariales | AF21 | Transacciones web | 10% |
| | | | CS3 | Base de datos, | 8% |
| Baja | Bronce | Administración de red | AF12 | SNMP, TELNET | 5% |
| Default | Best Effort | Aplicaciones sin garantía de QoS | AF11 | Default | 0 |

Elaborado por: Investigador

A continuación de detalla el proceso de simulación realizada en OPNET Modeler y GNS3.

4.6 Simulación de Calidad de Servicio QoS en OPNET Modeler

4.6.1 Esquema de Simulación en OPNET Modeler

Para el desarrollo del proyecto, se siguieron procesos, los cuales permitieron ejecutar la simulación de manera clara y ordenada. Estos procesos empieza en la creación de la

topología, en la figura 4.21 se puede visualizar la configuración lógica de la red MAN de EEASA que está basada en una arquitectura de enlaces inalámbricos punto a punto.

Este modelo consta de 8 estaciones base (BS), las cuales son los nodos centrales del sistema y varias SS ubicadas a cada BS correspondientes, también cuenta con varios servidores de aplicaciones y un enlace *backbone* entre la BS MATRIZ y los servidores. Otros objetos incluidos en el modelo de red, son los objetos WiMAX, *Applications* y *Profiles*. Estos objetos permiten la definición del modelo ya que especifica las características del sistema, tanto en la capa PHY y QoS, además define el tipo de aplicaciones y sus perfiles de operación. A continuación se detalla el procedimiento para configurar las aplicaciones de datos, voz, video, servicio de internet y correo electrónico en el simulador OPNET.

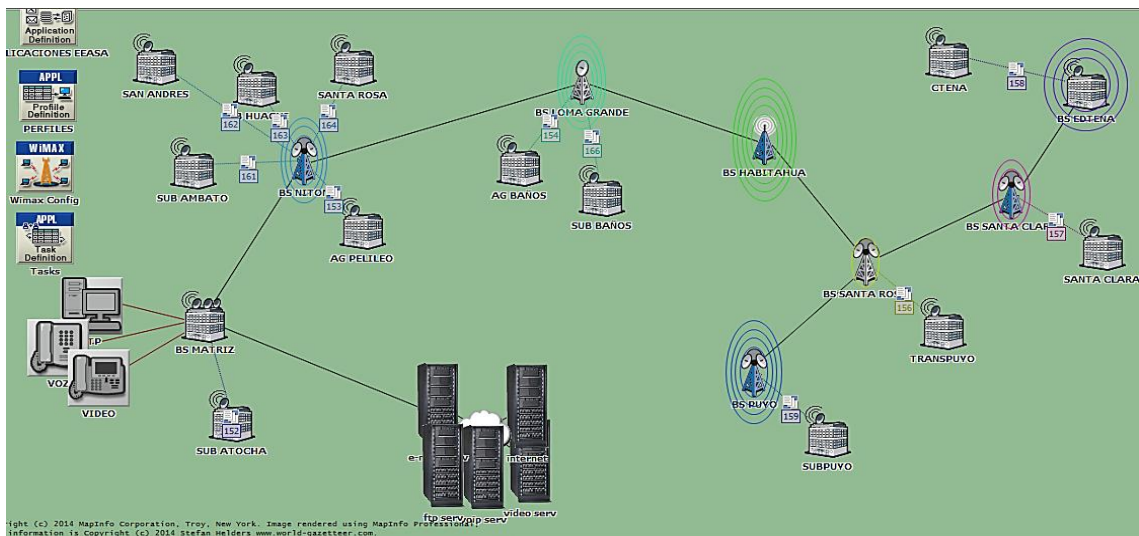


Figura 4.22 Escenario de prueba Wimax en OPNET
Elaborado por: Investigador

4.6.2 Configuración de Aplicaciones

Las aplicaciones deben ser configuradas en el simulador, para ellos se utiliza el nodo "*Application Conig Node*", en este objeto se puede especificar, crear y personalizar cada aplicación a simular, además ofrece una diversidad de opciones para modificar los atributos de cada aplicación a implementar [31]. A continuación se presenta el desarrollo de configuración:



Figura 4.23 *Application Definition* en OPNET
Elaborado por: Investigador

- ❖ De la paleta de objetos se elige *Application Conig Node*, y arrastramos al área de trabajo.
- ❖ En el objeto dar clic derecho, y seleccionamos *Edit Attributes*.
- ❖ Seleccionamos *Application Definitions*, en *number rows* ingresamos 6
- ❖ Ingresamos el nombre de la aplicación que en este caso será Aplicación VoIP como se muestra en la figura 4.24, y a continuación describimos el tipo de aplicación, para posteriormente configurar sus respectivas características [31].

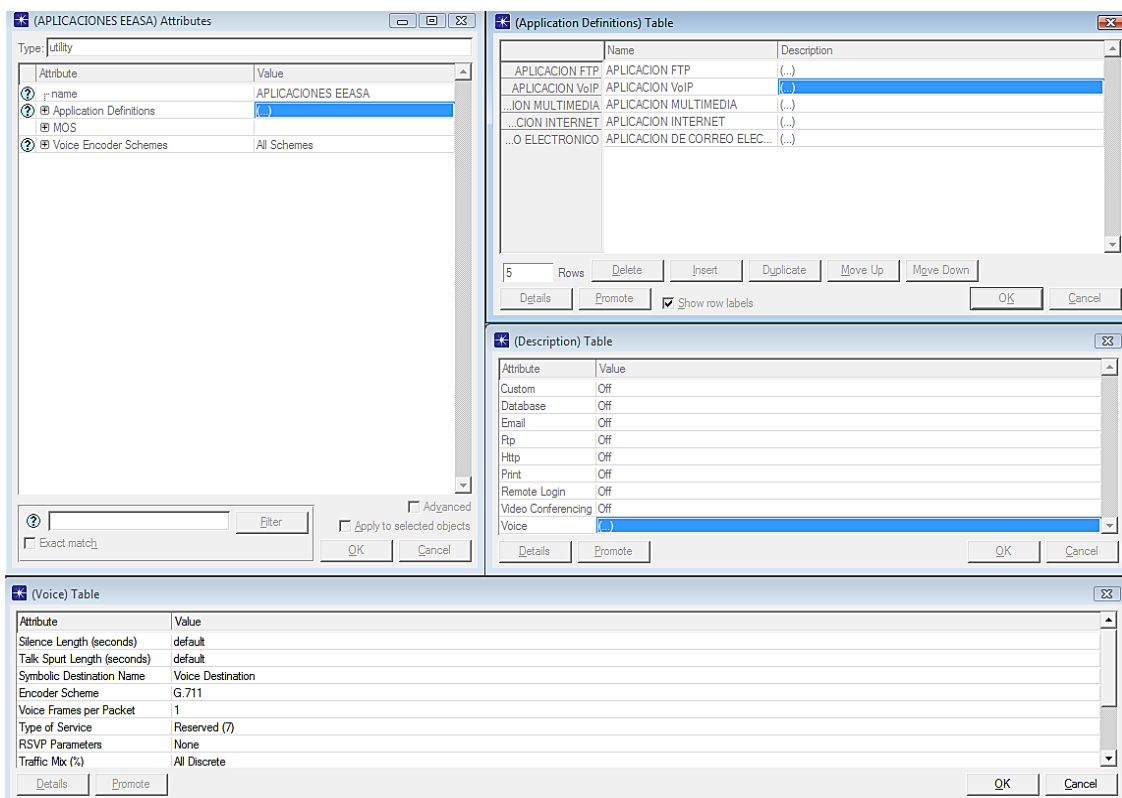


Figura 4.24: Configuración de Aplicación de VoIP
Elaborado por: Investigador

En la figura 4.24 se visualiza la configuración de la aplicación de voz, para la configuración procedemos a definir la aplicación, para posteriormente elegir una de las descripciones que caracterizara esta aplicación, y finalmente configurar los parámetros

con las que operara esta aplicación, en este caso se ha configurado con un Encoder Scheme G.711 y el tipo de servicio con el cual operara es Interactive Voice (6).

Las demás configuraciones de las aplicaciones desarrolladas en OPNET Modeler se pueden visualizar en el Anexo 2.

4.6.3 Configuración de Perfiles

De la misma manera que se crearon las aplicaciones, se tiene que crear los perfiles de las aplicaciones a usar en el modelo de red.

El objeto *Profiles* puede especificar los parámetros de tráfico de cada aplicación, de esta manera se podrá definir el modo de operación de las aplicaciones.

Se procede a configurar un nuevo perfil para aplicaciones creadas anteriormente esto se realiza en el *Profile Node* descrita a continuación.

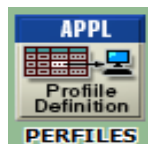


Figura 4.25: *Profile Definition* en OPNET
Elaborado por: Investigador

- ❖ Primero dar click derecho en el *Profile Node* y seleccionamos *Edit Attributes*, en la pantalla desplegar y dar doble clic en *Profile Configuration*.
- ❖ Ahora en el campo *rows* ingresamos 5
- ❖ Ingresamos el nombre del nuevo perfil, y luego dar doble click en el campo *Applications* del nuevo perfil.
- ❖ En la tabla de *Profile Configuration*, configurar *Constant (30)* en el campo *Duration (seconds)*, y editar el campo *Repeatability* y seleccionar *Inter-repetition Time (seconds)* en *constant (30)*, *Number of Repetitions* en *Unlimited*, *Repetition Pattern* en *Serial [30] [31]*.

En la figura 4.26 se puede observar los parámetros de tráfico de las aplicaciones de voz, video, datos (FTP), web y email que se configuraron. La cual se definen los modos de operación de cada una de las aplicaciones, el cual consta de características como el

nombre de la aplicación, tiempo de inicio *Offset*, modo de operación, tiempo de inicio y duración de compilación con el que se ejecutara cada una de las aplicaciones.

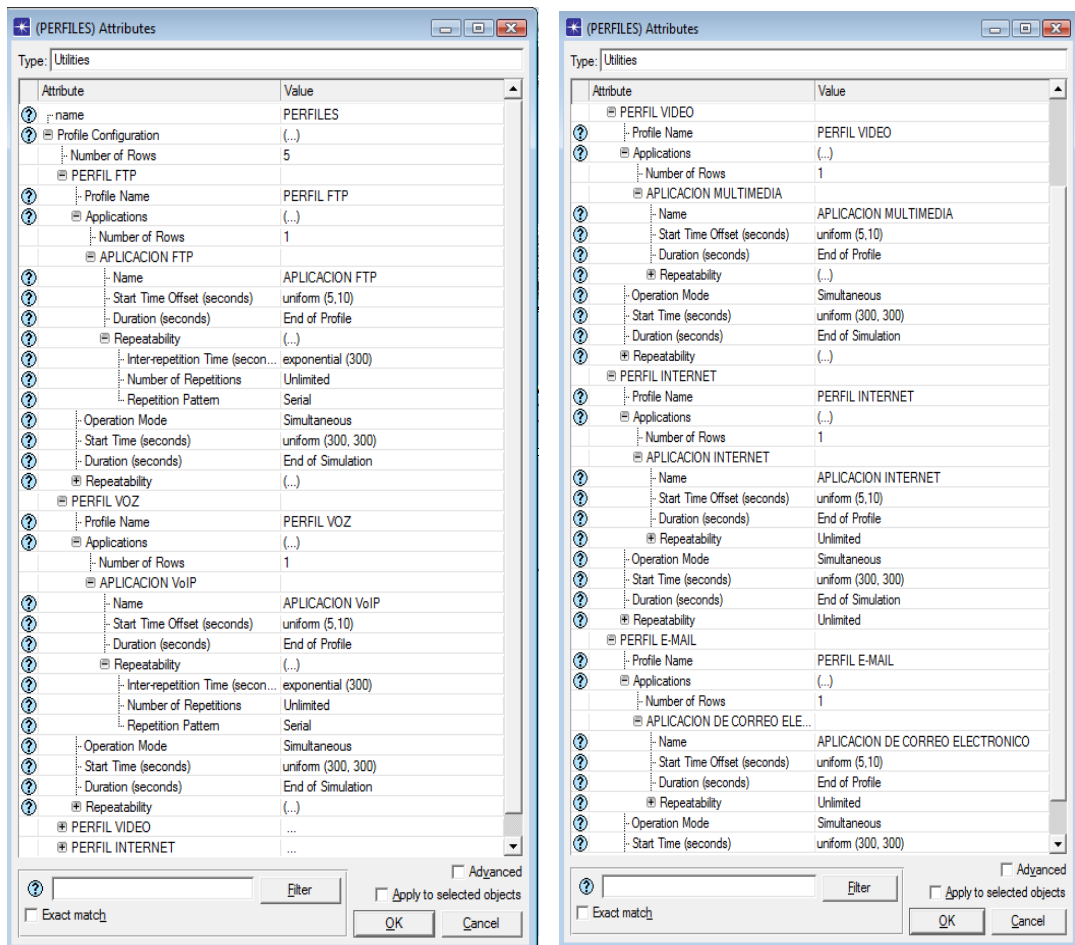


Figura 4.26 Configuración de Perfiles

Elaborado por: Investigador

4.6.4 Configuración de Servidores de aplicaciones

Representa la entidad donde residen las aplicaciones de datos, voz, video, etc. Para que cada aplicación genere tráfico se estableció la conexión entre las BS y el servidor se realiza mediante un enlace punto a punto.

Para realizar la configura se procede a seleccionar el nodo Servidor, dar clic derecho y seleccionar *Edit Attributes > Application: Supported Services* [30].

En la figura 4.27 se puede observar un cuadro de atributos con los servicios a soportar por cada aplicación en este caso FTP y multimedia, para la configuración se ingresara 1 en la casilla *rows*, en *name* ingresamos el nombre de la aplicación creada en el objeto

Application Conig Node, seleccionamos ok en los dos cuadros para poder visualizar el servicio que soporta esta aplicación.

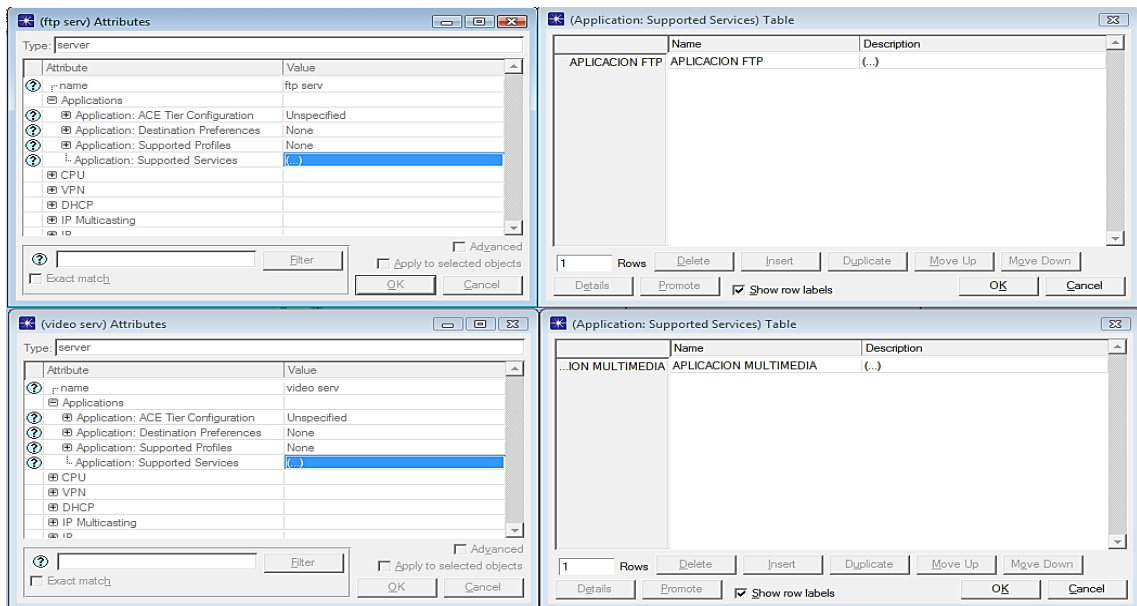


Figura 4.27 Configuración de Servidores de Aplicación.

Elaborado por: Investigador

4.6.5 Configuración de Estaciones Suscriptoras SS

Representa el equipo transceptor del usuario, realiza funciones del modelo de referencia TCP/IP. Estos procesos consisten en la capa de aplicación, las capas TCP y UDP (Transporte), la capa IP (Internet) y la capa Wimax MAC (Acceso a red) [30, 31].



Figura 4.28: Estaciones Suscriptoras.

Elaborado por: Investigador

En la figura 4.29 se observa la configuración de las estaciones suscriptoras, en este caso se configuro en el cliente SUBHUACHI, en el cual se definen las aplicaciones que soportara la subred a la cual pertenece, para realizar la configuración se realizó los siguientes pasos:

Se dio clic derecho en los SS SUBHUACHI, se seleccionó *Edit Attributes* > *Applications* > *Application: Supported Profiles* > *Rows (3)* > *Profiles name* (Ingresar el perfil creado creadas, FTP, voz, email) > seleccionar ok. Ahora seleccionamos *Application:*

Destination Preferences > Rows (3) seleccionamos *Application* (ingresamos la aplicación creada, FTP, VoIP, Correo Electrónico), seleccionamos *Symbolic name* (ingresamos el símbolo de servicio con la cual se creó la aplicación) y por ultimo seleccionamos *actual name* donde se ingresara el nombre del servidor que soporta la aplicación (FTP Server, Voice Destination, Email Server) [30] [31].

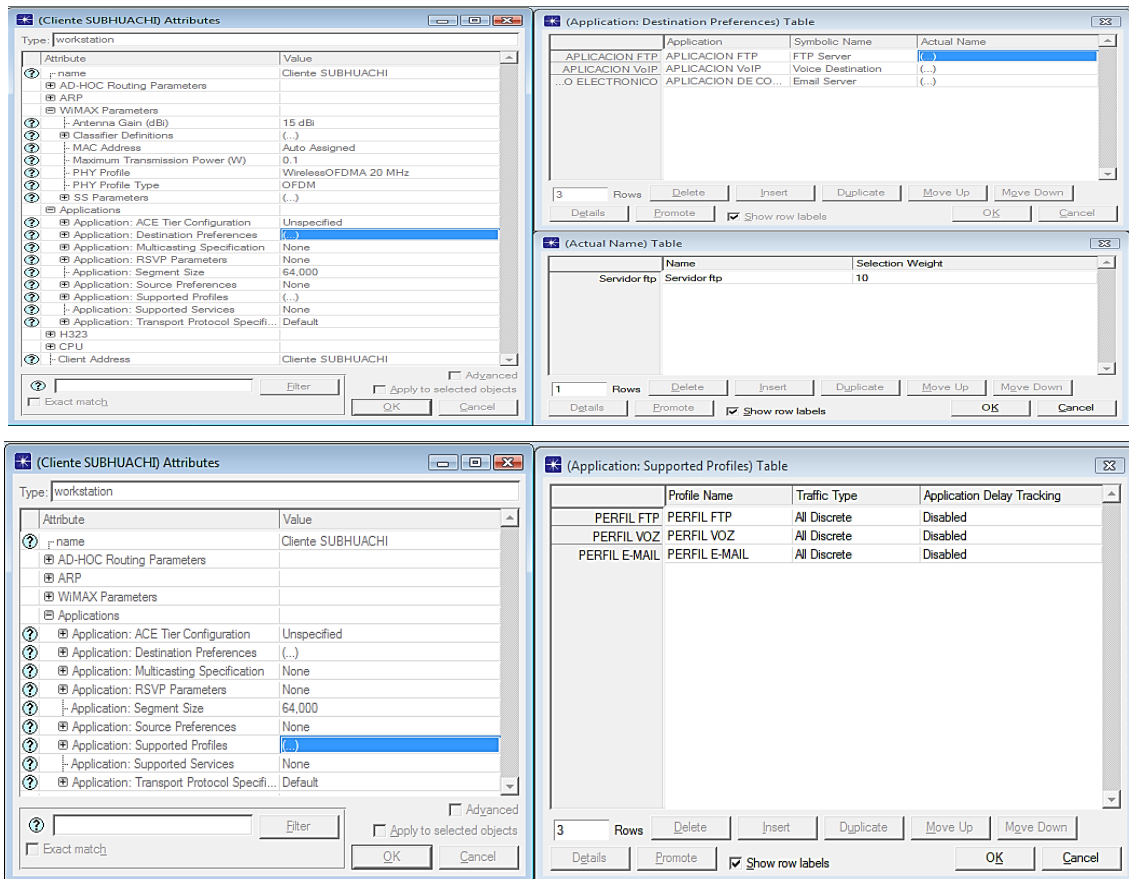


Figura 4.29 Configuración de Estaciones Suscriptoras y clientes.

Elaborado por: Investigador

4.6.6 Configuración de Wimax y entornos Inalámbricos

El objetivo del nodo Wimax es establecer qué clase de servicio se utilizara en uno o varios tipos de tráfico, los cuales son implementados en todos los nodos de la red [30]. Adicionalmente se configura el modo de eficiencia, que soporto la red wimax, esto permitió incrementar la exactitud de cada simulación, a continuación se describe los niveles de eficiencia:



Figura 4.30 Wimax Config.
Elaborado por: Investigador

- ❖ **Efficiency Enabled:** Su uso común es para la capacidad de planificación y calidad de servicio. Provee indicación de retrasos más precisos.
- ❖ **Framing Module Enabled:** Su uso más común es aplicaciones de calidad de servicio y la planificación para la implementación de las mismas.
- ❖ **Physical Layer Enabled:** Su uso más común es la transmisión en PHY y efectos de canal.
- ❖ **Mobility and Ranging Enabled:** Movilidad y alcance habilitados, permite determinar retrasos, niveles de potencia de estaciones móviles MS [30] [31].

En la figura 4.31 se puede observar que se utilizó el modelo *Framing Module Enabled* el cual proporciona el objetivo deseado en el proyecto. En anteriores capítulos del proyecto de investigación se estudiaron los diferentes tipos de planificadores para el soporte de QoS en una red *Wimax*, entre ellos tenemos *UGS o ertPS, ertPS, etPS y nrtPS*. A continuación se detalla la funcionalidad que posee *OPNET Modeler* para relacionar el tráfico proveniente de la capa IP con las clases de servicio en la capa MAC.

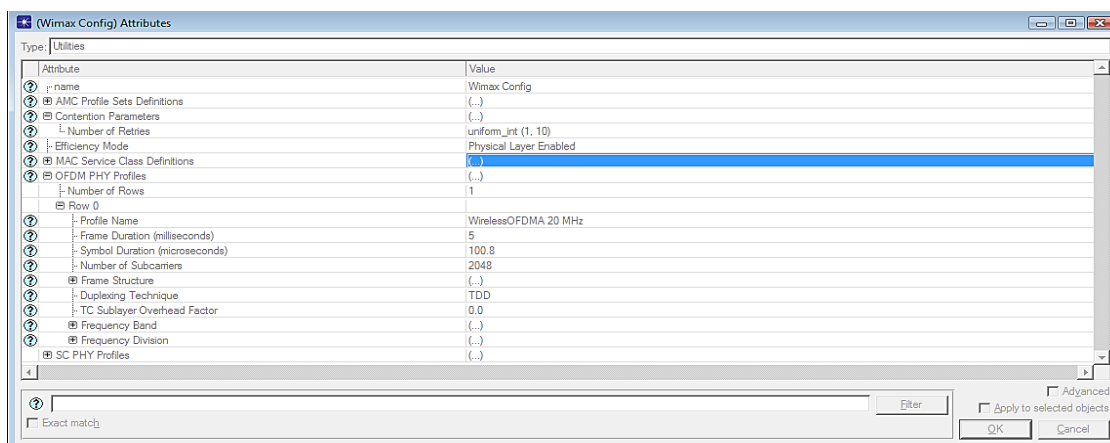
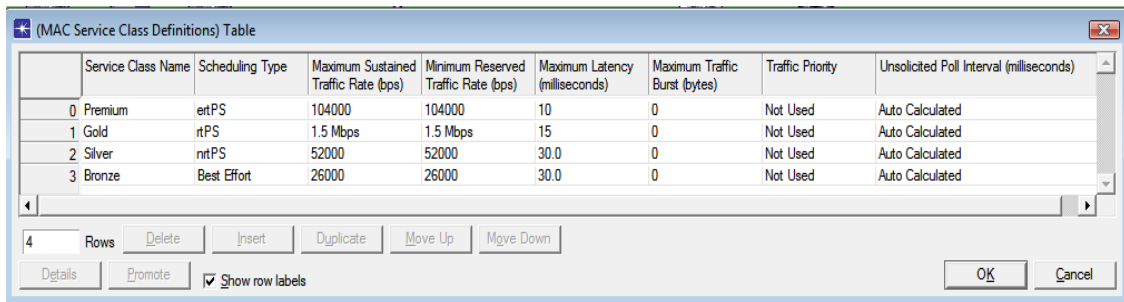


Figura 4.31 Configuración Parámetros de WiMAX
Elaborado por: Investigador

En la figura 4.32 se puede visualizar la configuración de la parametrización de aplicaciones para soporte de QoS. A continuación se listan los parámetros de QoS que se implementan en el estándar IEEE 802.16 y sus definiciones.

- ❖ **Maximum reserved traffic rate:** Tasa máxima de transferencia.
- ❖ **Minimum reserved traffic rate:** Cantidad mínima promedio de tráfico transportado.
- ❖ **Maximum latency (ms):** Tiempo máximo promedio entre el ingreso de un paquete a la sub capa de un convergencia y el direccionamiento de SDU al medio para ser transmitido. [30]
- ❖ **Tolerated Jitter:** Máxima variación del retardo soportada para la conexión
- ❖ **Traffic Priority:** Prioridad asignada a un flujo de servicio [31].

De acuerdo a lo anterior, la configuración se lo realiza de la siguiente manera, clic derecho en el objeto *WiMAX Config* luego *Edit Attributes > MAC Service Class Definitions*, luego aparecerá un recuadro para la clasificación de servicio como se puede observar en la figura 4.32.



| | Service Class Name | Scheduling Type | Maximum Sustained Traffic Rate (bps) | Minimum Reserved Traffic Rate (bps) | Maximum Latency (milliseconds) | Maximum Traffic Burst (bytes) | Traffic Priority | Unsolicited Poll Interval (milliseconds) |
|---|--------------------|-----------------|--------------------------------------|-------------------------------------|--------------------------------|-------------------------------|------------------|--|
| 0 | Premium | rtPS | 104000 | 104000 | 10 | 0 | Not Used | Auto Calculated |
| 1 | Gold | rtPS | 1.5 Mbps | 1.5 Mbps | 15 | 0 | Not Used | Auto Calculated |
| 2 | Silver | nrtPS | 52000 | 52000 | 30.0 | 0 | Not Used | Auto Calculated |
| 3 | Bronze | Best Effort | 26000 | 26000 | 30.0 | 0 | Not Used | Auto Calculated |

Figura 4.32: Configuración Parámetros de *WiMAX*
Elaborado por: Investigador

4.6.7 Configuración de Estación Base BS

Representa el equipo tranceptor del proveedor de servicios de telecomunicaciones, ya sea de datos, servicios de voz o video conferencia, se encarga de realizar tareas de enlace y ruteo entre diferentes entidades, como servidores, *switches*, *routers*, etc [30]. A continuación se detalla la configuración de la estación base.



Figura 4.33 Estación Base
Elaborado por: Investigador

Para la configuración de los parámetros de QoS se requiere configurar los flujos de servicio y clasificadores en los nodos wimax, para ello se sigue los pasos mencionados a continuación. Dar clic derecho sobre BS y seleccionar *Edit Attributes > WiMAX Parameters > SS Parameters > Downlink Service Flows* creando cuatro rows [30] [31]. Del mismo modo se configurara en la casilla *Uplink Service Flows*, en cada uno de estas opciones se crearon cuatro líneas y se realizaron su respectiva configuración como se muestran en las figuras 4.34

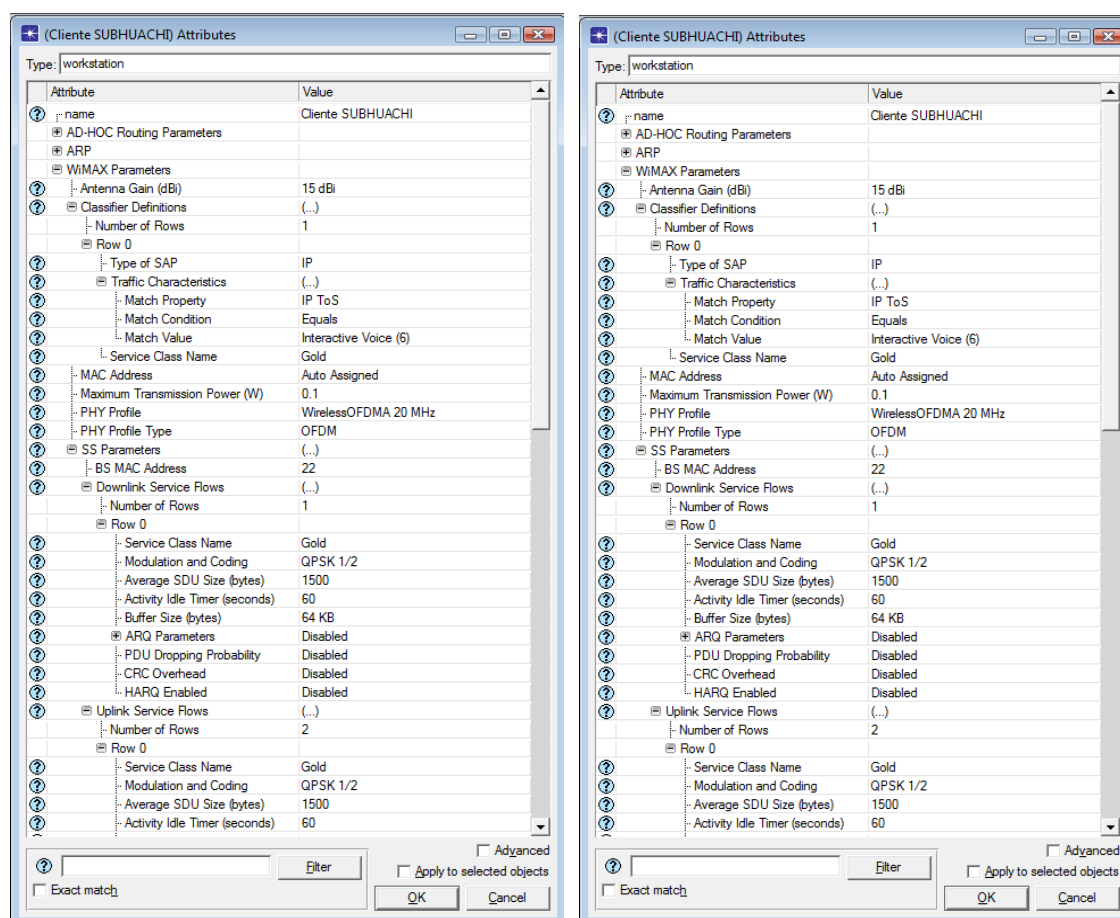


Figura 4.34: Configuración de Downlink/Uplink Service Flows

Elaborado por: Investigador

Posterior mente se configuraron las clases de servicios tanto en las estaciones base (BS) como las estaciones suscriptoras (SS), estas poseen un atributo *denominado Classifier Difinitions*. Para buscar, dar clic derecho sobre cada nodo, elegir *Edit Attributes > WiMAX Parameters > Classifier Difinitions* [30].

Esto permitirá relacionar el tráfico la capa IP con las clases de servicio de la capa MAC.

En la figura 4.35 se puede observar la configuración de parámetros de WiMAX, donde se puede visualizar tres columnas, *Type of SAP* (escoger IP), *Traffic Characteristics* que indica el tipo de tráfico que se tiene en la capa de red) y *Service class name* que indica la clase de servicio correspondiente a WiMAX que se requiera.

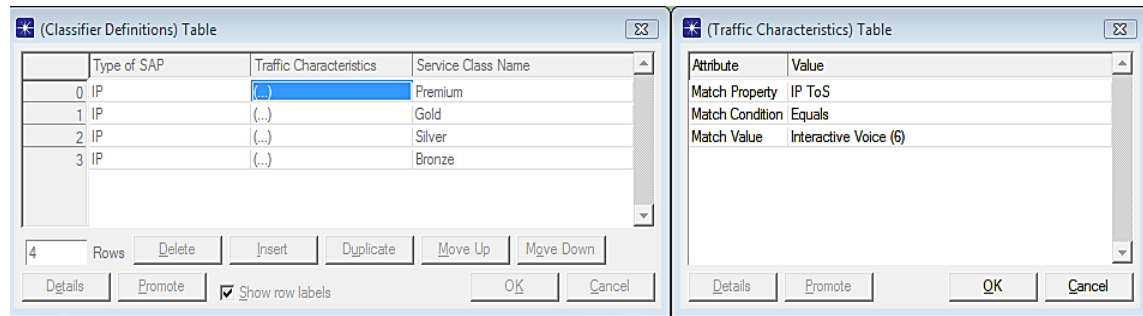


Figura 4.35 Configuración Parámetros de WiMAX

Elaborado por: Investigador

Al realizar todas las configuraciones se procede a ejecutar la simulación sin aplicar las políticas de QoS, esto se basa a que todas las aplicaciones simuladas se trabajen bajo servicios *Best Effort*, para posteriormente determinar los parámetros como: Tasa máxima de transferencia, cantidad mínima de tráfico transportado, máxima latencia en la transmisión de datos, máxima variación del retardo soportado por la conexión.

Estos datos permitieron determinar el método adecuado a la hora de implementar QoS en la red inalámbrica.

4.6.8 Implementación de Calidad de Servicio (QoS) en OPNET Modeler

En esta etapa se efectuaron pruebas en diferentes escenarios implementando calidad de servicio, permitiendo analizar el impacto en el rendimiento y confiabilidad en las aplicaciones que se ejecutaron sobre la red inalámbrica.

En el escenario simulado en OPNET se despliega una red de enlace inalámbrica que trabaja en estándares IEEE 802.16 y IEEE 802.11 que se tiene implementado en la red de EEASA.

Esta red se encuentra conformada por 8 nodos BS (Estación Base) y aproximadamente 4 SS (Estaciones Suscriptoras) enlazadas a su respectivo BS, como se detalla en la figura

4.36. El esquema planteado se basa en la topología lógica de la red MAN de enlace inalámbrica detallado al inicio del capítulo 4.

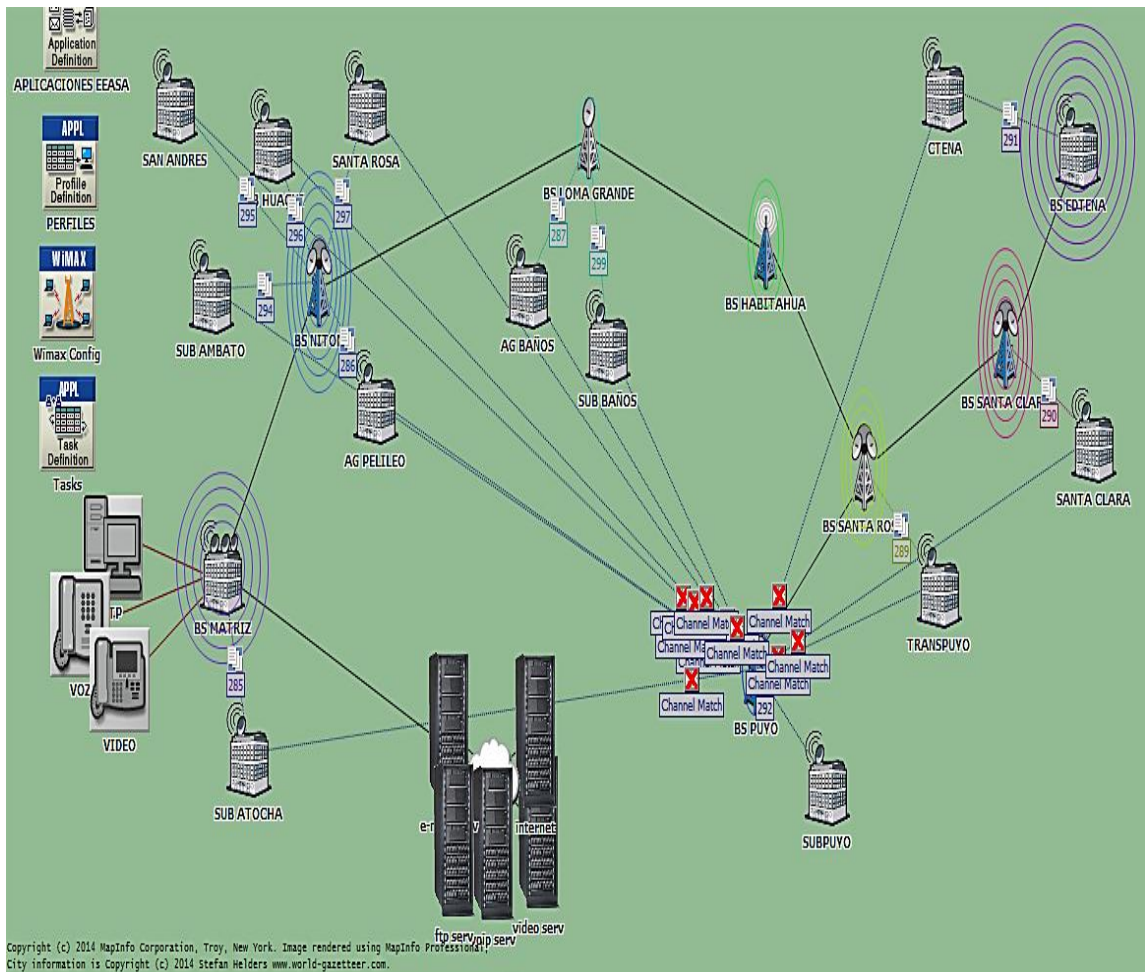


Figura 4.36 Ejecución de Simulador para redes Inalámbricas

Elaborado por: Investigador

Se analizó las aplicaciones de voz, video y datos, las dos primeras con altos requerimientos de calidad de servicio, mientras que la aplicación de datos que está conformada por FTP, http, correo electrónico y otras aplicaciones, no se aplicó mayores requerimientos de parámetros de calidad para la transferencia de información.

El modo operativo utilizado es Punto a Punto soportado por los estándares que se simularon. Cada agencia podrá realizar transferencia de archivos vía FTP y realizar llamadas VoIP, pero se configuro para solo los nodos Matriz EEASA, AGBaños, EDPuyo y AGTena realicen videoconferencia.

Debido a que existen varios tipos de aplicaciones que circulan en la red de EEASA, se procedió analizar las más importantes, cada uno de estas aplicaciones tomadas posee unos requerimientos únicos de calidad de servicio.

En la tabla 4.15 se describe la relación de parámetros de calidad de servicio para las aplicaciones simuladas en OPNET para el enlace inalámbrico, esta relación permite optimizar el rendimiento de cada una de ellas.

Tabla 4.15: Algoritmos para la implementar QoS

| Aplicación | Clase de Servicio | IP QoS | MAC QoS | MAC Máxima Latencia(ms) | Maxima Sustained Traffic Rate (bps) | Esquema de Codificación |
|--------------------|-------------------|--------------------------|-------------|-------------------------|-------------------------------------|-------------------------|
| Voz | Gold | Interactive Voice(6) | UGS o rtPS | 10 | 64000 | G711 |
| Voz | Gold | Interactive Voice(6) | UGS o rtPS | 10 | 96000 | G711 |
| Video | Bronze | Streaming Multimedia (4) | rtPS | 15 | 1000000 | - |
| FTP | Silver | Excellent Effort (3) | nrPS | N.A | 10000 | - |
| HTTP | Bronze | Best Effort (0) | Best Effort | N.A | 450000 | - |
| Correo Electrónico | Bronze | Best Effort (0) | Best Effort | N.A | 12000 | - |

Elaborado por: Investigador

Entre la gran cantidad de estadísticas que OPNET Modeler ofrece se procedió a tomar las adecuadas para el análisis del objetivo planteado en el proyecto de investigación, las estadísticas que se utilizaron para la simulación se observa en la tabla 4.16.

Tabla 4.16 Estadísticas a medir en la simulación de redes inalámbricas

| Variable | Descripción | Tipo de Estadística |
|----------------------------|------------------------------|---------------------|
| Load(bits/sec) | Tráfico incidente | Nodo Statistic |
| Throughput (bits/sec) | Tráfico transmitido | Nodo Statistic |
| Delay end to end (sec) | Retardo de extremo a extremo | Global Statistic |
| Jitter (sec) | Variación de retardo | Global Statistic |
| Traffic dropped (bits/sec) | Tráfico rechazado | Nodo Statistic |

Elaborado por: Investigador

4.7 Simulación de la red MAN en GNS3

Para un detallado análisis se realizó la simulación utilizando el software GNS3, el objetivo de la simulación ayudo a determinar si los equipos soportan calidad (QoS) de servicio, ya que el simulador permite interactuar con los sistemas operativos de los

equipos, además se analizara que beneficio trae implementar QoS en la red MAN de EEASA, tanto en los routers como los switches que confirman el backbone de la red.

Para realizar la simulación se basó en la topología lógica indicada al inicio del capítulo 4, el primer paso de la simulación se basa en cargar los IOS de cada router y switch, permitiendo tener un entorno más realista a la hora de ejecutar la simulación.

En la figura 4.37 se puede observar el diseño de la topología implementada en GNS3, la topología está compuesto por router cisco 3845, 2921, 282. Para el caso del switch 2960 se utilizó la imagen IOS del switch 2960-24TT-L Versión 15.0 (2) SE5, se habilito el MQOC de cisco que permite todas las configuración de QoS.

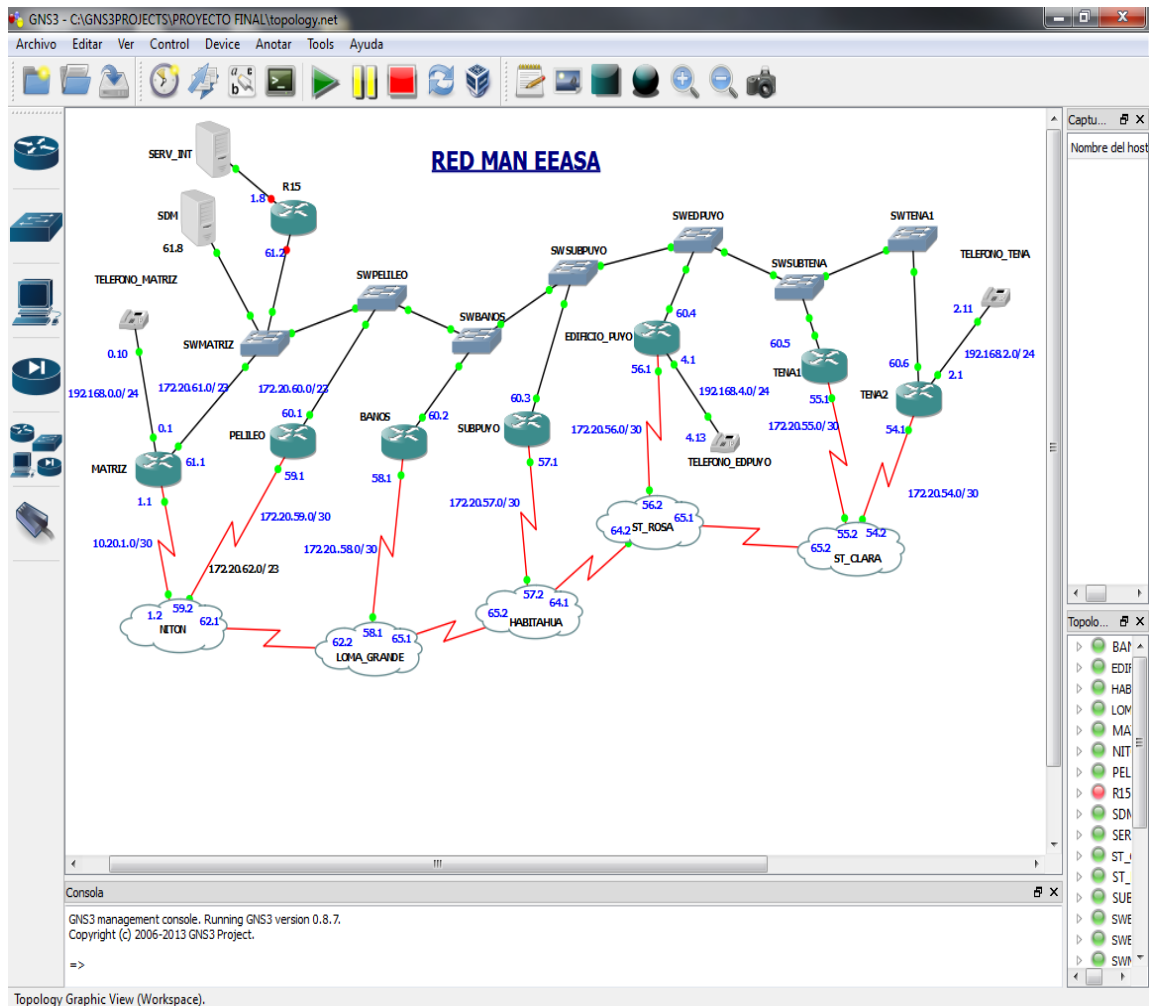


Figura 4.37 Red MAN de EEASA en GNS3
Elaborado por: Investigador

El inconveniente que se tiene con GNS3 es que no soporta todos los modelos de equipos que componen la red de EEASA, por tal motivo se procedió a modificar sus script, en donde se modificó y se incorporó características similares a los equipos que conforman el esquema de simulación de la red de EEASA.

Para la simulación de la red se utilizó otras direcciones IP para el backbone con interfaces FasEthernet porque se escogió una plataforma inferior de routers para facilitar el procesamiento del PC.

4.7.1 Configuración de Equipos

Debido a la gran cantidad de equipos que está conformada la red de EEASA, se pondrá como ejemplo la configuración de los equipos de un solo nodo en este caso se tomó la configuración realizada en el router Matriz

Comandos para la configuración

A continuación se presentan la configuración de OSPF y Netflow implementados en los equipos conformados por la red MAN de EEASA. La configuración se presenta de uno de los routers, en este caso el de la Matriz.

Configuración de OSPF y NetFlow

```
Matriz> enable
Matriz# configure terminal
Matriz(config)# router ospf <identificador del proceso OSPF >
Matriz (config) # router ospf 1
Matriz(config-router)# network <dirección IP> <wildcard-mask> area <area-id>
Matriz(config-router)# network 192.168.0.10 0.0.0.3 area 0
```

Configuración de NetFlow

```
MATRIZ(config)#interface fastEthernet 0/0
MATRIZ(config-if)#ip flow egress
MATRIZ(config-if)#exit
MATRIZ(config)#interface fastEthernet 0/1
MATRIZ(config-if)#ip flow ingress
MATRIZ(config-if)#exit
MATRIZ(config)#ip flow-export version 5
MATRIZ(config)#ip flow-export destination 192.168.0.10 4444
MATRIZ(config)#exit
```

4.7.2 Instalación y configuración de servidor VoIP

Para determinar la eficiencia de calidad de servicio en tráfico de voz, se procedió a realizar el prototipo de voz sobre IP con una arquitectura cliente-servidor, los softphone (Cliente) y *Call manager* Expres (Servidor), encargado de recibir las peticiones de todas los Softphone, la configuración se realizó en el router matriz, a continuación se detalla los pasos para la creación del *Call Manager Express* en el router y la instalación y configuración del *softphone Cisco IP Communicator*, se detalla en el Anexo 3. Cada teléfono se instaló en máquinas virtuales como se visualiza en la figura 4.39.



Figura 4.38: Inicio del Cisco IP Communicator.

Elaborado por: Investigador

En la figura 4.39 se puede observar los tres teléfonos que fueron configurados, para el presente trabajo de investigación se creó tres teléfonos uno para el nodo matriz, EDPuyo y Tena, cada uno de ellos instalados en una máquina virtual, configurados como cliente final.



Figura 4.39 Teléfonos instalados en nodo Matriz, EDPuyo y Tena.

Elaborado por: Investigador

4.7.3 Configuración de *Call Manager* en Router Matriz

A continuación se detalla la configuración que se realizó en el router Matriz don se describe de líneas máximas que se tendrá así como la cantidad máxima de teléfonos, los comandos se pueden visualizar a continuación.

```
MATRIZ#conf terminal
```

```
MATRIZ(config)#telephony-service /Modo de configuración de teléfonos
```

```
MATRIZ(config-telephony)#max-ephones 50/ Cantidad máxima de teléfonos
```

```
MATRIZ(config-telephony)#max-dn 50/ Cantidad máxima de líneas
```

```
MATRIZ(config-telephony)#create cnf-files/ Archivo de configuración de teléfonos
```

```
MATRIZ(config-telephony)#exit
```

```
MATRIZ(config)#ephone-dn 1 dual-line / Creación de línea doble
```

```
MATRIZ(config-ephone-dn)#number 101 / Creación de numero de extensión
```

```
MATRIZ(config-ephone-dn)#name Matriz / Creación de nombre de usuario
```

```
MATRIZ(config-ephone-dn)#label Matriz / Creación de extensión para visualizar en pantalla
```

```
MATRIZ(config-ephone-dn)#exit
```

```
MATRIZ(config)#ephone 1 /Creación de telefono
```

```
MATRIZ(config-ephone)#mac-address 000C.297C.60B9/ Asociar el teléfono con dirección MAC
```

```
MATRIZ(config-ephone)#codec g711ulaw / Codec para tráfico de voz
```

```
MATRIZ(config-ephone)#exit
```

```
MATRIZ(config)#ephone 1
```

```
MATRIZ(config-ephone)#button 1:1 / Asociación de línea telefónica: línea
```

```
MATRIZ(config-ephone)#reset / Resetear el teléfono y cargar nueva configuración
```

```
MATRIZ(config-ephone)#exit
```

4.7.4 Servidor Video

VLC es sin duda es el mejor reproductor multimedia que existe. Además funciona como servidor para la distribución de video en una red, reproduce casi todo tipo de vídeo y archivos de audio de forma nativa a través de redes que utilizan una gran cantidad de protocolos, puede ser controlado remotamente a través de un navegador web y mucho más. Por tal motivo se eligió este software para la generación de tráfico de video a través de la red simulada en la red MAN de EEASA.

Como se detalla en la tabla 4.15 la configuración de los equipos con políticas de calidad de servicio están distribuidos de la siguiente manera, Best Effort corresponderá al nombre AF11, Bronce a AF12, Plata a dos clases AF21 y AF22, la clase Oro toma el nombre de AF31 y finalmente la clase Premium corresponde a AF32, estas políticas se aplicaran en los equipos tanto routers como en los switches.

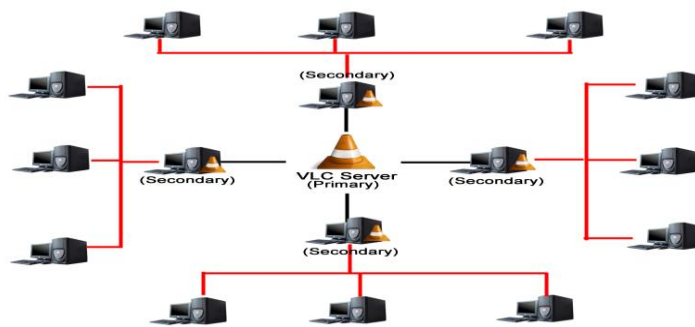


Figura 4.40 VLC actúa como servidor de Video

Elaborado por: Investigador

Existen tres pasos para la configuración de calidad de servicio, a continuación se detalla cada uno de ellos.

4.7.5 Configuración de Lista de Acceso ACLs

El primer paso para la implantación de calidad de servicio (QoS) es identificar el tráfico y clasificar los paquetes, para esto se hace uso de ACLs el cual permite configurar la clasificación del tráfico creando clases de tráfico.

En la figura 4.41 se puede visualizar la configuración realizada en el router matriz donde se clasifica el tráfico circulante en la red MAN provenientes tanto de los enlace de fibra optica como el inalámbrico generados en el simulador.

```

172.20.61.1 - PuTTY
MATRIZ (config)#ip access-list extended MULTIMEDIA-CONFERENCIA
MATRIZ (config-ext-nacl)#permit UDP any any range 16384 32767
MATRIZ (config-ext-nacl)#exit
MATRIZ (config)#ip access-list extended TRANSACCION-DATOS
MATRIZ (config-ext-nacl)#permit tcp any any eq 443
MATRIZ (config-ext-nacl)#permit tcp any any eq 1521
MATRIZ (config-ext-nacl)#permit udp any any eq 1521
MATRIZ (config-ext-nacl)#permit icmp any host 192.168.0.10
MATRIZ (config-ext-nacl)#permit tcp any host 192.168.0.10 eq www
MATRIZ (config-ext-nacl)#exit
MATRIZ (config)#ip access-list extended DATOS
MATRIZ (config-ext-nacl)#permit tcp any any range 20 21
MATRIZ (config-ext-nacl)#permit tcp any any eq ftp-data
MATRIZ (config-ext-nacl)#remark SSH/SFTP
MATRIZ (config-ext-nacl)#permit tcp any any eq 22
MATRIZ (config-ext-nacl)#permit tcp any any eq 25
MATRIZ (config-ext-nacl)#exit
MATRIZ (config)#ip access-list extended VoIP-CONTROL
MATRIZ (config-ext-nacl)#permit tcp any any range 2000 2002
MATRIZ (config-ext-nacl)#permit udp any any range 5060 5061
MATRIZ (config-ext-nacl)#permit tcp any any range 5060 5061
MATRIZ (config-ext-nacl)#exit
MATRIZ (config)#ip access-list extended MULTIMEDIA-CONFERENCIA
MATRIZ (config-ext-nacl)#permit tcp any any range 16384 32767
MATRIZ (config-ext-nacl)#exit

```

Figura 4.41 Configuración de ACLs

Elaborado por: Investigador

Como se puede apreciar en la figura 4.41 se detalla la creación de las Listad de Control de Acceso, que permite clasificar el tráfico tanto de origen como destino, así como los puertos que usan las diferentes aplicaciones en cada conexión, también hay que tomar en cuenta que el tráfico se lo puede clasificar por protocolos, puerto, por host y por red.

El comando para crear una lista de acceso extendida donde MULTIMEDIA-CONFERENCIA es el nombre de la lista de acceso

```
MATRIZ(config)#ip access-list extended MULTIMEDIA-CONFERENCIA
```

A continuación se configura el permiso para los equipos donde se configure el protocolo, en este caso *any* significa cualquier origen, y el otro *any* significa cualquier destino y por último los puertos destino en este caso se utilizó un rango de puertos

```
MATRIZ(config-ext-nacl)#permit UDP any any range 16384 32767  
MATRIZ(config-ext-nacl)#permit tcp any any range 16384 32767
```

4.7.6 Marcado y clasificación del tráfico en el router

El segundo paso se define que pasara con el tráfico clasificado; es decir es la construcción real de una política de calidad de servicio. Los comandos utilizados se detallan a continuación.

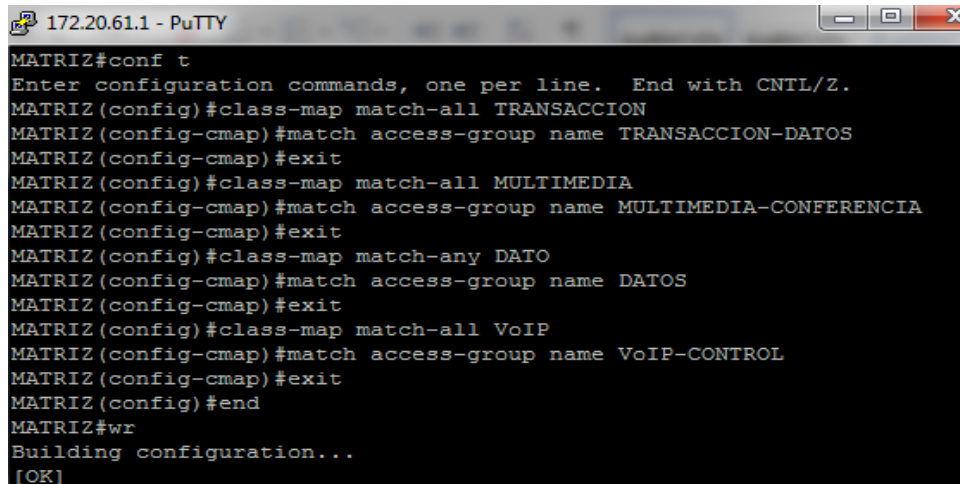
El comando *class-map match-all* crea la clase TRANSACCION, el cual indica que toda la clase debe cumplir todos los parámetros que estén en la lista de acceso para asignar a esta clase los paquetes.

```
MATRIZ(config)#class-map match-all TRANSACCION
```

Con esta configuración se realiza el enlace entre la lista de acceso y clases creadas.

```
MATRIZ(config-cmap)#match access-group name TRANSACCION-DATOS
```

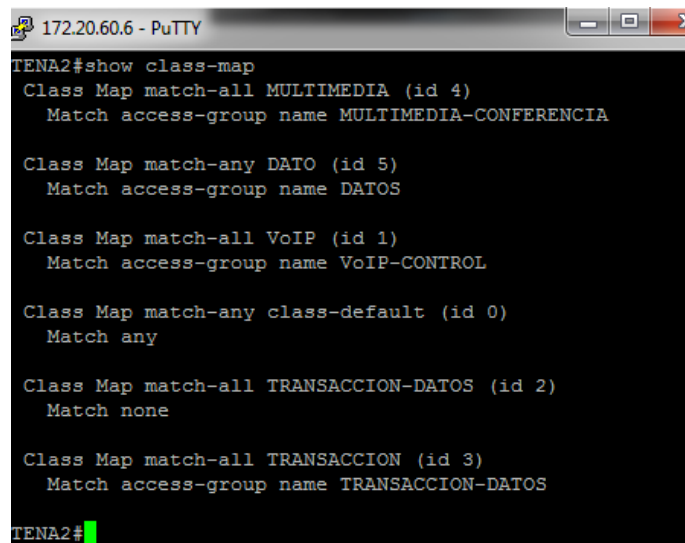
A continuación se visualiza en la figura 4.42 la configuración realizada en el router Matriz para crear las clases.



```
172.20.61.1 - PuTTY
MATRIZ#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MATRIZ(config)#class-map match-all TRANSACCION
MATRIZ(config-cmap)#match access-group name TRANSACCION-DATOS
MATRIZ(config-cmap)#exit
MATRIZ(config)#class-map match-all MULTIMEDIA
MATRIZ(config-cmap)#match access-group name MULTIMEDIA-CONFERENCIA
MATRIZ(config-cmap)#exit
MATRIZ(config)#class-map match-any DATO
MATRIZ(config-cmap)#match access-group name DATOS
MATRIZ(config-cmap)#exit
MATRIZ(config)#class-map match-all VoIP
MATRIZ(config-cmap)#match access-group name VoIP-CONTROL
MATRIZ(config-cmap)#exit
MATRIZ(config)#end
MATRIZ#wr
Building configuration...
[OK]
```

Figura 4.42 Configuración de Clases
Elaborado por: Investigador

Para visualizar las clases creadas se utiliza el comando *Show Class-map*, como se muestra en la figura 4.43



```
172.20.60.6 - PuTTY
TENA2#show class-map
Class Map match-all MULTIMEDIA (id 4)
  Match access-group name MULTIMEDIA-CONFERENCIA

Class Map match-any DATO (id 5)
  Match access-group name DATOS

Class Map match-all VoIP (id 1)
  Match access-group name VoIP-CONTROL

Class Map match-any class-default (id 0)
  Match any

Class Map match-all TRANSACCION-DATOS (id 2)
  Match none

Class Map match-all TRANSACCION (id 3)
  Match access-group name TRANSACCION-DATOS
TENA2#
```

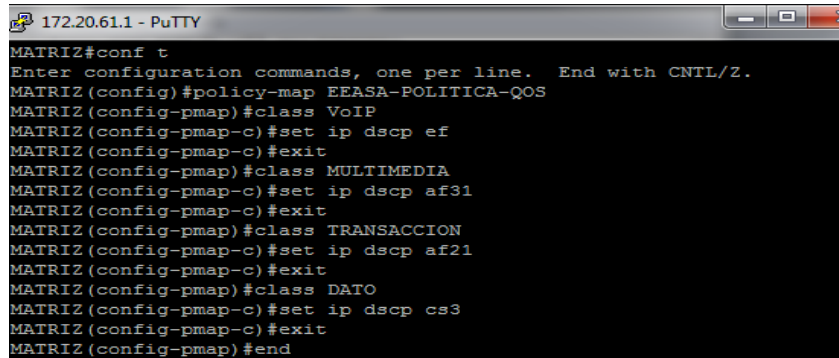
Figura 4.43 Verificación de Clases creadas
Elaborado por: Investigador

4.7.7 Creación de la política

Este es el tercer paso donde se aplicara la política, es decir, las interfaces o sub-interfaces deseadas, en este paso se aplicara la política de tránsito para el tráfico entrante o saliente en las interfaces, sub-interfaces, o circuitos virtuales utilizando el comando de la política.

Una vez que los paquetes están clasificados se someten a ciertas reglas que son especificadas dentro de una política a la entrada por el router.

En la gráfica 4.44 se visualiza la creación de las políticas que permitirán marcar cada paquete con un valor de DSCP y asignarle cierto porcentaje de ancho de banda dependiendo de la clase a la cual pertenece. Finalmente para verificar las políticas creadas se utiliza el comando *Show policy-map* como se muestra en la figura 4.45



```
MATRIZ#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MATRIZ (config)#policy-map EEASA-POLITICA-QOS
MATRIZ (config-pmap)#class VoIP
MATRIZ (config-pmap-c)#set ip dscp ef
MATRIZ (config-pmap-c)#exit
MATRIZ (config-pmap)#class MULTIMEDIA
MATRIZ (config-pmap-c)#set ip dscp af31
MATRIZ (config-pmap-c)#exit
MATRIZ (config-pmap)#class TRANSACCION
MATRIZ (config-pmap-c)#set ip dscp af21
MATRIZ (config-pmap-c)#exit
MATRIZ (config-pmap)#class DATO
MATRIZ (config-pmap-c)#set ip dscp cs3
MATRIZ (config-pmap-c)#exit
MATRIZ (config-pmap)#end
```

Figura 4.44 Configuración de Políticas
Elaborado por: Investigador

Con este comando se crea la política EEASA-POLITICA-QOS-S

```
MATRIZ(config)#policy-map EEASA-POLITICA-QOS-S
```

Se crea la clase

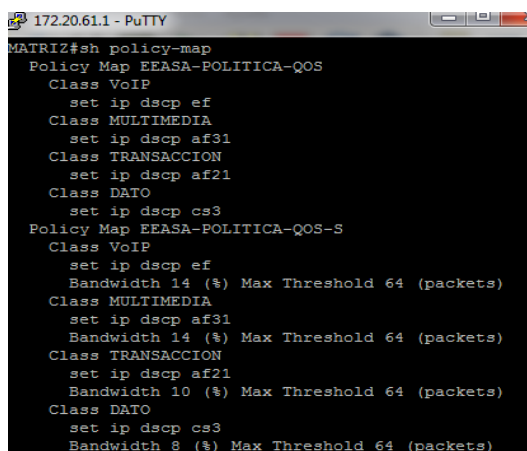
```
MATRIZ(config-pmap)#class VoIP
```

Se marca al paquete con el DSCP que pertenece a la clase creada.

```
MATRIZ(config-pmap-c)#set ip dscp ef
```

Se asigna la política al paquete

```
MATRIZ(config-pmap-c)#bandwidth percent 14
```



```
MATRIZ#sh policy-map
Policy Map EEASA-POLITICA-QOS
  Class VoIP
    set ip dscp ef
    Bandwidth 14 (%) Max Threshold 64 (packets)
  Class MULTIMEDIA
    set ip dscp af31
    Bandwidth 14 (%) Max Threshold 64 (packets)
  Class TRANSACCION
    set ip dscp af21
    Bandwidth 10 (%) Max Threshold 64 (packets)
Policy Map EEASA-POLITICA-QOS-S
  Class VoIP
    set ip dscp ef
    Bandwidth 14 (%) Max Threshold 64 (packets)
  Class MULTIMEDIA
    set ip dscp af31
    Bandwidth 14 (%) Max Threshold 64 (packets)
  Class TRANSACCION
    set ip dscp af21
    Bandwidth 10 (%) Max Threshold 64 (packets)
  Class DATO
    set ip dscp cs3
    Bandwidth 8 (%) Max Threshold 64 (packets)
```

Figura 4.45 Verificación de Políticas Creadas
Elaborado por: Investigador

```

172.20.61.1 - PuTTY
Service-policy input: EEASA-POLITICA-QOS

Class-map: VoIP (match-all)
0 packets, 0 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: access-group name VoIP-CONTROL
QoS Set
dscp ef
Packets marked 0

Class-map: MULTIMEDIA (match-all)
0 packets, 0 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: access-group name MULTIMEDIA-CONFERENCIA
QoS Set
dscp af31
Packets marked 0

Class-map: TRANSACCION (match-all)
0 packets, 0 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: access-group name TRANSACCION-DATOS
QoS Set
dscp af21
Packets marked 0

Class-map: DATO (match-any)
0 packets, 0 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: access-group name DATOS
0 packets, 0 bytes
5 minute rate 0 bps
QoS Set
dscp cs3
Packets marked 0

Class-map: class-default (match-any)
492 packets, 45264 bytes
5 minute offered rate 1000 bps, drop rate 0 bps
Match: any

172.20.61.1 - PuTTY
Service-policy output: EEASA-POLITICA-QOS-S

Class-map: VoIP (match-all)
0 packets, 0 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: access-group name VoIP-CONTROL
QoS Set
dscp ef
Packets marked 0
Queueing
Output Queue: Conversation 265
Bandwidth 14 ($)
Bandwidth 1400 (kbps)Max Threshold 64 (packets)
(pkts matched/bytes matched) 0/0
(depth/total drops/no-buffer drops) 0/0/0

Class-map: MULTIMEDIA (match-all)
0 packets, 0 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: access-group name MULTIMEDIA-CONFERENCIA
QoS Set
dscp af31
Packets marked 0
Queueing
Output Queue: Conversation 266
Bandwidth 14 ($)
Bandwidth 1400 (kbps)Max Threshold 64 (packets)
(pkts matched/bytes matched) 0/0
(depth/total drops/no-buffer drops) 0/0/0

Class-map: TRANSACCION (match-all)
0 packets, 0 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: access-group name TRANSACCION-DATOS
QoS Set
dscp af21
Packets marked 0
Queueing
Output Queue: Conversation 267
Bandwidth 10 ($)
Bandwidth 1000 (kbps)Max Threshold 64 (packets)
(pkts matched/bytes matched) 0/0
(depth/total drops/no-buffer drops) 0/0/0

Class-map: DATO (match-any)
0 packets, 0 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: access-group name DATOS
0 packets, 0 bytes
5 minute rate 0 bps
QoS Set
dscp cs3

```

Figura 4.46 Verificación de Políticas output e input

Elaborado por: Investigador

4.7.8 Asignación de la política a la interfaz de entrada

La política es aplicada a la interfaz f0/1 al ingreso a la red de la siguiente manera:

```

172.20.61.1 - PuTTY
MATRIZ#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MATRIZ (config)#fas
MATRIZ (config)#int
MATRIZ (config)#interface fas
MATRIZ (config)#interface fastEthernet 0/1
MATRIZ (config-if)#service-policy output EEASA-POLITICA-QOS
MATRIZ (config-if)#service-policy input EEASA-POLITICA-QOS
MATRIZ (config-if)#exit
MATRIZ (config)#interface fastEthernet 0/0
MATRIZ (config-if)#service-policy output EEASA-POLITICA-QOS
MATRIZ (config-if)#exit
MATRIZ (config)#interface se
MATRIZ (config)#interface serial 0/0
MATRIZ (config-if)#service-policy output EEASA-POLITICA-QOS
MATRIZ (config-if)#exit
MATRIZ (config)#^Z
MATRIZ#wr
Building configuration...
[OK]

```

Figura 4.47 Asignación de políticas a interfaces

Elaborado por: Investigador

Configuración del Switches 2960

Para el caso del switch 2960 se utilizó la imagen IOS del switch 2960-24TT-L Versión 15.0 (2) SE5, se habilitó el MQOC de Cisco que permite toda la configuración de QoS.

Los switches que conforman la red MAN de EEASA envían y reciben tráfico pre-marcado, por tal motivo la función son los de agrupar los paquetes y encolarlos de acuerdo al DSCP marcado y enviarlos al siguiente nodo. De la misma manera se tomó la configuración realizada de uno de los switches en este caso se tomó la de la matriz.

```
Switch(config)# mls qos
Switch(config)# exit
Switch(config)# mls qos map policed-dscp 10 to 8 // Mapa para remarcar tráfico
Switch(config)# mls qos map cos-dscp 0 8 10 24 32 46 48 50 // Asigna mapeo Cos a código DSCP

SWMATRIZ(config)#class-map match-all TRANSACCION // Creación de Clases para identificar el Flujo
SWMATRIZ(config-cmap)#match dscp af21
SWMATRIZ(config-cmap)#exit

SWMATRIZ(config)#class-map match-all VoIP
SWMATRIZ(config-cmap)#match dscp ef
SWMATRIZ(config-cmap)#exit

SWMATRIZ(config)#class-map match-any DATO
SWMATRIZ(config-cmap)#match dscp cs3
SWMATRIZ(config-cmap)#exit

SWMATRIZ(config)#class-map match-all MULTIMEDIA
SWMATRIZ(config-cmap)#match dscp af31
SWMATRIZ(config-cmap)#exit

SWMATRIZ(config)#policy-map EEASA-POLITICA-QOS-S //Creación de mapa política
SWMATRIZ(config-pmap)#class VoIP
SWMATRIZ(config-pmap-c)#set ip dscp ef
SWMATRIZ(config-pmap-c)#bandwidth percent 14
SWMATRIZ(config-pmap-c)#exit

SWMATRIZ(config-pmap)#class MULTIMEDIA
SWMATRIZ(config-pmap-c)#set ip dscp af31
SWMATRIZ(config-pmap-c)#bandwidth percent 14
SWMATRIZ(config-pmap-c)#EXIT

SWMATRIZ(config-pmap)#class TRANSACCION
SWMATRIZ(config-pmap-c)#set ip dscp af21
SWMATRIZ(config-pmap-c)#bandwidth percent 10
SWMATRIZ(config-pmap-c)#exit

SWMATRIZ(config-pmap)#class DATO
SWMATRIZ(config-pmap-c)#set ip dscp cs3
SWMATRIZ(config-pmap-c)#bandwidth percent 8
SWMATRIZ(config-pmap-c)#exit
SWMATRIZ(config-pmap)#end
```

Configuración de Cola de Ingreso (Ingress Queueing)

Mapeo de ingreso DSCP-Queue permite a que los valores DSCP se asignen a cada cola de ingreso.

```
SWMATRIZ(config)# mls qos srr-queue input dscp-map queue 1 threshold 1 0 1 2 3 4 5 6
SWMATRIZ(config)# mls qos srr-queue input dscp-map queue 1 threshold 2 20 21 22 23 24 25 26
SWMATRIZ(config)# mls qos srr-queue input threshold 1 50 70
```

Se configura el buffer a cada cola, la suma de del porcentaje debe ser 100.

```
Switch(config)# mls qos srr-queue input buffers 60 40
```

De la misma manera se realiza la configuración del ancho de banda a cada cola, la sumatoria de estos porcentajes asignados deben ser 100.

```
Switch(config)# mls qos srr-queue input bandwidth 25 75
```

Esta configuración indica a la interfaz que la cola 1 será prioritaria con un ancho de banda garantizado de 10 %.

```
Switch(config)# mls qos srr-queue input priority-queue 1 bandwidth 10
Switch(config)# mls qos srr-queue input bandwidth 4 4
```

Configuración de Cola de Egreso (Egress Queueing)

Mapeo de egreso DSCP-Queue, se lo realiza de la misma manera que la cola de entrada son las mismas condiciones asignando valores DSCP a cada cola de salida.

```
Switch(config)# mls qos srr-queue output dscp-map queue 1 threshold 2 10 11
```

Se configure la salida de la cola y se ajusta el umbral de egreso

```
SWMATRIZ(config)# mls qos queue-set output 1 buffers 40 20 20 20
SWMATRIZ(config)# mls qos queue-set output 1 threshold 2 40 60 100 200
```

Se aplica la cola de egreso en la interfaz correspondiente con los comandos especificados.

```
SWMATRIZ(config)# interface gigabitethernet1/0/1
SWMATRIZ(config-if)# queue-set 2
Switch(config-if)# srr-queue bandwidth share 30 20 25 25
Switch(config-if)# priority-queue out
Switch(config-if)# end
```


4.8 Análisis de Resultados en simulador GNS3

Se procede a realizar el análisis estadístico del funcionamiento e impactos que genera la implementación de calidad de servicio (QoS) en la red MAN de EEASA, simulado en GNS3. Para realizar el análisis de las políticas de QoS implementadas en el simulador, se muestra capturas de la configuración de cada equipo y de los resultados que presenta cada uno de ellos, esto demuestra el correcto funcionamiento de QoS en los Routers y Swiches.

En la figura 4.49 se muestra el esquema utilizado para la generación de tráfico real, para posteriormente aplicar a la red simulada en GNS3.

En el computador PC se encuentra la aplicación GNS3, el cual permite la simulación de la red MAN de EEASA, además en este equipo se instaló una máquina virtual con Windows XP que a su vez es uno de los cliente telefónicos del nodo Matriz, también a este equipo se le asignó para que trabaje como servidor Video y Archivos.

En el portátil se instaló dos máquinas virtuales uno con Windows XP y otro con Windows Vista, cada uno de ellos tiene la función de trabajar como cliente telefónico, que estarán conectados a los routers ED Puyo y Tena respectivamente. Cabe indicar que en cada uno de estas máquinas virtuales se instaló VLC para efectuar la simulación de Video Streaming.



Figura 4.48: Prototipo basado en simuladores de red y generador de tráfico real.

Elaborado por: Investigador

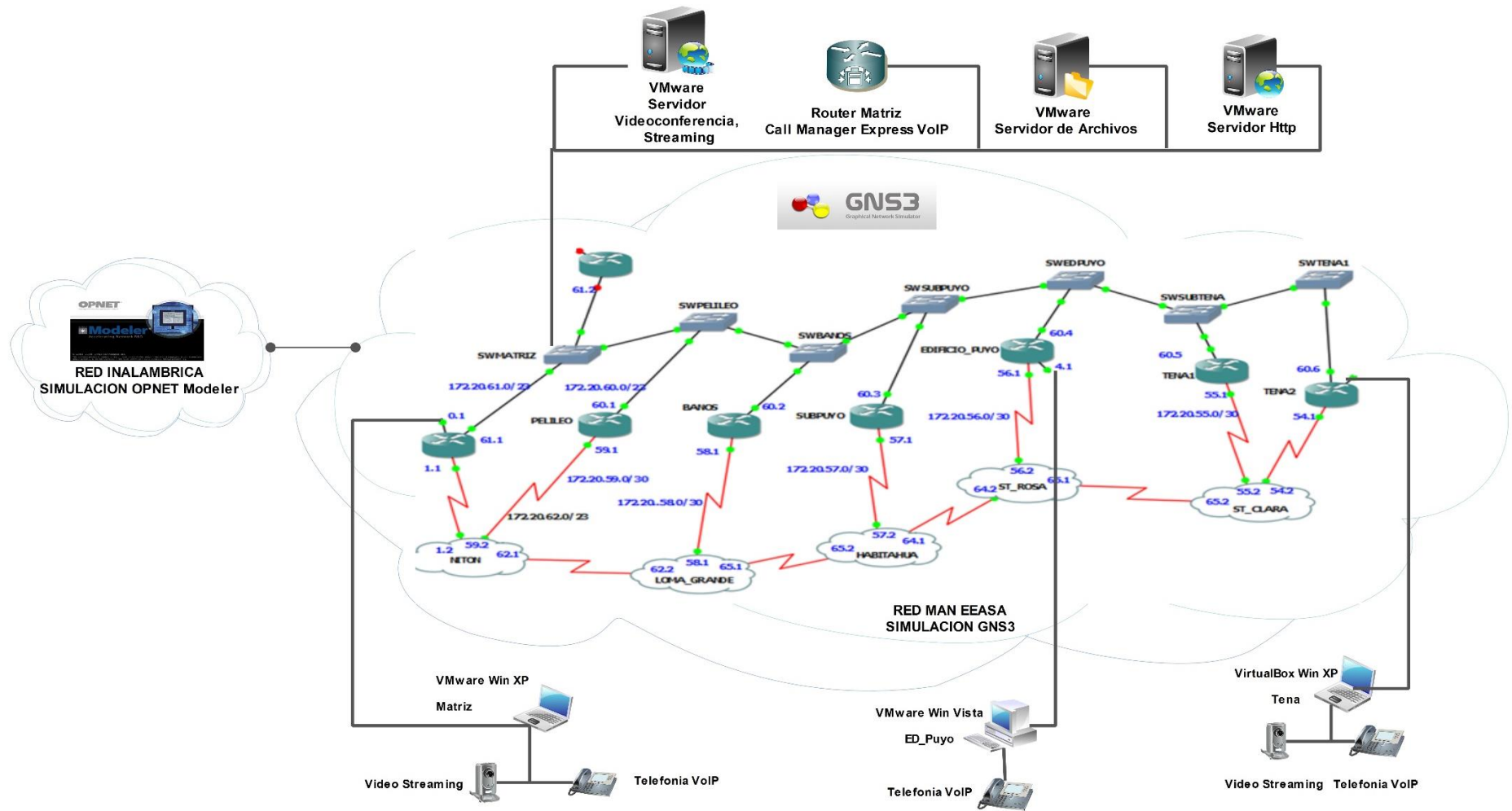


Figura 4.49 Esquema utilizado para sección de Pruebas

Elaborado por: Investigador

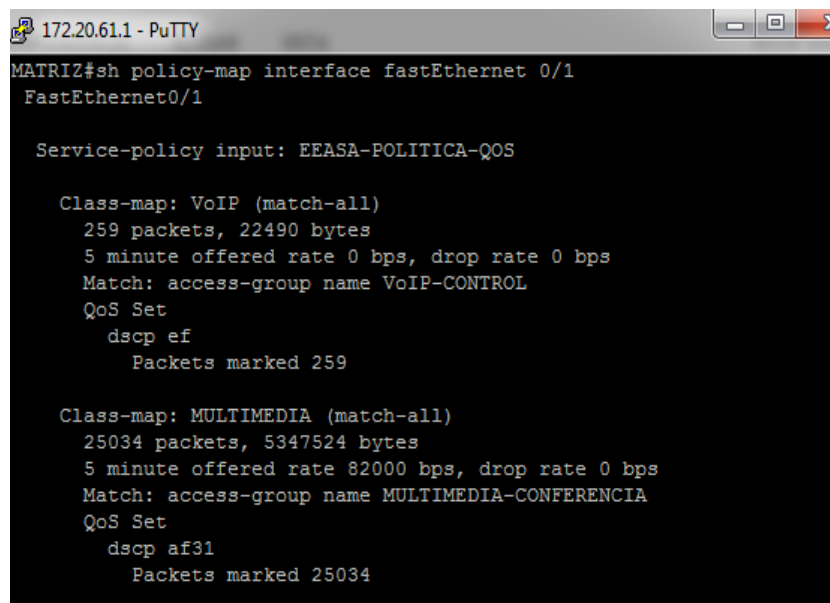
4.8.1 Clasificación y marcado de paquetes en el router Matriz de la red MAN de EEASA.

En la anterior sección se realizó la configuración de la clasificación, marcado y asignación de políticas a los paquetes que ingresen y salgan del router, en las siguientes figuras se puede apreciar el funcionamiento de dichas configuraciones realizadas en cada router de la red.

En la figura 4.50 se muestra las estadísticas del marcado de paquetes en la clase VoIP, que está configurado en la interfaz del router Matriz con una política QoS de entrada de paquetes, en esta se puede visualizar el valor DSCP asignado que es EF (Expedited Forwarding) y el número de paquetes que son marcados, en este caso 259 paquetes fueron marcados con un tráfico de 22490 bytes.

En la clase MULTIMEDIA también se aprecia el valor DSCP con el que esta clase trabaja, en este caso af31 con un número de paquetes marcados de 25034.

En base a estas estadísticas se puede verificar que el router está aplicando Calidad de servicio (QoS), dependiendo del tipo de tráfico que circule por el router.



```
172.20.61.1 - PuTTY
MATRIZ#sh policy-map interface fastEthernet 0/1
FastEthernet0/1

Service-policy input: EEASA-POLITICA-QOS

Class-map: VoIP (match-all)
 259 packets, 22490 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
Match: access-group name VoIP-CONTROL
QoS Set
  dscp ef
  Packets marked 259

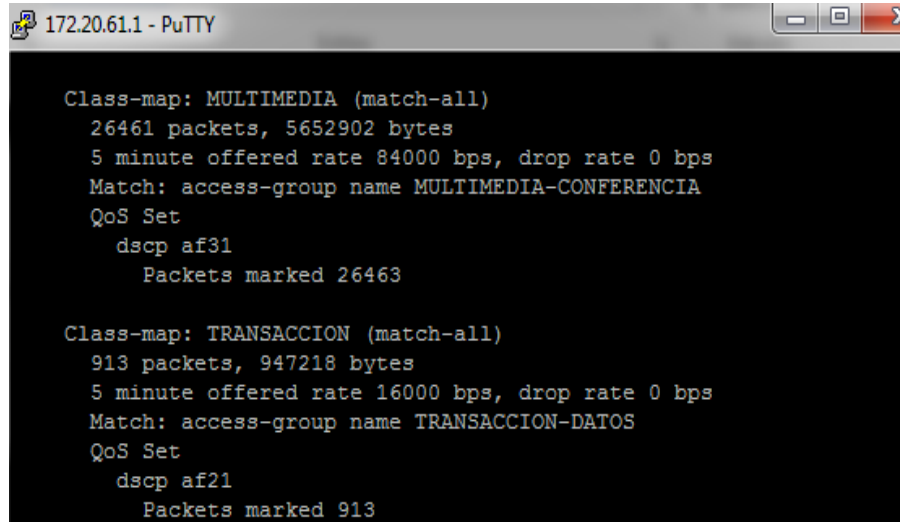
Class-map: MULTIMEDIA (match-all)
25034 packets, 5347524 bytes
 5 minute offered rate 82000 bps, drop rate 0 bps
Match: access-group name MULTIMEDIA-CONFERENCIA
QoS Set
  dscp af31
  Packets marked 25034
```

Figura 4.50 Verificación de tráfico marcado

Elaborado por: Investigador

En la figura 4.51 se muestra las estadísticas del marcado de paquetes de la clase TRANSACCION, que están entrando a la interfaz del router matriz, se observa que este

tipo de tráfico se le asigna un valor DSCP de af21, con un numero de paquetes marcados de 913, para este tipo de tráfico la política de QoS está aplicando un ancho de banda de 16000bps, dependiendo del tráfico que se esté generando.



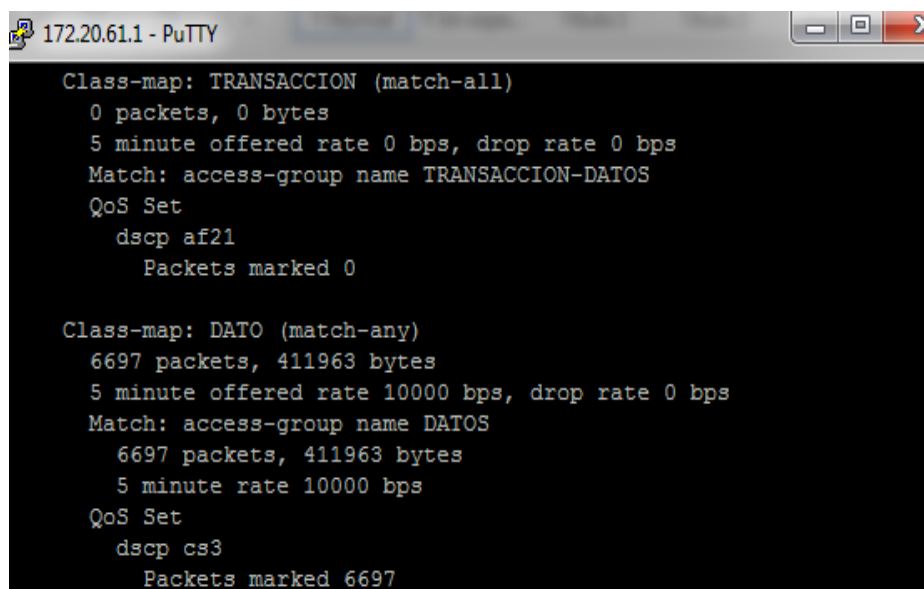
```
172.20.61.1 - PuTTY
Class-map: MULTIMEDIA (match-all)
 26461 packets, 5652902 bytes
 5 minute offered rate 84000 bps, drop rate 0 bps
Match: access-group name MULTIMEDIA-CONFERENCIA
QoS Set
  dscp af31
    Packets marked 26463

Class-map: TRANSACCION (match-all)
 913 packets, 947218 bytes
 5 minute offered rate 16000 bps, drop rate 0 bps
Match: access-group name TRANSACCION-DATOS
QoS Set
  dscp af21
    Packets marked 913
```

Figura 4.51 Verificación de tráfico marcado en Multimedia

Elaborado por: Investigador

En la figura 4.52 se observa la estadística del marcado de paquetes de la clase DATOS que está entrando en las interfaces del router matriz, se puede visualizar que a este tipo de tráfico se le asigna un valor DSCP cs3, y que no existe un descarte de paquetes.



```
172.20.61.1 - PuTTY
Class-map: TRANSACCION (match-all)
 0 packets, 0 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
Match: access-group name TRANSACCION-DATOS
QoS Set
  dscp af21
    Packets marked 0

Class-map: DATO (match-any)
 6697 packets, 411963 bytes
 5 minute offered rate 10000 bps, drop rate 0 bps
Match: access-group name DATOS
 6697 packets, 411963 bytes
 5 minute rate 10000 bps
QoS Set
  dscp cs3
    Packets marked 6697
```

Figura 4.52 Verificación de tráfico marcado en Dato

Elaborado por: Investigador

4.8.2 Análisis de rendimiento de la red simulado en GNS3

Para realizar el análisis del rendimiento de la red se realizaron pruebas con aplicaciones que permitan evaluar el rendimiento de la red, las pruebas se realizaron en escenarios en la cual la red no tenía aplicado QoS y luego aplicado QoS.

Las aplicaciones para las pruebas fueron la de video streaming, el cual permite observar de forma gráfica el rendimiento de la red basándose en la calidad de imagen, voz y cuadros del video recibido.

La aplicación de VoIP configurado en tres router (Matriz, EDPuyo y Tena2), que permite evaluar el rendimiento de la red con tráfico de voz y verificando la calidad de transmisión.

Transferencia de archivos snmp y ftp lo cual permitirá determinar la velocidad de transferencia de un archivo dependiendo de la política de QoS aplicada.

Ping para evaluar la conectividad y tiempo de respuesta del enlace de un punto a otro con saturación de canal.

Para realizar las pruebas en la red sin QoS se generó tráfico de voz, video, transferencia de archivos y ping extendido al mismo tiempo.

Para el análisis del rendimiento de la red se generó video streaming entre dos usuarios en este caso entre EDPuyo y Teana2 utilizando el servidor VLC, se realizó llamada telefónica entre Matriz, Puyo y Tena, se descarga un archivo 700Mbyte aproximadamente y se genera un ping extendido de 10000 bytes.

Aplicaciones sin políticas de calidad de servicio (QoS)

Se realizó pruebas de video streaming sin aplicar calidad de servicio (QoS), en la figura 4.53 se puede apreciar que la calidad de video se presenta pixelado y presenta retardos en la imagen debido a que se genera pérdida de paquetes, la pérdida de paquetes se debe a que el canal presenta congestión al aplicar video y las demás aplicaciones consumen recursos de la red.

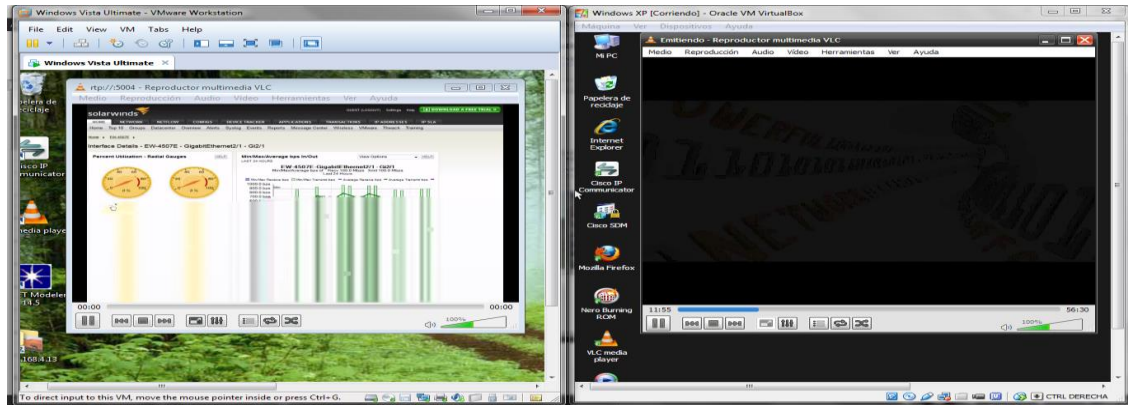


Figura 4.53 Ejecución de tráfico de video

Elaborado por: Investigador

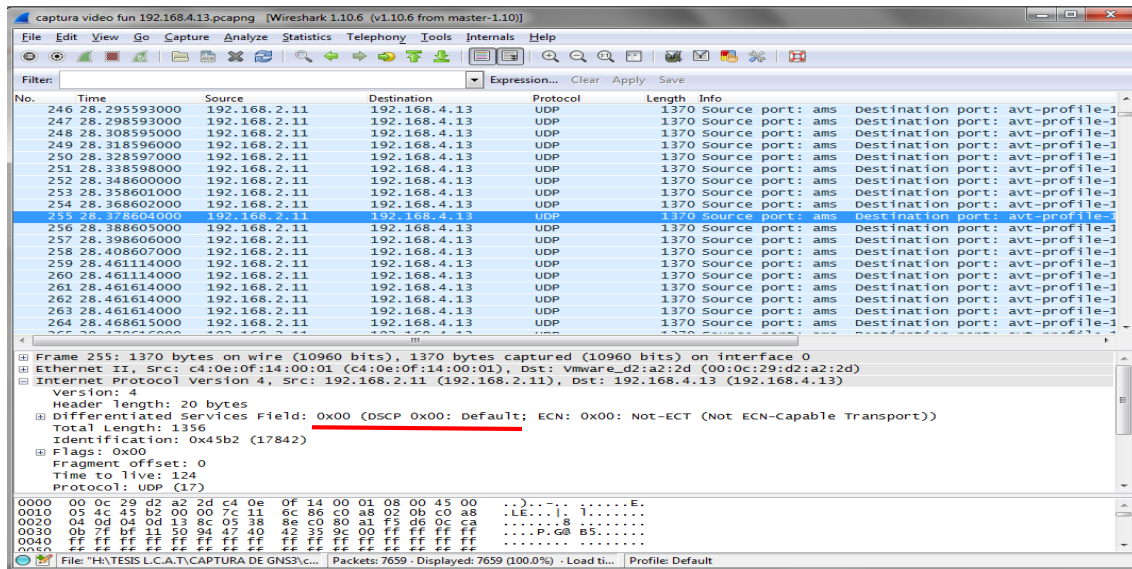
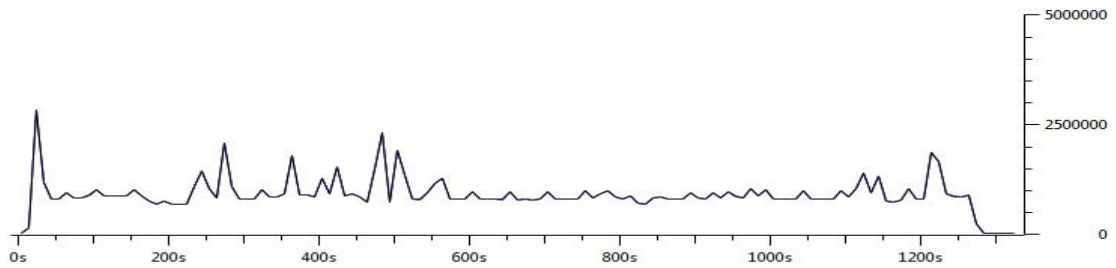


Figura 4.54: Verificación de Tráfico generado con Wireshark

Elaborado por: Investigador

Se puede visualizar en la figura 4.54 con la ayuda de Wireshark que el tráfico generado al enviar video streaming, que el protocolo UDP transmitido no está marcado y el tráfico que circula trata de llegar de la mejor manera hacia su destino en este caso hacia la sucursal EDPuyo.

Para el caso del tráfico de voz la importancia es más alta ya que el usuario desea siempre ser escuchado y que le escuchen en todo momento, y al no tener configurado QoS, este tipo de tráfico podría tener una falla en la red, generando saturación en el canal, y causando interrupciones o retardos en la comunicación.

Se realizaron pruebas aplicando VoIP, en la cual se realizó una conversación entre 3 teléfonos usando sofphone en la gráfica 4.55 se puede visualizar los paquetes perdidos y *jitter* obtenido después de realizar llamadas con duración aproximadamente de 8 minutos, enviando paquetes RTP con códec G711 PCM de 64 Kbps. Esta recopilación de estos datos se obtuvo gracias a las estadísticas de wireshark en donde se puede apreciar el retardo y el jitter que genera esta aplicación. Además se puede apreciar que se tiene un retardo de 660.51 ms y un jitter máximo de 43.90 ms generado en la sucursal Tena, mientras que en la sucursal Puyo presenta un retardo 2261.64 ms y un Jitter 311.66 ms, en esta prueba no se presentaron pérdidas de paquetes, pero los picos presentados en la sucursal Puyo presentan cortes en la voz al realizar las llamadas.

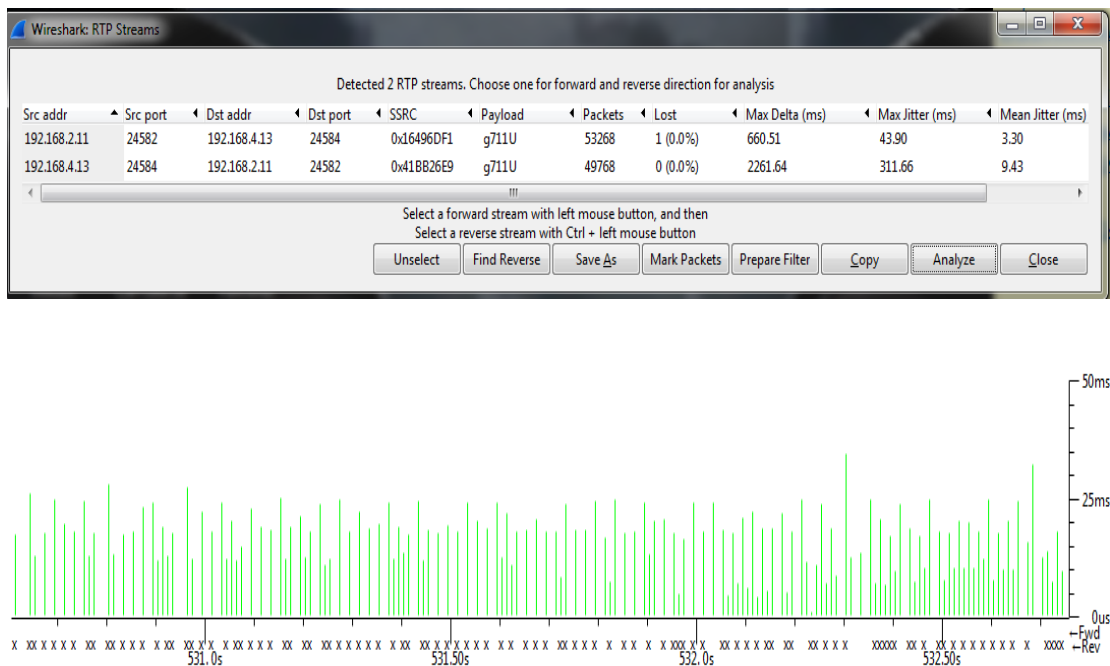


Figura 4.55 Verificación de Tráfico generado en VoIP

Elaborado por: Investigador

Para el tráfico FTP las intermitencias o tiempos en el canal pueden ser imperceptibles ya que con la política de mejor esfuerzo (BE), los paquetes pueden ser renviados y al final el usuario recibirá la información completa.

Se realizaron pruebas en la simulación en la cual se aplicó una transferencia de archivos, para este caso se descargó un archivo de 100Mbytes el cual se encuentra en el servidor de archivos, aproximadamente se puede visualizar que la velocidad de transferencia es mínima debido a que esta aplicación funciona con políticas de BE.



Figura 4.56 Tráfico generado al enviar información
Elaborado por: Investigador

En la figura 4.56 se puede observar que el tiempo de la descarga de un archivo desde el servidor 192.168.2.11 es aproximadamente 43 minutos esto debido a que este tipo de tráfico no tiene prioridad sobre la red, y el tráfico hace su mejor esfuerzo para llegar a su destino.

El tráfico icmp o ping es utilizado para realizar pruebas de conectividad entre dos puntos, permitiendo evidenciar si se presentan pérdidas de servicio, tiempos altos o intermitencia en un circuito de red. Para la comprobación de QoS se utiliza dos escenarios, en el primero no se aplica QoS y en el segundo se utiliza comandos extendidos para poder emular el tráfico de voz y garantizar un 100% de paquetes entregados a su destino.

En el primer escenario se realiza una prueba de ping extremo – extremo sin aplicar QoS en la interfaz. En la figura 4.57 se puede verificar un ping extendido entre dos de los clientes configurados, ya que la simulación depende la capacidad de la memoria del computador, se presentó una pérdida de paquetes.

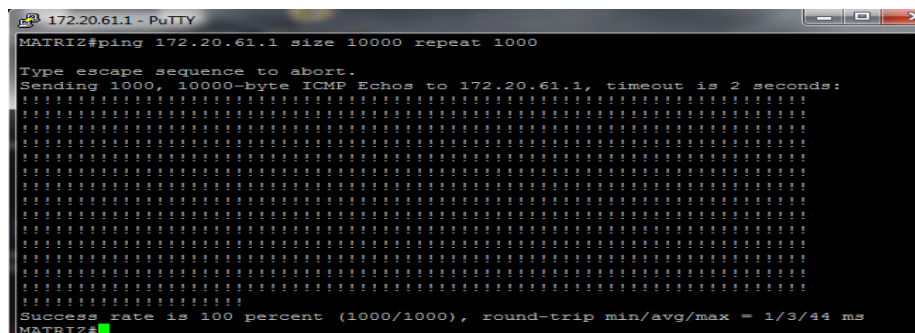


Figura 4.57 Tráfico generado por pin extendido
Elaborado por: Investigador

Aplicaciones con políticas de calidad de servicio (QoS)

En la figura 4.58 se puede apreciar que la aplicación de video streaming presenta mejoras en la calidad y fluidez de la imagen en comparación con las pruebas realizadas sin aplicar QoS mostradas en la figura 4.53. Se puede determinar que al implementar políticas de calidad de servicio QoS se logró reducir la pérdida de paquetes ya que cada equipo prioriza este tipo de tráfico por ser un servicio en tiempo real. La función que realiza cada router es clasificar, marcar, priorizar y aplicar políticas de salida QoS a este servicio.

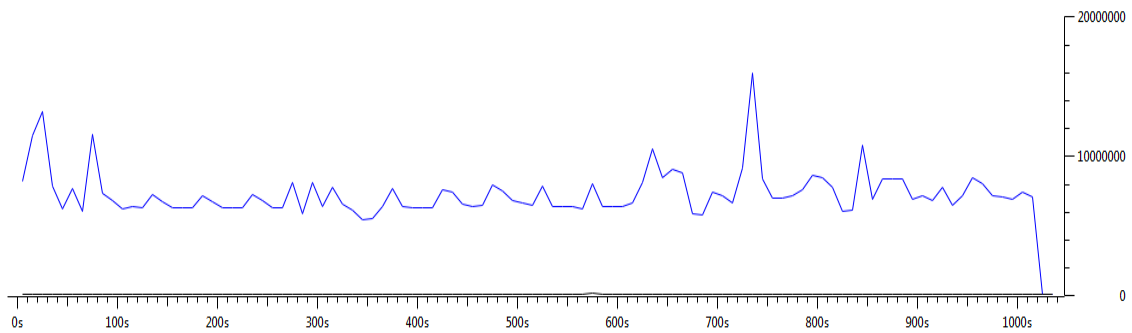
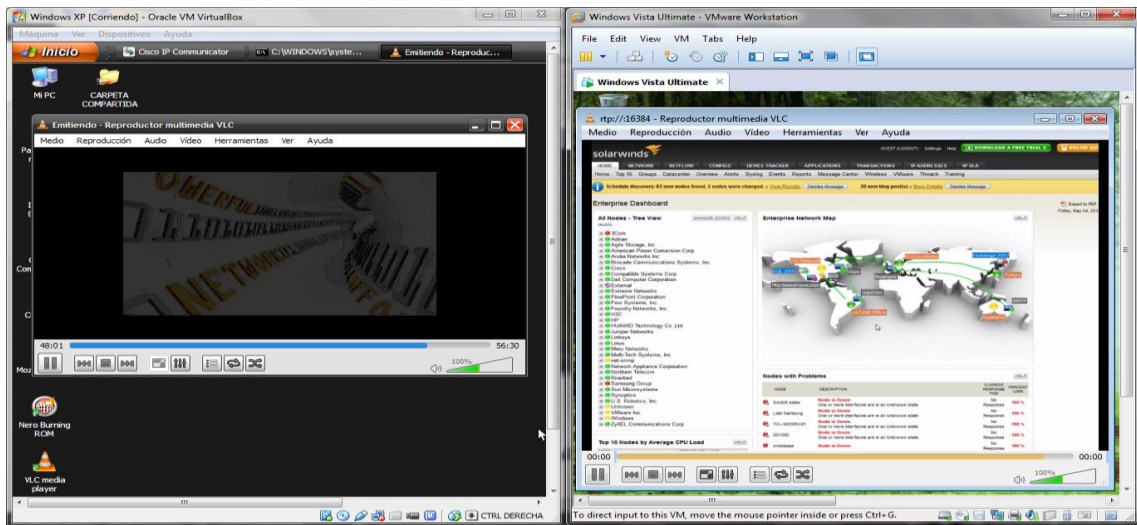


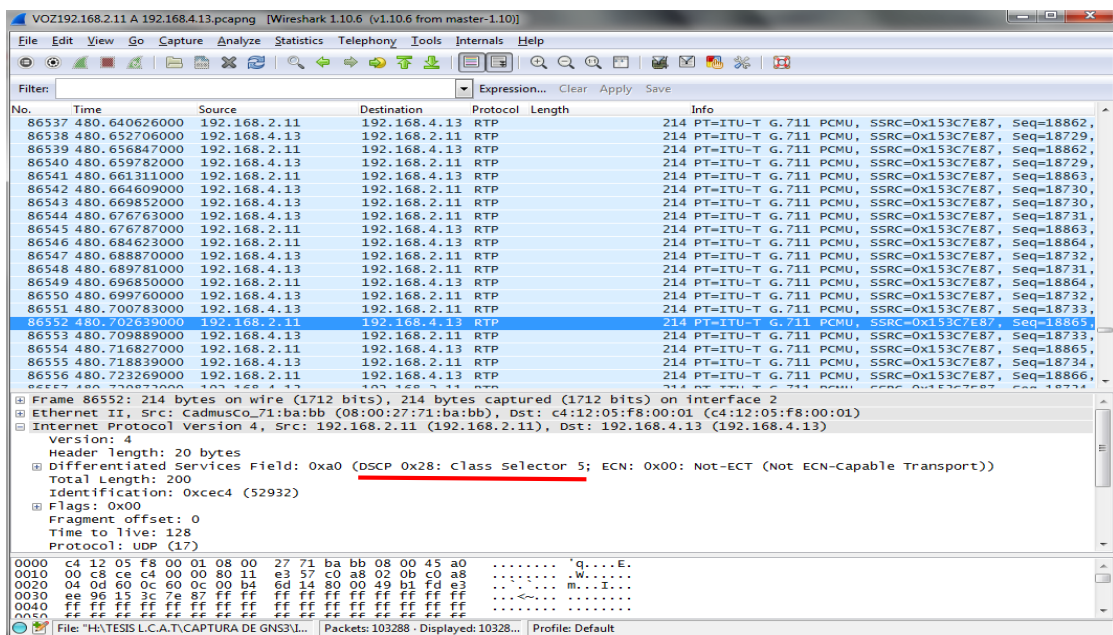
Figura 4.58 Tráfico generado por Video con QoS

Elaborado por: Investigador

En la figura 4.58 se observa el monitoreo del tráfico generado al aplicar políticas de QoS, el cual presenta pequeñas pico al transmitir el video en comparación con la gráfica 4.54, esto debido a que el tráfico es marcado, para posteriormente ser priorizado con un valor DSCP AF31 de acuerdo a los niveles de importancias que se asigna a aplicaciones en tiempo real.

Para el caso de la aplicación de voz se realizó la llamada desde un computador hacia el otro y se pudo evidenciar una comunicación eficaz, clara y sin cortes donde el jitter es bajo en comparación con las pruebas realizadas sin QoS como se aprecia en la figura 4.55 El análisis del tráfico se puede visualizar en la gráfica 4.59 la precedencia que recibe el tráfico rtp es de clase (5) para lograr una comunicación eficiente este es el marcado que cada equipo de comunicación da a este tipo de protocolo.

Como se observa en la figura 4.59 al aplicar calidad de servicio QoS en la aplicación de voz se puede apreciar que el retardo y jitter se reducen notablemente obteniendo valores de 23,94 ms como jitter máximo y con un retardo de 291 ms, estos valores son muy bajos en comparación con los valores obtenidos sin aplicar políticas de QoS. Puesto que no se puede eliminar el jitter se puede visualizar que este servicio opera bajo los parámetros permitidos el cual es de 150ms según la ITU. En la figura 4.59 se puede apreciar que el valor máximo del jitter es aproximadamente 9ms, lo que conlleva a determinar que este tipo de servicio tiene prioridad en la red simulada.



Wireshark: RTP Streams

Detected 6 RTP streams. Choose one for forward and reverse direction for analysis

| Src addr | Src port | Dst addr | Dst port | SSRC | Payload | Packets | Lost | Max Delta (ms) | Max Jitter (ms) | Mean Jitter (ms) |
|--------------|----------|--------------|----------|------------|---------|---------|----------|----------------|-----------------|------------------|
| 192.168.2.11 | 24584 | 192.168.4.13 | 24584 | 0x418B26E9 | g711U | 14056 | 1 (0.0%) | 81.34 | 7.10 | 3.28 |
| 192.168.2.11 | 24586 | 192.168.4.13 | 24586 | 0xB832EA6 | g711U | 292 | 0 (0.0%) | 49.97 | 5.70 | 3.57 |
| 192.168.2.11 | 24588 | 192.168.4.13 | 24588 | 0x153C7E87 | g711U | 36247 | 0 (0.0%) | 121.84 | 9.47 | 3.30 |
| 192.168.4.13 | 24584 | 192.168.2.11 | 24584 | 0x418B26E9 | g711U | 13876 | 0 (0.0%) | 194.06 | 20.11 | 8.23 |
| 192.168.4.13 | 24586 | 192.168.2.11 | 24586 | 0xB832EA6 | g711U | 260 | 0 (0.0%) | 73.52 | 8.87 | 7.55 |
| 192.168.4.13 | 24588 | 192.168.2.11 | 24588 | 0x153C7E87 | g711U | 35911 | 1 (0.0%) | 291.56 | 23.94 | 8.42 |

Select a forward stream with left mouse button, and then
 Select a reverse stream with Ctrl + left mouse button

Unselect Find Reverse Save As Mark Packets Prepare Filter Copy Analyze Close

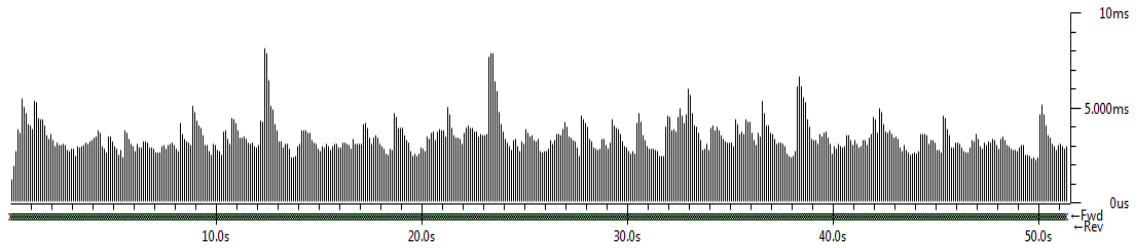
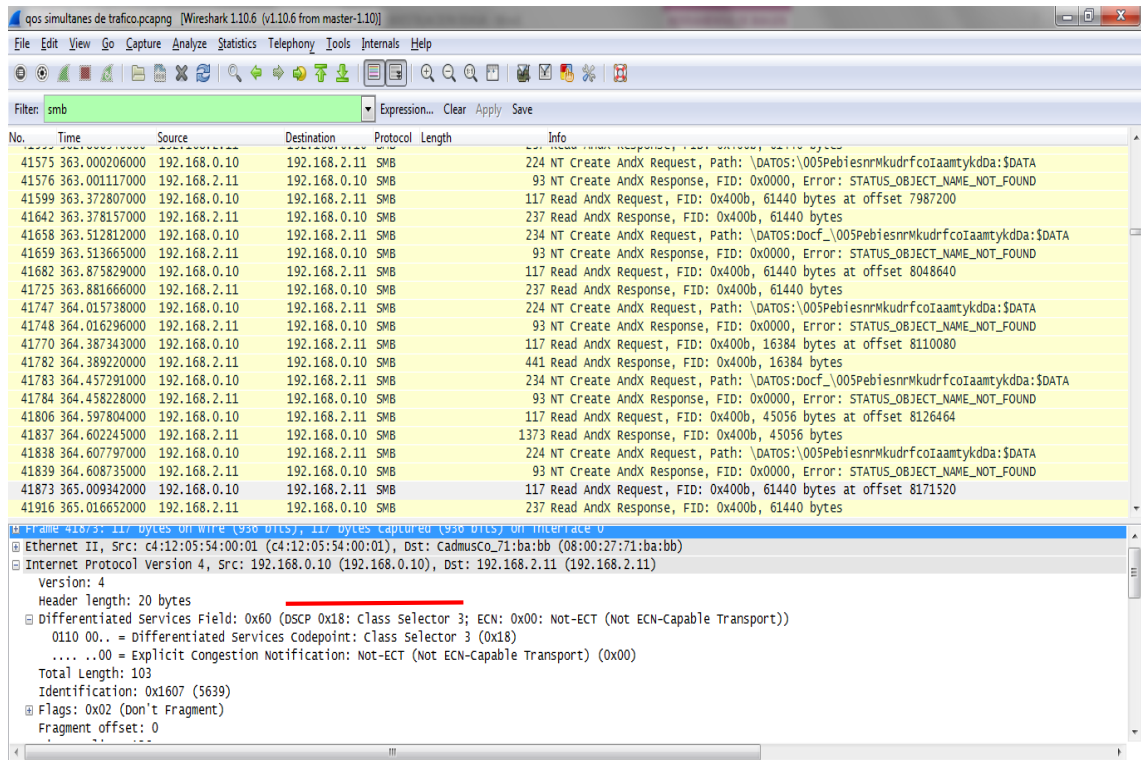


Figura 4.59: Tráfico generado por VoIP con QoS

Elaborado por: Investigador

En la figura 4.60 se observa que al aplicar calidad de servicio QoS en la aplicación denominada transferencia de archivos se puede notar que la velocidad de transmisión aumenta en comparación con la transferencia de archivo realizada sin aplicar QoS mostrada en la figura 4.56. Esto se debe a que no tiene una prioridad crítica debido a que este tipo de tráfico no opera en tiempo real y admite retardos, cabe indicar que la transmisión demora menos tiempo debido a que a esta aplicación se le dio una prioridad bajo y el router marca el paquete dándole una la clase 3, para efectos de prueba se le agrupo en TRANSACCION-DATOS, aplicándole un DSCP cs3 con clase 3, el cuales tienen un ancho de banda garantizada.



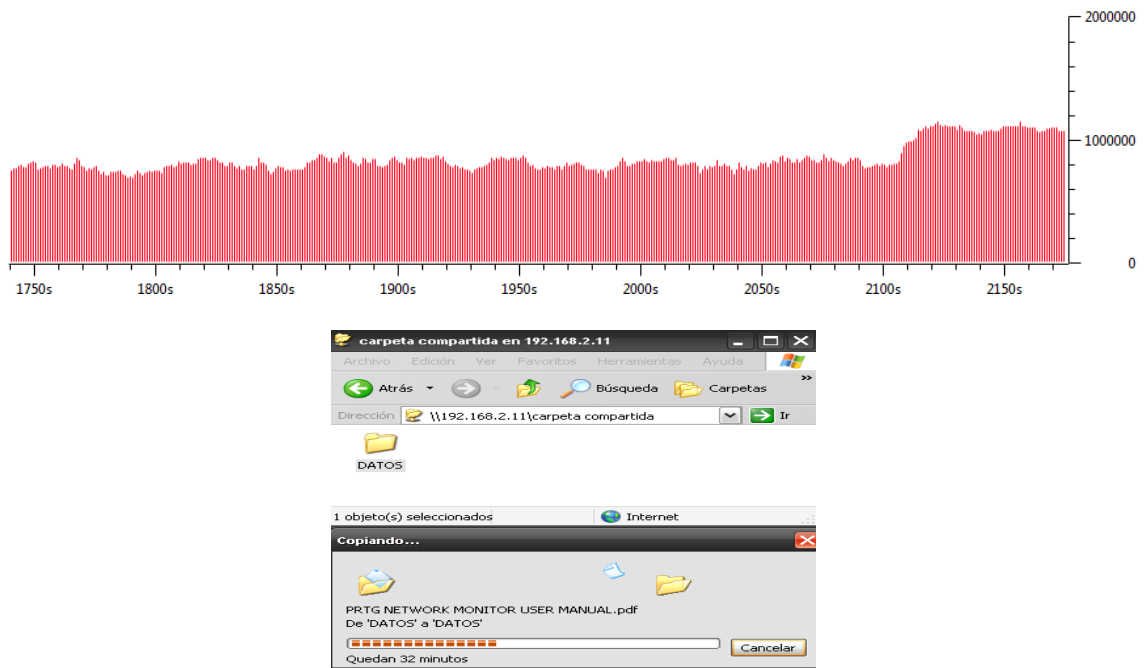


Figura 4.60: Tráfico generado por transferencia de archivo con QoS

Elaborado por: Investigador

Al realizar la aplicación de calidad de servicio para este tipo de tráfico se puede visualizar que su rendimiento y tiempo de respuesta son constantes sin pérdida de paquetes esto se debe a que en el router se configuró a esta aplicación ICMP con un DSCP af21

Al comparar con la figura 4.57 en el cual no se aplica QoS se puede determinar que para este tipo de tráfico la priorización es mínima debido a que no opera en tiempo real, la configuración de QoS se realizó en la interfaz y utilizando comandos extendidos, se puede verificar que se garantiza un 100% en la entrega de paquetes icmp; esta eficiencia se debe a que el tipo de servicio especificado (160) hace que se le entregue la precedencia crítica (5).

A continuación en la figura 4.61 se puede visualizar los comandos extendidos utilizados donde se observa la optimización, también se realizó el monitoreo del tráfico con wireshark que muestra la precedencia.

Además en la gráfica 4.61 se aprecia en ciertos momentos de congestión la red optimiza al tráfico de mayor prioridad por tal motivo se presenta retardos al transmitir este tipo de tráfico.

```

172.20.61.1 - PuTTY
MATRIZ#ping 192.168.2.11 size 10000 repeat 1000

Type escape sequence to abort.
Sending 1000, 10000-byte ICMP Echos to 192.168.2.11, timeout is 2 seconds:
.....
Success rate is 99 percent (996/1000), round-trip min/avg/max = 144/356/1904 ms
MATRIZ#

```

qos simulanes de trafico pcapng [Wireshark 1.10.6 (v1.10.6 from master-1.10)]

Filter: Expression... Clear Apply Save

| No. | Time | Source | Destination | Protocol | Length | Info |
|-------|---------------|--------------|--------------|----------|--------|--|
| 31429 | 300.174887000 | 192.168.2.11 | 192.168.0.10 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 31430 | 300.174889000 | 192.168.2.11 | 192.168.0.10 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 31431 | 300.113419000 | 172.20.61.8 | 172.20.61.1 | TCP | 54 | 49254 > telnet [ACK] Seq=80 Ack=1807 Win=17056 Len=0 |
| 31432 | 300.213537000 | 172.20.61.1 | 172.20.61.8 | TELNET | 60 | Telnet data ... |
| 31433 | 300.232542000 | 172.20.61.1 | 192.168.2.11 | IPV4 | 1514 | Fragmented IP protocol (proto=ICMP 1, off=0, ID=0a01) [Reassembled in #31439] |
| 31434 | 300.242463000 | 172.20.61.1 | 192.168.2.11 | IPV4 | 1514 | Fragmented IP protocol (proto=ICMP 1, off=1480, ID=0a01) [Reassembled in #31439] |
| 31435 | 300.252476000 | 172.20.61.1 | 192.168.2.11 | IPV4 | 1514 | Fragmented IP protocol (proto=ICMP 1, off=2960, ID=0a01) [Reassembled in #31439] |
| 31436 | 300.262514000 | 172.20.61.1 | 192.168.2.11 | IPV4 | 1514 | Fragmented IP protocol (proto=ICMP 1, off=4440, ID=0a01) [Reassembled in #31439] |
| 31437 | 300.272514000 | 172.20.61.1 | 192.168.2.11 | IPV4 | 1514 | Fragmented IP protocol (proto=ICMP 1, off=5920, ID=0a01) [Reassembled in #31439] |
| 31438 | 300.282471000 | 172.20.61.1 | 192.168.2.11 | IPV4 | 1514 | Fragmented IP protocol (proto=ICMP 1, off=7400, ID=0a01) [Reassembled in #31439] |
| 31439 | 300.292476000 | 172.20.61.1 | 192.168.2.11 | ICMP | 1134 | Echo (ping) request id=0x0001, seq=1561/6406, ttl=254 (reply in 31446) |
| 31440 | 300.293359000 | 192.168.2.11 | 172.20.61.1 | IPV4 | 1514 | Fragmented IP protocol (proto=ICMP 1, off=0, ID=1a56) [Reassembled in #31446] |
| 31441 | 300.293362000 | 192.168.2.11 | 172.20.61.1 | IPV4 | 1514 | Fragmented IP protocol (proto=ICMP 1, off=1480, ID=1a56) [Reassembled in #31446] |
| 31442 | 300.293364000 | 192.168.2.11 | 172.20.61.1 | IPV4 | 1514 | Fragmented IP protocol (proto=ICMP 1, off=2960, ID=1a56) [Reassembled in #31446] |
| 31443 | 300.293367000 | 192.168.2.11 | 172.20.61.1 | IPV4 | 1514 | Fragmented IP protocol (proto=ICMP 1, off=4440, ID=1a56) [Reassembled in #31446] |
| 31444 | 300.293370000 | 192.168.2.11 | 172.20.61.1 | IPV4 | 1514 | Fragmented IP protocol (proto=ICMP 1, off=5920, ID=1a56) [Reassembled in #31446] |
| 31445 | 300.293369000 | 192.168.2.11 | 172.20.61.1 | IPV4 | 1514 | Fragmented IP protocol (proto=ICMP 1, off=7400, ID=1a56) [Reassembled in #31446] |
| 31446 | 300.293878000 | 192.168.2.11 | 172.20.61.1 | ICMP | 1134 | Echo (ping) reply id=0x0001, seq=1561/6406, ttl=128 (request in 31439) |
| 31447 | 300.302446000 | 192.168.0.10 | 192.168.2.11 | SMB | 224 | NT Create AndX Request, Path: \DATOS:\005QebiesnrMkudrfcoIaantykdDa:\$DATA |
| 31448 | 300.312514000 | 192.168.0.10 | 192.168.2.11 | TCP | 54 | inst1-bootc > microsoft-ds [ACK] Seq=134239 Ack=3889293 Win=64240 Len=0 |

Frame 31437: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0

Ethernet II, Src: c4:12:05:54:00:01 (c4:12:05:54:00:01), Dst: cadmusco_71:ba:bb (08:00:27:71:ba:bb)

Internet Protocol Version 4, Src: 172.20.61.1 (172.20.61.1), Dst: 192.168.2.11 (192.168.2.11)

Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x48 (DSCP 0x12: Assured Forwarding 21; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
Total Length: 1500
Identification: 0x0a01 (2561)
Flags: 0x01 (More Fragments)
Fragment offset: 5920
Time to live: 254
Protocol: ICMP (1)
Header checksum: 0xde2a [validation disabled]

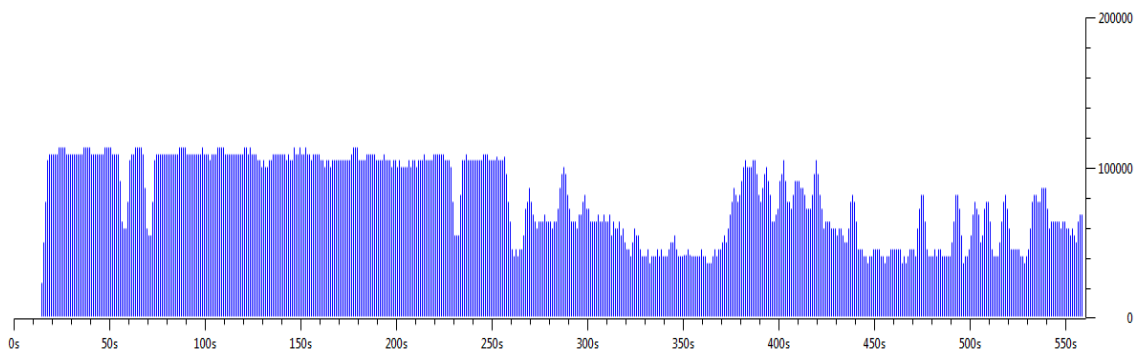


Figura 4.61 Tráfico generado por ping extendido con QoS

Elaborado por: Investigador

```
172.20.61.1 - PuTTY
Class-map: MULTIMEDIA (match-all)
  783 packets, 166942 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: access-group name MULTIMEDIA-CONFERENCIA
  QoS Set
    dscp af31
    Packets marked 783
  Queuing
    Output Queue: Conversation 266
    Bandwidth 14 (%)
    Bandwidth 1400 (kbps)Max Threshold 64 (packets)
    (pkts matched/bytes matched) 306/65140
    (depth/total drops/no-buffer drops) 0/0/0

Class-map: TRANSACCION (match-all)
  89 packets, 6466 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: access-group name TRANSACCION-DATOS
  QoS Set
    dscp af21
    Packets marked 89
  Queuing
    Output Queue: Conversation 267
    Bandwidth 10 (%)
    Bandwidth 1000 (kbps)Max Threshold 64 (packets)
    (pkts matched/bytes matched) 77/5578
    (depth/total drops/no-buffer drops) 0/0/0

Class-map: DATO (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: access-group name DATOS
  0 packets, 0 bytes
  5 minute rate 0 bps
  QoS Set
    dscp cs3
    Packets marked 0
  Queuing
    Output Queue: Conversation 268
    Bandwidth 8 (%)
    Bandwidth 800 (kbps)Max Threshold 64 (packets)
    (pkts matched/bytes matched) 0/0
    (depth/total drops/no-buffer drops) 0/0/0
```

Figura 4.62 Verificación de Estadísticas y marcado de tráfico en router matriz
Elaborado por: Investigador

Se puede determinar que la red presenta una optimización en aplicaciones de tiempo real, gracias a la clasificación, marcado de paquetes, priorización y encolamiento que cada equipo de comunicación proporciona a un determinado tipo de tráfico. La elaboración del prototipo basado en simuladores de red ha permitido analizar cómo la implantación de QoS mejora los servicios que operan en tiempo real, como es el caso de VoIP y videoconferencia.

4.9 Análisis de Resultados OPNET

En esta etapa se analizaron los resultados obtenidos en la implementación de una calidad de servicio en la red inalámbrica de EEASA compuesta por los estándares IEEE 802.16 y IEEE 802.11b, y se analizará su impacto en el rendimiento de las aplicaciones simuladas a través de resultados obtenidos en gráficos y datos estadísticos.

Para el análisis del rendimiento y eficiencia de los mecanismos de calidad de servicio (QoS) en redes inalámbricas en el modelo de red, se realizó el estudio de los datos estadísticos que OPNET ofrece, en este caso se tomó el *Throughput*, *delay*, *jitter* y *data Dropped*. En las figuras se podrán observar las estadísticas globales de las variables de estudio contra el tiempo de simulación.

Del escenario visualizado en la figura se examinarán las aplicaciones de voz, multimedia, FTP, http, correo electrónico y base de datos Oracle, creados anteriormente con el objeto *Application Definition*. La simulación se ejecutó primero sin la aplicación de calidad de servicio, pero aplicaciones de voz y video requieren de reglas de mapeo debido a que estos son intolerables al retraso y *jitter* para que trabajen en su forma normal, las demás aplicaciones tendrán un mapeo Best Effort (0) sin calidad de servicio. Todos los datos son tomados de la tabla mencionados anteriormente. A continuación se analiza el rendimiento en el tráfico de voz incidente en la red mediante los parámetros descritos en la tabla 4.15

Se ejecuta la simulación con un tiempo de 420 segundos de duración con tráfico de voz, FTP, internet, e-mail, para un modelo de red con 16 subestaciones creadas para el presente estudio, el codificador G.711 fue asignado para transmisión de voz y se tomaron estadísticas del el *Throughput*, *delay* y *data Dropped* tanto en entornos de nodos estáticos como globales.

Para el caso de la aplicación de voz se puede observar en la figura 4.63, que el tráfico generado o carga en cada nodo suscriptor es aproximadamente 96000bps identificado con la línea azul, esto se debe a que cada paquete de voz tiene 640 bits, una llamada de voz genera 100 paquetes/sec, para un total de 64000 bps, a esto tráfico se le agregan 160 bits de cabecera en la capa de aplicación y la capa MAC, dando un total de 96000bps.

En la grafica 4.63 tambien se observa la linea roja que representa el throughput de la conexión la cual esaproximadamente 64000bps. Se puede determinar que la diferencia entre la carga y el throughput provoca retardos que resultan inaceptables en el tráfico de VOZ.

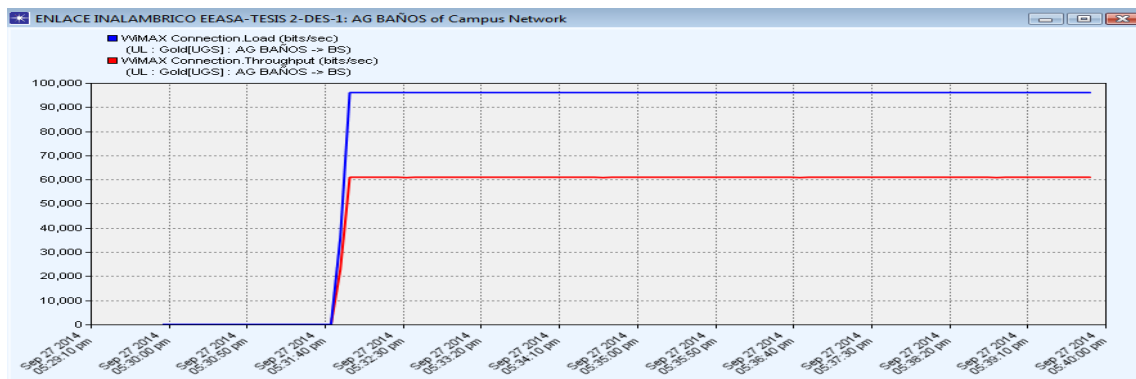
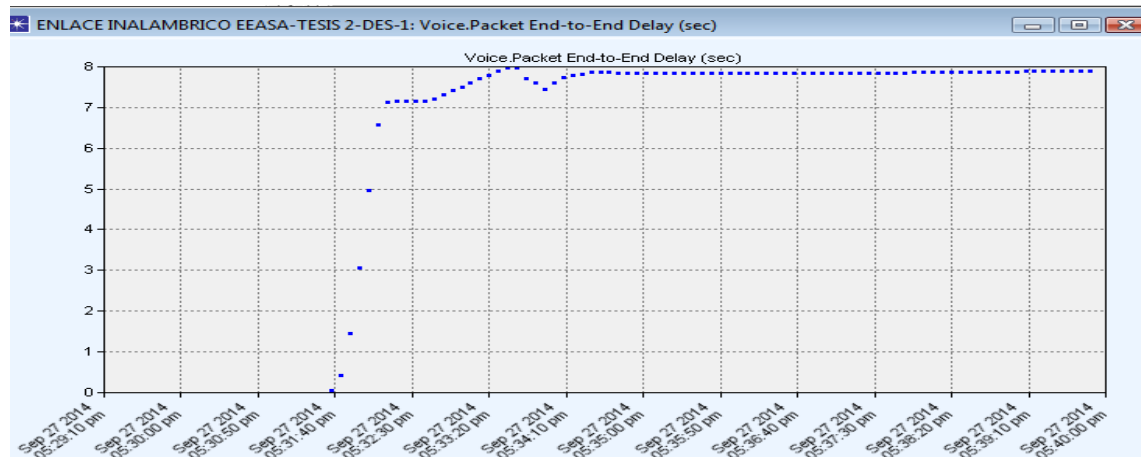
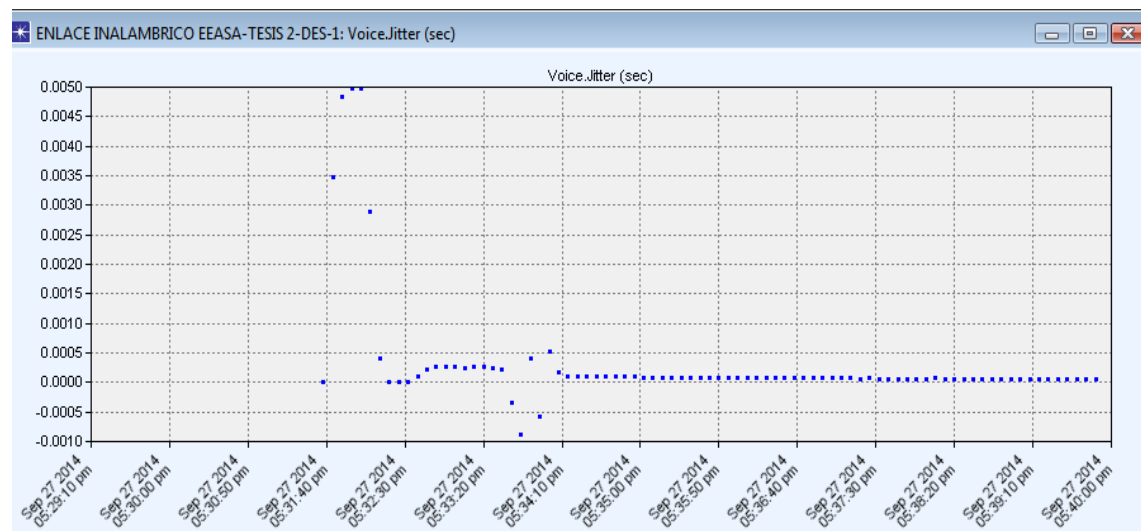


Figura 4.63 Carga y Throughput generado en AGBaños
Elaborado por: Investigador

En el grafico 4.64 se puede observar que el retardo de extremo a extremo del tráfico de voz tiende a ser alrededor de los 8 segundos en el caso más crítico, generando una reducción en su rendimiento, en tráfico sensible a retardos. Además se puede observar la variación de retardo, que en su forma ideal debería ser cero segundos, en este caso se puede visualizar que tiene un promedio aproximado de 0.0050 segundos generado por las características del throughput del canal de transmisión.



a)



b)

Figura 4.64 a) Retardo de extremo a extremo, b) *Jitter* generado en AGBaños
Elaborado por: Investigador

En la figura 4.65 se visualiza el tráfico rechazado, el cual es elevado, el cual tiene un valor aproximado de 37000bps, esto se genera a que el ancho de banda disponible en la red inalámbrica es limitado para el tráfico de voz.

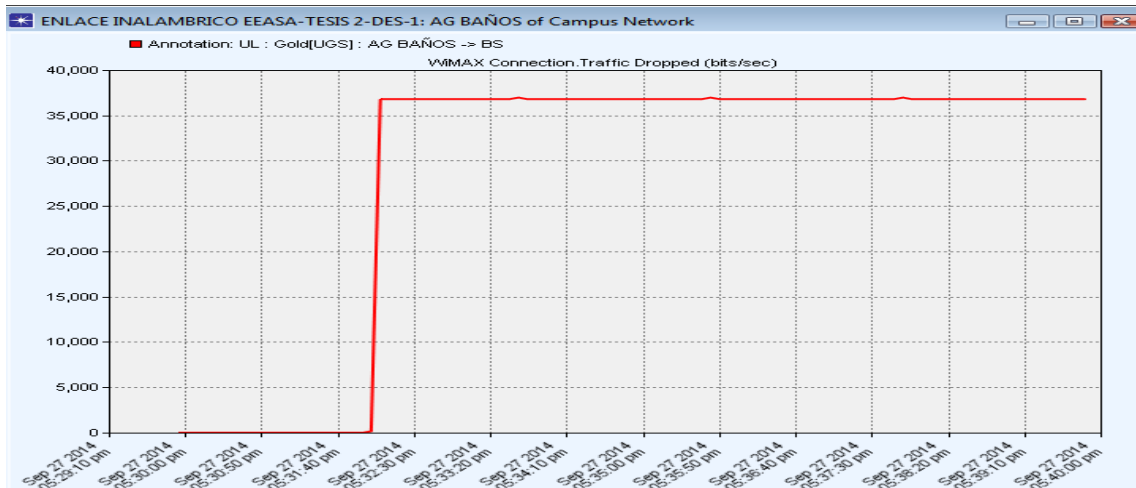


Figura 4.65 Tráfico rechazado en el nodo AGBaños
Elaborado por: Investigador

Para solucionar esta diferencia en el tráfico de voz, se procede a ingresar el valor adecuado en los *MAC Service Class Definitions* en la configuración de *Wimax Config Nodo*, para la aplicación de voz. En este caso el ancho de banda para la aplicación debe ser de 96000bps debido a las condiciones indicadas al inicio del análisis de tráfico de voz y también se configuro la máxima latencia a un valor de 10 mseg,

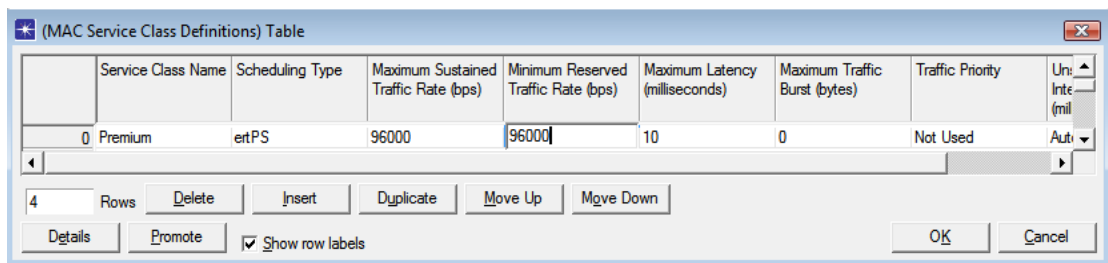


Figura 4.66 Configuración de Ancho de banda para aplicación de voz
Elaborado por: Investigador

Después de realizar la configuración se puede evaluar y verificar cómo se comporta la red inalámbrica para la aplicación de voz, en la figura 4.67 se aprecia que el ancho de banda para la aplicación de voz en la red inalámbrica aumento considerablemente, en comparación con la gráfica 4.63 que no opera con QoS, se puede determinar que la carga ofrecida por el servicio de voz, producida por cada agencia o SS sea igual al throughput de la estación base. También se puede observar en la gráfica 4.68 que existe una ligera diferencia entre la carga ofrecida y el throughput, esto se genera por efectos de interferencia y pérdidas de propagación en el espacio libre.

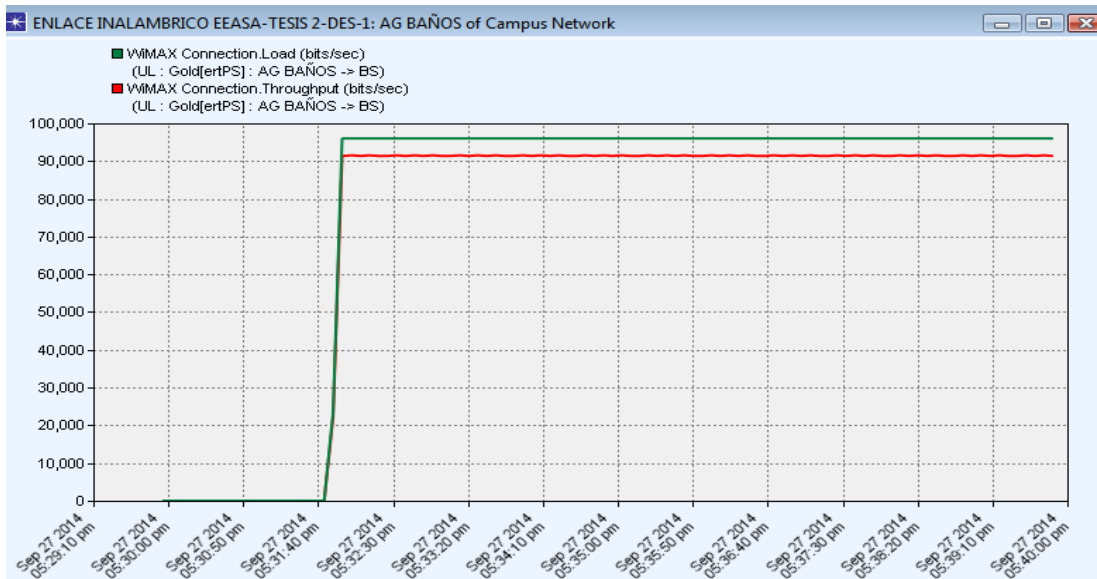


Figura4.67 Carga y Throughput generado en AGBaños, aplicación de voz

Elaborado por: Investigador

En la figura 4.68 el *jitter* o variación de retardo bajo las nuevas condiciones establecidas, se comporta de mejor manera ya que se tiene unos valores bajos y tienden aproximadamente a cero, al comparar con esta aplicación sin QoS visualizada en la gráfica 4.64 se puede determinar que para que el jitter tiene un valor máximo de 0.0005 ms a comparación de los 0.0050 ms al no aplicar QoS, en este caso también se observa que se tiene datos negativos, esto se debe a que el jitter es negativo lo cual indica que un paquete llego al nodo destino con un tiempo de retardo menor al retardo promedio de los paquetes de un flujo de datos.

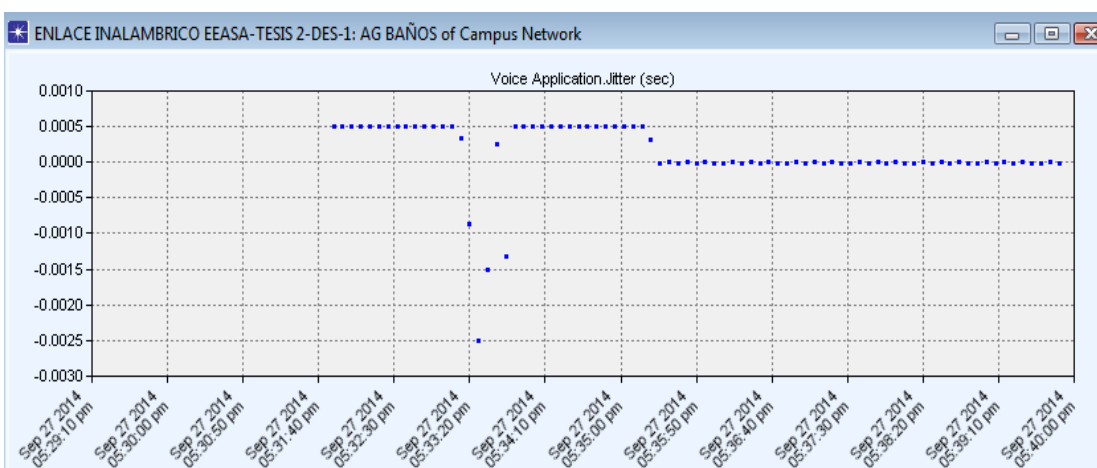


Figura 4.68 Jitter en nuevo mapeo en aplicación de voz

Elaborado por: Investigador

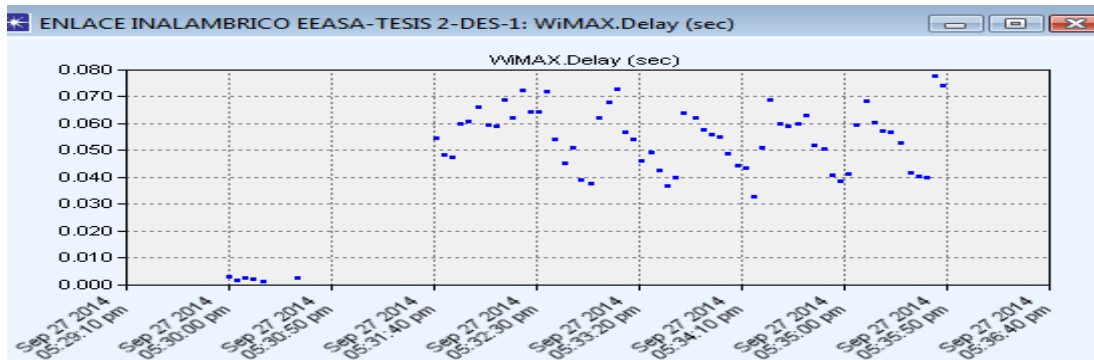


Figura 4.69 Retardo nuevo mapeo en aplicación de voz

Elaborado por: Investigador

En la figura 4.70 se presenta el tráfico de video generado en la red inalámbrica, la cantidad aproximada que genera la carga es aproximadamente de 4,2 Mbps, identificada con línea azul, mientras que el *Throughput* tiene un volumen similar, se determina que el tráfico generado por la aplicación de video presenta un rendimiento óptimo en la red inalámbrica, con pequeñas diferencias debido a las pérdidas generadas por la propagación en el espacio libre.

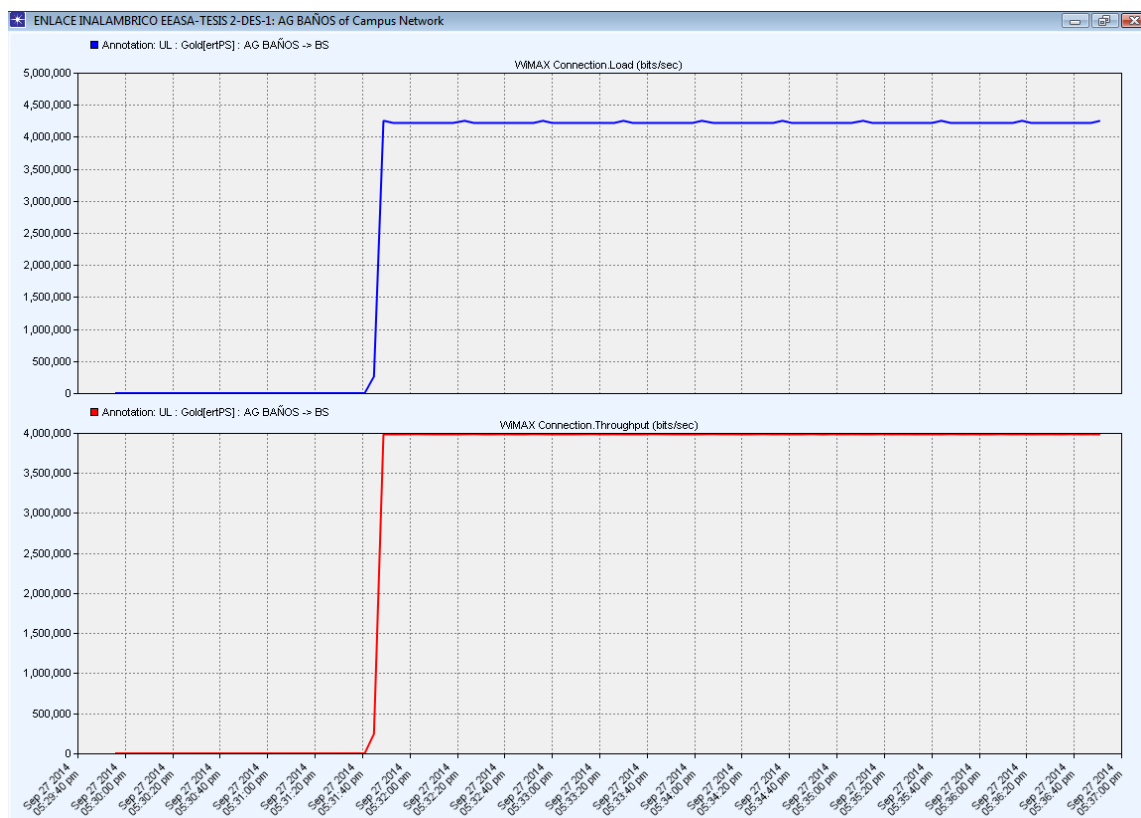


Figura 4.70 Carga y Throughput generado en AGBaños, aplicación de video

Elaborado por: Investigador

De la misma manera se analiza el retardo presente en el tráfico de video, el valor aproximado que presenta es de 0.072 segundos, esto determina que el retardo es mínimo a la hora de entregar paquetes de video en la red inalámbrica. Para mejorar o reducir el retardo se tiene que configurar en la red inalámbrica una relación multicapa de calidad de servicio, el cual permita garantizar el rendimiento adecuado de las aplicaciones.

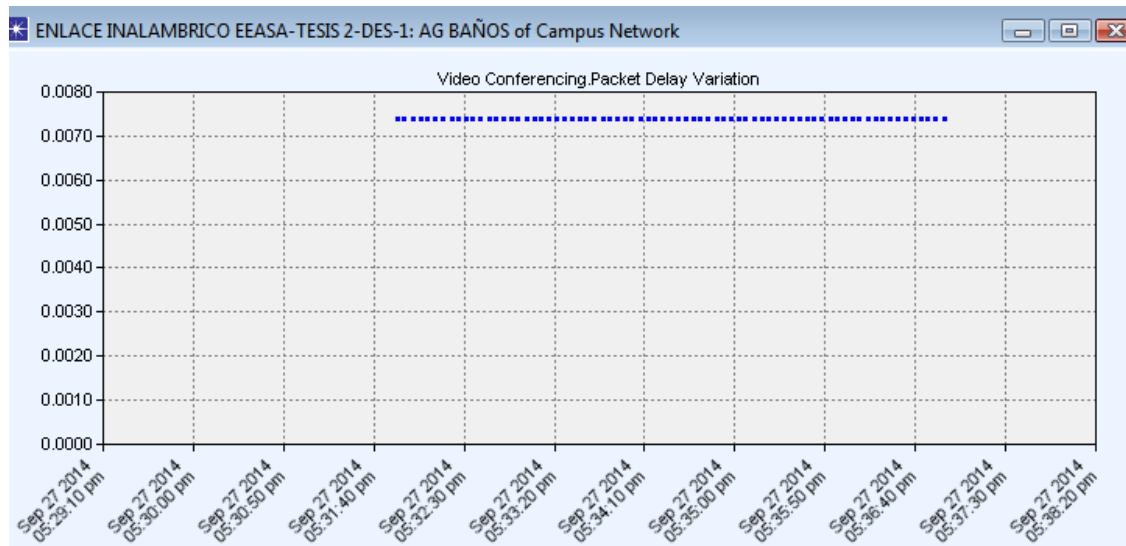


Figura 4.71 Retardo presente en aplicación de video

Elaborado por: Investigador

En la figura 4.72 se puede observar la carga generada en el tráfico FTP por uno de las estaciones suscriptoras o agencias, cabe indicar que cada una de estas estaciones puede generar tráfico al mismo tiempo para las cinco aplicaciones implementadas en la red inalámbrica tanto para Wimax como WLAN.

De manera que se realiza un mapeo en esta aplicación, para que tanto el rendimiento de la aplicación de voz, como el tráfico generado por la aplicación FTP sea eficientemente transmitido a través de la red inalámbrica. Se analiza el tráfico FTP en condiciones donde la aplicación de voz tiene un *Scheduling Type: ertPS*.

También se analiza el tráfico generado por la conexión de datos entre la base de datos y cada estación suscriptoras, en donde se puede apreciar que el tráfico fue entregado satisfactoriamente con pequeñas diferencias debido a la pérdida de propagación.

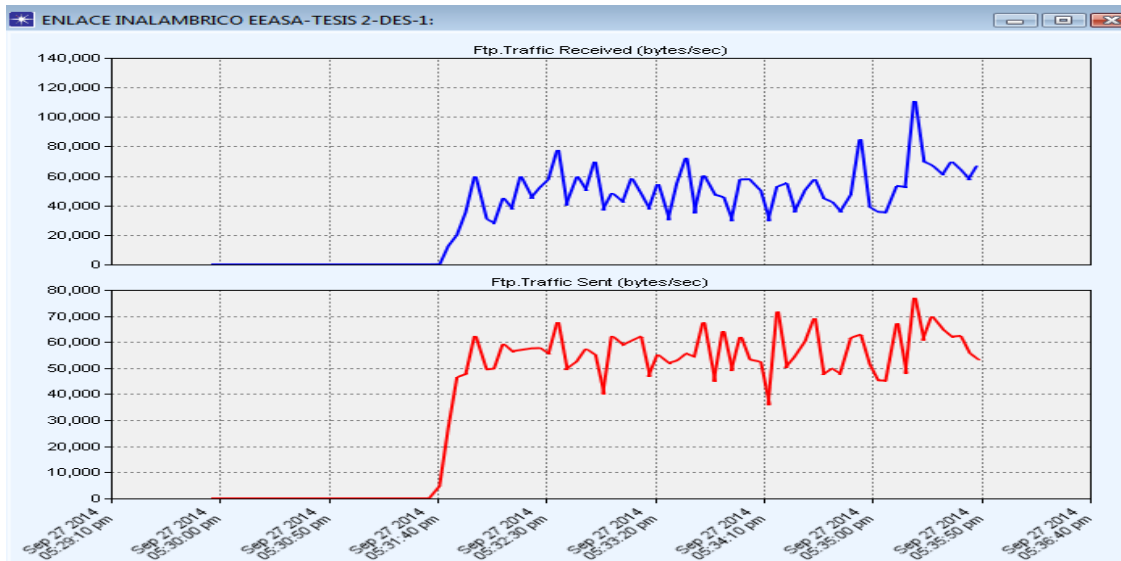


Figura 4.72 Carga generado en aplicación FTP en cada nodo SS

Elaborado por: Investigador

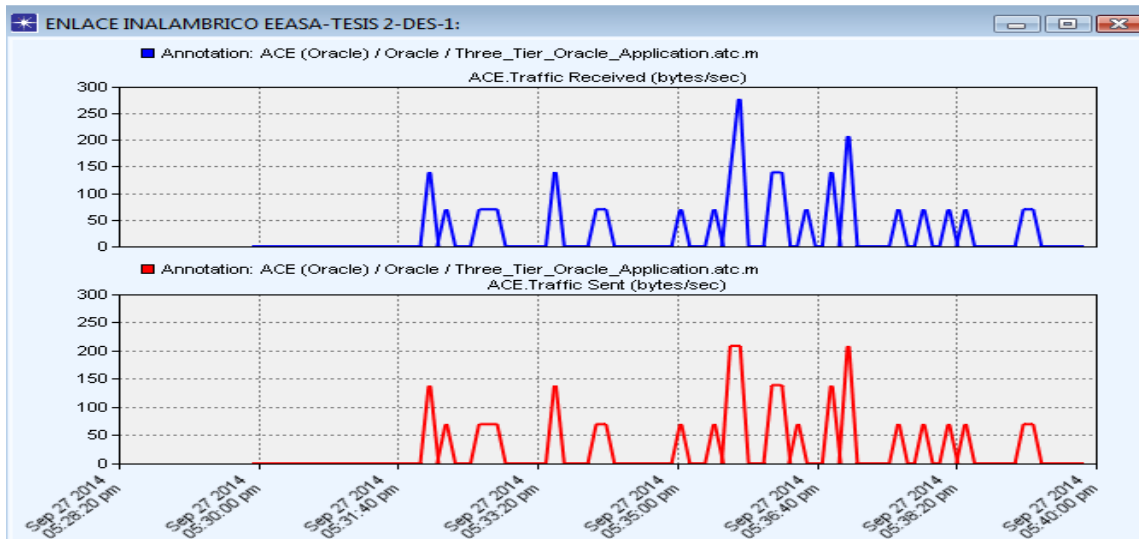


Figura 4.73 Carga generado en la aplicación Oracle

Elaborado por: Investigador

A continuación se observa el retardo generado en la red inalámbrica en la transferencia de datos perteneciente a la aplicación FTP, se determina que el retardo es elevado pero esto no afecta al rendimiento de la aplicación debido a que esta aplicación no transmite en tiempo real. Como se mencionó anteriormente al momento que se presente congestión en la red, los equipos priorizan el trafico dependiendo del marcada y priorización que se le dé al tráfico.

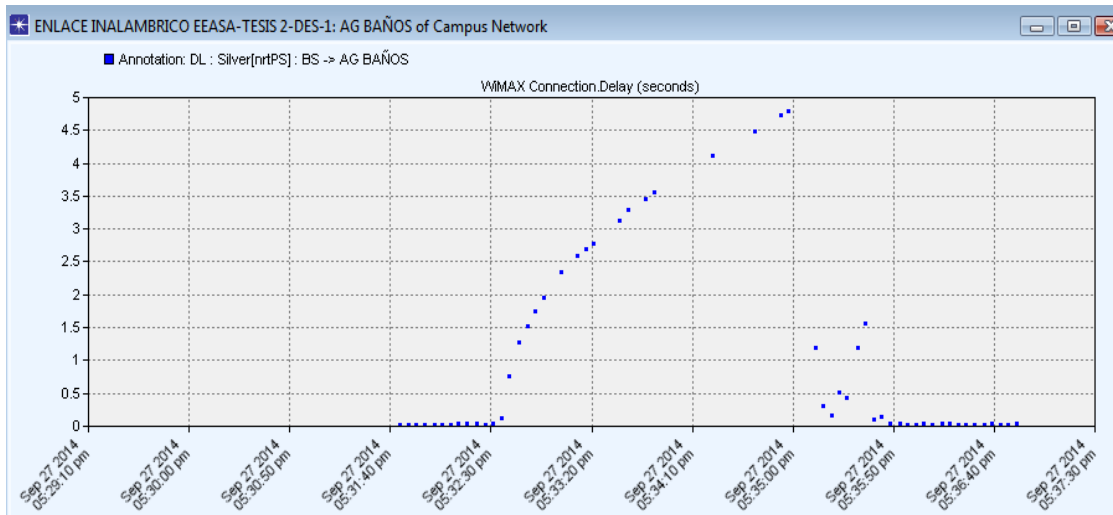


Figura 4.74 Retardo generado en aplicación FTP

Elaborado por: Investigador

En la figura 4.75 se puede visualizar el comportamiento de tráfico HTTP generado por cada estación suscriptora de la red inalámbrica. Se puede visualizar que la carga recibida presenta una similitud al *Throughput* esto debido a que el tráfico de voz no consume los recursos del canal de transmisión usados por la aplicación HTTP, debido a que los parámetros de calidad de servicio en la red inalámbrica se relacionan correctamente. En el presente estudio se asignó un tráfico web máximo sea de 26000bytes/sec, el comportamiento irregular se debe a los componentes de la página web las cuales no siempre son las mismas.

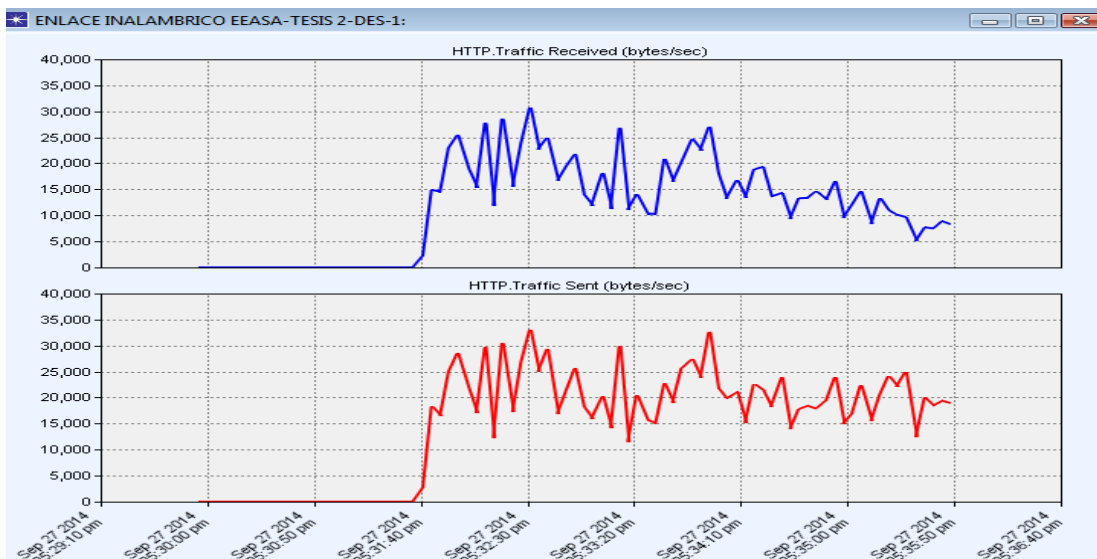


Figura 4.75 Tráfico Recibido y *Throughput* en aplicación Http.

Elaborado por: Investigador

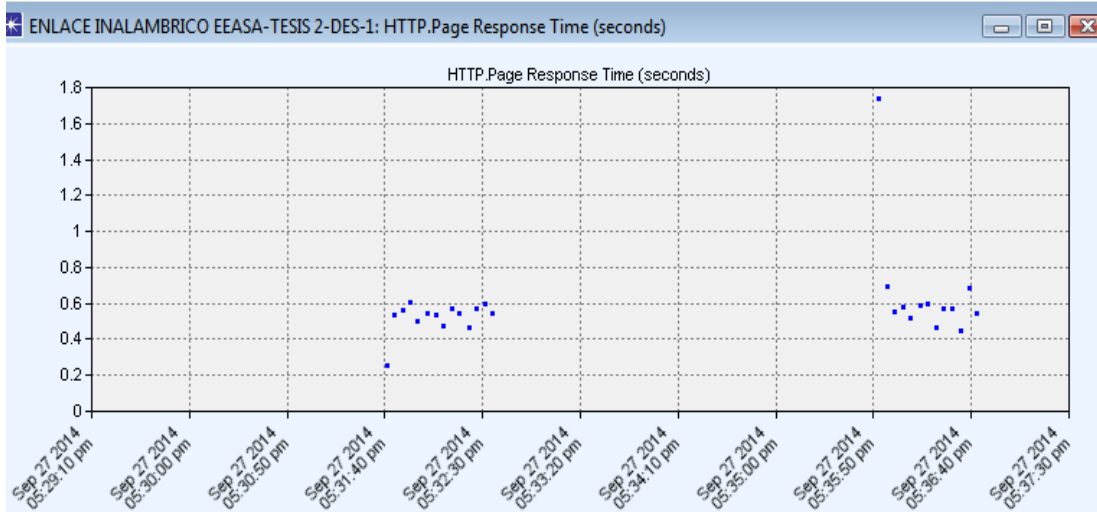


Figura 4.76 Tiempo de respuesta en aplicación Http

Elaborado por: Investigador

En el grafico 4.77 se puede observar el tráfico generado por la aplicación de correo electrónico sobre la red inalámbrica, como se puede visualizar la carga es la misma que el *Throughput*, permitiendo que la aplicación trabaje con un rendimiento óptimo, esto se debe a que los parámetros de calidad de servicio en la aplicación de voz y video están solo consumiendo los recursos del canal asignados a cada aplicación, sin afectar el rendimiento en este caso de la aplicación de correo electrónico.

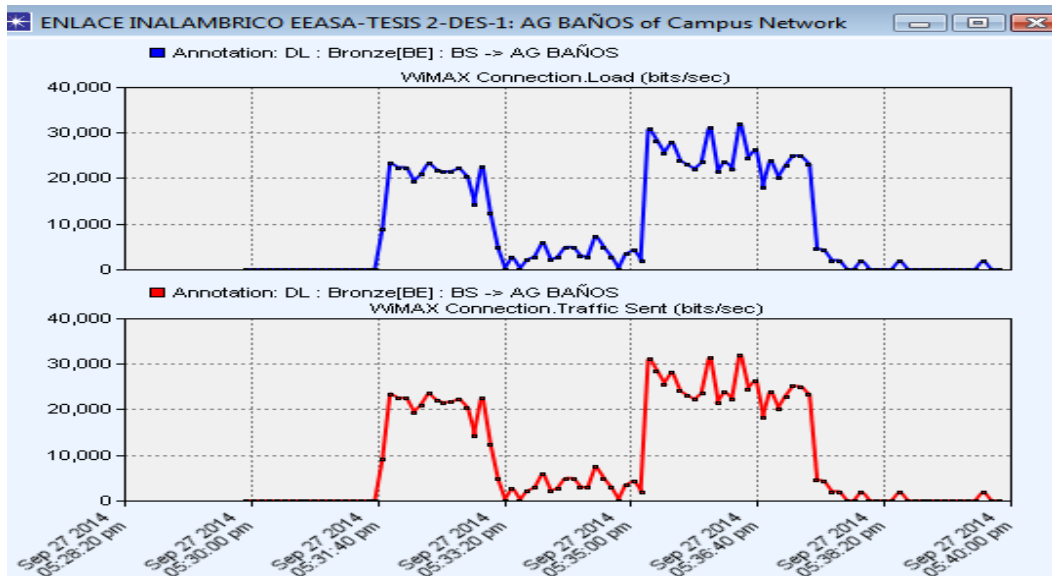


Figura 4.77 Carga y tráfico enviado en aplicación Http

Elaborado por: Investigador

En la figura 4.78 se presenta el retardo generado en uno de los nodos suscriptores, el tráfico de correo electrónico presenta un promedio aproximado de 0,09 segundos en atravesar la red inalámbrica, se puede determinar que el valor de retardo es mínimo permitiendo tener un adecuado rendimiento en la aplicación, debido a que esta aplicación es tolerante a los retrasos en la red.

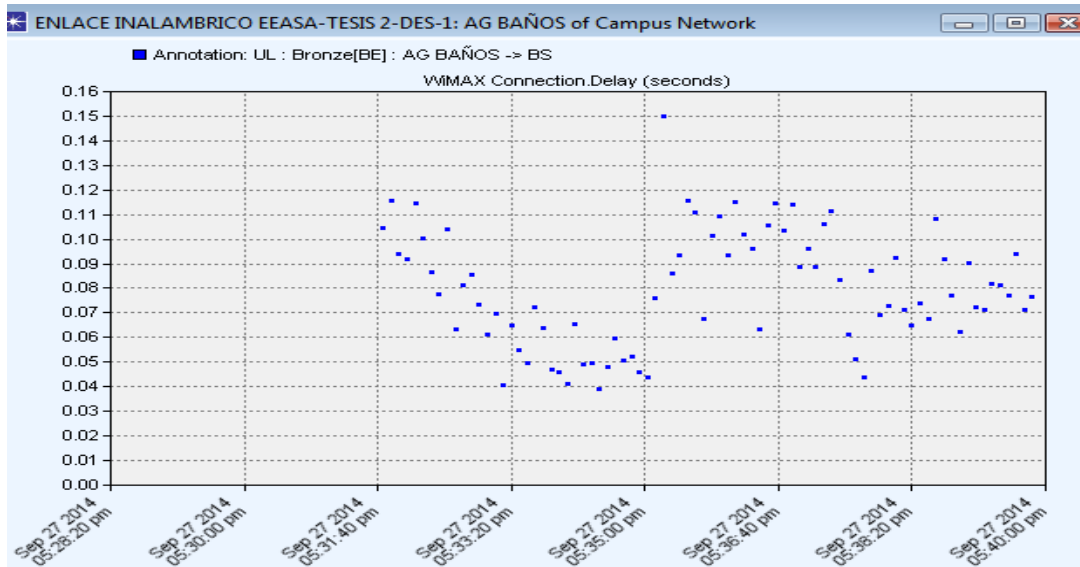


Figura 4.78 Delay en aplicación Http

Elaborado por: Investigador

Para el caso de la simulación de enlace inalámbrico se puede determinar que es factible la implementación de calidad de servicio, ya a posteriores análisis se determinó que los equipos soportan rtPS como método para optimizar el rendimiento de aplicaciones en tiempo real.

4.10 Análisis de Factibilidad de QoS en la red MAN de EEASA.

Para determinar la factibilidad de implementar QoS en la red MAN de EEASA, se analizó la topología física y lógica de la red MAN de EEASA, y un levantamiento de información de equipos que componen la red, en el cual se concluye que si es factible la implementación de calidad de servicio (QoS), tanto en routers, switches y equipos de enlace inalámbrico, debido a que la red está conformada por una estructura jerárquica y se puede aplicar QoS en cada uno de los niveles de la red. Esto permite a que los administradores de la red de EEASA manejar aplicaciones sensibles al jitter, como audio,

video y sistema SCADA, asimismo el manejo de tráfico sensible al retardo, como es el caso de la voz en tiempo real.

El análisis de factibilidad también se basó en determinar que modelos de calidad de servicio (QoS) soportan los equipos, para ello se realizó un estudio detallado de los modelos IntServ y DiffServ, que realizan diferentes operaciones para ofrecer priorización de tráfico, la elección dependerá de requerimientos como ancho de banda, retardo, jitter y demás variaciones a la que está sometida la red de EEASA. Por tanto para una buena escalabilidad y velocidad se aplicó el método DiffServ que es el más utilizado debido a que brinda versatilidad al no reservar previamente recursos, ni introduce sobrecargas en la red para brindar QoS, lo cual ayuda a que el rendimiento de la misma sea óptimo.

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- ❖ Analizando los resultados al implementar QoS en los simuladores de red como GNS3 y OPNET Modeler, permitieron determinar que QoS es una solución para priorizar el tráfico, ante situaciones de saturación de canal o congestión en la red ya que cada equipo administrara el tráfico de manera diferenciada, y debido a las prioridades que los paquetes toman para el mejorar el desempeño de respuesta en aplicaciones críticas que operan en tiempo real, gracias al encolamiento y marcado de paquetes. Mientras que para escenarios donde la red no presente congestión de canal, los paquetes de diferentes aplicaciones son gestionados con similitud en la red, pero el tráfico con mayor prioridad posee mejores resultados en cuanto a latencias ocasionadas por el jitter y retardo.
- ❖ La elaboración de un prototipo basado en simuladores de red, como GNS3 y OPNET Modeler, permitió determinar cómo se comporta el modelo DiffServ en los diferentes tipos de enlaces que conforman la red MAN de EEASA, con el objetivo de verificar la optimización de la misma y realizar pruebas prácticas antes de poner en funcionamiento un esquema final.

- ❖ Al simular diferentes escenarios de tráfico tanto en GNS3 como OPNET Modeler, se pudo observar el rendimiento y comportamiento de la red bajo diferentes demandas de tráfico, en términos de QoS. Lo que permitió determinar qué tan eficiente es la optimización de los servicios, con la implementación de QoS, simulando altos niveles de tráfico que circulan en la red MAN de EEASA, conformadas por equipos de marca cisco, proxim, ubiquiti y microtik.

- ❖ Siempre que exista saturación del canal, tanto para el enlace de fibra óptica como el inalámbrico, se ejecutarán los algoritmos de encolamiento y planificación, implementados en los equipos routers y switches, permitiendo gestionar de manera ordenada el envío de paquetes en las colas de salida y controlar la congestión de la red, distribuyendo el ancho de banda a las aplicaciones con mayor prioridad, y evitando así la pérdida de paquetes en aplicaciones que operan en tiempo real en la red MAN de EEASA.

- ❖ La calidad de servicio, mejora el rendimiento de una red inalámbrica de extremo a extremo, porque aumenta la estabilidad y el rendimiento de cualquier aplicación. En el presente trabajo se propuso un mecanismo de calidad de servicio en sistemas inalámbricos basados en estándares IEEE 802.11b y IEEE 802.16. Se puede concluir que al aplicar un tipo de Scheduler a un determinado tráfico este trabaja sobre cada uno de forma particular, para que pueda brindar una buena calidad de servicio, esto se debe a que es una política que permite regular el número de conexiones de flujos y asigna la capacidad del transmisión de un paquete para solicitudes de ancho de banda con servicios de tráfico constante como el de voz y video, y también para tráficos que no operan en tiempo real como FTP, el tipo de scheduler aplicable es rtPS soportado por equipos Proxim y Ubiquiti.

5.2 Recomendaciones

- ❖ Cuando EEASA adquiera nuevos equipos de comunicación se recomienda verificar las versiones de IOS, ya que dependiendo de las versiones se establecerá si soportan los comandos de calidad de servicio (QoS), como el caso de los switches 2960 que actualmente poseen y trabajan con la Versión 15.0 (2) SE5 que es un estándar y remplazarlo por una imagen mejorada (EI) para así poder utilizar todas las características que provee la implementación de QoS.
- ❖ Para trabajos futuros realizados tanto en GNS3 como OPNET Molder donde se simulen redes a escalas mayores, usar equipos con características mínimas que son: procesador de 4 núcleos, 8GB de RAM y 2 tarjetas Ethernet. Esto debido a que tanto GNS3 como OPNET Modeler usan muchos recursos del computador.
- ❖ El simulador GNS3 opera con IOS reales, pero este presenta limitaciones debido a que no soporta todas las versiones de equipos más avanzados, por tal motivo se recomienda para trabajos futuros, asegurarse que las versiones de IOS sean las adecuadas para GNS3 y así tener una simulación a su máxima capacidad.
- ❖ Para tener un control adecuado de la red MAN, el departamento de planificación de EEASA debería incorporar a SolarWinds herramientas de monitoreo de ancho de banda que permitirán determinar el rendimiento de la red y ver qué aplicaciones están consumiendo mayor ancho de banda y generando más tráfico. Esto ayudará a tener mayor cantidad de datos cuyos resultados permitan validar experimentalmente los beneficios de implementar QoS en la red MAN de EEASA.
- ❖ Se recomienda que los equipos utilizados para el enlace inalámbrico, tengan nuevas configuraciones de transmisión como para el de telefonía móvil y no solo operen como enlaces punto a punto, debido a que los equipos tiene características que ofrecer gran capacidad de ancho de banda a través de su protocolo worp, similar a wimax incorporada en los equipos Proxim, lo cual beneficiaría a futuro la implementación de nuevas tecnologías.

6. REFERENCIAS BIBLIOGRÁFICAS

[1] A. Quintana, E. Pérez, F. Hernández “Encaminamiento en redes orientadas a flujo con imprecisión en los datos”, Universidad de Málaga, E.T.S.I Telecomunicaciones. Disponible en:

http://pitagoras.usach.cl/~eflores/lcc/cd_redes/encamina-datos-imprecisos.pdf

[2] A. Omar, M. Moyoral, “Contribución para QoS en Redes Metropolitanas Ethernet”, Bogotá, Revista de Ingeniería 2007 #26. Pág. 1, 2, 3. Disponible en: <https://revistaing.uniandes.edu.co/pdf/26a1.pdf>

[3] M. Cruz, R. Martínez, C. García, “Análisis de la QoS en redes inalámbricas”, Revista Cubana de Ciencias Informáticas, Vol. 7, Marzo, 2013, Pág. 86-96, Disponible en: <http://scielo.sld.cu/pdf/rcci/v7n1/rcci10113.pdf>

[4] S. Álvarez, A Valenzuela “Estudio y configuración de QoS para protocolos ipv4 e ipv6 en una red de fibra o WDM” Universidad de Tarapacá, Marzo 2005, Pág. 104-11, Disponible en: <http://www.scielo.cl/pdf/rfacing/v13n3/art15.pdf>

[5] Fonseca Hugo. “Calidad de Servicio (QoS) para el mejoramiento de la Red de Datos en la Fábrica de Calzado LIWI”. UNIVERSIDAD TÉCNICA DE AMBATO. [En línea], Biblioteca Facultad de Ingeniería en Sistemas, Electrónica e Industrial Ambato, Diciembre 2012.

[6] Llerena Diego, “Algoritmos de Calidad de Servicio (Qos) y la Congestión en los enlaces de Comunicación de los Usuarios de la Empresa Uniplex Systems de la Ciudad de Quito”. UNIVERSIDAD TÉCNICA DE AMBATO [En línea], Biblioteca Facultad de Ingeniería en Sistemas, Electrónica e Industrial Tesis de Posgrado, 2011. Disponible en: <http://repo.uta.edu.ec/handle/123456789/42>

[7] D. Quevedo y P. Vaca, “Diseño e Implementación de Calidad de Servicio (QoS) en la Red de Transporte de Datos del Municipio del Distrito Metropolitano de Quito (MDMQ)”. Universidad Politécnica Nacional [Online], Quito, Diciembre 2011. Disponible en: <http://bibdigital.epn.edu.ec/handle/15000/4409>

- [8] J. Arrobo y M. Sarmiento, “Implementación de QoS en la red LAN de la Universidad Técnica Particular de Loja, UTPL”. Universidad Técnica Particular de Loja [Online], Loja, Abril 2013
Disponible en: <http://dspace.utpl.edu.ec/handle/123456789/6572>
- [9] E. Cruz. y F. Álvarez. “Evaluación de la calidad de los servicios en redes E-MAN”. Colombia: Artículo de Ingeniería & Desarrollo, 2008 Pág. 102,103. Disponible en: <http://www.redalyc.org/articulo.oa?id=85201908>
- [10] J. Joskowicz, “Redes Corporativas y Redes de Datos”, Montevideo, Uruguay. Versión 5. 2008, Pág. 4, 5, 11. Disponible en:
<http://iiie.fing.edu.uy/ense/asign/redcorp/material/2008/Redes%20de%20Datos%202008.pdf>
- [11] Stallings William, Comunicaciones y Redes de Computadoras, 6 ta Edición, Prentice Hall, Granada, Ed. 2000, Pág. 101-119.
- [12] Zuñiga Vicente. “Redes de transmisión de datos”, Tesis de Pregrado Noviembre 2005. Pág. 25-45. Disponible en:
<http://www.uaeh.edu.mx/docencia/Tesis/icbi/licenciatura/documentos/redes%20de%20transmision%20de%20datos.pdf>
- [13] Cisco Systems. INTEL, Gigabit Ethernet en Fibra y Cobre, 2001 Pág. 3-7. Disponible en: http://www.abox.com/documentos/wp_cisointe.pdf
- [14] PACKETLIFE.NET (Noviembre -2012). Quality of Service. Pág. 1-2. Disponible en: <http://media.packetlife.net/media/library/19/QoS.pdf>
- [15] Zavala Angélica, “Estudio de QoS sobre WLAN Utilizando el Estándar 802.11e a Transmisiones de Sistemas Multimediales en Tiempo Real”, Escuela Superior Politécnica de Chimborazo [Online], Riobamba 2010, Pag.27-29. Disponible en: <http://dspace.esPOCH.edu.ec/bitstream/123456789/328/1/18T00409.pdf>
- [16] Balakrishnan Ram, Advanced QoS for Multi-Service IP/MPLS Networks. Canada. Alcatel-Lucent 2008. SRA No.10. Pág. 33, 64, 371.

[17] España María Carmen, Servicios Avanzados de Telecomunicaciones, Madrid-España, Díaz de Santos S.A. Ed. 2003 Pág. 248-302

[18] Ariganello Ernesto y Barrietos Sevilla. REDES CISCO CCNP a Fondo, Guía de estudio para profesionales. Alfoamega Grupo Editor S.A. Ed. 2010, México, Junio. Pag.796-797.

[19] Garcia Carlos, “Propuesta de Arquitectura de QoS en entorno Inalámbrico 802.11e”, Universidad Carlos III de Madrid [Online], Madrid 2006, Pág. 26, 27, 28,29. Disponible en: <http://gredes.ifto.edu.br/wp-content/uploads/tesis-carlos-garcia-15jun.pdf>

[20] Albentia, Systems.” Implementación de QoS en redes Wimax”, Abril 2010, Pág.4-7. Disponible en: <http://www.albentia.com/Docs/WP/ALB-W-000001spA3-QoS.pdf>

[21] Doménico Javier, "Medición Y Análisis de Tráfico en Redes MPLS", Pontificia Universidad Católica Del Perú [Online]. Lima 2012, Disponible en: http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/212/LUNA_JAVIER_MEDICION_ANALISIS_TRAFICO_REDES_MPLS.pdf?sequence=2

[22] Guerrero, Sidnei de Oliveira. “Una propuesta de arquitectura MPLS/DIFFSERV para proveer mecanismos de calidad de servicio en el transporte de la telefonía IP”, Tesis doctoral, Universidad politécnica de Madrid [Online], Madrid 2004.

[23] Catalyst 2960-S and Switch Software Configuration Guide, Disponible en: http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-s-series-switches/data_sheet_c78-726680.html

[24] Mikrotik RouterOS, Catalog Q1-Q2, Ed 2010 Disponible en: http://www.mikrotik.com/pdf/what_is_routeros.pdf

[25] Mikrotik, RouterOS, “Workshop Lets talk about QoS”, Las Vegas, USA 2011 Disponible en: <http://mum.mikrotik.com/presentations/US11/us11-megis.pdf>

- [26] Installation and Initialization Tsunami QB-8100 Series, Disponible en: http://proximtechnicalservice.com/support/tsunami/QB81XX-CPE50-12/2.3.4/QB-8100-Series-50+12Mbps_Inst&MgtGuidev1.4_SW2.3.4.pdf
- [27] Tsunami MP.11 Model 5054-R and 2454-R “Installation and Management” Disponible:http://proximtechnicalservice.com/support/tsunami/mp11/tmp25/MP.11-R_InstallManage_v2.5.pdf
- [28] SolarWinds Network Performance Monitor, datasheet, Disponible en: <http://www.solarwinds.com/resources/datasheets/oriondatasheet.pdf>
- [29] Felice Santiago “Evaluación de mecanismos de calidad de servicio en los routers para servicios multimedia”, Sistemas y Servicios Telemáticos, disponible en: <http://es.scribd.com/doc/76489835/docto-2-qos>
- [30] Gonzales Jaime, Agosto 2011, “Análisis y Diseño de una Técnica de Calendarización Para Redes Wimax Móviles Basadas IEEE 802.16e”. Universidad Autónoma de México [Online], Universitaria-México-D.F. disponible en: <http://132.248.52.100:8080/xmlui/bitstream/handle/132.248.52.100/4695/gonzalezmandez.pdf?sequence=1>
- [31] Ariza Julieth y Ranci Sergio, Bucaramanga, 2009 “Calidad de Servicio Multicapa en una red IP basada en Wimax” Universidad Pontificia Bolivariana [Online]. Bucaramanga, Noviembre 2009 Disponible en: http://repository.upb.edu.co:8080/jspui/bitstream/123456789/1032/1/digital_18496.pdf
- [32] RIVERBED, OPNET Application and Network Performance, Technologies Inc, Disponible en: <http://www.riverbed.com/products/performance-management-control/opnet.html>
- [33] GNS3, Empowering the Network Professional, 2014 Disponible en: <http://www.gns3.com/about-us.php>

[34] Orosco Wilson, AIMARA Mayra, “Interconectividad de routers emulados mediante gns3 con routers emulados físicos”, Escuela Politécnica de Chimborazo [Online], Riobamba, 2013, disponible en:

<http://dspace.espoch.edu.ec/bitstream/123456789/2714/1/18T00533.pdf>

[35] Cevallos Mario, Bermudez Verónica, “Integración de la materia laboratorio de telemática para la Facultad Técnica usando el simulador gráfico de redes GNS3”. Universidad Católica Santiago de Guayaquil [Online], Guayaquil, Septiembre 2013, Disponible en: <http://repositorio.ucsg.edu.ec/bitstream/123456789/1354/1/T-UCSG-PRE-TEC-ITEL-6.pdf>

ANEXOS

ANEXO 1

Análisis y monitoreo de los nodos pertenecientes al enlace de fibra óptica e inalámbrica de la red MAN de EEASA

A continuación se muestran las capturas del consumo de tráfico obtenidas con SolarWinds realizadas en el área operativa del que componen la red MAN de EEASA.

Nodo Switch Pelileo

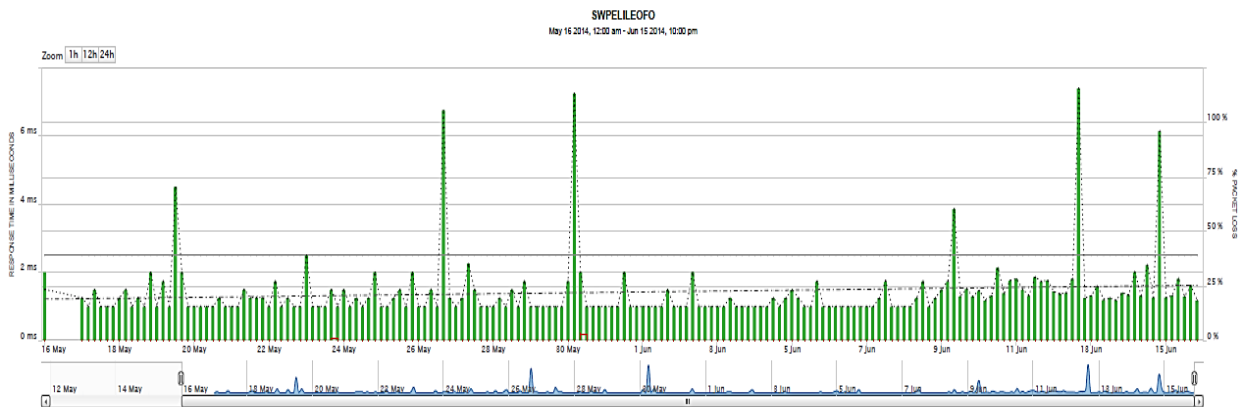


Figura 1. Tráfico Generado en Switch Pelileo
Elaborado por: Investigador

En el gráfico 1 se puede observar que el tráfico generado en el nodo de pelileo, en este se determinó que el tiempo de respuesta promedio está entre 1,5 ms y presenta una pérdida de paquetes de 6%, con un promedio de transmisión de información de 100Gbytes, en la figura 2 se visualiza la cantidad de bytes transmitidos en cada interfaz. Se concluye que el equipo presenta pequeñas pérdidas de paquetes debido a que la interfaz se congestiona.

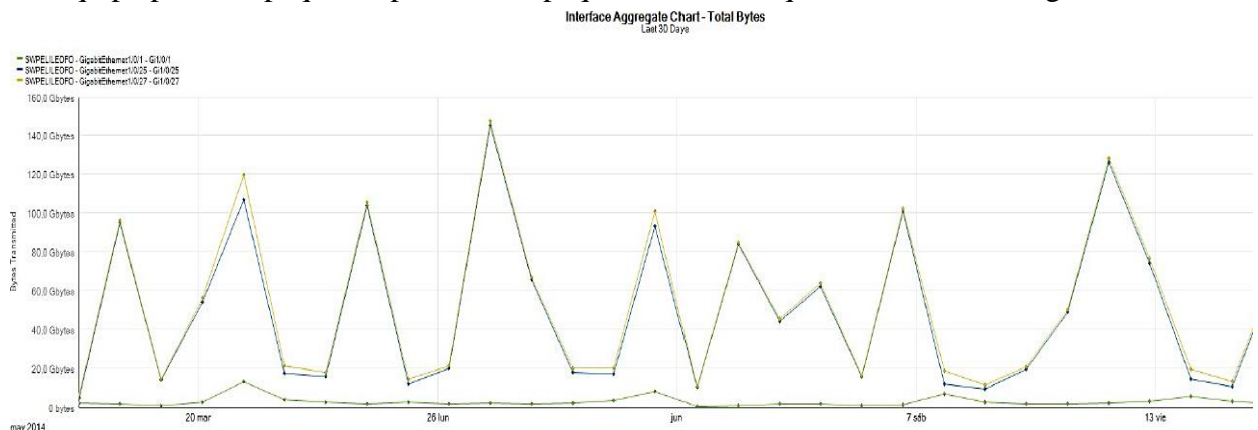


Figura 2. Bytes transmitidos en Switch Pelileo
Elaborado por: Investigador

Nodo Switch Baños

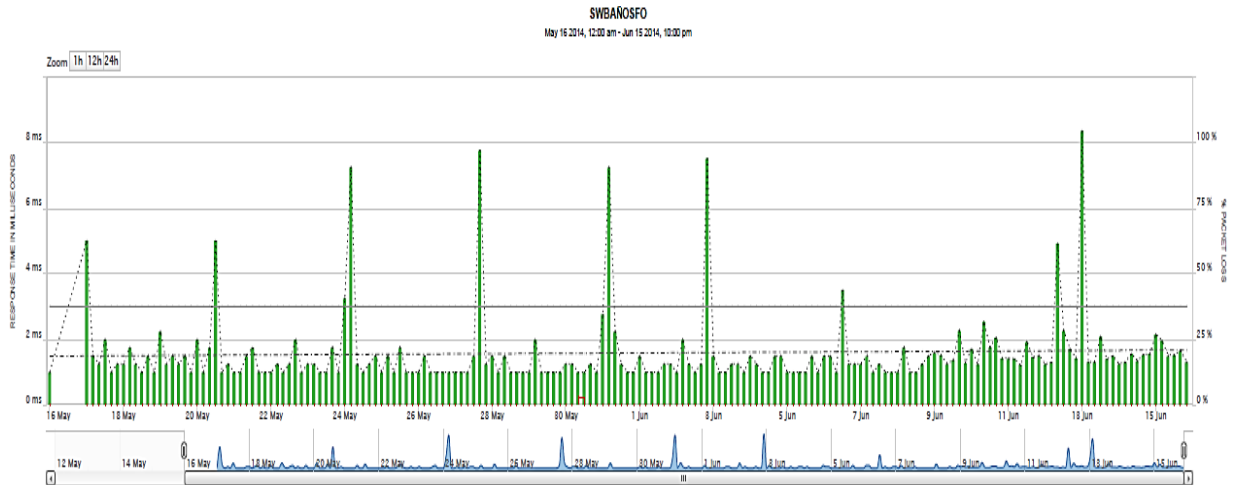


Figura 3. Tráfico Generado en Switch Baños
Elaborado por: Investigador

En el switch utilizado en el nodo Baños, se determinó que el tiempo de respuesta tiene un promedio de 1,64 ms con un promedio de bytes transmitidos de 95 Gbytes aproximadamente en cada interface como se muestra en la figura 4, se puede determinar que este equipo presenta una pérdida de paquetes de un 6%, se puede concluir que el equipo genera pequeños picos de congestión debido a la gran cantidad de información transmitida a través de sus interfaces.

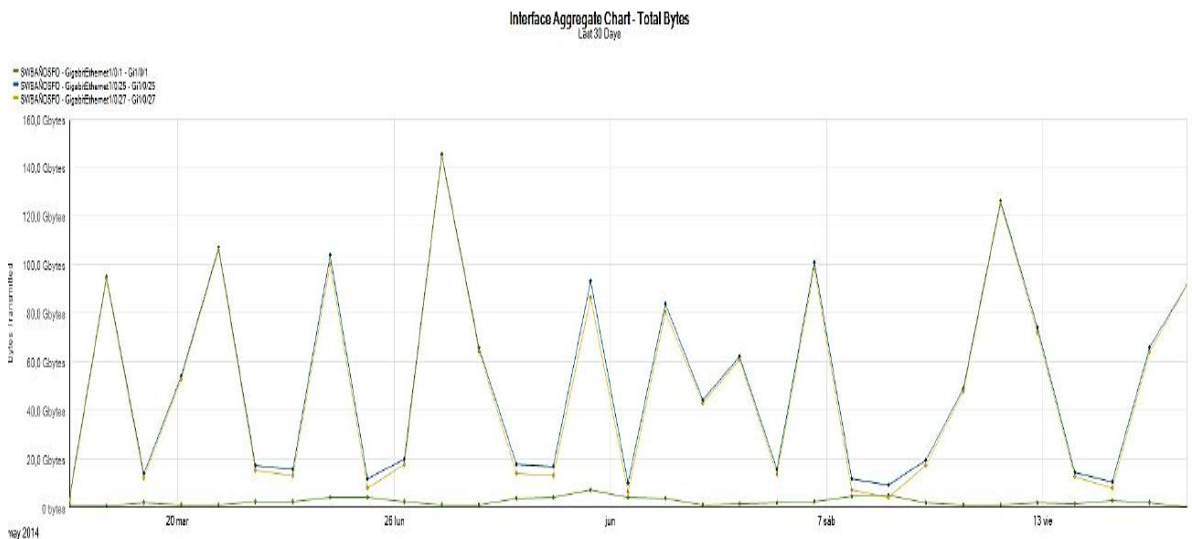


Figura 4. Bytes transmitidos en Switch Baños
Elaborado por: Investigador

Nodo Router Subestación Puyo

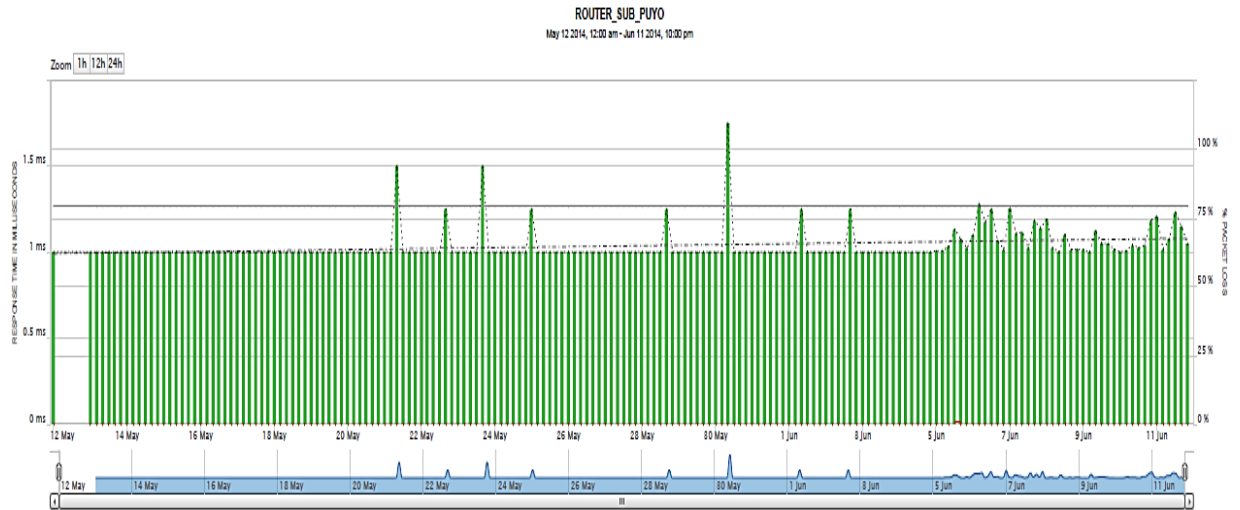


Figura 5. Tiempo de respuesta en Nodo Router SubPuyo
Elaborado por: Investigador

En el router utilizado en la subestación puyo, se puede visualizar en la figura 6 el tiempo de respuesta tiene un promedio de 1,1 ms en transmitir los datos, también se determinó con un promedio de bytes transmitidos de 121 Gbytes en vlan 20 de Transelectric, en el cual se analizó y se determinó que no presenta pérdida de paquetes en la transmisión de datos, se puede concluir que el equipo no presenta congestión debido a que la información es transmitida a través de fibra óptica.

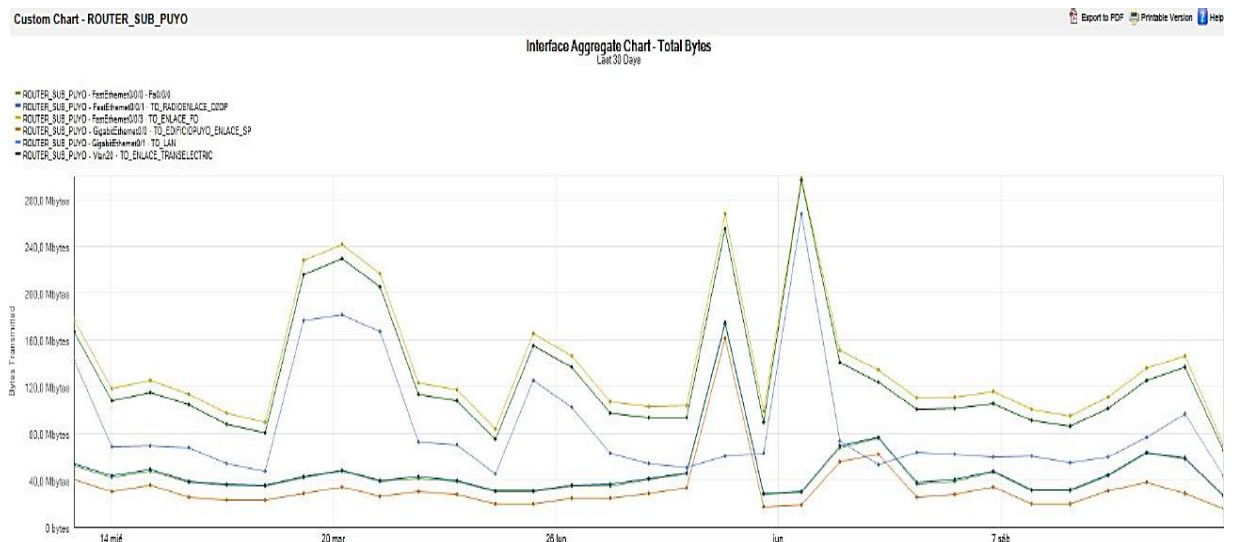


Figura 6. Bytes transmitidos en Router SubPuyo
Elaborado por: Investigador

Nodo Switch Subestación Puyo

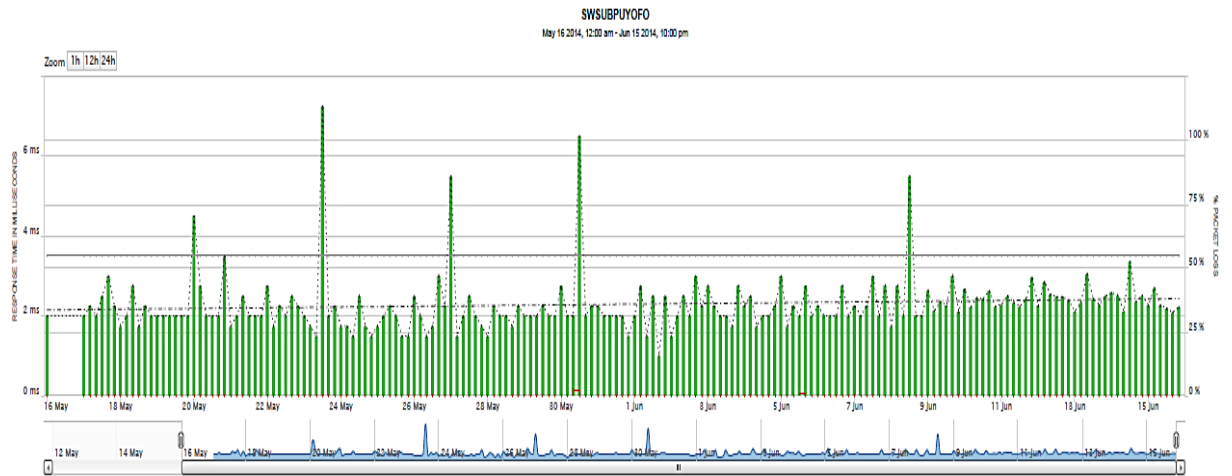


Figura 7. Tiempo de respuesta en Nodo Switch SubPuyo
Elaborado por: Investigador

En la figura 8 se puede visualizar el tiempo de respuesta monitoreado a través de SolarWinds, los datos obtenidos permitieron determinar que el tiempo de respuesta promedio generado en la Subestación Puyo es de 2.39ms, con un promedio de bytes transmitidos de 86 Gbytes, y con una pérdida de paquetes de 0%, se puede concluir que el nodo genera picos en los tiempos de respuesta, debido al tráfico que circula en la red, esto genera que disminuya su velocidad en la transmisión de información a través de sus interfaces.

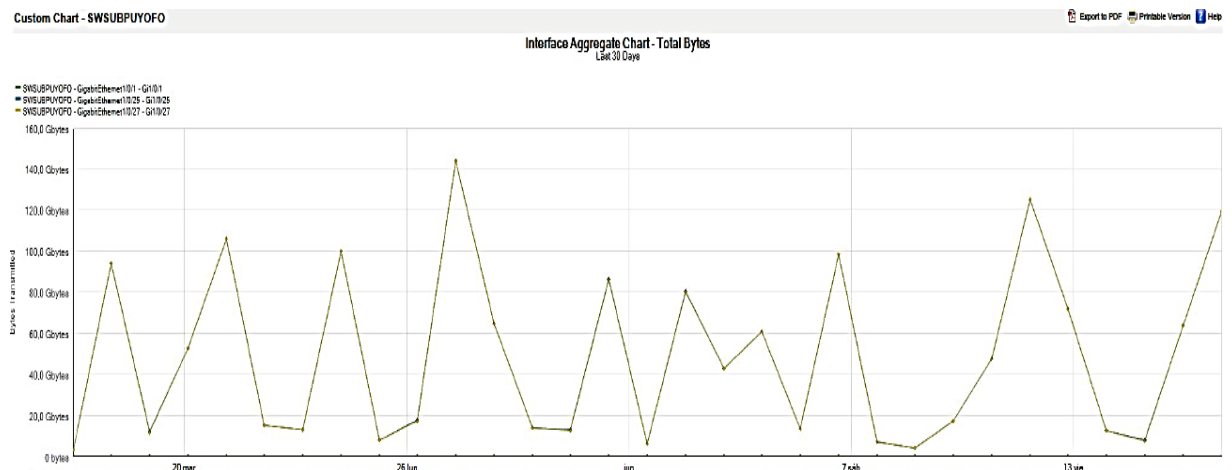


Figura 8. Bytes transmitidos en Switch SubPuyo

Elaborado por: Investigador

Nodo Router Puyo 1

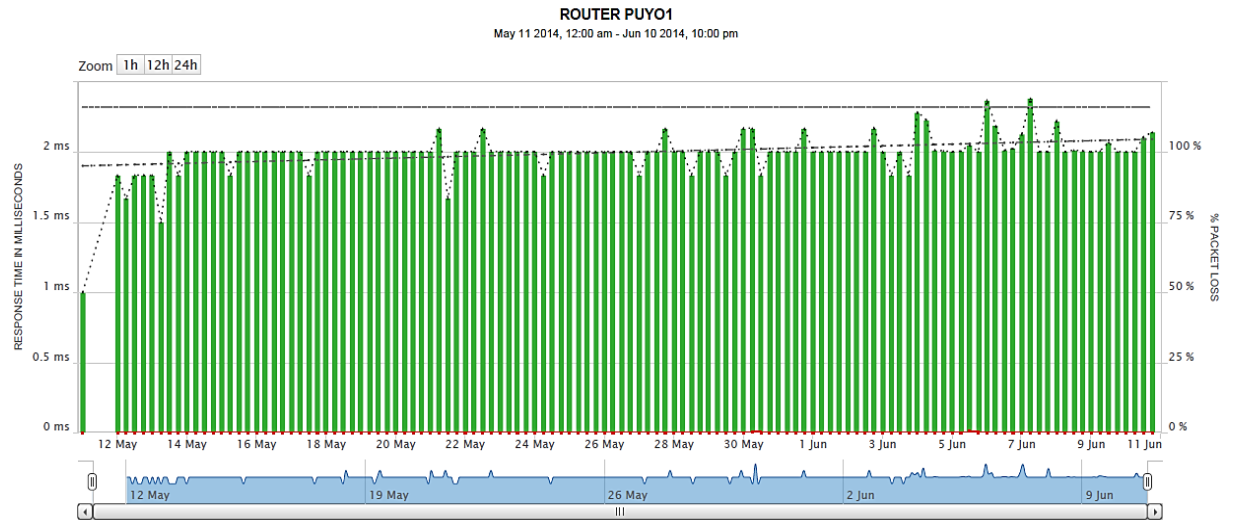


Figura 9. Tiempo de respuesta en Nodo Router Puyo 1

Elaborado por: Investigador

Al realizar el monitoreo del router Puyo 1 a través de SolarWinds se pudo obtener datos como se muestran en la figura 10 y 11, que el tiempo de respuesta promedio en este nodo está en 2,01ms con un promedio de bytes transmitidos de 22,2 Gbytes, y una pérdida de paquetes de 0%, esto indica que el tiempo de respuesta es normal a la hora de transmitir aplicaciones en tiempo real como es el caso de las video conferencias.

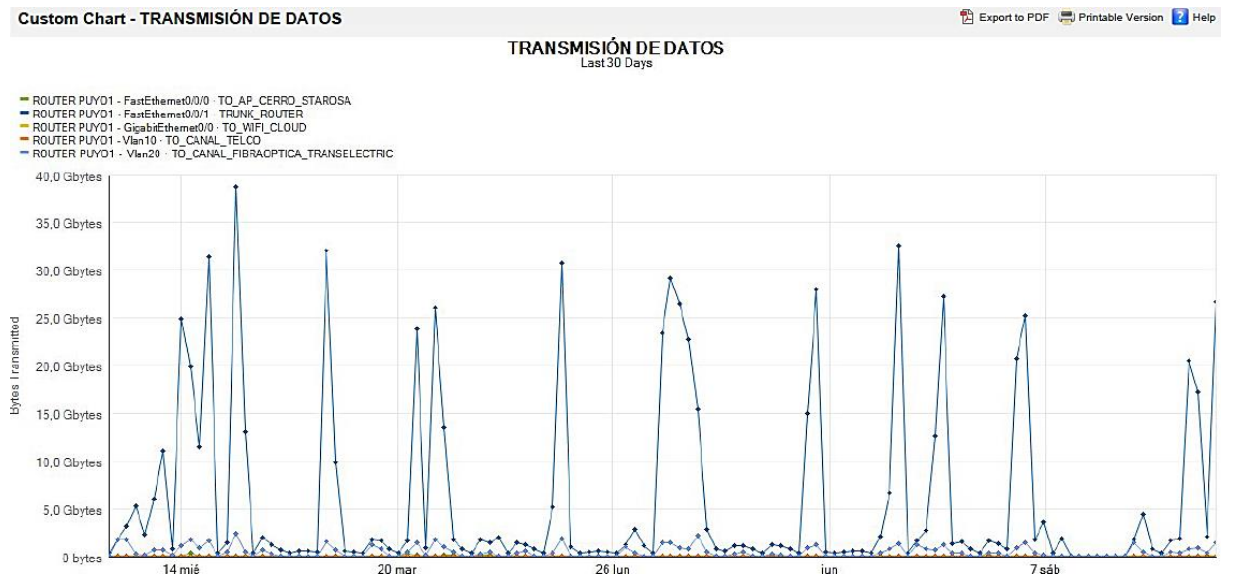


Figura 10. Bytes transmitidos en Nodo Router Puyo 1

Elaborado por: Investigador

Nodo Switch Subestación Tena

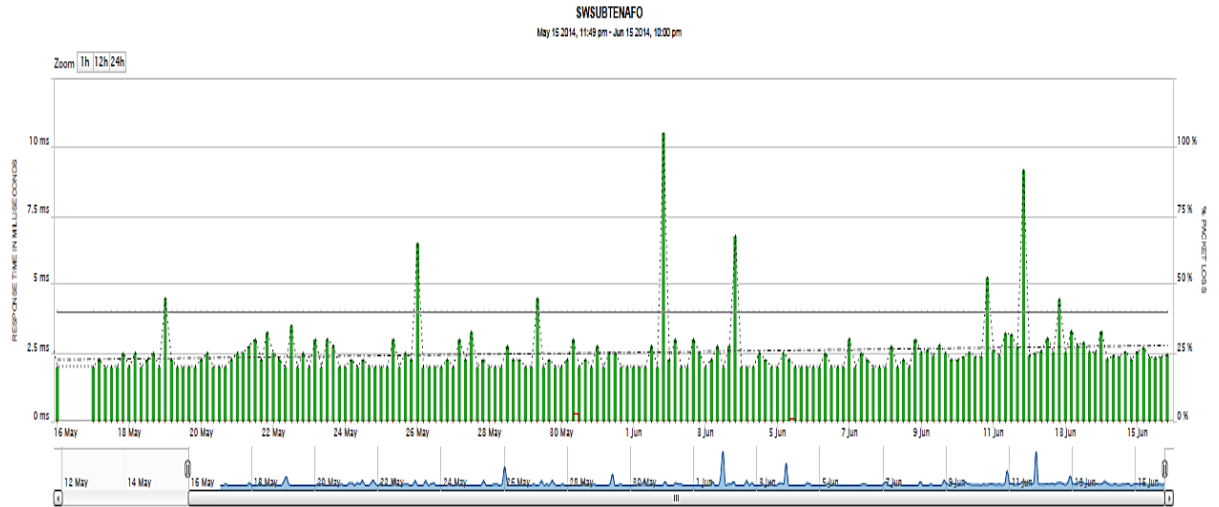


Figura 11. Tiempo de respuesta en Nodo Switch SubTena

Elaborado por: Investigador

Como se puede apreciar en la figura 12 el tiempo de respuesta promedio obtenido es a través del monitoreo de SolarWinds es de 2,59ms, mientras en la figura 13 se determina un promedio de 8.3 Gbytes transmitidos a través de las interfaz GigabitEthernet 1/0/25, con un promedio en la pérdida de paquetes de 0%. Se analiza que la interconexión mediante fibra óptica tiene como ventaja que el tiempo de respuesta sea baja, pero presenta latencia debido a las largas distancias en la interconexión.

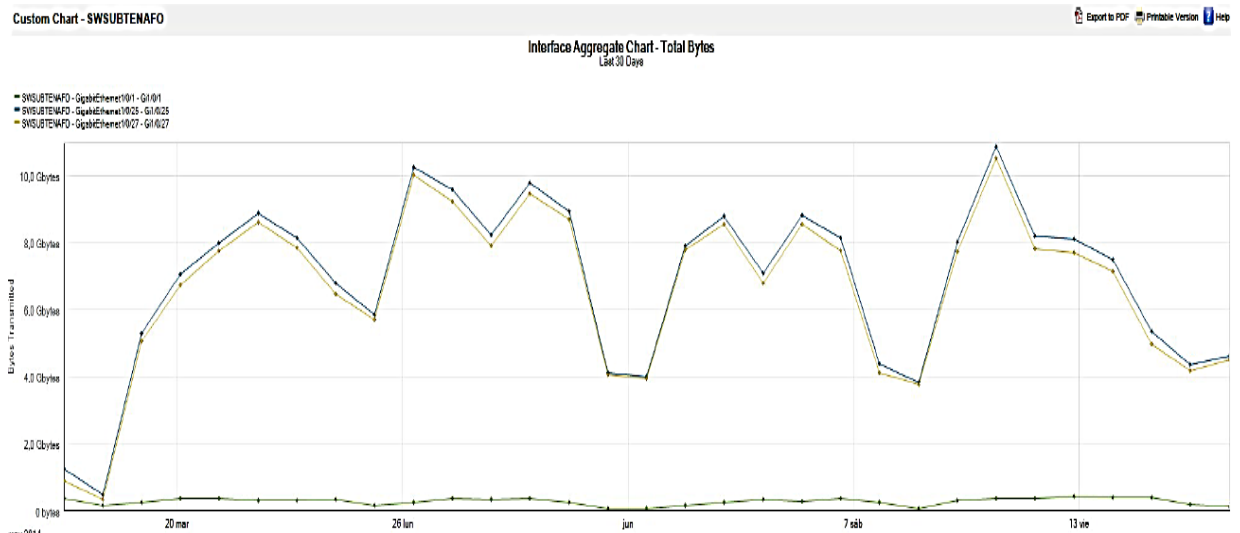


Figura 12. Bytes transmitidos en Nodo Switch SubTena

Elaborado por: Investigador

Router Subestación Tena

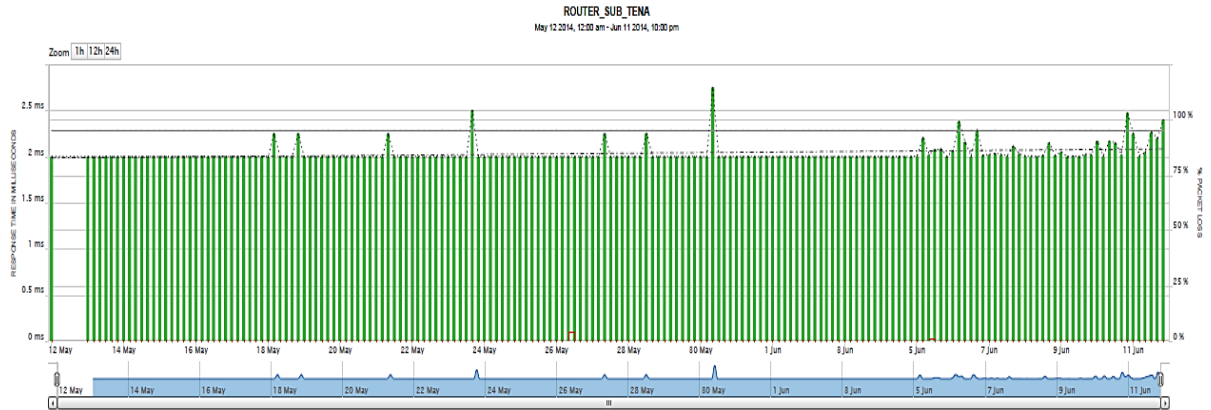


Figura 13. Tiempo de respuesta en Nodo Router SubTena

Elaborado por: Investigador

En este caso se realizó el análisis de los tiempos de respuesta generados en el router de la Subestación Tena como se puede observar en la figura 14, en el cual se puede determinar que el promedio de respuesta a la hora de la transmisión de paquetes es de 2,03ms, en este caso la cantidad de bytes transmitidos en este nodo tiene un promedio de 387 Mbytes, como se puede apreciar en la figura 1, lo cual indica que el router no presenta una alta congestión de tráfico de datos, debido a que los datos transmitidos no son tan altos y por ende presenta pérdida de datos del 0%.

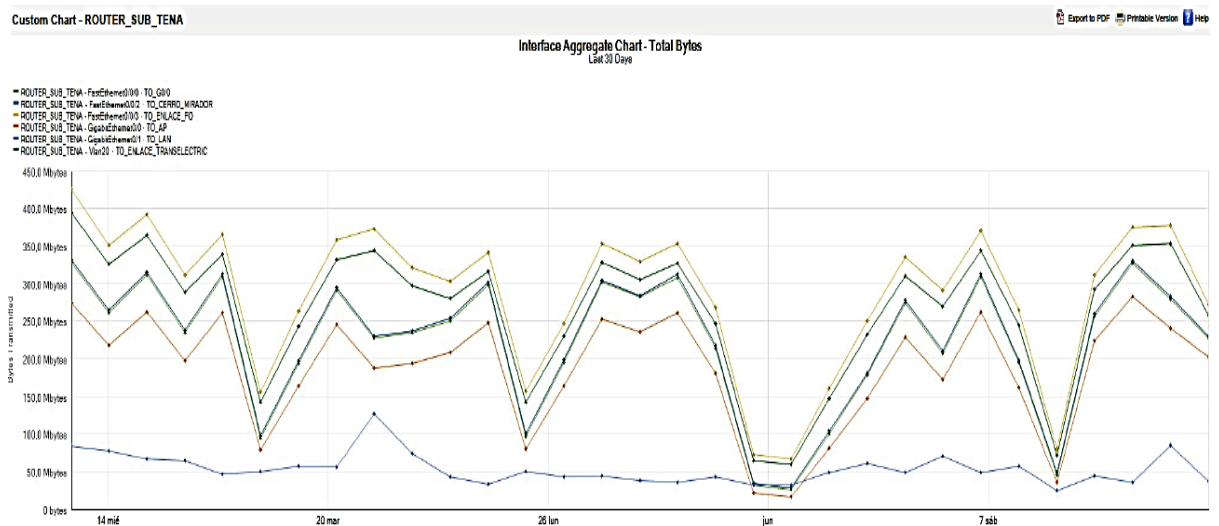


Figura 14. Bytes transmitidos en Nodo Router SubTena

Elaborado por: Investigador

Router Tena1

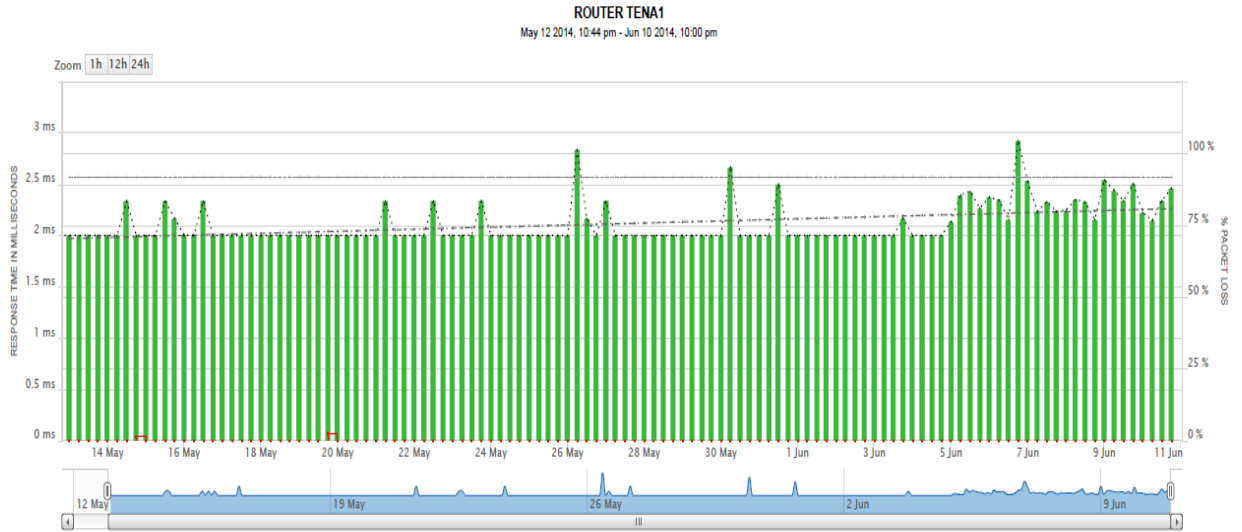


Figura 15. Tiempo de respuesta en Nodo Router Tena 1

Elaborado por: Investigador

A igual que los anteriores nodos el router Tena 1 presenta un promedio en el tiempo de respuesta de 2.06ms, con una pérdida de paquetes de 0%, debido a que la interconexión es a través de fibra óptica y un promedio de bytes transmitidos de 6,82 Gbytes en interfaces GigabitEthernet.

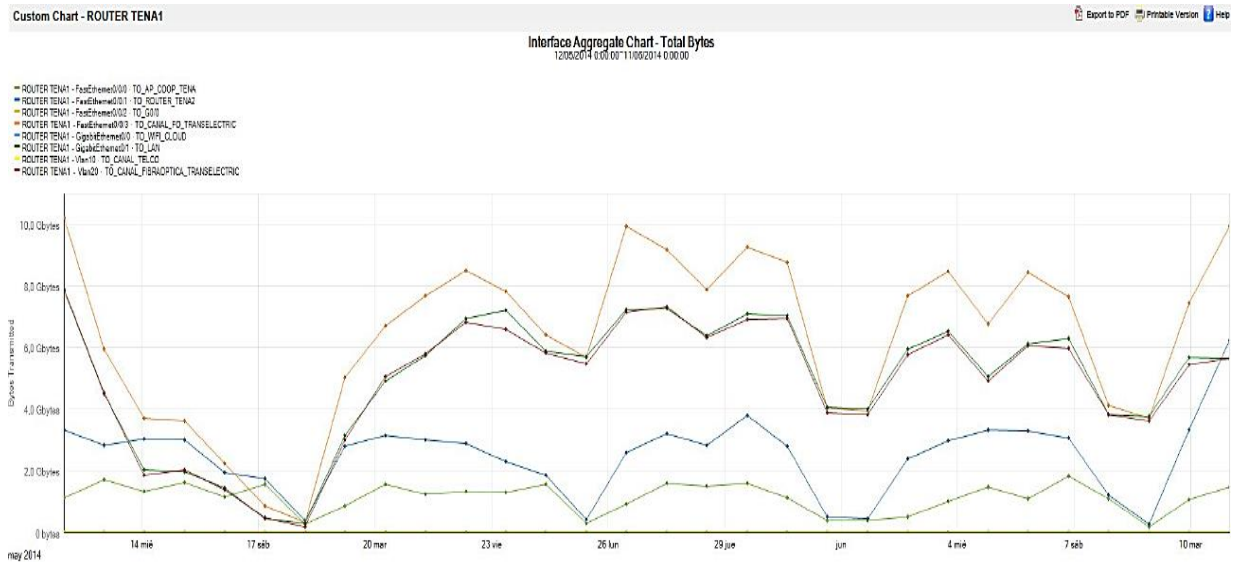


Figura 16. Bytes transmitidos en Nodo Router Tena 1

Elaborado por: Investigador

Router Tena 2

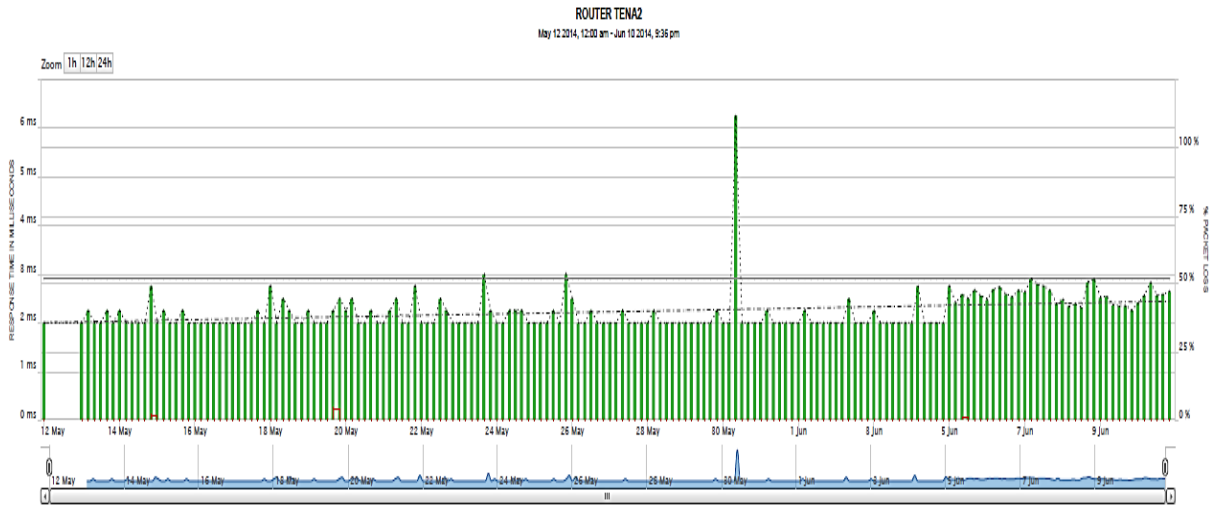


Figura 17. Tiempo de respuesta en Nodo Router Tena 2

Elaborado por: Investigador

En el router utilizado en Tena 2, se puede visualizar que el tiempo de respuesta tiene un promedio de 2,59 ms con un promedio de bytes transmitidos de 5.2 Gbytes, en el cual se analizó que este equipo presenta una pérdida de paquetes de un 0%, debido al enlace a través de fibra óptica.

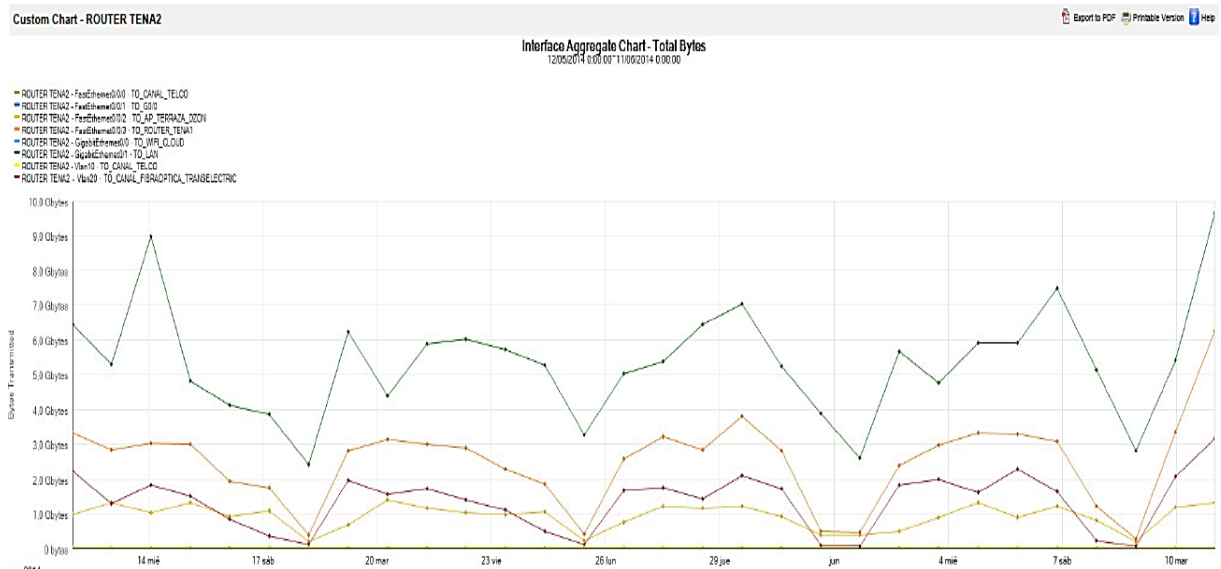


Figura 18. Bytes transmitidos en Nodo Router Tena 2

Elaborado por: Investigador

A continuación se presenta los tiempos de respuesta monitoreados a través de SolarWinds aplicado a los Radioenlaces que permiten la interconexión de la red MAN, el tiempo de respuesta promedio, la pérdida de paquetes se visualiza en la tabla perteneciente al Capítulo 4.

NODO RADIOENLACE NITÓN-SANTA ROSA (PUYO)

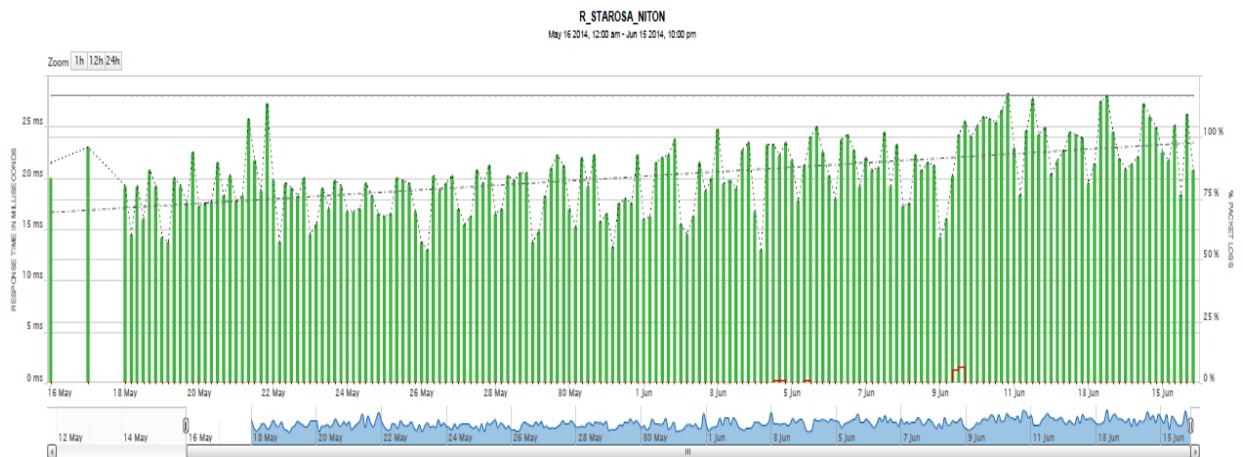


Figura 19. Tiempo de respuesta en Nodo Nitón-Santa Rosa

Elaborado por: Investigador

NODO RADIOENLACE LOMAGRANDE – BAÑOS

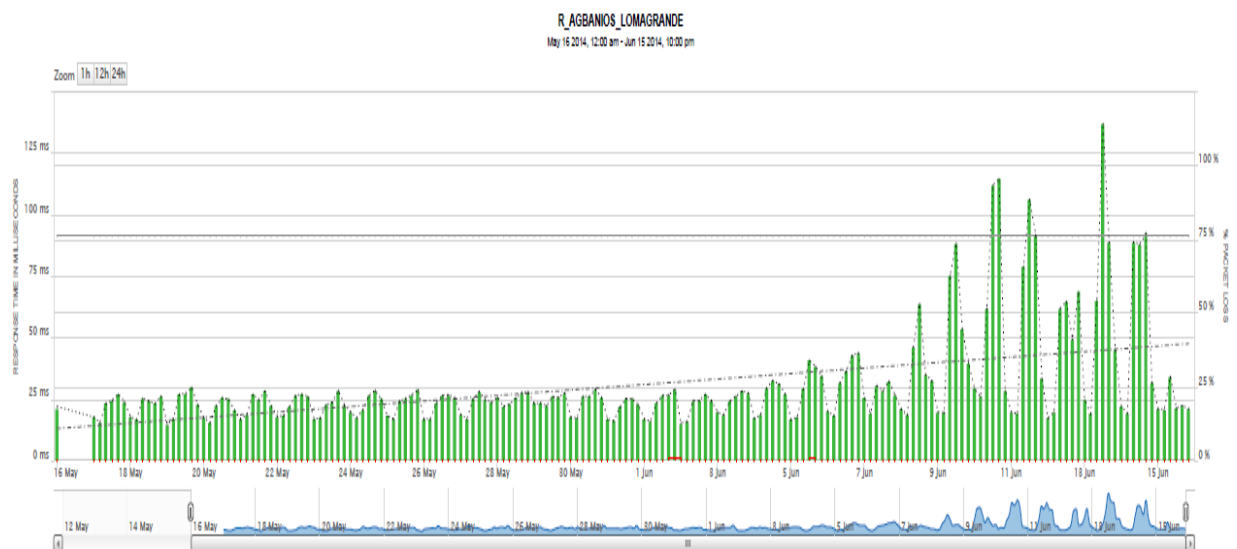


Figura 20. Tiempo de respuesta en Nodo Loma Grande-Baños

Elaborado por: Investigador

NODO RADIOENLACE LOMAGRANDE – SANTA ROSA

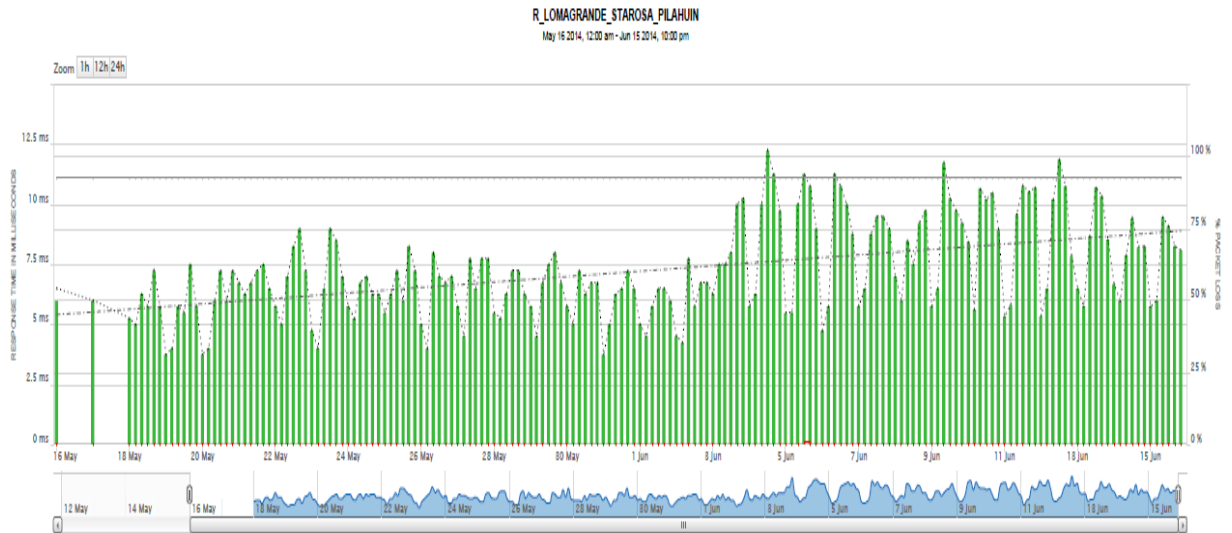


Figura 21. Tiempo de respuesta en Nodo Router Tena 2

Elaborado por: Investigador

NODO RADIOENLACE NITON - SUBHUACHI

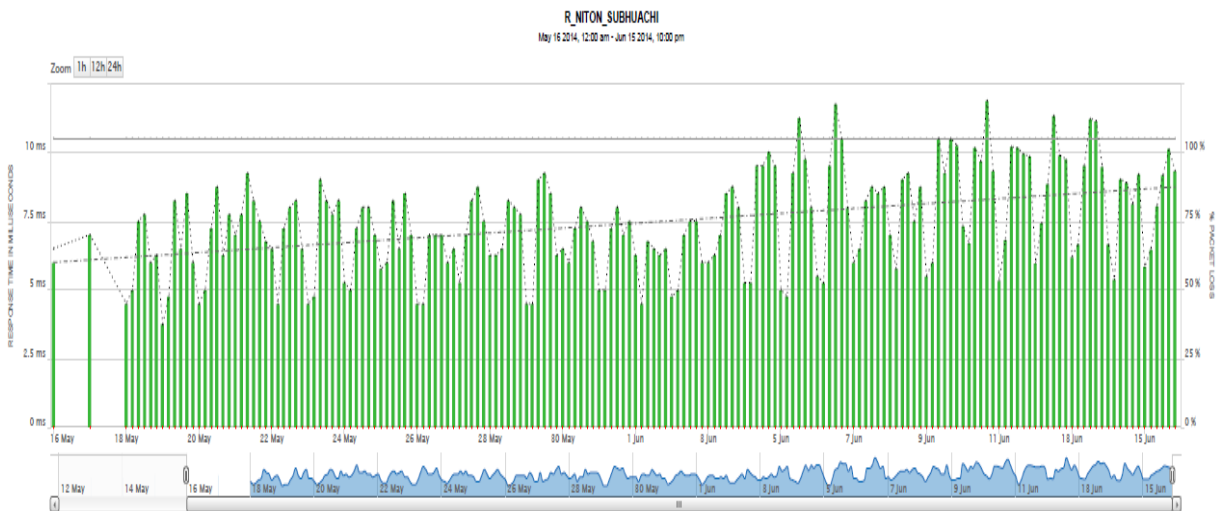


Figura 22. Tiempo de respuesta en Nodo Router Tena 2

Elaborado por: Investigador

NODO RADIOENLACE NITON - SUBAMBATO

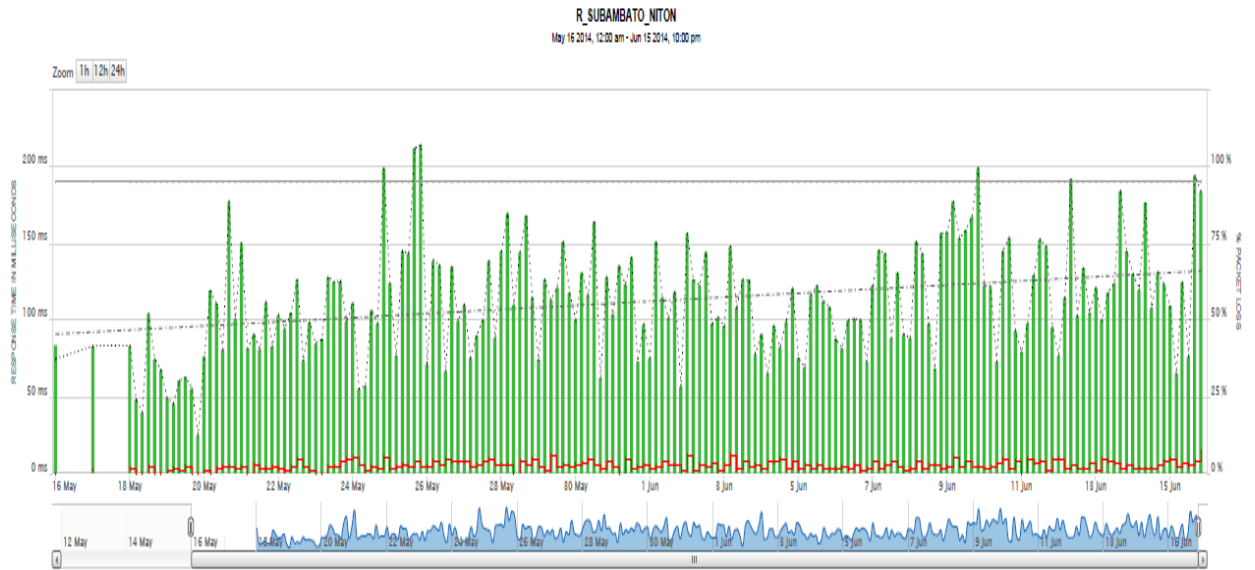


Figura 23. Tiempo de respuesta en Nodo Router Tena 2

Elaborado por: Investigador

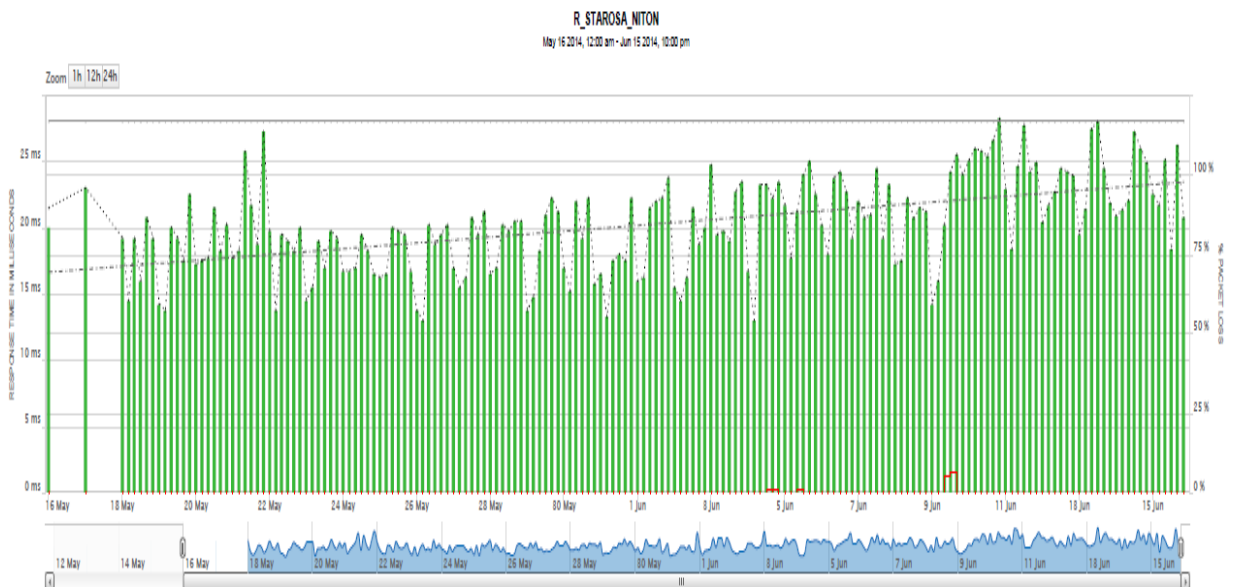


Figura 24. Tiempo de respuesta en Nodo Router Tena 2

Elaborado por: Investigador

NODO RADIOENLACE NITON - SUBPELILEO

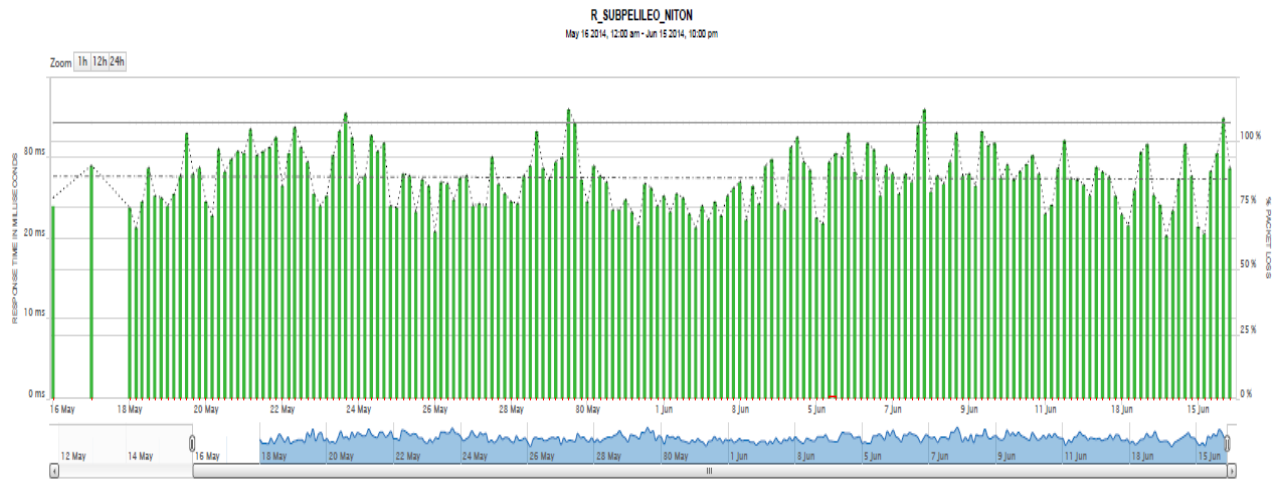


Figura 25. Tiempo de respuesta en Nodo Router Tena 2

Elaborado por: Investigador

NODO RADIOENLACE EDIFICIO PRINCIPAL

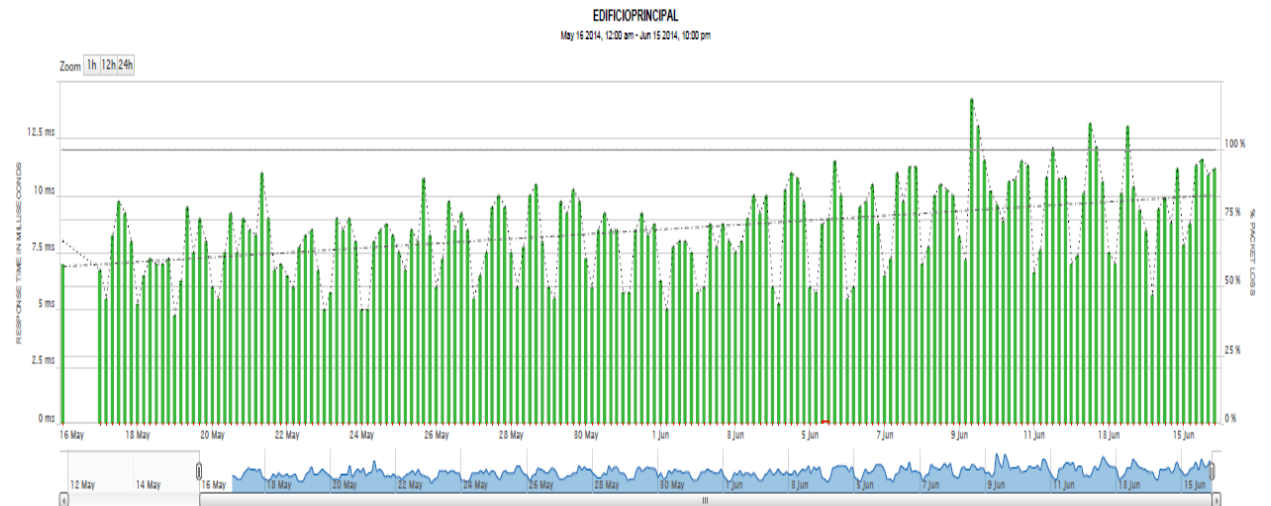


Figura 26. Tiempo de respuesta en Nodo Router Tena 2

Elaborado por: Investigador

ANEXO 2

Configuraciones desarrolladas en OPNET MODELER

A continuación se puede visualizar la configuración de las diferentes aplicaciones generadas en OPNET Modeler, el cual permitirá generar tráfico en la red Inalámbrica.

En la figura 1 se visualiza la configuración de la aplicación de FTP, en la cual se define la aplicación en este caso FTP, para posteriormente elegir una de las descripciones que caracterizara esta aplicación, para finalmente configurar los parámetros con cual la aplicación se ejecutara. En este caso el tamaño del archivo será de 500 bytes, con un tipo de priorización de Best Effort (0).

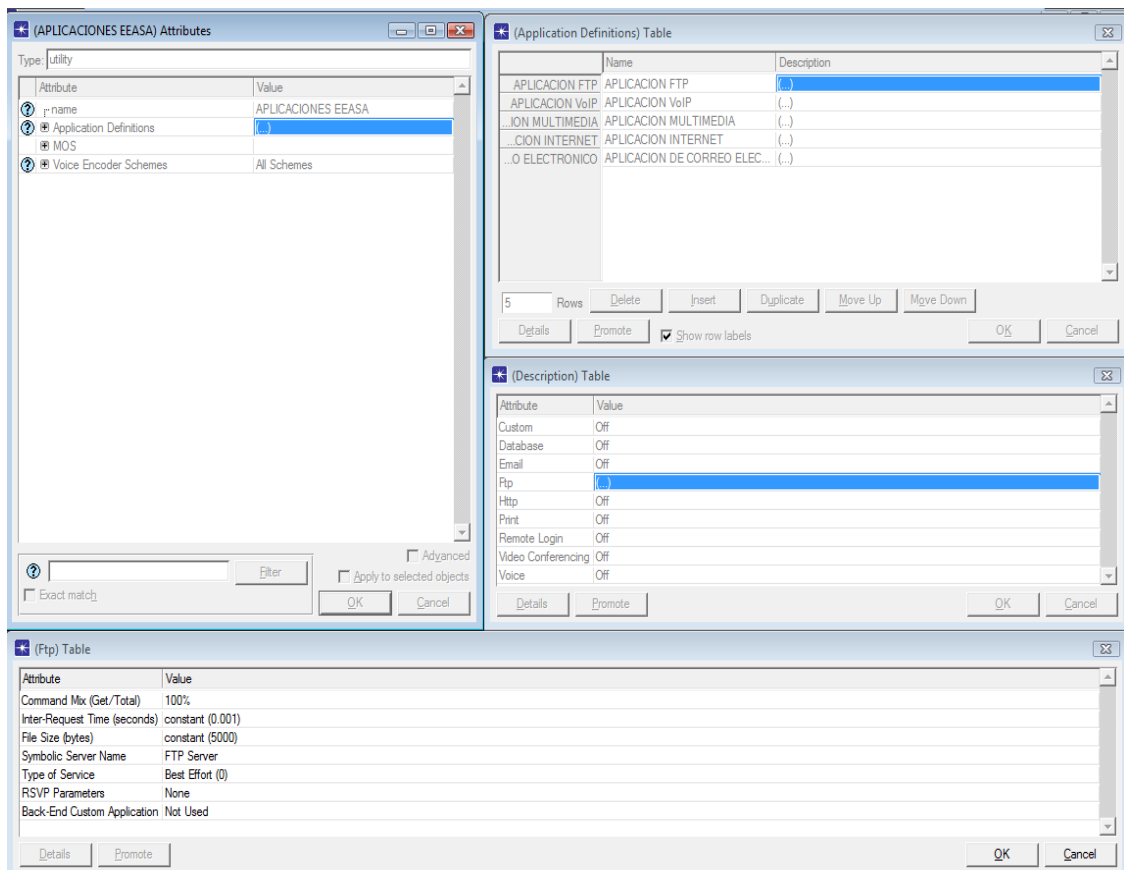


Figura 1. Configuración de Aplicación de FTP
Elaborado por: Investigador

Del mismo modo en la figura 2 se visualiza la configuración de la aplicación de video, para la configuración procedemos a definir la aplicación, para posteriormente elegir una de las descripciones que caracterizara esta aplicación, para finalmente configurar los parámetros con las que operara esta aplicación, en este caso el tamaño de la trama es de 128x120 y el tipo de servicio con el cual operara es Interactive multimedia (5).

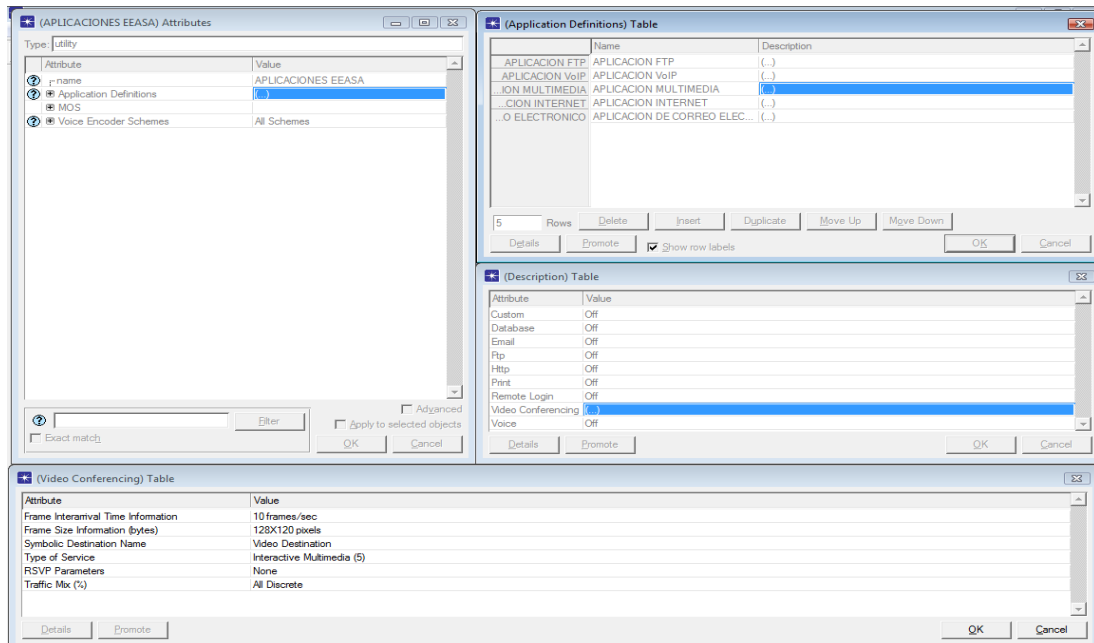


Figura 2. Configuración de Aplicación de Video
Elaborado por: Investigador

En la figura 3 se visualiza la configuración de la aplicación web, para la configuración procedemos a definir la aplicación, para posteriormente elegir una de las descripciones que caracterizara esta aplicación, para finalmente configurar los parámetros con las que operara esta aplicación el tipo de servicio configurado es de Best Effort.

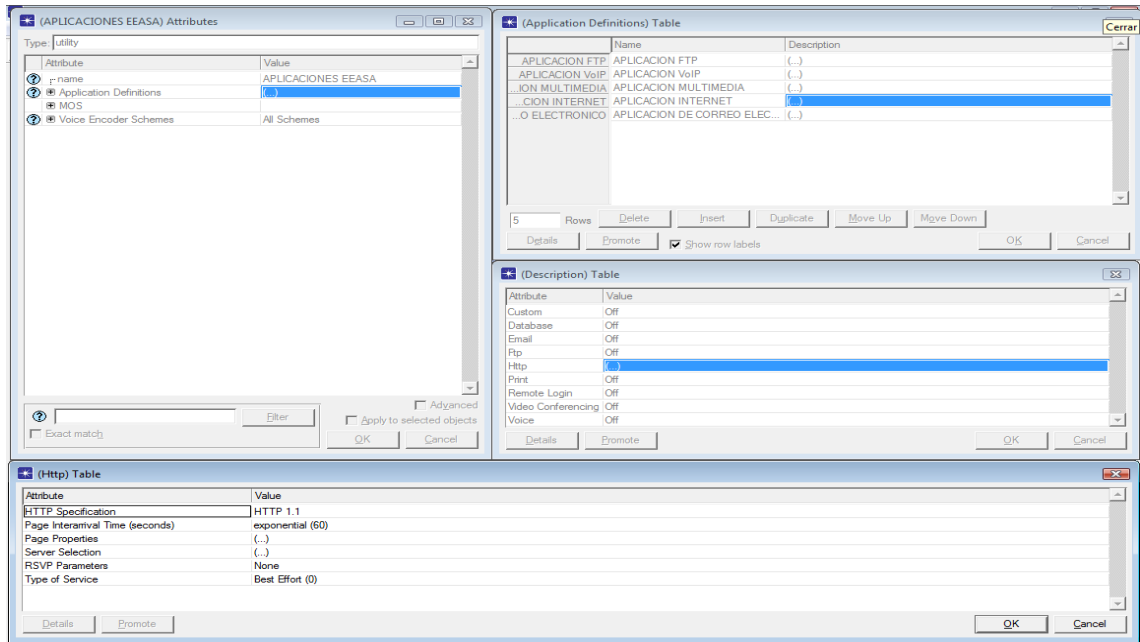


Figura 3. Configuración de Aplicación HTTP
Elaborado por: Investigador

En la figura 4 se visualiza la configuración de la aplicación de correo electrónico, para la configuración procedemos a definir la aplicación, para posteriormente elegir una de las descripciones que caracterizara esta aplicación, para finalmente configurar los parámetros con las que operara esta aplicación.

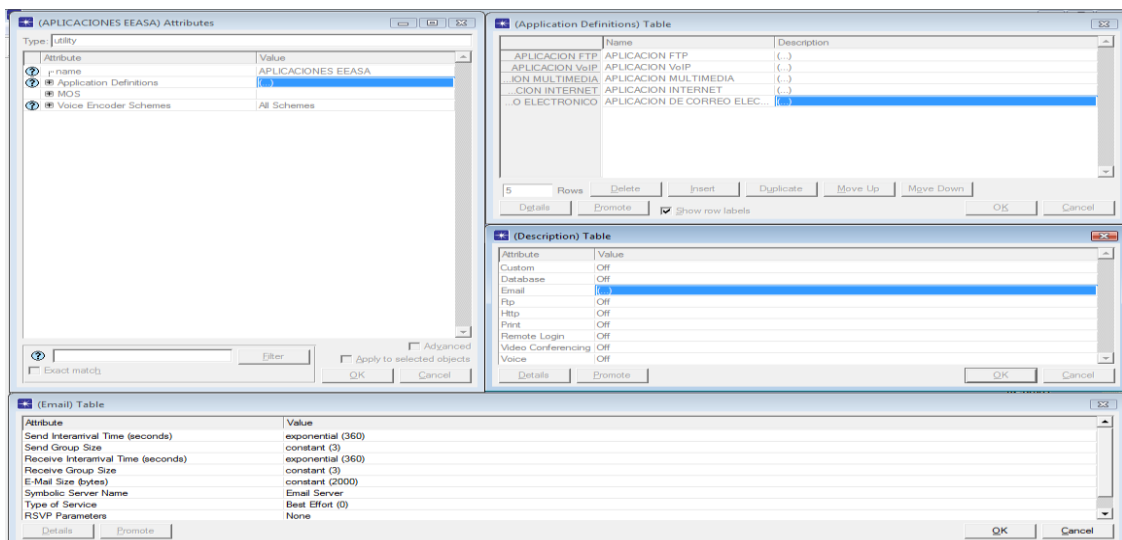


Figura 4. Configuración de Aplicación de E-MAIL
Elaborado por: Investigador

En la figura 5 se visualiza la configuración de los perfiles que tendrá cada aplicación, en el que soportara servicios de VoIP, web y email.

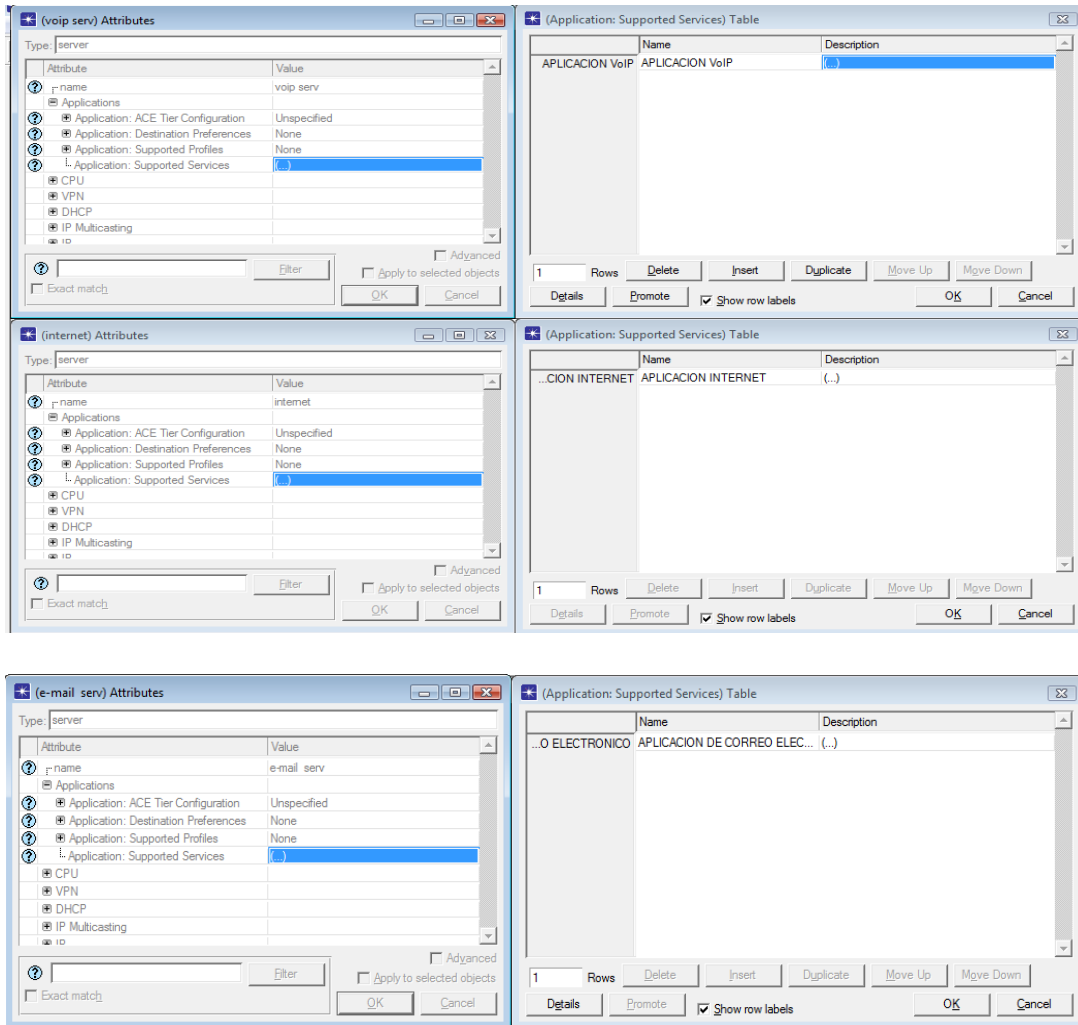


Figura 5. Configuración de Perfiles

Elaborado por: Investigador

ANEXO 3

Configuración de Servidores Simulados en GNS3

Configuración de Servidores de VoIP.

Configuración del Cisco IP Communicator.

Ahora que el Cisco IP Communicator se encuentra instalado en el ordenador, al iniciarlo, mostrara un nuevo asistente, el cual realizara el reconocimiento de los dispositivos de audio, una vez que certificada la funcionalidad de estos, clic en finalizar para iniciar el softphone.

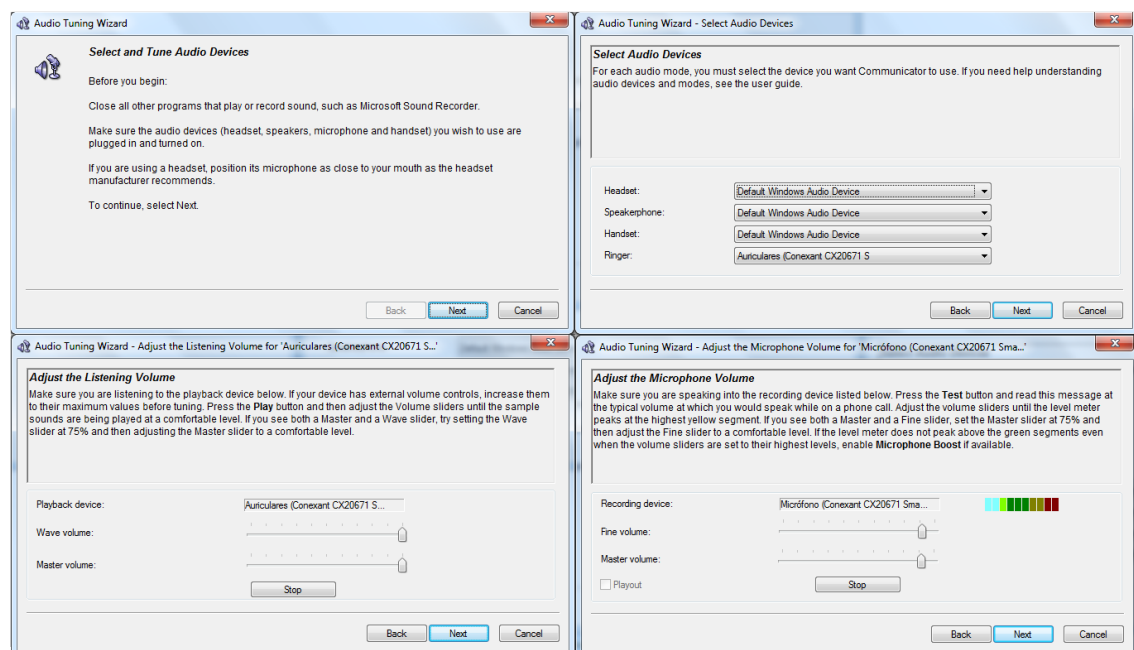


Figura 1 Reconocimiento de los dispositivos de audio.

Ya comprobados los dispositivos de audio necesarios para el funcionamiento óptimo del Cisco IP Communicator, mostrara un mensaje informativo indicando que no se ha configurado un servidor TFTP para el softphone, clic en aceptar y aparecerá una ventana donde se colocara la dirección IP del servidor TFTP, en este caso será la misma IP del Call Manager Express ya que este también actuara como un servidor TFTP para los softphone y en la parte superior seleccionamos la interfaz física del ordenador que utilizara el Cisco IP Communicator para realizar la comunicación de voz, una vez configurado el servidor TFTP y realiza la elección de la interfaz a utilizar, luego clic en aceptar.

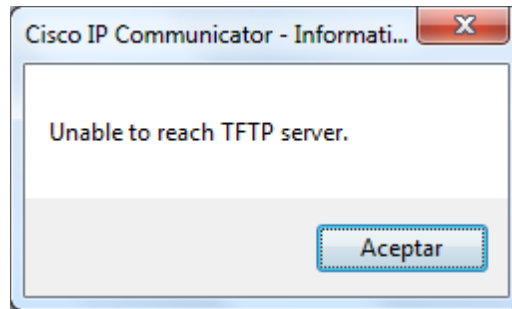


Figura 2 Mensaje informativo.

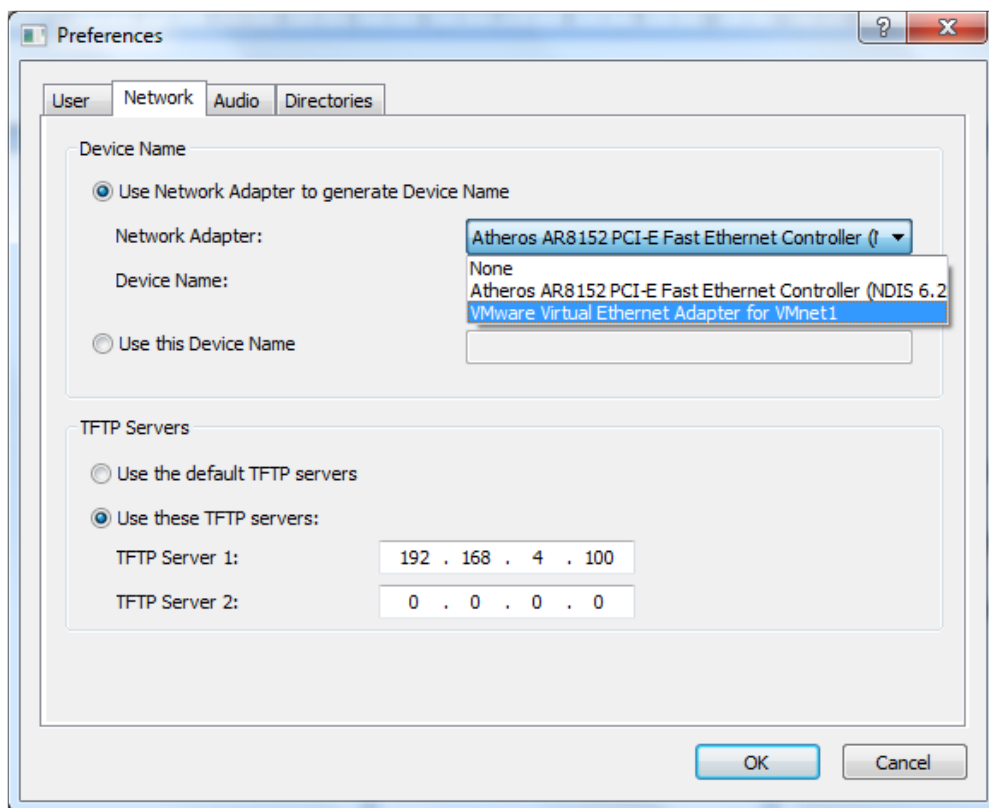


Figura 3. Configuración del servidor TFTP é Interfaz a utilizar

Ahora que el softphone tiene la configuración deseada, iniciara la búsqueda de su perfil de usuario en el servidor TFTP para tener comunicación con los demás softphone.

Configuración de Servidores de Video

Para generar tráfico de Video Streaminfg se utilizó el Software de VLC, a continuación se detalla los pasos para la configuración de la herramienta.

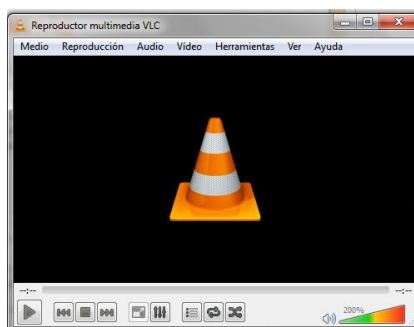


Figura 4. Presentación VLC

Para el iniciar el proceso de emisión, pulsamos en *Medio->Emitir*

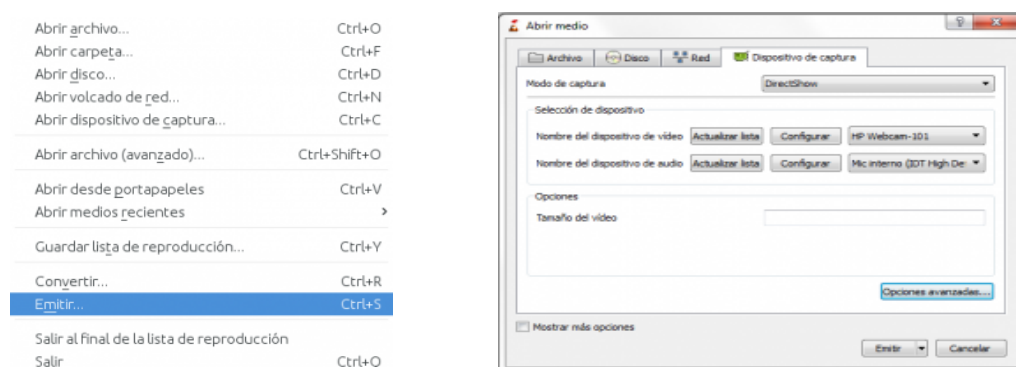


Figura 5. Esquema de Emisión de Video

Tras esto Vlc nos muestra una ventana en la que podemos seleccionar el contenido que queremos emitir. Podemos elegir archivos de vídeo que tengamos en el ordenador o videos streams procedentes de otras fuentes, como internet, finalmente, seleccionar como fuente de contenido a emitir algún dispositivo de captura que tengamos en el ordenador.

Seleccionamos como dispositivo de vídeo y audio la webcam y el micrófono interno disponibles en el portátil para emitir a otros ordenadores lo que captura la webcam. El resto del proceso para configurar la emisión es igual seleccionemos la fuente de vídeo que elijamos, así que no hay problema si se quiere realizar pruebas con alguna de las otras fuentes disponibles.

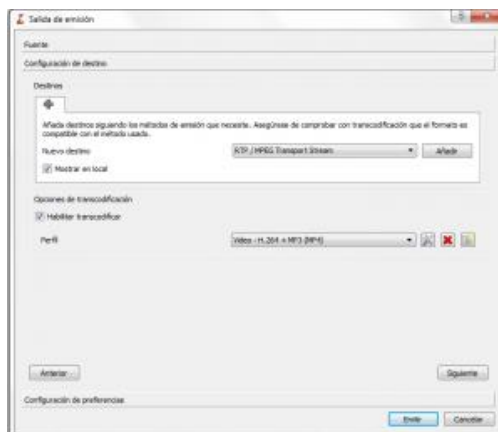


Figura 6. Esquema de Emisión de Video

Una vez configurada la fuente de la emisión configuramos las opciones con las que se emitirá.

Cuenta con tres apartados:

- ❖ **Fuente:** en el que se muestra el dispositivo que seleccionamos en el paso anterior como fuente del flujo.
- ❖ **Configuración de destino:** donde seleccionamos con qué formato y medio queremos realizar la emisión.
- ❖ **Configuración de preferencias:** donde podemos ajustar algunos parámetros finales.

Para movernos entre estos tres pasos para configurar la salida de la emisión lo podemos hacer mediante los botones de Siguiente y Anterior o pulsando sobre el nombre del apartado. Para configurar nuestra emisión dejamos el primer paso como está, y en el segundo, Configuración de destino, seleccionamos RTP/MPEG Transport Stream como destino de la emisión. Tras pulsar en Añadir, hay que indicar la dirección ip del dispositivo donde queramos ver la emisión.

Tras esto pulsamos Siguiente para ir al último paso de la configuración de la emisión, Configuración de preferencias.

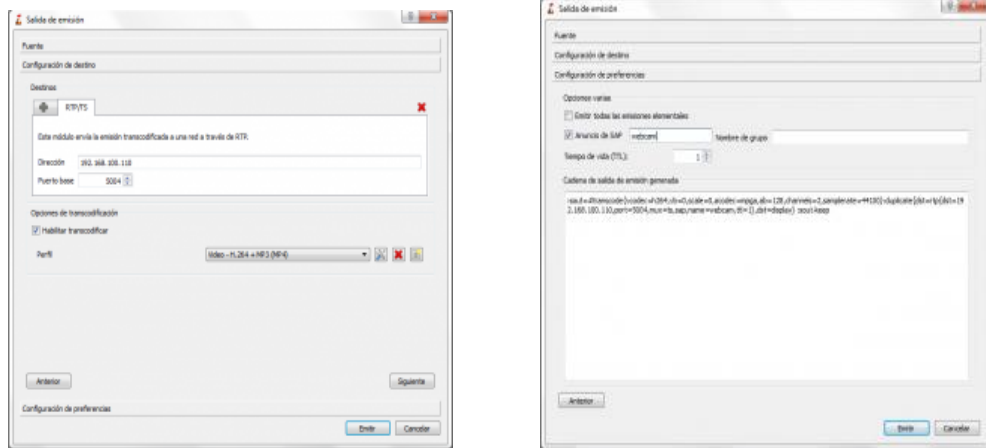


Figura 7. Fuente de emisión y destino

En este apartado activamos la casilla *Anuncio de SAP* y le asignamos un nombre para que la emisión se anuncie en el dispositivo con la *ip* que hemos indicado anteriormente.

Hecho esto, pulsamos en el botón de *Emitir* y comenzamos la emisión.

Visionar la emisión en la red

Una vez iniciada la emisión arrancamos Vlc en el otro ordenador donde queramos verla, con la *ip* que indicamos anteriormente.

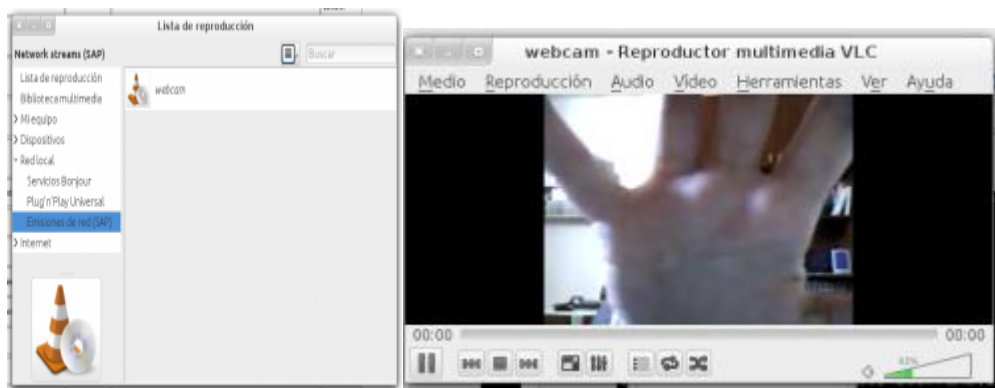


Figura 8. Emisor de Video Streaming

Si todo ha ido bien, una vez en Vlc, abrimos la lista de reproducción, en *Red local* -> *Emissiones de red (SAP)* debe aparecer el nombre de la emisión que acabamos de crear. Al hacer doble click sobre ella iniciaremos la visualización de la emisión.

http:// seguido de la dirección *ip* del equipo que está emitiendo vídeo para acceder al mismo.

ANEXO 4

Configuración de Routers realizado En Gns3

Router Matriz

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname MATRIZ
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
!
no ip domain lookup
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
!
crypto pki trustpoint TP-self-signed-4279256517
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-4279256517
revocation-check none
rsa-keypair TP-self-signed-4279256517
!
!
crypto pki certificate chain TP-self-signed-4279256517
certificate self-signed 01
3082023E 308201A7 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
69666963 6174652D 34323739 32353635 3137301E 170D3032 30333031 30303030
32355A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D34 32373932
35363531 3730819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
8100C281 2BCAB98B 4513E7D2 3AAD95FF 3BA4850A 1C9BBD36 B1AC2FA3 004B4A2C

quit
username matriz privilege 15 secret 5 $1$Q9uy$a6haQmbTiguq5Bh2gtEbc/
!
!
ip tcp synwait-time 5
!
class-map match-all MULTIMEDIA
match access-group name MULTIMEDIA-CONFERENCIA
class-map match-any DATO
match access-group name DATOS
```

```

class-map match-all VoIP
  match access-group name VoIP-CONTROL
class-map match-all TRANSACCION
  match access-group name TRANSACCION-DATOS
!
!
policy-map EEASA-POLITICA-QOS
  class VoIP
    set ip dscp ef
  class MULTIMEDIA
    set ip dscp af31
  class TRANSACCION
    set ip dscp af21
  class DATO
    set ip dscp cs3
policy-map EEASA-POLITICA-QOS-S
  class VoIP
    set ip dscp ef
    bandwidth percent 14
  class MULTIMEDIA
    set ip dscp af31
    bandwidth percent 14
  class TRANSACCION
    set ip dscp af21
    bandwidth percent 10
  class DATO
    set ip dscp cs3
    bandwidth percent 8
!
!
interface FastEthernet0/0
  ip address 172.20.61.1 255.255.254.0
  ip flow egress
  ip route-cache flow
  speed 100
  full-duplex
  service-policy output EEASA-POLITICA-QOS-S
!
interface Serial0/0
  ip address 10.20.1.1 255.255.255.252
  clock rate 2000000
  service-policy output EEASA-POLITICA-QOS-S
!
interface FastEthernet0/1
  ip address 192.168.0.1 255.255.255.0
  ip flow ingress
  duplex auto
  speed auto
  service-policy input EEASA-POLITICA-QOS
  service-policy output EEASA-POLITICA-QOS-S
!
interface Serial0/1
  no ip address
  shutdown
  clock rate 2000000
!
router ospf 1
  log-adjacency-changes

```

```

network 10.20.1.0 0.0.0.3 area 0
network 172.20.60.0 0.0.1.255 area 0
network 192.168.0.0 0.0.0.255 area 0
!
router rip
version 2
network 172.20.0.0
network 192.168.0.0
!
ip forward-protocol nd
!
ip flow-export version 5
ip flow-export destination 192.168.0.10 4444
!
ip http server
ip http authentication local
ip http secure-server
!
ip access-list extended DATOS
permit tcp any any range ftp-data ftp
permit tcp any any eq ftp-data
remark SSH/SFTP
permit tcp any any eq 22
permit tcp any any eq smtp
permit tcp host 192.168.2.11 host 192.168.0.11 eq 8080
permit tcp any any eq 445
permit udp any any eq 445
permit udp any host 192.168.0.10 eq 445
permit tcp any host 192.168.0.10 eq 445
permit udp any host 192.168.0.10 range netbios-ns netbios-dgm
permit tcp any host 192.168.0.10 eq 139
permit udp host 192.168.2.11 host 192.168.0.10 eq 8080
permit udp host 192.168.4.13 host 192.168.0.10 eq 8080
permit tcp host 192.168.2.11 host 192.168.0.10 eq 8080
permit tcp host 192.168.4.13 host 192.168.0.10 eq 8080
ip access-list extended MULTIMEDIA-CONFERENCIA
permit udp any any range 16384 32767
permit tcp any any range 16384 32767
ip access-list extended TRANSACCION-DATOS
permit tcp any any eq 443
permit tcp any any eq 1521
permit udp any any eq 1521
permit icmp any host 192.168.0.10
permit tcp any host 192.168.0.10 eq www
ip access-list extended VoIP-CONTROL
permit tcp any any range 2000 2002
permit udp any any range 5060 5061
permit tcp any any range 5060 5061
!
control-plane
!
!
telephony-service
max-ephones 50
max-dn 50
ip source-address 192.168.0.1 port 2000
system message EMPRESA ELECTRICA AMBATO S.A
create cnf-files version-stamp Jan 01 2002 00:00:00

```

max-conferences 8 gain -6

```
ephone-dn 1 dual-line
number 101
label Matriz
name Matriz
!
!
ephone-dn 2 dual-line
number 102
label Loreto
name Loreto
!
!
ephone-dn 3 dual-line
number 105
label EDPuyo
name EDPuyo
!
!
ephone-dn 4 dual-line
number 108
label Tena
name Tena
!
!
ephone 1
mac-address 000C.297C.60B9
button 1:1 2:2
!
ephone 2
mac-address 0800.2771.BABB
button 5:3 8:2
!
ephone 3
mac-address 000C.29D2.A22D
button 5:1 8:4
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
password cisco
logging synchronous
login local
!
!
end
```

Router Tena

```
TENA2(config)#interface fastEthernet 0/1
TENA2(config-if)#ip flow egress
```

```

TENA2(config-if)#ip flow ingress
TENA2(config-if)#exit
TENA2(config)#ip flow-export version 5
TENA2(config)#ip flow-cache timeout active 1
TENA2(config)#ip flow-cache timeout inactive 15
TENA2(config)#ip flow-export destination 192.168.0.10 4444
TENA2(config)#ip flow-export source fastEthernet 0/1
TENA2(config)#end
TENA2(config)#ip access-list extended MULTIMEDIA-CONFERENCIA
TENA2(config-ext-nacl)#permit UDP any any range 16384 32767
TENA2(config-ext-nacl)#exit

TENA2(config)#ip access-list extended TRANSACCION-DATOS
TENA2(config-ext-nacl)#permit tcp any any eq 443
TENA2(config-ext-nacl)#permit tcp any any eq 1521
TENA2(config-ext-nacl)#permit udp any any eq 1521
TENA2(config-ext-nacl)#permit icmp any host 192.168.2.11
TENA2(config-ext-nacl)#permit tcp any host 192.168.2.11 eq www
TENA2(config-ext-nacl)#exit

TENA2(config)#ip access-list extended DATOS
TENA2(config-ext-nacl)#permit tcp any any eq ftp
TENA2(config-ext-nacl)#permit tcp any any eq ftp-data
TENA2(config-ext-nacl)#remark SSH/SFTP
TENA2(config-ext-nacl)#permit tcp any any eq 22
TENA2(config-ext-nacl)#exit

TENA2(config)#ip access-list extended VoIP-CONTROL
TENA2(config-ext-nacl)#permit tcp any any range 2000 2002
TENA2(config-ext-nacl)#permit udp any any range 5060 5061
TENA2(config-ext-nacl)#exit

TENA2(config)#class-map match-all TRANSACCION
TENA2(config-cmap)#match access-group name TRANSACCION-DATOS

TENA2(config)#class-map match-all MULTIMEDIA
TENA2(config-cmap)#match access-group name MULTIMEDIA-CONFERENCIA
TENA2(config-cmap)#exit

TENA2(config)#class-map match-any DATO
TENA2(config-cmap)#match access-group name DATOS
TENA2(config-cmap)#exit

TENA2(config)#class-map match-all VoIP
TENA2(config-cmap)#match access-group name VoIP-CONTROL
TENA2(config-cmap)#exit
TENA2(config)#end

TENA2(config)#policy-map EEASA-POLITICA-QOS
TENA2(config-pmap)#class VoIP
TENA2(config-pmap-c)#set ip ?
    dscp    Set IP DSCP (DiffServ CodePointint)
    precedence Set IP precedence

TENA2(config-pmap-c)#set ip dscp ef
TENA2(config-pmap-c)#exit

TENA2(config-pmap)#class MULTIMEDIA

```

TENA2(config-pmap-c)#set ip dscp af31
TENA2(config-pmap-c)#exit

TENA2(config-pmap)#class TRANSACCION
TENA2(config-pmap-c)#set ip dscp af21
TENA2(config-pmap-c)#exit

TENA2(config-pmap)#class DATO
TENA2(config-pmap-c)#set ip dscp cs3
TENA2(config-pmap-c)#exit
TENA2(config-pmap)#end
TENA2(config)#interface fastEthernet 0/1
TENA2(config-if)#service-policy output EEASA-POLITICA-QOS
TENA2(config-if)#exit

TENA2(config)#interface fastEthernet 0/0
TENA2(config-if)#service-policy output EEASA-POLITICA-QOS
TENA2(config-if)#exit
TENA2(config)#^Z

TENA2(config)#interface serial 0/0
TENA2(config-if)#service-policy output EEASA-POLITICA-QOS
TENA2(config-if)#exit

Santa Clara

SANTA_CLARA(config)#class-map match-all TRANSACCION
SANTA_CLARA(config-cmap)#match dscp af21
SANTA_CLARA(config-cmap)#exit

SANTA_CLARA(config)#class-map match-all VoIP
SANTA_CLARA(config-cmap)#match dscp ef
SANTA_CLARA(config-cmap)#exit

SANTA_CLARA(config)#class-map match-any DATO
SANTA_CLARA(config-cmap)#match dscp cs3
SANTA_CLARA(config-cmap)#exit

SANTA_CLARA(config)#class-map match-all MULTIMEDIA
SANTA_CLARA(config-cmap)#match dscp af31
SANTA_CLARA(config-cmap)#exit

SANTA_CLARA(config)#policy-map EEASA-POLITICA-QOS-S
SANTA_CLARA(config-pmap)#class VoIP
SANTA_CLARA(config-pmap-c)#set ip dscp ef
SANTA_CLARA(config-pmap-c)#bandwidth percent 14
SANTA_CLARA(config-pmap-c)#exit

SANTA_CLARA(config-pmap)#class MULTIMEDIA
SANTA_CLARA(config-pmap-c)#set ip dscp af31
SANTA_CLARA(config-pmap-c)#bandwidth percent 14
SANTA_CLARA(config-pmap-c)#EXIT

SANTA_CLARA(config-pmap)#class TRANSACCION
SANTA_CLARA(config-pmap-c)#set ip dscp af21
SANTA_CLARA(config-pmap-c)#bandwidth percent 10
SANTA_CLARA(config-pmap-c)#exit

```

SANTA_CLARA(config-pmap)#class DATO
SANTA_CLARA(config-pmap-c)#set ip dscp cs3
SANTA_CLARA(config-pmap-c)#bandwidth percent 8
SANTA_CLARA(config-pmap-c)#exit
SANTA_CLARA(config-pmap)#end

SANTA_CLARA(config)#interface serial 0/2
SANTA_CLARA(config-if)#service-policy output EEASA-POLITICA-QOS-S
SANTA_CLARA(config-if)#exit

```

Configuración de Swiches

```

SWPELILEO#vlan database
SWPELILEO(vlan)#vlan 99 name eeasa
VLAN 99 added:
  Name: eeasa
SWPELILEO(vlan)#exit
APPLY completed.
Exiting...
Enter configuration commands, one per line. End with CNTL/Z.
SWPELILEO(config)#interface vlan 99
SWPELILEO(config-if)#ip address 10.20.4.250 255.255.254.0
SWPELILEO(config-if)#no shutdown
SWPELILEO(config-if)#exit

```

```

SWPELILEO(config)#interface fastEthernet 0/0
SWPELILEO(config-if)#switchport mode trunk
SWPELILEO(config-if)#no shutdown
SWPELILEO(config-if)#exit

```

```

SWPELILEO(config)#interface fastEthernet 0/1
SWPELILEO(config-if)#switchport mode trunk
SWPELILEO(config-if)#no shutdown
SWPELILEO(config-if)#exit

```

Configuración Proxim T8000

```

T8000-C1:65:7E>enable
T8000-C1:65:7E #configure
T8000-C1:65:7E(config)#worp-qos
T8000-C1:65:7E(config-worpqos)# class-list
T8000-C1:65:7E(config-worpqos-classlist)# rowadd 0 sfc-index 0 pir-index 0 class-name G711 VoIP
T8000-C1:65:7E(config-worpqos-classlist)# rowadd 0 sfc-index 0 pir-index 0 pir-priority 1
T8000-C1:65:7E(config-worpqos-classlist)# rowadd 0 sfc-index 0 pir-index 0 pir-value 6
T8000-C1:65:7E(config-worpqos-classlist)# rowadd 0 sfc-index 0 pir-index 0 sfc-value 5
T8000-C1:65:7E(config-worpqos-classlist)# rowadd 0 sfc-index 0 pir-index 0 entry-status 4
T8000-C1:65:7E(config-worpqos-classlist)#exit
T8000-C1:65:7E(config-worpqos)#exit
T8000-C1:65:7E(config)#exit
T8000-C1:65:7E#
T8000-C1:65:# show worp-qos class-list
Index 3.2.2
SFC Value : 5
PIR Value : 6
Class Name : G711 VoIP
Priority : 1
Entry status : enable

```

ANEXO 5

Monitoreo de Equipos de La red MAN de EEASA y sus direcciones Ip de administración

MONITOREO DE EQUIPOS RED MAN EEASA ROUTER Y SWITCH

| NODO CISCO | IP | EQUIPO |
|-------------------|---------------|-----------------------------|
| ROUTER PUYO1 | 172.20.7.253 | Cisco 2821 |
| ROUTER PUYO2 | 172.20.7.252 | Cisco 2821 |
| ROUTER TENA1 | 172.20.11.253 | Cisco 2821 |
| ROUTER TENA2 | 172.20.11.252 | Cisco 2821 |
| ROUTER_BACK_FO | 10.20.5.2 | Cisco 2921K9 |
| ROUTER_BANOS | 172.20.3.254 | Cisco 2901K9 |
| ROUTER_CAR_TENA | 172.20.13.30 | Cisco 2901K9 |
| ROUTER_CATIGLATA | 172.20.54.254 | Cisco 2911K9 |
| ROUTER_FICOA | 172.20.29.254 | Cisco 2901K9 |
| ROUTER_HUACHI | 172.20.34.254 | Cisco 2901K9 |
| ROUTER_IZAMBA | 172.20.28.254 | Cisco 2901K9 |
| ROUTER_LORETO | 172.20.4.62 | Cisco 2921K9 |
| ROUTER_MIRADOR | 172.20.62.4 | Cisco 2921K9 |
| ROUTER_NITON | 10.20.1.254 | Cisco 2921K9 |
| ROUTER_PALORA | 172.20.8.254 | Cisco 2901K9 |
| ROUTER_PATATE | 172.20.3.126 | Cisco 2901K9 |
| ROUTER_PELILEO | 172.20.3.190 | Cisco 2901K9 |
| ROUTER_PILLARO | 172.20.3.62 | Cisco 2901K9 |
| ROUTER_SANTA_ROSA | 172.20.61.1 | Cisco 2921K9 |
| ROUTER_SHYRIS | 172.20.4.30 | Cisco 2901K9 |
| ROUTER_SUB_PUYO | 172.20.74.254 | Cisco 2901K9 |
| ROUTER_SUB_TENA | 172.20.23.129 | Cisco 2901K9 |
| ROUTER1 MATRIZ | 172.20.1.242 | Cisco 3845 |
| ROUTER2 MATRIZ | 172.20.1.243 | Cisco 3845 |
| SWAGPELILEO1 | 172.20.3.188 | Cisco Catalyst 2960S-24TS-S |
| SWBAÑOSFO | 10.20.4.249 | Cisco Catalyst 29xxStack |
| SWCAPCATIGLATA | 172.20.54.248 | Cisco Catalyst 29xxStack |
| SWEDPUYOFO | 10.20.4.247 | Cisco Catalyst 29xxStack |
| SWGTCATIGLATA | 172.20.54.249 | Cisco Catalyst 29xxStack |
| SWGTCATIGLATA | 172.20.54.250 | Cisco WS-C2960-2 4PC-L |
| SWLORETO | 172.20.4.41 | Cisco Catalyst 2960S-24TS-S |
| SWLORETOFO | 10.20.4.251 | Cisco Catalyst 29xxStack |
| SWMATRIZPBFO | 10.20.4.252 | Cisco Catalyst 29xxStack |
| SWPCATIGLATA1 | 172.20.54.251 | Cisco Catalyst 29xxStack |
| SWPCATIGLATA2 | 172.20.54.252 | Cisco Catalyst 29xxStack |
| SWPELILEOFO | 10.20.4.250 | Cisco Catalyst 29xxStack |
| SWPILLARO1 | 172.20.3.60 | Cisco Catalyst 2960-24TC-S |
| SWSUBPUYOFO | 10.20.4.248 | Cisco Catalyst 29xxStack |
| SWSUBTENAF0 | 10.20.4.246 | Cisco Catalyst 29xxStack |
| SWTENA1FO | 10.20.4.245 | Cisco Catalyst 2960S-24TS-S |

ANEXO 6

Características de los equipos pertenecientes a la red de EEASA

CARACTERÍSTICAS DE EQUIPOS Mikrotik WIRELESS



RB433

Perfect for building custom AP devices

The RB433 is a multi port device. Use it in an outdoor case for a sector AP installation, or for a wireless backhaul. Three ports give you plenty of configuration options for many wireless scenarios.

New to the RB433 family is the RB433L series - a light version with only the most essential features and available at a lower cost.

We currently have six different models in the RB433 series.

| | |
|-------------------|--|
| CPU | Atheros AR7130/ AR7161 |
| Memory | DDR SDRAM onboard memory |
| Boot loader | RouterBOOT |
| Data storage | NAND memory chip |
| Ethernet | Three 10/100 Mbit/s Ethernet ports with Auto-MDI/X |
| miniPCI | Three MiniPCI Type IIIA/IIIB slots |
| Extras | Reset switch, beeper, voltage monitor |
| LEDs | Power, NAND activity, 6 user LEDs |
| Power options | PoE: 8-28V DC on Ether1 (Non 802.3af) |
| Dimensions | 105 mm x 154 mm, Weight: 137g |
| Power consumption | 2W board only, 14W available to miniPCI cards |
| Operating System | MikroTik RouterOS |

| Feature / Model | 433L | 433 | 433AH | 433UAHL | 433UAH | 433QL |
|---------------------|--------|--------|--------|---------|----------|--------|
| CPU MHz | 300MHz | 300MHz | 680MHz | 680MHz | 680MHz | 680MHz |
| RAM MB | 64MB | 64MB | 128MB | 128MB | 128MB | 128MB |
| Power jack | - | yes | yes | yes | yes | yes |
| Serial port | - | yes | yes | - | yes | - |
| USB | - | - | - | yes | yes, two | yes |
| Integrated wireless | L4 | L4 | L5 | L5 | L5 | L5 |
| Gigabit LAN | - | - | - | - | - | Yes |
| RouterOS Licence | L3 | L3 | L4 | L4 | L4 | L4 |

Figura 1. Mainboard Mikrotik Wirelles

En la figura 1 se puede visualizar le mainboard con el cual opera el enlace inalámbrico punto a punto con tecnología Mikrotik.

CARACTERÍSTICAS DE EQUIPOS PROXIM WIRELESS

PERFORMANCE AND SCALABILITY

| | |
|-------------------------------------|--|
| Best-in-class Performance with WORP | By eliminating in-the-air collisions and maximizing data content for each transmission, Wireless Outdoor Router Protocol (WORP) significantly improves performance |
| Near Line of Sight Capable | Line of sight and near line of sight connectivity extends deployment flexibility in rural as well as high-density urban areas |
| Highest Performance Per Cell | Supports 6 sectors per cell with an aggregate data rate of 324 Mbps |
| Dense Subscriber Support Per Cell | Supports up to 1,500 subscribers with 6 sectors |
| Guaranteed Data Rate While Roaming | Allows bandwidth-intensive applications, such as high-definition video streaming, in mobile environments |

QUALITY OF SERVICE (QoS)

| | |
|---|---|
| WiMAX 802.16 QoS | Supports up to 8 QoS Classes; Supports up to 8 Service Flows per class |
| Traffic Prioritization Parameters Supported | IP ToS (Layer 3 QoS identification), IP Protocol List, 802.1p tag (Layer 2 QoS identification), Source IP Address+Mask, Destination IP Address+Mask, Source TCP/UDP port ranges, Destination TCP/UDP port ranges, Source MAC addresses, Destination MAC address, VLAN ID, Ethertype |
| Committed Information Rate (CIR) | Users can set CIR for each Subscriber Unit |
| Minimum Information Rate (MIR) Support | User defined MIR |

SECURITY

| | |
|--|---|
| Unicast, Multicast and Broadcast Storm | User definable threshold levels prevent excessive bandwidth consumptions from degrading network control performance |
| Packet Filtering | MAC, Ethertype, IP address filtering provides very granular network security |
| Intracell Blocking | Allows the BSU to act as the central policy enforcer for SU to SU communications, further enhancing subscriber units' privacy |
| WORP as a Secure Protocol | Un-snoopable by wireless decryptors, WORP provides critical feature support for secure long-range wireless deployments in unlicensed frequency spectrum |
| Secure Encryption and Authentication | Supports for WEP, WEP+ and AES 128 bit for over the air encryption and Radius for user authentication |
| Interference Mitigation Tool | Variable Receive Threshold, Transmit Power Control and Dynamic Frequency Selection |

LOWER COST OF OWNERSHIP

| | |
|--|--|
| Dynamic Data Rate Selection (DDRS) | Automatically optimizes throughput as link conditions change or as subscribers roam; connectivity is automatically maintained when link quality degrades |
| Flexible and Secure Remote Management | Supports remote management via Telnet, SNMP and web interfaces with password protections |
| Antenna Alignment Tool | Audible tone and CLI with running statistics displaying real-time signal strength ease antenna system installation |
| Comprehensive Station Statistics network | Unit and group statistics are available for monitoring, planning and management of a wireless network |
| Lower Recurring Lease Cost | Co-locating unit on rooftops with plenty of available space lowers lease cost |
| Antenna Flexibility | Subscriber unit with type-N connector supports a broad selection of standard-based external antennas; subscriber unit with integrated antennas supports dual polarizations, vertical and horizontal, to minimize installation time |
| Remote Reboot | System reboot or reset to factory default can be performed remotely via a power injector button |

Figura 2. Características de Equipo Proxim Modelo

En la figura 2 se visualiza las características técnicas con las que cuenta los equipos proxim, además de los parámetros necesarios para la aplicación de calidad de servicio (QoS).

CARACTERÍSTICAS DE EQUIPOS UBIQUITI WIRELES

| AG-HP-5G23 | |
|------------------------|---|
| Dimensions | 370 x 270 x 260 mm (Mount Included) |
| Weight | 1452 g (Mount Included) |
| Networking Interface | (1) 10/100 Ethernet Port |
| Enclosure | Outdoor UV Stabilized Plastic |
| Frequency | Worldwide: 5170 – 5875 MHz USA: 5725 – 5850 MHz |
| Gain | 23 dBi |
| Output Power | 25 dBm |
| Max. Power Consumption | 3.0 W |
| Power Supply | 24V, 0.5A PoE Adapter (Included) |
| Power Method | Passive Power over Ethernet (Pairs 4, 5+; 7, 8 Return) |
| Max. VSWR | 1.5:1 |
| Wind Survivability | 125 mph |
| Wind Loading | 7.8 lbf @ 125 mph |
| ETSI Specification | EN 302 326 DN2 |
| Shock and Vibration | ETSI300-019-1.4 |
| Certifications | FCC, IC, CE |
| Operating Temperature | -30 to 75° C |
| Operating Humidity | 5 to 95% Condensing |

Figura 3. Características técnicas de Ubiquiti Wireless

En la figura 3 se puede observar las diferentes características que cuenta los equipos ubiquiti. Los cuales permiten la comunicación del enlace inalámbrico entre diferentes puntos de la red de EEASA.