



**Máster Oficial en Redes de Telecomunicación para Países en
Desarrollo**

**ESCUELA TÉCNICA SUPERIOR DE
INGENIERÍA DE TELECOMUNICACIÓN**

PROYECTO FIN DE MÁSTER

Diseño e Implementación de una red inalámbrica IEEE 802.11n de
Telemedicina en el distrito de Balsapuerto con soporte de QoS para
teleconsultas

Autor: Carlos David Guerra Anicama
Ingeniero Electrónico y Telecomunicaciones

Tutor: Francisco Javier Simó Reigadas
Doctor Ingeniero de Telecomunicaciones

Curso académico 2011/2012

Madrid, España

ACTA DEL TRABAJO FIN DE MÁSTER

DATOS DEL ESTUDIO DE MÁSTER

ESTUDIOS CURSADOS: <i>Máster en Redes de Telecomunicación para Países en Desarrollo</i>
CURSO ACADÉMICO: 2011/2012
CONVOCATORIA: Especial de finalización

DATOS DEL ALUMNO

APELLIDOS: Guerra Anicama	NOMBRE: Carlos David
DNI: 02563153X	E-mail: cdga12@gmail.com
	Teléfono: 670809194

TÍTULO DEL TRABAJO FIN DE MÁSTER

Diseño e implementación de una red inalámbrica IEEE 802.11n de Telemedicina en el distrito de Balsapuerto con soporte de QoS para teleconsultas

DIRECTOR/ES		
DNI	NOMBRE Y APELLIDOS	UNIVERSIDAD

MIEMBROS DEL TRIBUNAL	ACTUA EN CALIDAD DE:
	Presidente/a
	Vocal/es
	Secretario/a
	Suplente

Reunido el Tribunal de Evaluación con fecha _____, ACUERDA otorgar al alumno la calificación global de _____.

Indicar, en su caso, si se propone la concesión de la mención Matrícula de Honor

EL PRESIDENTE/A	SECRETARIO/A	VOCAL/ES
Fdo:	Fdo:	Fdo:

Resumen

Este trabajo presenta el diseño, la implementación y el funcionamiento de una red de Telemedicina llevada a cabo en una de las zonas de la selva amazónica más pobres y subdesarrolladas de Perú: el distrito de Balsapuerto, en la provincia del Alto Amazonas.

El sistema implementado está enfocado a ofrecer la posibilidad a que puestos y centros de salud totalmente aislados, puedan comunicarse con un hospital de apoyo para realizar consultas médicas a través de audio y video.

Esta red consta de tres radioenlaces troncales que unen cuatro poblaciones: tres comunidades indígenas (Balsapuerto, San Gabriel de Varadero y San Juan del Armanayacu) y una capital de distrito (Yurimaguas).

La tecnología utilizada en estos radioenlaces es IEEE 802.11n modificada para poder operar en largas distancias.

Aprovechando que el estándar IEEE 802.11n ofrece la posibilidad de utilizar radioenlaces con múltiples transmisores y receptores, se dotó a la red de dos radioenlaces MIMO 2x2 (San Gabriel de Varadero-San Juan del Armanayacu y San Juan del Armanayacu-Yurimaguas) y de un radioenlace SISO (Balsapuerto-San Gabriel de Varadero).

Esta red está constituida por repetidores troncales y locales. La señal viaja a través de los repetidores troncales interconectándose por medio de radioenlaces de larga distancia. Luego, la señal es distribuida a los diferentes clientes gracias a los repetidores locales.

La incursión de la técnica MIMO 2x2 empleada en radioenlaces con clima tropical dieron lugar a valores más estables de la relación señal/ruido (SNR) comparados con los obtenidos con SISO, con el subsecuente incremento del alcance máximo y del throughput de datos efectivo; y una disminución de la probabilidad de error de bit (BER). El resultado obtenido fueron capacidades cercanas a los 80 Mbps en radioenlaces de 29 Km.

En comunidades tan abandonadas, donde el acceso y los recursos son tan limitados, es imprescindible establecer un sistema de comunicación para intentar acortar estas distancias y dar una oportunidad de desarrollo a la población que habita en ellas.

Agradecimientos

En primer lugar a Dios.

Gracias a mi madre, quien es la inspiración de mi vida. A ti te dedico todos mis logros.

A mi familia, en especial a mis primos José Luis y César en España, gracias por todo su apoyo.

A Javier Simó, por toda su valiosa ayuda y tutela para la realización de este trabajo; También por su amistad, consejos y recomendaciones. Gracias por ser mi tutor.

A todos mis profesores del Máster, por compartir sus conocimientos y su valiosa experiencia.

A mis amigos del grupo GTR-PUCP y de la Fundación IEEE HTC, por todo el apoyo y su ayuda desinteresada. En especial la colaboración de River, como cotutor, gracias por compartir tus conocimientos y tu experiencia; También un agradecimiento especial a Jaime por recibirme con gran disponibilidad, por toda la ayuda, por tu amistad y por todas las facilidades que me has dado para la realización de este trabajo.

Gracias también por la ayuda del resto de mis amigos del Grupo y de España. Particularmente a Óscar (el paisano), gracias por tu ayuda, aliento y tú amistad. También a José Luis por toda la ayuda y compartir tus conocimientos conmigo. Gracias a César, Reynaldo, Gerson, Alejandro, Juan, Leopoldo, Cynthia, Martín, Luis y muy especialmente a Rómulo (Dios te tenga en su gloria).

A mis amigos en Yurimaguas, en especial a Roel y Roy, gracias por toda la ayuda y por su amistad. También agradezco a todas las personas que directa o indirectamente han colaborado haciendo realidad este Proyecto.

Índice General

Índice General

Resumen.....	iii
Agradecimientos	iv
Índice General.....	v
Índice de Ilustraciones.....	x
Índice de Tablas	xii
Capítulo I.....	1
Introducción	1
1.1. Objetivos y Características de este trabajo.....	1
1.1.1. Razones sociales para la existencia de la red	1
1.1.2. Desafíos de tipo técnico en el diseño y en el funcionamiento. Medidas preventivas y correctivas.....	1
1.1.3. Antecedentes 802.11 para largas distancias y las referencias que usaron y describir cómo este proyecto se diferencia de los demás.....	2
1.1.4. Mantenimiento y gestión remota.....	3
1.1.5. Colaboradores y financiadores	3
1.1.6. Estructura de este documento.....	4
Capítulo II	5
Fundamentos Teóricos	5
2.1. Estándar 802.11	5
2.2. Introducción al estándar 802.11n.....	5
2.2.1. Sistema MIMO	7
2.2.1.1. Esquema de modulación y codificación (Modulation and Coding Schema – MCS)	10
2.3. Problemática del uso de WiFi para largas distancias	11
2.3.1. Límites en la capa física	11
2.3.1.1. Potencia de recepción.....	11
2.3.1.2. Pérdidas de propagación.....	12

2.3.2. Límites en la subcapa MAC	12
2.3.2.1. ACKTimeout y CTSTimeout	13
2.3.2.2. aSlotTime y <i>CWmin</i>	13
2.3.2.3. Network Allocation Vector (NAV).....	14
2.4. Calidad de Servicio (Quality of Service – QoS)	14
2.4.1. Disciplina de colas sin clases	15
2.4.2. Disciplina de colas con clases	16
2.4.2.1. Hierarchical Token Bucket (HTB).....	16
2.5. Tecnología para la transmisión de voz y videoconferencia sobre IP	19
2.5.1. Códecs de Audio.....	19
2.5.2. Códecs de Video.....	20
2.5.3. Asterisk.....	21
2.5.4. Protocolos de señalización para videoconferencia y voz sobre IP (VoIP) 23	
2.5.4.1. Protocolo SIP.....	23
Capítulo III.....	25
Materiales y métodos.....	25
3.1. Metodología.....	25
3.1.1. Procedimiento para la realización de este trabajo	25
3.2. Software de Simulación.....	26
3.2.1. Uso de Radio Mobile y Google Earth para el cálculo de Radio Enlaces 27	
3.2.2. Iperf.....	28
3.2.3. Herramienta ‘Bandwith Test’ de MikroTik.....	29
3.2.4. D-ITG (Distributed Internet Traffic Generator).....	29
3.2.5. Winbox	29
Capítulo IV	30
Diseño de Red	30
4.1. Introducción.....	30
4.2. Estudio de campo inicial.....	33
4.2.1. Resultados del estudio	35
4.3. Descripción de la Red de Telecomunicaciones	37
4.3.1. Funcionamiento de la Red.....	39

4.3.1.1.	Repetidores Troncales	39
4.3.1.1.1.	Sistema de Telecomunicaciones de los Repetidores Troncales ...	40
4.3.1.1.2.	Sistema de Infraestructura de los Repetidores Troncales	40
4.3.1.1.3.	Sistema de Energía de los Repetidores Troncales	47
4.3.1.1.4.	Sistema de Protección Eléctrica de los Repetidores Troncales	47
4.3.1.2.	Red de Distribución Local.....	48
4.3.1.2.1.	Repetidores Locales de Distribución	48
4.3.1.2.2.	Estaciones Finales o clientes.....	49
4.3.1.2.2.1.	Sistema de Telecomunicaciones de las Estaciones Finales	49
4.3.1.2.2.2.	Sistema de Infraestructura de las Estaciones Finales.....	50
4.3.1.2.2.3.	Sistema de Energía de las Estaciones Finales.....	53
4.3.1.2.2.4.	Sistema de Protección Eléctrica de las Estaciones Finales.....	54
4.3.2.	Equipos utilizados y especificaciones técnicas	58
4.4.	Diseño de radioenlaces	63
4.4.1.	Estudio radioeléctrico.....	63
4.4.2.	Resultados del diseño de Radioenlaces	68
4.5.	Direccionamiento IP y enrutamiento de la Red.....	73
4.6.	Estudio de la viabilidad de los enlaces	76
4.6.1.	Cálculo del presupuesto del enlace: Yurimaguas y San Juan del Armanayacu	76
4.6.2.	Cálculo del presupuesto del enlace: San Gabriel de Varadero y Balsapuerto.....	78
4.6.3.	Cálculo del presupuesto del enlace: San Gabriel de Varadero y Balsapuerto.....	79
4.7.	Medición de las prestaciones de la red empleando la gestión avanzada de tráfico utilizando HTB en MikroTik para soporte de QoS	80
4.7.1.	Criterios de diseño	81
4.7.2.	Simulación y preparación de flujos	84
➤	Preparación de flujos	84
4.7.3.	Justificación: ¿Por qué usamos HTB en MikroTik?	85
4.7.4.	Configuración de HTB en MikroTik.....	85
4.7.5.	Discusión de los resultados	87
4.7.5.1.	Resultados.....	88
Capítulo V	92

Resultados.....	92
5.1. Introducción.....	92
Con la realización de un protocolo de pruebas se pretende demostrar y justificar los resultados obtenidos según las hipótesis formuladas en el diseño previo realizado en el laboratorio.....	92
5.2. Pruebas y resultados	93
5.2.1. Escaneo de la señal en la banda de 5.8 GHz	94
5.2.2. Monitoreo del enlace con SSID: ‘Balsa5’	95
5.3. Capacidad del enlace	98
5.3.1. Enlaces con tecnología MIMO	99
5.3.2. Enlaces con tecnología SISO.....	102
5.3.3. Enlaces locales.....	103
5.3.4. Capacidad extremo a extremo.....	105
5.3.4.1. Santa Gema (hospital) a cliente de San Juan.....	105
5.3.4.2. Santa Gema (hospital) a cliente de Varadero	106
5.3.4.3. Santa Gema (hospital) a cliente de Balsapuerto.....	108
5.3.4.4. Mediciones de tráfico TCP utilizando la aplicación ‘iperf’	110
5.4. Problemas encontrados	114
Capítulo VI.....	115
Conclusiones.....	115
Anexos	117
Anexo A: Configuración de las Placas MikroTik.....	118
1. YURIMAGUAS	118
1.1. Repetidor Santa Gema (Torre).....	118
1.2. Cliente: Oficina de coordinación de la Municipalidad de Balsapuerto	119
1.3. Cliente: Red de Salud de Alto Amazonas	120
2. SAN JUAN.....	121
2.1. Repetidor San Juan (Torre).....	121
Placa Mikrotik Routerboard 433AH – Placa 1 (Torre).....	121
2.2. Cliente: Puesto de Salud de San Juan	123
3. VARADERO	124
3.1. Repetidor Varadero (Torre)	124

3.2. Cliente: Puesto de Salud de Varadero	126
3.3. Servidor Asterisk.....	127
4. BALSAPUERTO	140
4.1. Repetidor Balsapuerto (Torre)	140
4.2. Cliente: Municipalidad de Balsapuerto	141
4.3. Cliente: Centro de Salud de Balsapuerto.....	142
Anexo B: Configuración de HTB en las Placas MikroTik	144
1. YURIMAGUAS	144
1.1. Repetidor Santa Gema (Torre).....	144
1.3. Cliente: Red de Salud de Alto Amazonas.....	145
2. SAN JUAN.....	147
2.1. Repetidor San Juan (Torre).....	147
Placa Mikrotik Routerboard 433AH – Placa 1 (Torre).....	147
2.2. Cliente: Puesto de Salud de San Juan	149
3. VARADERO	150
3.1. Repetidor Varadero (Torre)	150
3.2. Cliente: Puesto de Salud de Varadero.....	153
4. BALSAPUERTO	154
4.1. Repetidor Balsapuerto (Torre)	154
4.3. Cliente: Centro de Salud de Balsapuerto	155
Bibliografía.....	158

Índice de Ilustraciones

Ilustración 1: Sistema MIMO	8
Ilustración 2: Disciplina HTB	17
Ilustración 3: Diagrama de flujos de paquetes para soportar calidad de servicio (QoS)	18
Ilustración 4: Ejemplo de “Inner queue”	18
Ilustración 5: videoconferencia entre los técnicos de enfermería de San Juan y Balsapuerto a través del softphone Linphone	21
Ilustración 6: Esquema de conexión a través de Asterisk	22
Ilustración 7: Distrito de Balsapuerto	33
Ilustración 8: Estudio de campo realizado en la zona de Balsapuerto	35
Ilustración 9: Diseño de la Red WIFI del proyecto de Telemedicina de Balsapuerto	36
Ilustración 10: Redes troncales y redes locales de distribución de la red WiFi	38
Ilustración 11: Esquema de conexiones – Repetidor Troncal Balsapuerto	41
Ilustración 12: Red de distribución local – Repetidor Troncal Balsapuerto	42
Ilustración 13: Esquema de conexiones – Repetidor Troncal Varadero	43
Ilustración 14: Esquema de conexiones – Repetidor Troncal San Juan	44
Ilustración 15: Esquema de conexiones – Repetidor Troncal Santa Gema	46
Ilustración 16: Red de distribución local – Repetidor Troncal Santa Gema	46
Ilustración 17: Red de distribución local – Repetidor Troncal Santa Gema (II)	47
Ilustración 18: esquema de conexión de una estación final con sistema fotovoltaico – Centro de Salud de Balsapuerto	51
Ilustración 19: Esquema de conexión de una estación final con sistema fotovoltaico – Puesto de Salud de Varadero	51
Ilustración 20: Esquema de conexión de una estación final con energía convencional – Municipalidad de Balsapuerto	52
Ilustración 21: Esquema de conexión de una estación final con energía convencional – Red de Salud de Yurimaguas	52
Ilustración 22: Fotografía Antena Parabólica 5.8 GHz	55
Ilustración 23: Placa MikroTik RB 433 y Tarjeta Inalámbrica R52Hn	55
Ilustración 24: Fotografía de los enlaces Balsapuerto y Varadero	56
Ilustración 25: Fotografía de los enlaces Balsapuerto y Varadero	57
Ilustración 26: Parámetros de la configuración de las Redes	64
Ilustración 27: Parámetros de la configuración del nodo Santa Gema	64
Ilustración 28: Parámetros de la configuración del nodo Santa Juan	65
Ilustración 29: Configuración del sistema	65
Ilustración 30: Perfil del enlace	67
Ilustración 31: Mapa de Repetidores Troncales de la Red WiFi de Telemedicina de Balsapuerto	67
Ilustración 32: Perfil del radioenlace entre Santa Gema y San Juan	68
Ilustración 33: Detalles del radioenlace entre Santa Gema y San Juan	69
Ilustración 34: Resultados del radioenlace entre Santa Gema y San Juan	69
Ilustración 35: Perfil del radioenlace entre San Juan y Varadero	70
Ilustración 36: Detalles del radioenlace entre San Juan y Varadero	70
Ilustración 37: Resultado del radioenlace entre San Juan y Varadero	71
Ilustración 38: Perfil del radioenlace entre S.G. de Varadero y Balsapuerto	71
Ilustración 39: Detalles del radioenlace entre S.G. de Varadero y Balsapuerto	72
Ilustración 40: Resultado del radioenlace entre S.G. de Varadero y Balsapuerto	72
Ilustración 41: Esquema del entorno de prueba	82
Ilustración 42: ‘throughput’ de datos o caudal total (extremo a extremo) en el entorno de prueba	83
Ilustración 43: Diagrama de flujos de paquetes para soportar QoS	86
Ilustración 44: ‘Bitrate’ (Inyección de tráfico extremo a extremo Santa Gema y San Juan)	88
Ilustración 45: ‘Jitter’ (Inyección de tráfico extremo a extremo Santa Gema y San Juan)	89

<i>Ilustración 46: 'Paquetes perdidos' (Inyección de tráfico extremo a extremo Santa Gema y San Juan)</i>	90
<i>Ilustración 47: Redes Troncales y Redes Locales</i>	93
Ilustración 48: <i>Throughput del enlace MIMO 2x2 'BALSA5'</i>	100
Ilustración 49: <i>Throughput del enlace MIMO 2x2 'BALSA5'</i>	100
<i>Ilustración 50: Throughput del enlace MIMO 2x2 'BALSA5'</i>	101
<i>Ilustración 51: Throughput del enlace MIMO 2x2 'BALSA5'</i>	101
Ilustración 52: <i>Throughput del enlace MIMO 2x2 'BALSA7'</i>	102
Ilustración 53: <i>Throughput del enlace MIMO 2x2 'BALSA7'</i>	102
<i>Ilustración 54: Throughput del enlace SISO 1x1 'BALSA17'</i>	103
<i>Ilustración 55: Throughput del enlace SISO 1x1 'BALSA17'</i>	103
<i>Ilustración 56: Red Local Hospital Santa Gema</i>	104
<i>Ilustración 57: Red Local Balsapuerto</i>	105
<i>Ilustración 58: Throughput cliente Santa Gema - cliente San Juan (dirección = transmisión)</i>	106
<i>Ilustración 59: Throughput cliente Santa Gema - cliente San Juan (dirección = recepción)</i>	106
<i>Ilustración 60: Throughput cliente Santa Gema - cliente Varadero</i>	107
<i>Ilustración 61: Throughput cliente Santa Gema - Repetidor Varadero</i>	108
<i>Ilustración 62: Throughput cliente Santa Gema - cliente Balsapuerto</i>	109
<i>Ilustración 63: Medición de capacidad extremo a extremo real de la red (incluyendo el enlace SISO) a través de 'iperf'</i>	112

Índice de Tablas

<i>Tabla 1: Comparación de los Estándares 802.11</i>	6
<i>Tabla 2: índice del Esquema de Modulación y Codificación</i>	10
<i>Tabla 3: Datos georreferenciales de todos los nodos de la red</i>	36
<i>Tabla 4: Coordenadas geográficas de los nodos troncales y repetidores locales</i>	39
<i>Tabla 5: Equipamiento del Sistema de Telecomunicación</i>	40
<i>Tabla 6: Equipamiento del Sistema de Energía de los Repetidores Troncales</i>	47
<i>Tabla 7: Clientes por repetidor local de distribución</i>	48
<i>Tabla 8: Equipamiento del Sistema de Telecomunicación</i>	50
<i>Tabla 9: Equipamiento del Sistema de Energía de las Estaciones Finales</i>	54
<i>Tabla 10: características de los equipos MikroTik RB R52Hn</i>	80
<i>Tabla 11: Valores de 'throughput' de datos (Mbit/s) en los enlaces troncales</i>	81
<i>Tabla 12: Repartición del ancho de banda por tipo de tráfico usando HTB</i>	83
<i>Tabla 13: Resultados de la gestión avanzada de tráfico</i>	90

Capítulo I

Introducción

1.1. Objetivos y Características de este trabajo

1.1.1. Razones sociales para la existencia de la red

La razón principal para diseñar esta red es permitir la comunicación entre centros de salud de comunidades aisladas con el hospital Santa Gema ubicado en la capital de la Provincia de Alto Amazonas, en el Departamento de Loreto, Perú.

Esta red permite realizar consultas médicas utilizando sesiones de audio y video. Estas sesiones permiten que el personal médico especializado del hospital pueda hacer diagnósticos a distancia y guiar en el tratamiento de diversas enfermedades.

Balsapuerto es, de acuerdo al Instituto de Estadística e Informática del Perú, uno de los distritos más pobres del Perú y menos desarrollado, con una población mayoritaria de indígenas de la tribu Chayahuita.

Actualmente sufren de carencias primarias, como es la falta de agua potable, comunicaciones y electricidad. Se dispone de energía dos horas al día cuando hay combustible y, además, se requiere de varias horas al día para desplazarse entre las comunidades, con una escasez de servicios de transporte público que depende de las épocas de creciente de los ríos.

1.1.2. Desafíos de tipo técnico en el diseño y en el funcionamiento. Medidas preventivas y correctivas.

Este trabajo tiene como objetivo diseñar e implementar una red inalámbrica IEEE 802.11n de Telemedicina utilizando un sistema básico MIMO (Multiple-Input/Multiple-Output) 2x2 con diversidad de polarización y además se desea dotar con QoS a esta red.

Con el uso de esta tecnología se pretende conseguir un mayor throughput de datos efectivo, asegurando un ancho de banda suficiente para los servicios de voz y videoconferencia.

Se realizaron muchas pruebas antes de la implementación in situ, entre las cuales se destaca un enlace piloto troncal de largas distancias con el mismo equipamiento y la tecnología que se ha utilizado en esta red. El cual se implementó en la ciudad de Lima y con la colaboración del **Grupo de Telecomunicaciones Rurales de la Pontificia Universidad Católica del Perú (GTR-PUCP)**.

El enlace piloto ha permitido evaluar muchos aspectos relacionados a su configuración. Se destaca el comportamiento del enlace frente al tamaño del ancho de banda del canal (20/40 MHz) y la duración del intervalo de guarda (400/800 nseg) en largas distancias.

Además, hay aspectos de gran relevancia en el diseño de los enlaces para soportar servicios de Videoconferencia y VoIP. Destacamos la importancia de disponer de completa visibilidad directa (Line of Sight – LoS), sin obstáculos y con suficiente despejamiento de la primera zona de Fresnel, para lo cual se ha dispuesto de antenas de hasta 60 mts de altura.

Es fundamental además una cuidadosa evaluación del balance de enlace (de potencias) en el diseño. También una óptima elección de la banda de frecuencias teniendo en cuenta las interferencias, para finalmente disponer de enlaces WiFi que aseguren una calidad constante y la mayor estabilidad posible.

1.1.3. Antecedentes 802.11 para largas distancias y las referencias que usaron y describir cómo este proyecto se diferencia de los demás.

Llevar a cabo la implementación de esta red logrando excelentes resultados ha sido posible gracias a la experiencia obtenida por el **Grupo de Telecomunicaciones Rurales de la Pontificia Universidad Católica del Perú (GTR-PUCP)**, con más de 10 años de experiencia implementando proyectos de ingeniería en zonas tan desfavorecidas como las pertenecientes al distrito de Balsapuerto.

El grupo GTR-PUCP es un equipo multidisciplinario dedicado a la investigación, desarrollo, análisis, evaluación del impacto y difusión de las Tecnologías de la Información y Comunicación (TIC) apropiadas para contribuir a la mejora de la calidad de vida de comunidades marginales que carecen o tienen acceso limitado a medios de comunicación, con énfasis en aquellas ubicadas en entornos rurales.

Antes de este trabajo, el grupo GTR-PUCP implementó muchas redes ubicadas en entornos rurales con climas variados (costa, sierra y selva). Se destaca las siguientes implementaciones:

- a) El proyecto **'EHAS-AMA08'** Ampliación de la Red NAPO Loreto: se trata de una red de Telemedicina ubicada en la provincia de Maynas, departamento de Loreto. Interconectando establecimientos de salud. Se dispone de enlaces troncales punto a punto IEEE 802.11b y IEEE 802.11a. Logrando una red en producción con un throughput de datos efectivo de hasta 10 Mbps.
- b) Una red de Telemedicina con enlaces troncales punto a punto IEEE 802.11n de largas distancias que se encuentra en producción, ubicada en la provincia de Cajamarca; esta Red utiliza enrutadores del mismo fabricante (Mikrotik). Lo cual ha permitido realizar pruebas y revisar aspectos de configuración de gran importancia para lograr los resultados esperados.

Los resultados obtenidos, son throughput de datos efectivos de hasta 81 Mbps en enlaces troncales de hasta 29 Kms. Lo cual ha demostrado que la tecnología IEEE 802.11n modificada para largas distancias con MIMO, es capaz de ofrecer un rendimiento muy superior a los otros estándares *WiFi*¹ conocidos hasta el día de hoy. Incluso en regiones con una difícil geografía como la selva amazónica peruana.

1.1.4. Mantenimiento y gestión remota

Actualmente, la red inalámbrica de Telemedicina se encuentra en producción, funcionando de forma óptima y estable.

También se dispone de conexión remota para su monitorización diaria y configuración. Además, se ha capacitado al personal encargado del mantenimiento de la red y se dispone de *'scripts'* con la configuración de todos los equipos, para que en caso de reparación, esta se pueda realizar rápida y eficazmente.

Este trabajo pretende además, documentar el proceso de diseño e implementación de esta red de Telecomunicaciones, con el fin de poder replicar su utilización y mejorar el desempeño de redes similares.

1.1.5. Colaboradores y financiadores

Se trata de un proyecto de cooperación que se ha realizado en esta localidad. Este proyecto se circunscribe dentro de los objetivos del grupo GTR-PUCP: **Contribuir al desarrollo humano a través de la implementación de TIC apropiadas.**

¹ WiFi (Wireless Fidelity): es una abreviatura de Wireless Fidelity (Fidelidad Inalámbrica), la cual es una tecnología que permite que dispositivos electrónicos se puedan conectar inalámbricamente.

Además se ajusta dentro del segundo desafío de los tres que especifica la **Fundación IEEE HTC (Humanitarian Technology Challenge): Data Connectivity for Telehealth (Conectividad para la Telemedicina)**. Esta fundación es el financiador y además ha colaborado activamente con el grupo GTR-PUCP en este proyecto.

1.1.6. Estructura de este documento

A continuación, en el **capítulo 2** se describe el marco teórico. Este capítulo contiene un resumen de los aspectos tecnológicos necesarios para comprender mejor este trabajo.

Se ha hecho hincapié en la tecnología WiFi y sistemas MIMO, especialmente en las características del estándar IEEE 802.11n y su aplicación para redes de larga distancia.

El **capítulo 3** presenta el mayor aporte de este trabajo, en él se ha comentado todo lo que se ha hecho.

Este se divide en siete partes: introducción al diseño de red, estudio de campo inicial, descripción de la red de telecomunicaciones, diseño de radioenlaces, direccionamiento IP y enrutamiento de la red, cálculo de presupuesto de potencia, mediciones de las prestaciones en la gestión avanzada de tráfico utilizando HTB en Mikrotik para soporte de QoS.

Se ha tenido en cuenta la justificación del trabajo realizado y de los criterios de diseño empleados.

El **capítulo 4** presenta los resultados obtenidos después de llevar a cabo un protocolo de pruebas, se especifican las pruebas finales luego de realizar una monitorización de los enlaces.

En este capítulo aparecen los resultados del throughput de datos o caudal obtenido por cada enlace y también los resultados '*extremo a extremo*' (correspondientes a las estaciones finales en puntos extremos de la red).

Finalmente, en los **Anexos** se ha adjuntado la configuración detallada de todos y cada una de las enrutadores inalámbricos que componen la red.

Se incluye la configuración del servidor Asterisk para disponer de los servicios de voz y videoconferencia. Se ha adjuntado además la configuración de la gestión avanzada de tráfico utilizando HTB, implementada en todos los nodos que componen la red.

Capítulo II

Fundamentos Teóricos

Este apartado define las bases teóricas de la tecnología utilizada. Se describen aquellas cuestiones más relevantes para comprender mejor el diseño e implementación de la red.

2.1. Estándar 802.11

Desde el año 2000, el estándar 802.11 ha sido muy utilizado y su uso es hegemónico. Los estándares que se utilizan como base para la realización de este trabajo son 802.11-2007 [IEE07] y 802.11n-2009 [IEE09n].

El estándar 802.11 fue aprobado por el IEEE en 1997 y especifica dos velocidades de transmisión de 1 y 2 Mbps. Al pasar el tiempo, el grupo de trabajo 802.11 mejoró las prestaciones del estándar inicial, es decir se añadieron nuevas técnicas de modulación en la capa física y se lograba mayor robustez en la conectividad, esto permitió mayores tasas de transmisión y dio orígenes a nuevos estándares (ver *Tabla 1*).

Para una mayor información de los estándares 802.11 y las características de la capa PHY y la subcapa MAC se puede consultar el Anexo A, en [Sim07].

2.2. Introducción al estándar 802.11n

El estándar IEEE 802.11n-2009 es una enmienda del estándar IEEE 802.11-2007, uno de sus propósitos es superar en mucho un throughput de datos efectivos de más de 100 Mbps.

El estándar permite utilizar un sistema MIMO con hasta 4 flujos espaciales y anchos de banda de 20 MHz y 40 MHz. También define un intervalo de guarda (Guard Interval – GI) de 800 nseg y la posibilidad de utilizar un intervalo de guarda corto de valor igual a 400 nseg.

El estándar tiene en cuenta la compatibilidad hacia atrás con sistemas en la misma banda de frecuencia e introduce mejoras. Se dispone de un OFDM más eficiente que permite mayores velocidades de transmisión.

<i>Estándar IEEE</i>	<i>Velocidades (Mbps)</i>	<i>Bandas de frecuencia (GHz)</i>	<i>Notas</i>
<i>802.11</i>	1 y 2	2.4	<i>Tres técnicas de transmisión en el PHY: FHSS, IR y DSSS (implementada en las primeras tarjetas 802.11 y complementa a 802.11b)</i>
<i>802.11b</i>	5.5 y 11	2.4	<i>Usa sistema de transmisión HR/DSSS, modulación CCK, tiene 14 canales de 22 MHz, en una porción de la banda ISM desde 2400 a 2484 MHz, se pueden usar hasta tres de forma no interferente.</i>
<i>802.11a</i>	Hasta 54	5	<i>Usa la técnica de transmisión OFDM, tiene 8 canales no interferentes de 20 MHz, opera en la banda ISM entre 5725 y 5850 MHz, y en una porción de la banda UNII entre 5150 y 5350 Mhz.</i>
<i>802.11g</i>	Hasta 54	2.4	<i>Es compatible con 802.11b, usa OFDM, utiliza el mismo rango ISM que 802.11b. Se define ERP (incluye): ERP-DSSS y ERP-CCK, ERP-OFDM (modo principal), ERP-PBCC, DSSS-OFDM</i>
<i>802.11n</i>	Superar (con creces) 100	2.4 y 5	<i>Usa tecnología MIMO, tiene en cuenta la compatibilidad hacia atrás con sistemas en la misma banda de frecuencia, canalización de 20 y 40 MHz, intervalo de guarda de 400 nseg.</i>
<i>802.11e</i>	-	-	<i>Extensión para proporcionar calidad de servicio (QoS) a las redes IEEE802.11a/g/h.</i>

Tabla 1: Comparación de los Estándares 802.11

Es conveniente listar algunas de las características más importantes del estándar por su importancia en el diseño e implementación de la red:

- Tecnología MIMO (Multiple-Input/Multiple-Output).

- Trabaja en dos bandas de frecuencia: 5 GHz y 2.4 GHz simultáneamente.
- Proporciona compatibilidad retroactiva con equipos 802.11a/b/g que se encuentren en la misma banda de frecuencia.
- Admiten el funcionamiento con ancho de banda de canal de 20 MHz y 40 MHz. Los canales de 40 MHz permiten incrementar el throughput de datos.

Para una mayor información del estándar 802.11n-2009: acerca de las mejoras incorporadas en el estándar, MIMO y aspectos como el OFDM mejorado y la reducción del intervalo de guarda se puede consultar en [[Lud11](#)].

En la Red de Telecomunicaciones que este trabajo expone, se dispone de tarjetas inalámbricas RouterBoard R52Hn y cumplen con las especificaciones del estándar. Las cuales permitieron implementar enlaces 802.11n de larga distancia con un sistema MIMO con dos flujos espaciales en transmisión y en recepción (2x2).

Este equipamiento facilita el uso de un ancho de banda de 40 MHz y reducir el intervalo de guarda corto a un valor igual a 400 nseg, resultando con velocidades de transmisión de hasta 300 Mbps y siendo útil en escenarios de interiores. Las pruebas realizadas en el interior de la universidad usando este tipo de configuración y un sistema MIMO 2x2 resultaron con velocidades de transmisión de datos mayores a 100 Mbps en enlaces de 100 metros aproximadamente.

2.2.1. Sistema MIMO

Las interfaces 802.11 tenían inicialmente una sola antena. También permiten una configuración de diversidad espacial empleando dos antenas.

En una configuración con diversidad de espacio solo se utiliza una antena (la mejor), aunque existan dos o más antenas, solo se puede procesar una señal o cadena de transmisión o recepción. Esto quiere decir que el receptor tiene una sola cadena de recepción a la entrada y el transmisor tiene una sola cadena de transmisión a la salida.

El siguiente paso posterior a la diversidad es el sistema MIMO, el cual permite añadir más cadenas o flujos espaciales al sistema. Cada uno de los flujos espaciales tiene la posibilidad de recibir o transmitir de forma simultánea consiguiendo mejorar la velocidad de transmisión de datos.

Además, se dispone de un procesamiento de recepción simultánea (Space Time Block Coding - STBC) que permite resolver las interferencias a causa del multitrayecto, mejorando la

calidad de la señal recibida mucho mejor que con la diversidad espacial. Cada antena independiente transmite un flujo espacial.

El estándar especifica la facilidad de utilizar un sistema MIMO con dos flujos espaciales en transmisión y dos en recepción (2x2), esto significa que se utilizan dos antenas con dos cadenas de transmisión y dos cadenas de recepción, ambos flujos espaciales se multiplexan a través del enlace radio; la Red de Telecomunicaciones que este trabajo expone utiliza un sistema MIMO 2x2.

Sin embargo un sistema MIMO facilita el uso de varios flujos espaciales (ver *Ilustración 1: Sistema MIMO*)

La ventaja de utilizar un sistema MIMO frente a un sistema SISO es que este saca provecho del multitrayecto, disminuyendo el número de bits incorrectamente recibidos (Bit Error Ratio – BER). Además, usar STBC mejora la relación señal a ruido (Signal to Noise Ratio – SNR).

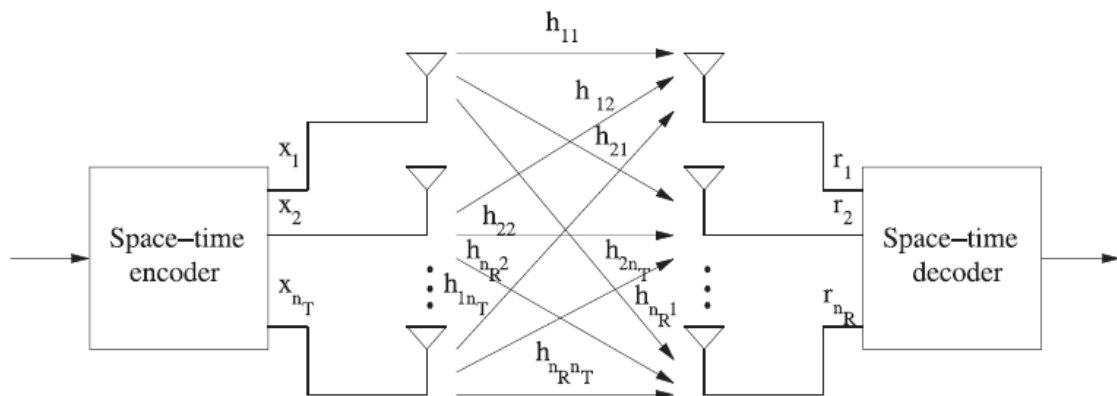


Figure 1.1 Block diagram of a MIMO system

Ilustración 1: Sistema MIMO

Beamforming:

Es una técnica de procesamiento de señal que permite incrementar la calidad de la señal con una menor atenuación respecto a la distancia y requiere un conocimiento previo sobre el canal de radio en el transmisor.

Obtener una calidad superior de la señal significa que se puede utilizar una determinada velocidad de transmisión de datos a un rango de cobertura más largo. Esta técnica permite conseguir un patrón bien definido y direccional; Además incrementa la relación señal a ruido y como consecuencia amplía la cobertura.

Codificación espacio temporal por bloques (Space Time Block Coding - STBC)

Es una técnica de codificación que permite transmitir múltiples copias de un flujo de datos a través de varias antenas. Permite transmitir más de un flujo de datos con redundancia para recibir una señal con una menor tasa de error; con esta técnica se consigue combinar las copias de la señal recibida obteniendo una mayor cantidad de información de cada copia y en consecuencia un mejor proceso de recepción.

El código de 'Alamouti' es históricamente el primer código STBC y provee una transmisión óptima utilizando diversidad espacial. Con sistemas MIMO y en los casos en los que no se dispone de conocimiento del canal este tipo de codificación puede ser de utilidad.

El estándar 802.11n especifica la utilización de STBC y además, admite el código de comprobación de paridad de densidad baja (Low Density Parity Check – LDPC) como código de corrección de errores, el cual combina aspectos del código de circunvolución de OFDM y del código bloque 'Reed Solomon'.

Multiplexación espacial (Spatial Multiplexing – SM)

Esta Técnica específica que una sola trama de datos se puede descomponer y multiplexar a través de varios flujos espaciales independientes. Estos flujos son transmitidos al mismo tiempo y simultáneamente por cada antena ocupando el mismo ancho de banda, lo que se consigue son múltiples cadenas de datos por cada par transmisor - receptor.

A diferencia de STBC, donde se transmite la misma información por caminos distintos, SM hace uso de todos los caminos para transmitir datos diferentes.

Esta técnica permite incrementar la eficiencia espectral del canal, consiguiendo velocidades de transmisión de datos más altos.

Además, es muy ventajosa en entornos con desvanecimiento plano y no necesita incrementar la potencia ni el ancho de banda; esta técnica está limitada por el número de antenas y no requiere un conocimiento previo del canal.

También se admite una combinación de las técnicas STBC y Spatial Multiplexing.

2.2.1.1. Esquema de modulación y codificación (Modulation and Coding Schema – MCS)

Modo	Flujo	Modulación	FEC	Data rate (Mbit/s)			
				20 MHz		40 MHz	
				800 ns	400 ns	800 ns	400 ns
0	1	BPSK	1/2	6.50	7.20	13.50	15.00
1	1	QPSK	1/2	13.00	14.40	27.00	30.00
2	1	QPSK	3/4	19.50	21.70	40.50	45.00
3	1	16-QAM	1/2	26.00	28.90	54.00	60.00
4	1	16-QAM	3/4	39.00	43.30	81.00	90.00
5	1	64-QAM	2/3	52.00	57.80	108.00	120.00
6	1	64-QAM	3/4	58.50	65.00	121.50	135.00
7	1	64-QAM	5/6	65.00	72.20	135.00	150.00
8	2	BPSK	1/2	13.00	14.40	27.00	30.00
9	2	QPSK	1/2	26.00	28.90	54.00	60.00
10	2	QPSK	3/4	39.00	43.30	81.00	90.00
11	2	16-QAM	1/2	52.00	57.80	108.00	120.00
12	2	16-QAM	3/4	78.00	86.70	162.00	180.00
13	2	64-QAM	2/3	104.00	115.60	216.00	240.00
14	2	64-QAM	3/4	117.00	130.00	243.00	270.00
15	2	64-QAM	5/6	130.00	144.40	270.00	300.00

Tabla 2: índice del Esquema de Modulación y Codificación

Se define como un esquema que define varios modos de operación (MCS0 al MCS31) para establecer una comunicación entre dos nodos, cada modo relaciona los siguientes parámetros: velocidad de transmisión de datos, la modulación, la codificación y el número de flujos espaciales.

Esto significa que cada modo de operación se corresponde con una tasa de transmisión, con un esquema de modulación y codificación específica. En la [Tabla 2](#) se describen los modos de operación que define el estándar para el caso de un sistema con un flujo o cadena espacial (SISO 1x1) y un sistema con dos flujos o cadenas espaciales (MIMO 2x2).

La elección de un adecuado modo de operación es de gran importancia para asegurar la estabilidad de los enlaces inalámbricos, esto quiere decir que analizar la calidad del enlace permitirá elegir un modo de operación adecuado que asegure la estabilidad del mismo.

El estándar especifica una capa física que permite utilizar hasta cuatro flujos espaciales, con anchos de banda de canal de 20 MHz y 40 MHz. También la posibilidad de configurar

intervalos de guarda de 800 nseg y 400 nseg, con lo que se puede conseguir tasas de transmisión teóricas de hasta 300 Mbps y 600 Mbps.

En [Lud11] se establece una revisión del rendimiento de la capa PHY y la subcapa MAC de 802.11n. También se comenta las características y ventajas de un sistema MIMO.

2.3. Problemática del uso de WiFi para largas distancias

El estándar IEEE 802.11 fue diseñado inicialmente para redes inalámbricas de área local, los resultados de varios experimentos y el uso de determinados equipos permitieron la posibilidad de alcanzar distancias superiores empleando amplificadores y antenas directivas.

2.3.1. Límites en la capa física

El estándar no especifica ninguna otra limitación acerca del alcance de WiFi para largas distancias respecto a la capa física, que no sea a causa del presupuesto de potencia o balance de enlace. Esto quiere decir que los límites que se impongan respecto a la distancia alcanzable por WiFi dependerán de los siguientes parámetros:

- ✓ La máxima potencia que podamos transmitir (PIRE)
- ✓ Las pérdidas de propagación
- ✓ La sensibilidad de recepción
- ✓ La mínima relación señal a ruido necesaria para lograr la viabilidad del enlace.

2.3.1.1. Potencia de recepción

En los enlaces IEEE 802.11n de largas distancias, como el que describe en este trabajo, se necesita obtener un valor de potencia de recepción que se encuentre por encima de la sensibilidad del receptor.

En la siguiente ecuación de balance de enlace se muestra la relación que tiene este valor con la potencia de transmisión, las ganancias de antenas y las pérdidas en el enlace.

$$P_{RX} = P_{TX} + G_{TX} - L_{CC_{TX}} - L_{CC_{RX}} - L_P + G_{RX} \dots \dots \dots (1)$$

P_{RX} : Potencia de recepción

P_{TX} : Potencia de transmisión

G_{TX} : Ganancia de transmisión

$L_{CC_{TX}}$: Pérdidas por cables y conectores en el transmisor

$L_{CC_{RX}}$: Pérdidas por cables y conectores en el receptor

L_P : Las pérdidas de propagación

G_{RX} : Ganancia de recepción

2.3.1.2. Pérdidas de propagación

Las pérdidas de propagación son difíciles de calcular de forma analítica porque dependen de muchos factores del entorno (relieve, tipo de cobertura del suelo, obstáculos, condiciones atmosféricas, etc.), pero la '*Fórmula de Friis*' proporciona una primera aproximación aceptable cuando hay línea de vista y suficiente despejamiento de la primera zona de Fresnel. No obstante, hay otros modelos más complejos para obtener aproximaciones mejores dependiendo del tipo de entorno y de la banda de frecuencias de trabajo.

$$L_p(dB) = 92,45 + 20 \cdot \log_{10}(f) (GHz) + 20 \cdot \log_{10}(d)(Km) \dots \dots \dots (2)$$

Dónde:

L_p : Pérdidas de propagación

f : Frecuencia de operación

d : Distancia entre los nodos

Esta es una expresión teórica y se empleará solo si se cumple la condición de la existencia de **Línea de Vista (Line of Sight - LoS)**. Se necesita además despejar por lo menos en un 60% de la primera zona de Fresnel y se considera la no existencia de efectos adversos como el multitrayecto.

2.3.2. Límites en la subcapa MAC

La existencia de restricciones en la subcapa MAC es a causa de la multitud de tiempos constantes que son definidos en el estándar, esto significa que tendremos efectos resultantes en función de la distancia que haya entre estaciones. El estándar especifica las siguientes limitaciones:

- ✓ El temporizador de espera de los ACKs (**ACKTimeout**) y el temporizador (**CTSTimeout**).

- ✓ Los tiempos relacionados con el tamaño de ranura (**aSlotTime**) o el parámetro (CW_{min}).
- ✓ El cálculo del cómputo NAV (**Network Allocation Vector**) para la detección de la portadora virtual.

2.3.2.1. ACKTimeout y CTSTimeout

El '**ACKTimeout**' es el tiempo que la estación transmisora espera para recibir la trama ACK de confirmación de transmisión de una trama de datos.

Para que una comunicación WiFi de largas distancias funcione se necesita que el ACKTimeout tenga un valor mayor al tiempo de propagación de ida y vuelta ($2 \cdot t_{prop}$) más un tiempo SIFS, se adiciona además el tiempo de duración del Slot estándar (**Standard aSlotTime**) o tamaño de ranura (σ_{std}) y la duración total del preámbulo más la cabecera de capa física. También la duración de la trama '**ACK**':

$$ACKTimeout = SIFS + \sigma_{std} + 2 \cdot t_{prop} + PLCP (Preamble) + PLCP (Header) + ACK$$

Además de mecanismo de acceso al medio **DCF** (*Distributed coordination Function*), el estándar contempla el modo **Request To Send** (RTS) y **Clear To Send** (CTS).

RTS/CTS evita el problema de los nodos ocultos, si se desea utilizar este modo en enlaces de larga distancia será conveniente ajustar también el '**CTSTimeout**'. El nodo transmisor esperara un intervalo de tiempo llamado CTSTimeout, que corresponde al tiempo de duración de las tramas CTS con las que responderá la estación receptora que escuche la trama RTS que envió el transmisor.

2.3.2.2. aSlotTime y CW_{min}

El '**aSlotTime**' es llamado también **Tiempo de Slot o ranura**. Los valores correspondientes al tiempo de ranura, SIFS y DIFS imponen restricciones al funcionamiento del MAC de WiFi a partir de ciertas distancias.

El estándar especifica que las estaciones transmisoras son oídas por las demás en un tiempo correspondiente al valor del SlotTime, estableciendo una limitación de hasta 3 Km. Esto significa que en enlaces de largas distancias las prestaciones de los enlaces empeoran, por lo que será necesario ajustar el Tiempo de Slot de la siguiente forma:

$$aSlotTime = \sigma_{std} + 2 \cdot t_{prop}$$

Este ajuste permitirá maximizar el throughput, minimizando el retardo y la pérdida de paquetes. Otra manera de optimizar el throughput es incrementando el valor mínimo de la ventana de contienda (CW_{min} – Minimum Contention Window).

2.3.2.3. Network Allocation Vector (NAV)

El cómputo de NAV para la detección de la portadora virtual es el cálculo correspondiente al tiempo de ocupación del canal.

Este valor no tiene en cuenta el tiempo de propagación de la señal, esto significa que a distancias mayores la efectividad del cómputo empeora. En el caso de utilizar el mecanismo RTS/CTS para evitar colisiones entre nodos ocultos, este mecanismo funcionara solo si el cómputo de NAV tiene en cuenta el tiempo de ocupación real del canal.

Es por esta razón que el mecanismo RTS/CTS no sirve para enlaces punto a multipunto de largas distancias.

En [SMR10] Javier Simó concluye las modificaciones necesarias en la subcapa MAC para solucionar la problemática del uso de WiFi para largas distancias.

También en [Sim07] Javier Simó comenta las limitaciones en la capa física y de la subcapa MAC, se recomienda consultar los capítulos: 5, 6, 7, 8 y 9.

También el capítulo 12 de la parte IV, en [Lud11] nos aporta información acerca de la viabilidad de características 802.11n en largas distancias.

2.4. Calidad de Servicio (Quality of Service – QoS)

Dotar a una red de calidad de servicio (Quality of Service – QoS) significa tener la habilidad de distinguir entre los diferentes tipos de tráfico y asignar recursos de acuerdo a sus parámetros, como por ejemplo: prioridades.

En el presente proyecto se ha medido las prestaciones de la red empleando la gestión avanzada de tráfico (HTB) en *MikroTik* para dotarla de calidad de servicio (QoS), se han realizado diversas pruebas.

En los Anexos se especifica la configuración en todos los nodos de la red. También, los comentarios de los resultados, como veremos en el apartado de ‘*Diseño de la Red*’.

En la Red de Telemedicina implementada decidimos que aplicaciones en tiempo real, como son la voz o el vídeo sobre IP, debían ser tratadas de manera especial por dos motivos:

- La Red de Telemedicina está enfocada a ofrecer servicios de voz y vídeo para poder realizar llamadas telefónicas y videoconferencias entre puestos de salud. Estas comunicaciones se realizan con el fin de poder obtener más información médica y que los profesionales de la sanidad puedan ser guiados por especialistas. Por esta razón, debido a la dedicación del sistema a temas de salud, las consultas telefónicas y las teleconsultas deben tener la máxima prioridad en nuestro análisis de tráfico.
- Las aplicaciones en tiempo real son muy sensibles en cuanto a retardos, aun cuando son tolerantes a la pérdida de paquetes IP. Retardos en sesiones de videoconferencia o llamadas telefónicas pueden ser críticos, por lo que hay que tenerlo en cuenta y ofrecer privilegios para que estas transmisiones puedan operar sin errores.

En el sistema operativo Linux es posible controlar el tráfico a través del uso de disciplinas de colas. Se pueden dividir en dos clases:

- **Disciplinas de colas sin clases**
- **Disciplinas de colas con clases**

A continuación veremos qué tipos existen dentro de estas dos clases.

2.4.1. Disciplina de colas sin clases

Las disciplinas de colas sin clases son aquéllas que aceptan datos y, después, se limitan a reordenarlos, ralentizarlos o descartarlos. Se suelen utilizar para administrar el tráfico de toda una interfaz, sin hacer ninguna división dentro de la misma.

Es decir, por poner un ejemplo, si tenemos un servidor que sirve Internet a un grupo de clientes por la interfaz *'eth0'*, todos los clientes dispondrán del mismo ancho de banda equitativamente. Por lo tanto, no podremos dividir a los clientes en dos subgrupos, de forma que el grupo "A" tenga más ancho de banda que el grupo "B".

Dentro de las disciplinas de colas sin clases, las más conocidas y utilizadas son tres: **Packets First-In First-Out Fast (PFIFO_FAST)**, **Token Bucket Filter (TBC)** y **Stochastic Fairness Queueing (SFQ)**.

2.4.2. Disciplina de colas con clases

Las disciplinas de colas con clases, a diferencia de las sin clases, sí nos permiten dar un trato especial a un grupo específico de clientes que forman una clase. Una disciplina con clases puede estar formada por infinidad de clases, que a su vez pueden desembocar en otras clases que pueden ser disciplinas con o sin clases, como en una topología de árbol.

La estructura es sencilla, sólo hay que tener en cuenta que una clase puede tener dos tipos de *padres*: una disciplina u otra cola. Si una cola no tiene ningún *hijo*, se le conoce como clase terminal y deberá tener una disciplina adjunta que será la encargada de transmitir los datos a la clase.

Así pues, las disciplinas con clases son aquéllas que nos permiten clasificar a nuestros tráficos y tratarlos de forma distinta según nuestras necesidades. Hay tres algoritmos de este tipo: **Priority Scheduler (PRIO)**, **Class-based Queueing (CBQ)** y **Hierarchical Token Bucket (HTB)**.

2.4.2.1. Hierarchical Token Bucket (HTB)

Debido a la complejidad de CBQ y a la impresión de no ser del todo óptimo de algunas situaciones específicas, surgió la disciplina **Hierarchical Token Bucket (HTB)**. HTB tiene un enfoque jerárquico que se ajusta bien a configuraciones donde se tiene una cantidad fija de ancho de banda a dividir entre diferentes propósitos o tipos de tráfico, dándole a cada uno una porción del ancho de banda total.

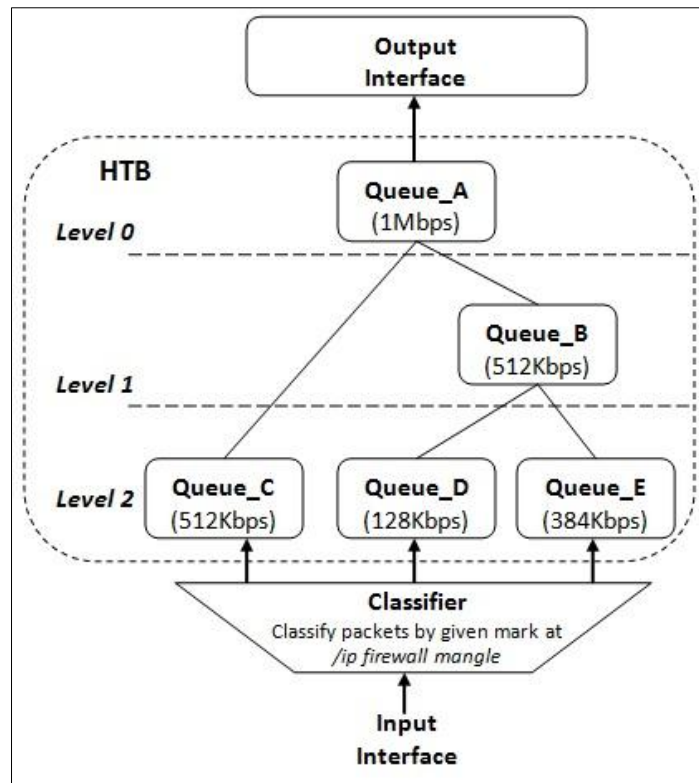


Ilustración 2: Disciplina HTB

Soportar calidad de servicio (QoS) usando *RouterOS*² no solamente se refiere a la limitación del ancho de banda, sino que también define la forma de distribución bastante equitativa que utiliza para repartir este ancho de banda.

La disciplina **Hierarchical Token Bucket (HTB)** es una parte importante en la calidad de servicio (QoS), la cual consiste en una hacer una estructura jerárquica como hemos comentado anteriormente y además determinar las relaciones entre sus diferentes colas (permitiendo establecer prioridades y la ventaja de conformar diferentes tamaños de ráfagas en las colas).

HTB se define como un remplazo más comprensible, intuitivo y más rápido para la disciplina de colas (qdisc) **Class-based Queueing (CBQ)** en Linux.

La disciplina HTB permite ser configurada a cualquier interfaz física o virtual, con lo cual se dispone de cuatro lugares donde limitar (global-in, global-out, global-total, out-interface), estas interfaces son definidas como agrupaciones de varias y tienen importancia en el estudio del flujo de paquetes (ver [Ilustración 3](#)) para dotar de calidad de servicio (QoS).

² RouterOS (Mikrotik Routeros): **RouterOS** es el sistema operativo y software del router el cual convierte a un PC Intel o un Mikrotik RouterBOARD en un router dedicado.

QoS Packet Flow

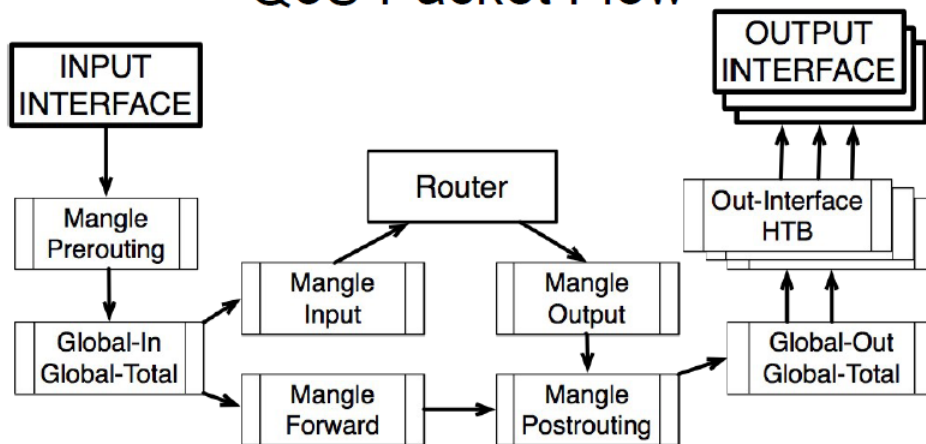


Ilustración 3: Diagrama de flujos de paquetes para soportar calidad de servicio (QoS)

Para una mayor información de la configuración del flujo de paquetes se puede consultar en [MMP11].

Como ya hemos comentado anteriormente la disciplina HTB permite crear una estructura jerárquica de colas y determinar las relaciones entre las colas, como de “padre a hijo” (parent-child) o “hijo a hijo” (child-child). En la siguiente *Ilustración 4* se observa un ejemplo de estructura utilizando la disciplina HTB.

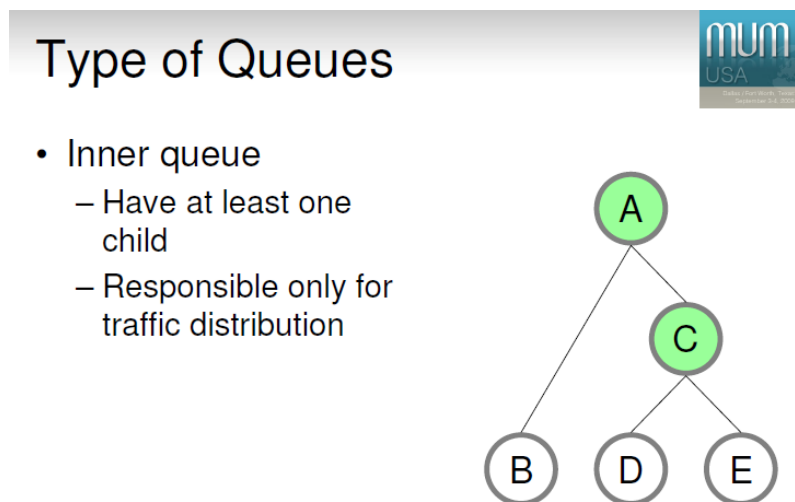


Ilustración 4: Ejemplo de “Inner queue”

En [MMH11], [Cle05], [Meg09] y [Val05] se detalla los aspectos para la configuración de HTB en RouterOS.

Además, en [Hub04] y [MBC06] se especifica la información necesaria para llevar a cabo la configuración de cada una de las disciplinas de colas.

2.5. Tecnología para la transmisión de voz y videoconferencia sobre IP

Voz sobre IP (Voice over IP - VoIP) es una tecnología de telecomunicaciones que permite que una señal de voz viaje a través de una red de datos (Internet) utilizando el protocolo TCP/IP. Para llevar a cabo la transmisión se utiliza la conmutación de paquetes, la señal de voz es transformada de analógica a digital.

En el caso de la telefonía convencional, la señal de voz es transmitida en su forma analógica a través de conmutación de circuitos utilizando la red PSTN³ (Public Switched Telephone Network).

La señal de voz o video es transformada a digital a través de un proceso de codificación y decodificación (Códec). Además de realizar la conversión, el códec comprime la secuencia de datos, proporciona la cancelación del eco y la supresión de silencios. Se disponen de Códecs variados que posibilitan utilizar diferentes valores de ancho de banda, calidad y retardo.

2.5.1. Códecs de Audio

En nuestros enlaces que son de larga distancia, sensibles muchas veces a las condiciones climáticas, necesitábamos un códec de audio sencillo, que diera como resultado una buena calidad de voz pero que ocupara lo mínimo de nuestro ancho de banda. Para ello, estuvimos probando las dos opciones que nos parecieron más interesantes: G.711 y GSM.

Ambos códecs podían ser configurados en nuestro *softphone* y, *a priori*, ofrecían buenos resultados. Inicialmente, nos inclinábamos más por GSM ya que operaba a tasas muy inferiores que G.711, en concreto a 13 Kbits/s, pero después de probarlo en diferentes horarios y condiciones atmosféricas, observamos que no funcionaba del todo bien.

Como el ancho de banda conseguido en nuestra red nos dejaba mucho margen de operatividad, decidimos hacer pruebas con G.711 que, pese a trabajar con tasas de 64 Kbits/s, ofrecía una mayor robustez que GSM ya que evitaba la compresión y esto hacía que su retardo fuera menor debido a que su tiempo de procesamiento también era menor.

³ Red PSTN: Corresponde a la **Red Telefónica Pública Conmutada o RTB** y está constituida por todos los medios de transmisión y conmutación necesarios para enlazar dos equipos terminales mediante un circuito físico que se establece para la comunicación y se libera cuando ésta ha finalizado.

Después de muchas pruebas y comunicaciones entre diferentes nodos, observamos que funcionaba perfectamente. La calidad de voz era nítida sin presencia de ruido, como si habláramos a través de un teléfono convencional.

En [CQC09] se describen las características de los códecs de audio soportados por Asterisk.

2.5.2. Códecs de Video

Un códec de video es un tipo de códec que permite comprimir y descomprimir vídeo digital. Normalmente, los algoritmos de compresión empleados conllevan una pérdida de información.

Asterisk puede trabajar con diferentes códecs de audio y vídeo. A continuación se enumeran los códecs soportados y su ancho de banda necesario:

- ✓ H.261 (entre 40 Kbits/s y 2 Mbits/s)
- ✓ H.263 (desde menos de 64 Kbits/s hasta 583.9 Mbits/s sin compresión)
- ✓ H.263p (Asterisk 1.4 y versiones superiores) (desde menos de 64 Kbits/s hasta 583.9 Mbits/s sin compresión)
- ✓ H.264 (Asterisk 1.4 y versiones superiores) (entre 64 Kbits/s y 960 Mbit/s)

Para el servicio de videoconferencia tuvimos en cuenta no sólo los códecs que podía soportar Asterisk, sino también los que podían funcionar en el *softphone* utilizado para realizar videollamadas.

En nuestra red de Telemedicina se necesitaba una calidad de imagen excelente para lograr que los especialistas pudieran ver a sus pacientes con el máximo detalle y, así, poder realizar un diagnóstico mucho más completo.

Los resultados han sido muy buenos, se ha empleado el códec H.264 de alta definición (High Definition –HD) y el softphone, Linphone v.3.4.3. La imagen es nítida sin retardos o ‘*delays*’, y con una gran resolución (ver *Ilustración 5*).



Ilustración 5: videoconferencia entre los técnicos de enfermería de San Juan y Balsapuerto a través del softphone Linphone

2.5.3. Asterisk

Asterisk es una aplicación de software libre (con licencia GPL) que proporciona funcionalidades de una central telefónica (Private Branch Exchange – PBX). Como en cualquier PBX, se pueden interconectar un número determinado de terminales para realizar llamadas telefónicas y sesiones de videoconferencia e incluso, conectar a proveedores de VoIP y de telefonía convencional tanto analógica como digital.

En sus inicios, Asterisk fue desarrollado para entornos GNU/Linux aunque, en la actualidad, existen versiones para sistemas operativos como MacOSX, BSD o Microsoft Windows.

Dentro de las funcionalidades de Asterisk, podemos encontrar los servicios de buzón de voz, conferencia, respuesta de voz interactiva (Interactive Voice Response – IVR), distribución automática de llamadas, etc. Los usuarios pueden crear nuevas funcionalidades escribiendo un *dial plan*⁴ en el lenguaje de *script* de Asterisk o añadiendo módulos escritos en lenguaje C o en cualquier otro lenguaje de programación soportado en GNU/Linux.

⁴ Dial plan (Plan de numeración): Un **dial plan** es un software residente en algunos gateways y en casi todas las IP-PBX que permite determinar el trato que se le debe ofrecer a un determinado número marcado.

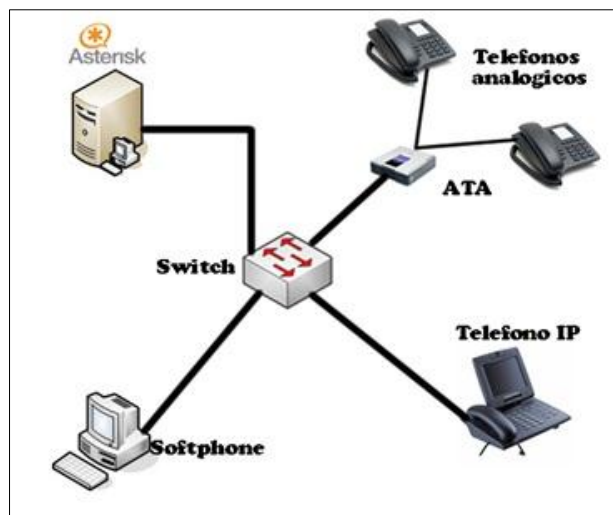


Ilustración 6: Esquema de conexión a través de Asterisk

Asterisk es el servidor software utilizado en este proyecto para gestionar las llamadas, sesiones de videoconferencia y envío de mensajes instantáneos entre los diferentes clientes de la red. Asterisk funciona bajo el sistema operativo '*Linux Voyage*', el cual es una distribución derivada de Debian que está optimizada para poder operar con plataformas x86 de propósito específico, tales como las placas de PC Engine ALIX utilizadas en la instalación.

Cabe decir que, inicialmente, se instaló la versión '**asterisk-1.4.24.1**' de Asterisk. Al tratar de configurar los *softphones* para establecer sesiones de videoconferencia, éstas no funcionaban correctamente y decidimos instalar una versión más actualizada del software. Finalmente, tras la instalación de la versión '**asterisk-1.8.3.3**', comprobamos que con ella sí se soportaban perfectamente los servicios de videoconferencia y los usuarios eran capaces de registrarse y realizar videollamadas entre sí.

Asterisk funciona del mismo modo que una centralita de una empresa. Con las extensiones configuradas podemos encaminar las llamadas de un cliente a otro, las sesiones de videoconferencia, las llamadas a tres, etc.

La configuración de Asterisk se lleva a cabo a través de archivos de configuración. Los más importantes, los que más modificamos durante la configuración de los equipos a la hora de realizar las pruebas y la puesta en marcha del sistema, son los archivos '*sip.conf*' y '*extensions.conf*'.

El archivo '*sip.conf*' está estructurado en tres bloques. Hay una parte general donde se define la configuración de nuestras extensiones. En el bloque central se establece el registro de

nuestros clientes. Por último, en la parte final se configuran nuestras extensiones externas e internas.

El archivo *'extensions.conf'* contiene el *dial plan* de Asterisk o plan de marcación, es el plan maestro de control o de flujo de ejecución para todas las operaciones. Controla cómo se manejan y se encaminan las llamadas entrantes y salientes. Aquí es donde se configura el comportamiento de todas las conexiones con tu PBX.

Tanto la configuración del archivo *'sip.conf'* como la del archivo *'extensions.conf'* se detallan en el apartado de Anexos. En ellos se pueden distinguir las extensiones adjudicadas a los clientes de nuestra red o los códecs de audio y vídeo soportados dentro de la comunicación entre ellos, parámetros de vital importancia para el buen funcionamiento del servicio de videoconferencia.

Asterisk permite integrar nuestra red con las redes telefónicas tradicionales por medio de interfaces analógicas y digitales, para la conexión con líneas analógicas se hace a través de dispositivos FXS (Foreign eXchange Station) y FXO (Foreign eXchange Office). En [CQC09] se describe estas interfaces, además los servicios que se pueden implementar y su arquitectura.

2.5.4. Protocolos de señalización para videoconferencia y voz sobre IP (VoIP)

Son los lenguajes que utilizarán los distintos dispositivos de videoconferencia y VoIP para su conexión, estos protocolos se encargan de los mensajes y procedimientos para establecer una comunicación. Esta parte es importante ya que de ella dependerá la eficacia y la complejidad de la comunicación.

2.5.4.1. Protocolo SIP

Session Initial Protocol o **SIP** es un protocolo desarrollado por el grupo de trabajo MMUSIC del IETF (Internet Engineering Task Force) con la intención de ser el estándar para la iniciación, modificación y finalización de sesiones multimedia (*'unicast'* o *'multicast'*), es decir se encarga de la señalización para el establecimiento de estas sesiones en redes IP.

En noviembre del año 2000, SIP fue aceptado como el protocolo de señalización de 3GPP y elemento permanente de la arquitectura IMS (IP Multimedia Subsystem).

SIP establece el flujo de establecimiento de una sesión a través de mensajes de señalización. Además se apoya en otros protocolos para lograr controlar y manejar llamadas telefónicas, sesiones de videoconferencia y mensajería instantánea. Los elementos básicos de los que se compone para establecer una sesión son los User agents (UA) y los servidores; estos últimos pueden ser del tipo de Registro, Proxy y Redirección.

En [CQC09] se describe los Protocolos VoIP que maneja Asterisk. También una mayor información del protocolo SIP: se definen sus elementos, mensajes, el flujo del establecimiento de una sesión, el inicio de una sesión, su finalización y los protocolos en los que se apoya.

Capítulo III

Materiales y métodos

En este capítulo se va a detallar la metodología empleada para el diseño y la implementación de la red. También las herramientas que han sido necesarias para su realización.

3.1. Metodología

Es importante destacar dos antecedentes de gran importancia para la realización de este trabajo:

- a) Una red de Telemedicina con enlaces troncales punto a punto IEEE 802.11n de largas distancias que se encuentra en producción, ubicada en la provincia de Cajamarca (Perú); el cual logró valores superiores de throughput de datos efectivos; empleando enrutadores y tarjetas inalámbricas del mismo fabricante '*MikroTik*'.
- b) El logro en relación a los valores de throughput de datos, por encima a los obtenidos en enlaces inalámbricos (WiFi) de largas distancias, en un enlace piloto troncal que utiliza el mismo equipamiento; el cual se implementó en la ciudad de Lima con la colaboración del grupo GTR-PUCP.

Teniendo en consideración el objetivo de diseñar e implementar una red inalámbrica IEEE 802.11n de Telemedicina utilizando un sistema básico MIMO (Multiple-Input/Multiple-Output) 2x2 con diversidad de polarización para lograr un mayor throughput de datos efectivo y además dotarla con QoS. Se ha llevado a cabo el siguiente procedimiento.

3.1.1. Procedimiento para la realización de este trabajo

Primero, se ha tenido en cuenta, una buena selección de equipos, con una exhaustiva prueba de los mismos. El enrutador debería tener una relación beneficio/costo muy alto y disponer de un óptimo soporte técnico (hardware/software), reconocido a través de los años.

Se eligió enrutadores MikroTik, el cual dispone de un sistema operativo versátil, potente y fácil de configurar, conocido como RouteOS y está basado en Linux. MikroTik dispone de muchas funciones a nivel de las capas 3 y 7 de la arquitectura OSI⁵.

MikroTik dispone de características para el enrutamiento y la conexión de redes, se destaca dos funciones: Gestor de ancho de banda y QoS.

Segundo, se realizaron muchas pruebas antes de la implementación de la red, ensayando enlaces inalámbricos con la misma tecnología. Se destaca la implementación de un enlace piloto troncal de largas distancias empleando el mismo equipamiento, la cual se llevó a cabo en la ciudad de Lima y con colaboración del grupo GTR-PUCP.

Finalmente, la evaluación de los óptimos resultados con la tecnología empleada, permitieron preparar y desarrollar una simulación en el laboratorio del grupo GTR-PUCP con las configuraciones de los equipos, preparando los servicios y la medición de las prestaciones de la red.

Las pruebas comprendían además, la medición de las prestaciones de la red empleando HTB para la gestión avanzada de tráfico. También la elección del '*Softphone*', los códecs de voz y videoconferencia más adecuados; finalmente, tras la instalación de la versión '**asterisk-1.8.3.3**', se comprobó que con ella si se soportaban los servicios de videoconferencia y los usuarios eran capaces de registrarse y realizar llamadas entre sí.

La realización de este trabajo siempre ha tenido en consideración lo crítico que es un diseño correcto para que la red instalada funcione según lo esperado. En este sentido, la experiencia de más de 10 años del grupo GTR-PUCP implementando proyectos de ingeniería en zonas aisladas, sus redes desplegadas y en producción han servido de base para este trabajo.

3.2. Software de Simulación

A continuación se presentan las herramientas software empleadas en las pruebas y resultados: se destaca el uso de Radio Mobile y Google Earth para el cálculo de Radio Enlaces, las herramientas '*Iperf*' y '*Bandwith Test*' de MikroTik para la medición del ancho de banda. También la utilización de una interfaz gráfica '*Winbox*' para este equipo; permitiendo una

⁵ OSI: Siglas que corresponden a '*Open System Interconnection*'

fácil configuración, reparación y medición gráfica con mayor detalle para el caso del ancho de banda de los enlaces.

3.2.1. Uso de Radio Mobile y Google Earth para el cálculo de Radio Enlaces

Radio Mobile es un software de libre distribución utilizado para calcular radio enlaces de larga distancia en terreno irregular. Radio Mobile realiza el cálculo teniendo en cuenta las siguientes características:

- ✓ Perfiles geográficos.
- ✓ Las características técnicas de los equipos (la potencia de transmisión, la sensibilidad del receptor, las características de las antenas, las pérdidas, etc.).
- ✓ Utiliza el Modelo Longley-Rice: Es un modelo de predicción troposférica para predecir las pérdidas en una transmisión de radio sobre terreno irregular en enlaces de medio y largo alcance. Para el cálculo de la propagación utiliza diferentes parámetros generales comunes al de otros modelos de propagación: la frecuencia de operación, *ERP*⁶, el tipo de antena y la altura de antena). También tiene en cuenta varios parámetros específicos: la polarización de la antena, la refractividad de la atmósfera, la permitividad relativa o constante dieléctrica del medio, la conductividad, diferentes modelos de climas y la variabilidad.
- ✓ Su uso se especifica para un rango de frecuencias entre 20 MHz y 40 GHz y para longitudes de trayecto del enlace de entre 1 Km y 2000 Km.

El software utiliza un plano digital que contiene la elevación del terreno, esto permite que se pueda obtener la intensidad de la señal recibida en diferentes puntos del trayecto. Muestra además las diferentes zonas de Fresnel y el área de cobertura generando un perfil entre dos puntos del mapa. Esta herramienta realiza una simulación calculando las pérdidas de propagación considerando además las pérdidas ocasionadas por los obstáculos.

El software acepta varios formatos de datos de elevación: GTOPO30 (Global Topographic Data), SRTM (Shuttle Radar Topography Mission) y DTED o DEM (Digital Elevation Model). La obtención de estos mapas se puede realizar desde una opción del software que

⁶ ERP (Equivalent Radiated Power): es una medida teórica estándar de la energía de radio frecuencia (RF) comúnmente expresada en Watts. Se puede calcular sumando la ganancia de la antena más la potencia de transmisión sin considerar las pérdidas del sistema.

permite descargarlos de Internet. El software se puede descargar en diferentes idiomas desde su página web: <http://www.cplus.org/rmw/download/download.html>

Teniendo en cuenta sus características y con el fin de simular y predecir el comportamiento de la red y poder, así, realizar un diseño más realista, se utilizó el software Radio Mobile. Esta aplicación permite calcular radioenlaces para diferentes tecnologías, ya que es posible escoger la frecuencia a la que queremos trabajar, los tipos de antenas, la potencia transmitida y muchos otros parámetros.

Además, puede trabajar con coordenadas reales, de manera que se pueden e incluir mapas de la zona que se sea necesaria. Estos mapas incluyen información orográfica del terreno, permitiendo saber la altura de cada punto y la presencia de ríos, montañas y otros accidentes geográficos. Se eligió trabajar con los mapas SRTM porque están más depurados de errores y brindan mejor resolución del relieve de los terrenos en estudio.

También se ha utilizado el software Google Earth para optimizar la simulación radioeléctrica, permitiendo realizar una vista previa de las zonas de intervención de los enlaces. Este software brinda imágenes detalladas de los lugares existentes, y permite identificar áreas donde existe mucho ruido en su espectro, también la existencia de obstáculos naturales que pudieran dificultar la comunicación inalámbrica.

Google Earth utiliza archivos con formato KML para representar datos geográficos en tres dimensiones. Con archivos KML se ofrece una forma sencilla de insertar información georreferenciada dentro de Google Earth, lo cual permite asociar a cada nodo los valores de: longitud, latitud, altitud, título y descripción.

En la realización de la simulación radioeléctrica de los enlaces, se dispone de un archivo generado por Radio Mobile que permite exportar los datos de la topología de la red. Este archivo tiene formato KML y es interpretado por Google Earth, con lo cual se ha permitido emular mejor la trayectoria de la señal y se mejora también la visualización de la línea de vista de los enlaces.

3.2.2. Iperf

Es una herramienta desarrollada por NLARN/DATS (NLARN Distributed Applications Support Team), para medir el ancho de banda y la calidad del enlace.

La herramienta permite medir throughput de datos utilizando el protocolo TCP y el retardo a través del comando *'ping'*. También permite ajustar parámetros del protocolo UDP para medir el *'Jitter'* (variación de retardo) y la pérdida de paquetes.

Iperf puede ser instalado en cualquier sistema operativo UNIX / Linux y Windows, además utiliza un sistema cliente/servidor.

Para una mayor información acerca del uso de esta herramienta se recomienda consultar en [\[Ehw\]](#).

3.2.3. Herramienta 'Bandwith Test' de MikroTik

Esta herramienta se usa para medir throughput de datos con otro enrutador, en el caso de redes cableadas e inalámbricas, la herramienta ayuda a descubrir cuellos de botella. También utiliza los protocolos TCP y UDP para las mediciones de ancho de banda.

Para la medición se utiliza todo el ancho de banda disponible, por esta razón es recomendable que la red no se encuentre en uso en el caso de realizar mediciones.

3.2.4. D-ITG (Distributed Internet Traffic Generator)

Esta herramienta es una plataforma capaz de generar tráfico a nivel de paquete y dispone de muchas características y ventajas apropiadas para una medición de las prestaciones de una red que dispone de servicios de tiempo real como son: VoIP y la videoconferencia.

D-ITG soporta ambos protocolos: IPv4 y IPv6, en la generación de tráfico. También, es capaz de generar tráfico en las capas 3, 4 y 7 de la arquitectura OSI. Actualmente soporta los sistemas operativos Linux, OSX y Windows.

La documentación y el software se pueden descargar desde el siguiente enlace [\[Dit\]](#).

3.2.5. Winbox

La configuración remota del enrutador MikroTik se puede hacer usando *'Telnet'*, *'SSH'*, *'Webbox'* o a través de la interfaz de usuario gráfica (GUI) de la consola Winbox.

La consola Winbox es usada para llevar a cabo la configuración del enrutador MikroTik, sus funciones y características de gestión, usando su interfaz gráfica.

Una breve descripción de la consulta Winbox se puede consultar en [\[MMW11\]](#).

Capítulo IV

Diseño de Red

4.1. Introducción

Se trata de una red de Telemedicina implementada en el distrito de Balsapuerto. Esta red dispone de los siguientes servicios:

- ✓ Voz: Se dispone de un servidor Asterisk que permite cursar llamadas (ToIP) entre el hospital y los puestos o centros de salud
- ✓ Videoconferencia: El mismo servidor Asterisk permite establecer sesiones de videoconferencia utilizando un Softphone.
- ✓ Datos: Para el cual se dispone de un sistema de carpetas compartidas controlado por un servidor central
- ✓ Internet: Se ha configurado un Gateway (cliente de la Red de Salud), el cual está conectado al ADSL de Telefónica contratado por la Red de Salud. A través de este equipo todos los nodos de la red salen a Internet.

Esta red permitió unir tres comunidades aisladas, San Juan del Armanayacu, San Gabriel de Varadero y Balsapuerto, con Yurimaguas (Hospital de apoyo Santa Gema de Yurimaguas), siendo esta última capital de distrito.

Para llevarlo a cabo, se contó con la colaboración de la Municipalidad y el Hospital. Logrando finalmente comunicar puestos y centros de salud con el Hospital, el cual dispone de médicos y especialistas que resolverán dudas, incluso realizarán diagnósticos a distancia (telemedicina) a través de Videoconferencia.

Es una red inalámbrica IEEE 802.11n de largas distancias. La siguiente ilustración contiene el diagrama de esta Red, la cual muestra la conexión que existe entre el hospital y los puestos o centros de salud de las comunidades mencionadas anteriormente, también la conexión de la Red de Salud y además la conexión con las dos oficinas de la Municipalidad ubicadas una en Balsapuerto y la otra en Yurimaguas.

Este diagrama de Red especifica la configuración WiFi de todos los equipos, su topología, las características de las antenas, el direccionamiento IP, el enrutamiento dinámico OSPF, entre otras características.

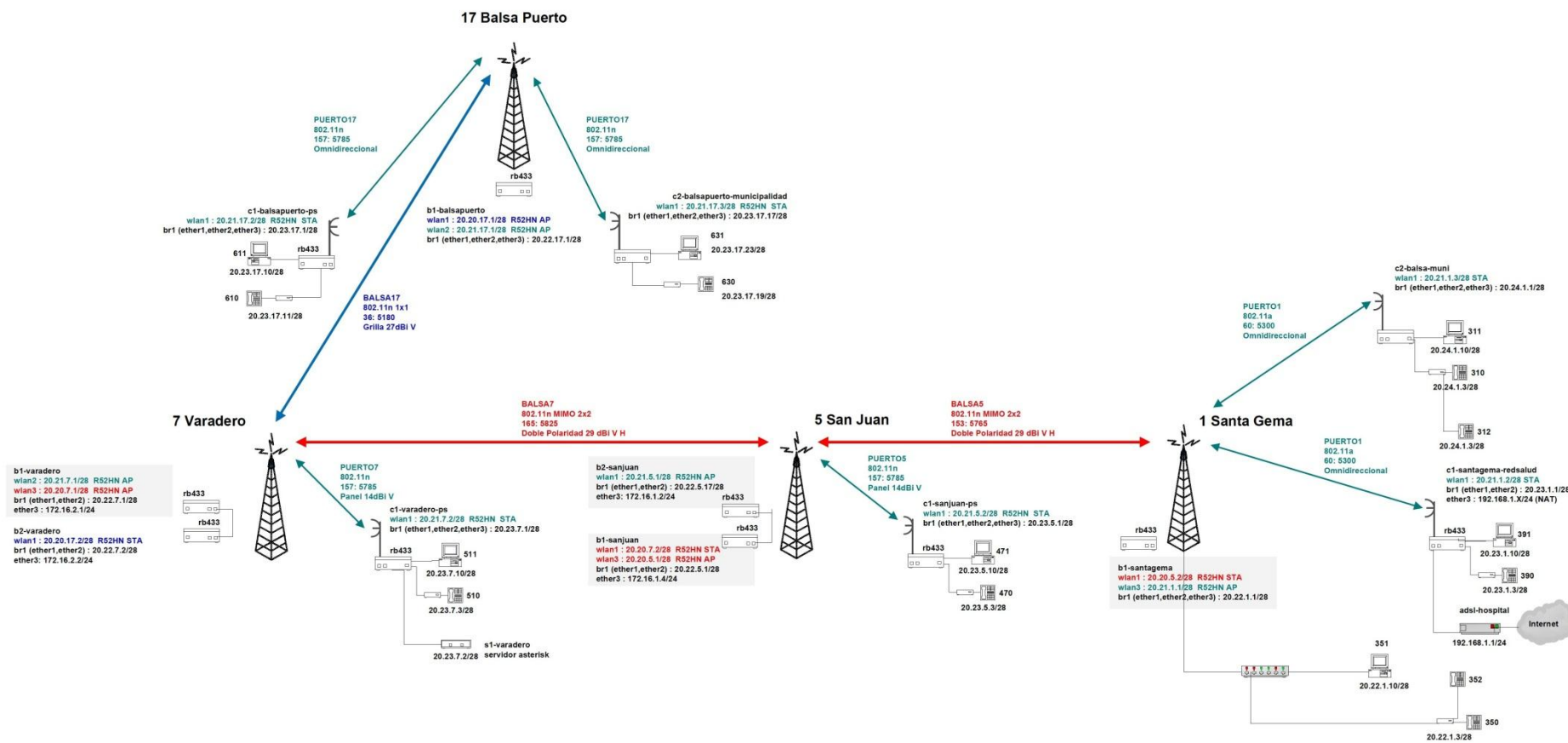
Se ha tenido en consideración que un diseño correcto es crítico para que la red instalada funcione según lo esperado. Para llevar a cabo este diseño y obtener los buenos resultados descritos en el siguiente capítulo (Calidad de la Red), se ha tenido en cuenta una buena selección de los equipos, una exhaustiva prueba de los mismos.

Además se realizó el despliegue de un enlace inalámbrico de prueba IEEE802.11n de largas distancias utilizando el mismo equipamiento empleado en esta red. Este enlace de prueba ha permitido obtener un mayor valor de throughput de los obtenidos hasta hoy utilizando un sistema MIMO con diversidad de polarización, este enlace también nos dio la oportunidad de utilizar eficientemente algunos valores de configuración del estándar como son: el uso del intervalo de guarda corto (400 nseg) y el uso ancho de banda de 40 Mhz.

El presente documento presenta información de los trabajos de instalación, implementación y puesta en operación de los sistemas de Telecomunicaciones, energía e infraestructura de la Red. Además se detalla las características de la Red Troncal y Red de Distribución.

También se ha medido las prestaciones de la red empleando la gestión avanzada de tráfico para dotarla de Calidad de Servicio, logrando priorizar el tráfico y asegurar un ancho de banda conveniente a la Videoconferencia y la VoIP. En este capítulo y en el anexo (B) se detalla su configuración y la discusión de los resultados.

Red de Telemedicina Balsapuerto 2011



4.2. Estudio de campo inicial

El proyecto de la Red de Telemedicina para el distrito de Balsapuerto, provincia de Alto Amazonas, departamento de Loreto, es una iniciativa del Grupo de Telecomunicaciones Rurales de la Pontificia Universidad Católica del Perú (GTR-PUCP) y de la Fundación *Humanitarian Technology Challenge* de la IEEE.

Se cuenta con el compromiso de colaboración tanto de la Red de Salud de Alto Amazonas, principal beneficiario del proyecto, como de la Dirección Regional de Salud de Loreto (DIRESA Loreto) y del Gobierno Regional de Loreto (GOREL).



Ilustración 7: Distrito de Balsapuerto

De acuerdo al Instituto Nacional de Estadística e Informática (INEI), Balsapuerto es uno de los distritos más pobres y menos desarrollados de Perú, con una población mayoritaria de indígenas de la etnia Chayahuita.

En el distrito hay 13 establecimientos de Salud (C.S. Balsapuerto, P.S. Centro América, P.S. Fray Martín, P.S. Nueva Vida, P.S. Nuevo Arica, P.S. Panam, P.S. Progreso, P.S. Pucallpillo, P.S. San Gabriel de Varadero, P.S. San Juan, P.S. Soledad, P.S. Vista Alegre y P.S. Nueva Esperanza), de los cuales, 5 son relativamente nuevos.

Unos meses antes del inicio de la instalación, el Grupo de Telecomunicaciones Rurales (GTR-PUCP) realizó un estudio de campo para valorar y delimitar la zona de operaciones. Este estudio comprendió la visita de todos los establecimientos de salud ubicados a orillas de los ríos Parapapura, Armanayacu y Cachiyacu.

Se obtuvieron datos georreferenciales de las posibles ubicaciones de las torres ventadas a implementar, información relevante para el diseño final de la red.

Los establecimientos de salud visitados fueron:

- | | |
|---------------------------------------|-----------------------|
| 1.- Hospital Santa Gema de Yurimaguas | |
| 2.- P.S. Munichis | Micro Red Yurimaguas |
| 3.- P.S. Santa Lucía | Micro Red Yurimaguas |
| 4.- P.S. Varaderillo | Micro Red Yurimaguas |
| 5.- P.S. San Juan | Micro Red Balsapuerto |
| 6.- P.S. Nueva Arica | Micro Red Balsapuerto |
| 7.- P.S. Centro América | Micro Red Balsapuerto |
| 8.- P.S. Fray Martín | Micro Red Balsapuerto |
| 9.- P.S. Varadero | Micro Red Balsapuerto |
| 10.- P.S. Nueva Esperanza | Micro Red Balsapuerto |
| 11.- C.S. Balsapuerto | Micro Red Balsapuerto |

Adicionalmente, se obtuvo información procedente de la base de datos del GTR-PUCP de los siguientes establecimientos de salud:

- | | |
|-----------------------|-----------------------|
| 1.- P.S. Panam | Micro Red Balsapuerto |
| 2.- P.S. Progreso | Micro Red Balsapuerto |
| 3.- P.S. Vista Alegre | Micro Red Balsapuerto |
| 4.- P.S. Nueva Vida | Micro Red Balsapuerto |
| 5.- P.S. Pucallpillo | Micro Red Balsapuerto |

6.- P.S. Soledad

Micro Red Balsapuerto

Para la elaboración del diseño de la red WIFI se ha empleado el software de diseño de radioenlaces '*Radio Mobile*', así como la herramienta de Internet '*Google Earth*' y el software propietario '*MapSource*' de la empresa GARMIN. Los criterios de diseño empleados en la simulación software de los radioenlaces WIFI en zonas de selva, son fruto de la experiencia obtenida por el grupo GTR-PUCP durante los últimos diez años de investigación.

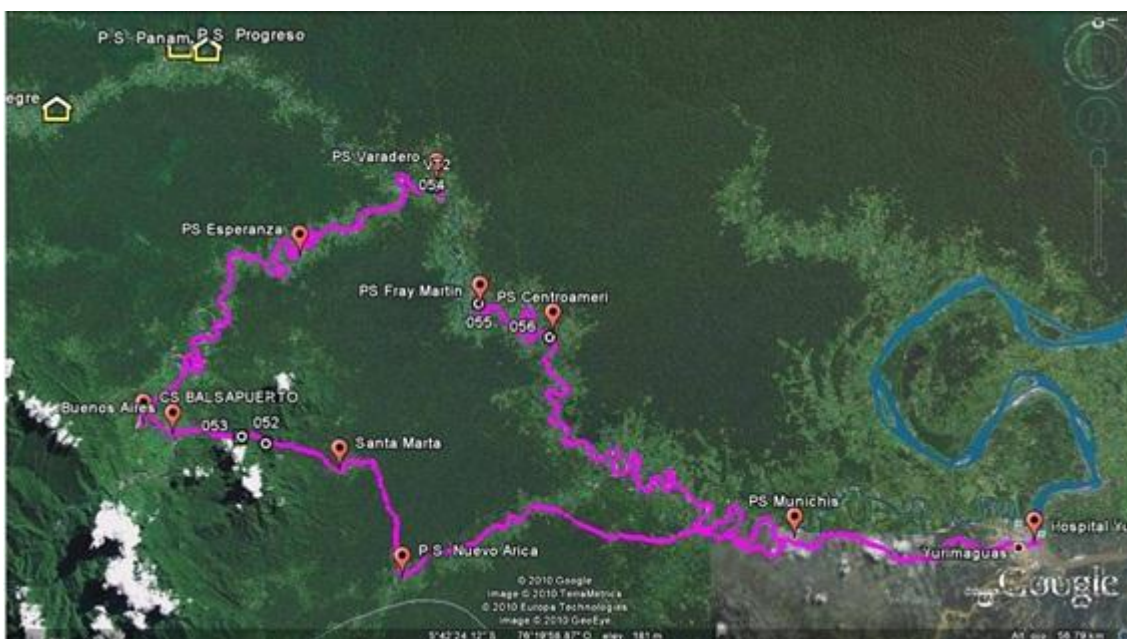


Ilustración 8: Estudio de campo realizado en la zona de Balsapuerto

En la [Tabla 3](#) se muestran los datos georreferenciales de los establecimientos de salud escogidos para instalar el sistema de transmisión de audio, vídeo y datos.

4.2.1. Resultados del estudio

Concluida la etapa de simulación de los radioenlaces WIFI, se llegó a la conclusión de que la implementación total de la red de Balsapuerto se desarrollaría por etapas.

La etapa inicial corresponde a la implementación de la red troncal, la cual interconectará a dos establecimientos de la municipalidad de Balsapuerto y a cuatro establecimientos de salud (Hospital de Apoyo Santa Gema de Yurimaguas, P.S. San Juan del Armanayacu, P.S. San Gabriel de Varadero y C.S. Balsapuerto).

Ítem	Establecimiento	Latitud (S)	Longitud (O)	Altura (msnm)		
				Mapa SRTM	GPS	Diferencia
01	Balsapuerto	05°42'48.1"	76°24'38.3"	207.55	219.00	-11.45
02	Varadero	05°50'04.8"	76°33'33.7"	163.89	176.00	-12.11
03	Centro América	05°47'21.3"	76°21'57.0"	155.20	163.00	-7.80
04	Varaderillo	05°52'03.7"	76°18'41.7"	148.74	149.00	-0.26
05	Munichis	05°53'31.9"	76°13'43.6"	146.11	155.00	-8.89
06	Santa Gema	05°53'38.5"	76°06'24.5"	145.07	162.0	-16.93
07	Nueva Arica	05°54'43.00"	76°25'41.2"	166.66	171.00	-4.34
08	Nueva Esperanza	05°45'00.1"	76°28'48.5"	172.01	183.00	-10.99
09	Fray Martín	05°46'26.0"	76°23'20.0"	169.89	179.00	-9.11
10	Red Alto Amazonas	05°53'47.1"	76°06'50.9"	144.70	170.00	-25.30
11	Santa Lucía	05°53'26.4"	76°16'45.6"	152.04	158.00	-5.96
12	San Juan	05°52'51.9"	76°21'34.8"	171.38	0.00	171.38
13	Panam	05°38'40.2"	76°32'12.3"	180.41	0.00	180.41
14	Progreso	05°39'01.4"	76°32'54.5"	176.76	0.00	176.76
15	Nueva Vida	05°34'29.2"	76°40'20.4"	188.83	0.00	188.83
16	Vista Alegre	05°40'58.9"	76°36'53.9"	184.34	0.00	184.34
17	Soledad	05°40'21.3"	76°35'36.4"	183.96	0.00	183.96
18	Pucalpillo	05°36'23.4"	76°37'18.8"	183.94	0.00	183.94

Tabla 3: Datos georreferenciales de todos los nodos de la red

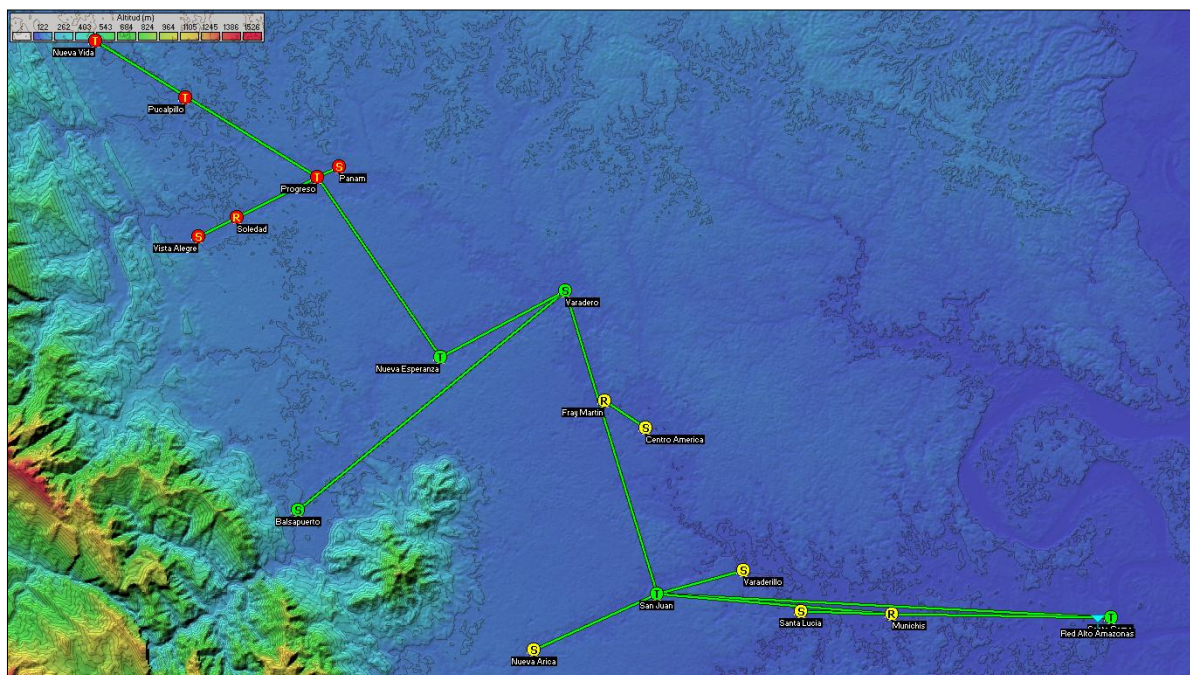


Ilustración 9: Diseño de la Red WIFI del proyecto de Telemedicina de Balsapuerto

Tras la finalización de esta etapa inicial, estarán interconectados dos puestos de salud, un centro de salud y el hospital Santa Gema de Yurimaguas. También, debido a su colaboración y estrecha vinculación, se conectarán la Red de Salud de Yurimaguas y dos sedes pertenecientes a la Municipalidad de Balsapuerto, una en Yurimaguas y otra en el mismo Balsapuerto.

En las siguientes etapas se procederá a la ampliación de la red troncal y de las redes de distribución. De esta manera, se permitirá la conexión con los demás nodos correspondientes a los establecimientos de salud antes mencionados.

El proyecto contempla la instalación de sistemas de transmisión de audio, vídeo y datos, como detallaremos más detenidamente en apartados posteriores.

4.3. Descripción de la Red de Telecomunicaciones

En el presente proyecto se ha desplegado una red de Telecomunicaciones con los siguientes servicios: VoIP, videoconferencia, datos y acceso a Internet. Con lo cual se dispone de estos servicios en las instalaciones de la municipalidad, en los establecimientos de salud, es decir en todas las localidades beneficiarias de este proyecto.

Las localidades de intervención son: Yurimaguas, San Juan del Armanayacu, San Gabriel de Varadero y Balsapuerto.

La red de telecomunicación del proyecto GTR – IEEE está constituida por enlaces inalámbricos empleando el estándar IEEE802.11n, la cual está constituida por **redes troncales (color rojo)** y **redes locales de distribución (color azul)**, tal como se puede observar en la siguiente *Ilustración 10*.

Las **redes troncales** están conformadas por tres enlaces inalámbricos, los cuales permiten la interconexión de las cuatro localidades de intervención antes mencionadas: Yurimaguas, San Juan del Armanayacu, San Gabriel de Varadero y Balsapuerto. Estas localidades tienen acceso a Internet a través de la estación cliente llamada Red de Salud de Yurimaguas.

Los tres enlaces que conforman las **redes troncales** son enlaces punto a punto conectados a través de cuatro repetidores troncales conocidos como: Balsapuerto, Varadero, San Juan y Santa Gema.

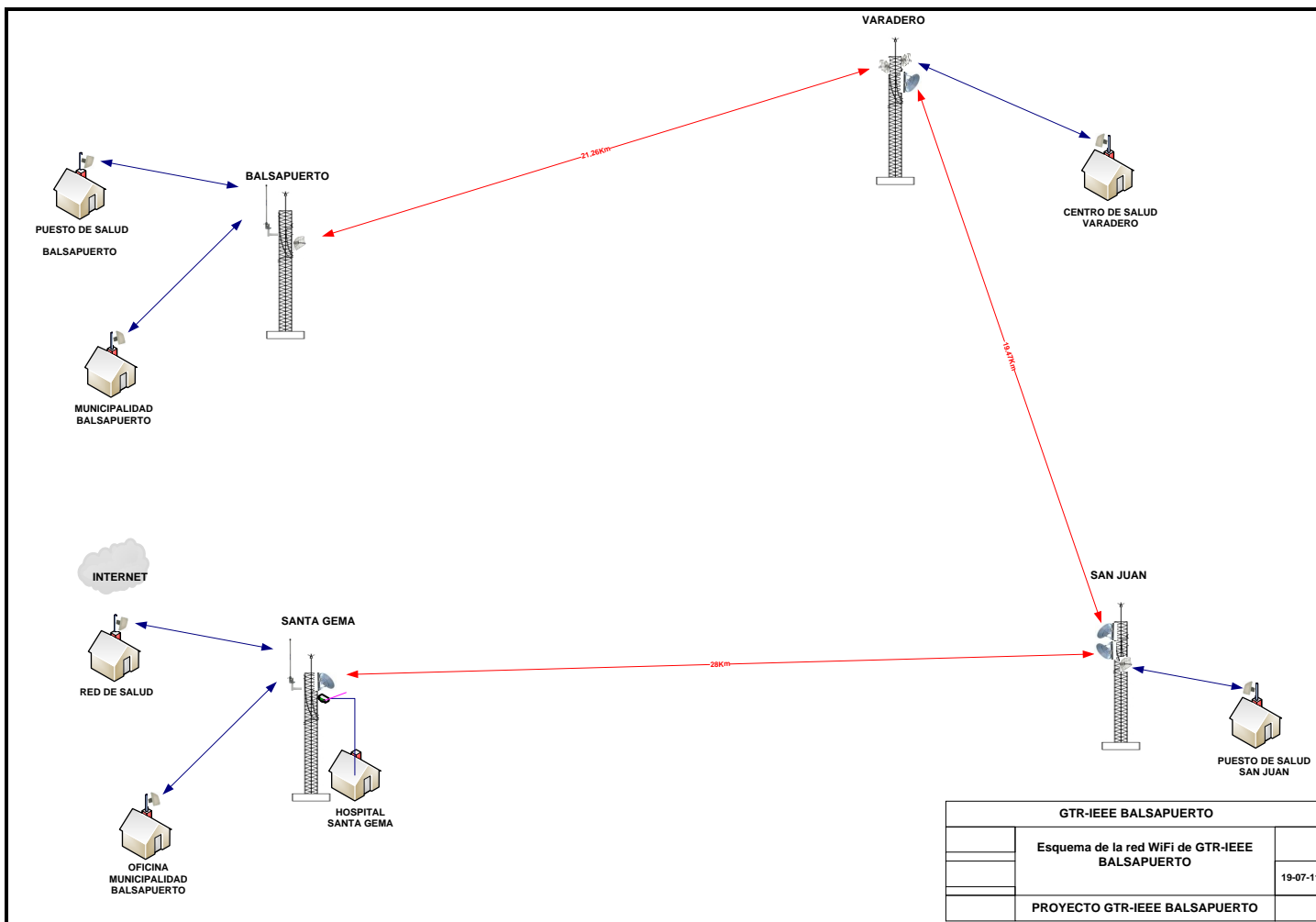


Ilustración 10: **Redes troncales** y **redes locales de distribución** de la red WiFi

Estos enlaces inalámbricos IEEE802.11n son de larga distancia, con un máximo de 28 Km y un mínimo de 19,47 Km.

Estos enlaces inalámbricos que conforman las **redes troncales** emplean antenas directivas de doble polaridad y se ha utilizado sistemas MIMO en su implementación.

Las **redes locales de distribución** están compuestas por enlaces inalámbricos punto a multipunto, estos enlaces conectan un repetidor local y sus clientes. El repetidor local recibe la señal de la red troncal y la distribuye a sus clientes, estos repetidores locales están ubicados en las cuatro localidades de intervención identificadas anteriormente.

Los repetidores locales ubicados en Yurimaguas y Balsapuerto emplean antenas omnidireccionales para comunicar varios clientes. Además, los repetidores locales ubicados en San Juan y Varadero emplean antenas panel para comunicar un solo cliente.

En la siguiente tabla se observa las coordenadas geográficas y las alturas de los puntos correspondientes a los nodos troncales y a los repetidores locales (las cuatro localidades de intervención identificadas anteriormente son nodos troncales y repetidores locales a la vez).

ÍTEM	UBICACIÓN	Latitud (S)	Longitud (O)	Altura (msnm)		
				Mapa SRTM	GPS	Diferencia
1	NODOS TRONCALES					
1.1	Balsapuerto	05°42'48.1"	76°24'38.3"	207.55	219.00	-11.45
1.2	San Gabriel de Varadero	05°50'04.8"	76°33'33.7"	163.89	176.00	-12.11
1.3	Santa Gema	05°53'38.5"	76°06'24.5"	145.07	162.0	-16.93
1.4	San Juan del Armanayacu	05°52'51.9"	76°21'34.8"	171.38	0.00	171.38

Tabla 4: Coordenadas geográficas de los nodos troncales y repetidores locales

4.3.1. Funcionamiento de la Red

4.3.1.1. Repetidores Troncales

Como ya se ha comentado la red troncal está constituida por cuatro repetidores troncales, y está conformada por tres enlaces inalámbricos punto a punto, en la banda de 5.8 Ghz.

La red troncal sale a internet a través de un cliente (Red de Salud) conectado al repetidor local de distribución ubicado en Santa Gema de Yurimaguas.

Como ya se ha comentado los repetidores troncales son además repetidores locales de distribución, los cuales repiten la señal que viaja a través de la red troncal, logrando comunicar así a los clientes finales.

A continuación se describen los sistemas de telecomunicaciones, infraestructura, energía y protección eléctrica pertenecientes a los repetidores troncales.

4.3.1.1.1. Sistema de Telecomunicaciones de los Repetidores Troncales

En la tabla siguiente se especifican los equipos que conforman el sistema de telecomunicaciones, cada repetidor troncal de la red dispone del equipamiento descrito a continuación. Los elementos principales son:

- ✓ Router Mikrotik modelo RB 433AH.
- ✓ Tarjeta inalámbrica modelo R52Hn.
- ✓ Antenas directivas de alta ganancia (grilla y doble polaridad) y antena omnidireccional.

Descripción de equipos del Sistema de Telecomunicación
Torre ventada de 60m de altura
Antena Grilla 5.8 Ghz 27 dBi (HG5827G) – Hyperlink
Antena de Doble Polaridad 5.8 Ghz 29 dBi (HG5158DP-29D) – Hyperlink
Antena Omnidireccional o Antena de panel
Cable coaxial N macho – N macho – x metros
Caja o Tablero metálico + plancha para equipos en torre CRN 600 x 400 x 200
Caja metálica + plancha para equipos en caseta CRN 800 x 600 x 200
Caja metálica para batería en torre 600 x 400 x 250
Protector de línea 5.8 Ghz (1/4 onda) (N Macho –hembra)
Case para placa Mikrotik – Alix
Placa Mikrotik RB 433AH
Tarjeta Inalámbrica Mikrotik R52Hn
Pigtail MMCX – N Hembra
Alimentación 12v – batería – borneras

Tabla 5: Equipamiento del Sistema de Telecomunicación

4.3.1.1.2. Sistema de Infraestructura de los Repetidores Troncales

La infraestructura de un repetidor troncal está constituida básicamente por una torre ventada y una caja para albergar equipos.

En la red de telecomunicaciones del proyecto GTR – IEEE se han construido solamente dos torres ventadas en las localidades de San Gabriel de Varadero y en San Juan del Armanayacu. El tipo de tramo de torre y accesorios es del tipo (B), este tipo de tramo respeta la medida estándar de 3 m. y están preparadas para soportar condiciones ambientales extremas.

En Balsapuerto y Yurimaguas se han utilizado las torres existentes, las cuales fueron construidas anteriormente para la realización de otros proyectos.

Para tener una idea clara del equipamiento de telecomunicaciones instalado en la torre de cada repetidor troncal, detallamos a continuación los esquemas de conexión correspondientes a los cuatro repetidores troncales. La *Ilustración 11* describe el Repetidor Troncal de Balsapuerto.

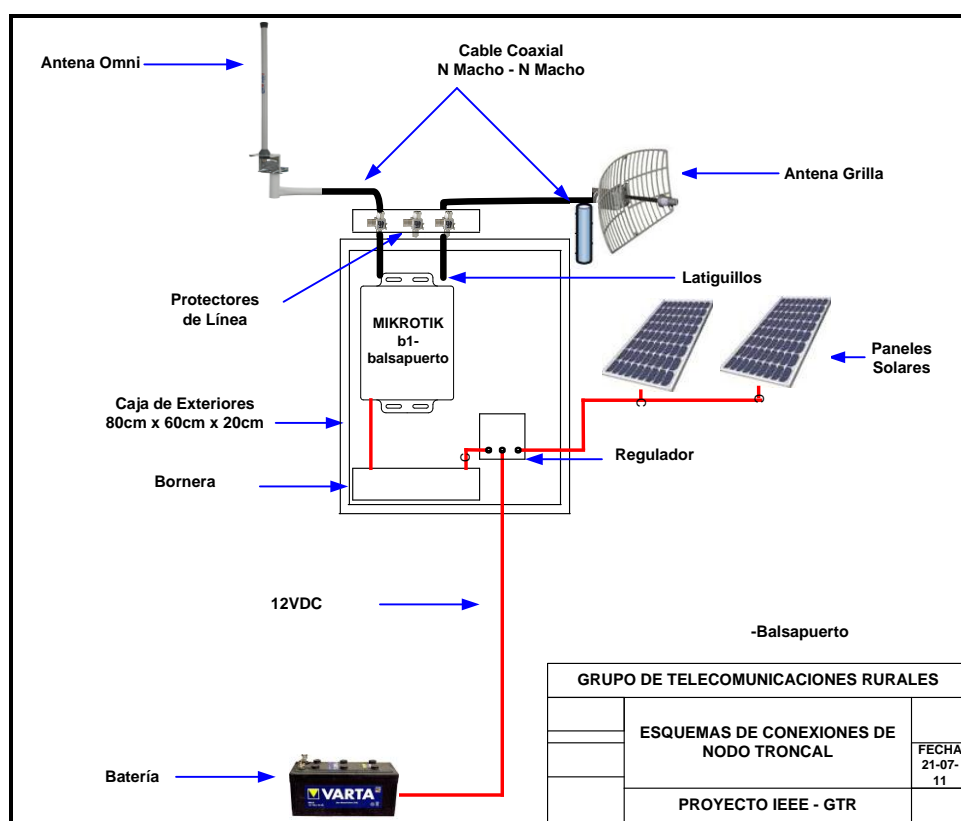


Ilustración 11: Esquema de conexiones – Repetidor Troncal Balsapuerto

En Balsapuerto se tiene un repetidor troncal (altura de la torre de 42 metros), el cual se comunica con otro repetidor troncal ubicado en San Gabriel de Varadero (altura de la torre de 60 metros) a través de un enlace troncal empleando un sistema SISO 1x1.

Se decidió la utilización de un sistema SISO 1x1 para este enlace inalámbrico debido a que este enlace se diseñó como piloto (fue el primero en implementarse). Este enlace nos ha permitido comparar sus prestaciones frente a los implementados con sistemas MIMO.

a) Características del enlace (troncal) inalámbrico que comunica San Gabriel de Varadero y Balsapuerto:

- ✓ Es un enlace inalámbrico IEEE802.11n punto a punto de largas distancias empleando un sistema SISO 1x1.
- ✓ La distancia del enlace es de 21,26 Km.
- ✓ Ambos repetidores troncales utilizan antenas Grilla de 27 dBi en la banda de 5.8 GHz, con polarización vertical.
- ✓ Respetar las regulaciones existentes.

Para el caso de la red de distribución local en este nodo, se utiliza una antena omnidireccional instalada en la torre de comunicaciones del Repetidor Troncal de Balsapuerto, la cual permite comunicar a dos clientes (centro de salud y una de las sedes de la Municipalidad del distrito) a través de un enlace punto a multipunto. Ambos clientes utilizan antenas panel de 17 dBi de ganancia. La **Ilustración 12: Red de distribución local – Repetidor Troncal Balsapuerto** describe la red de distribución local:

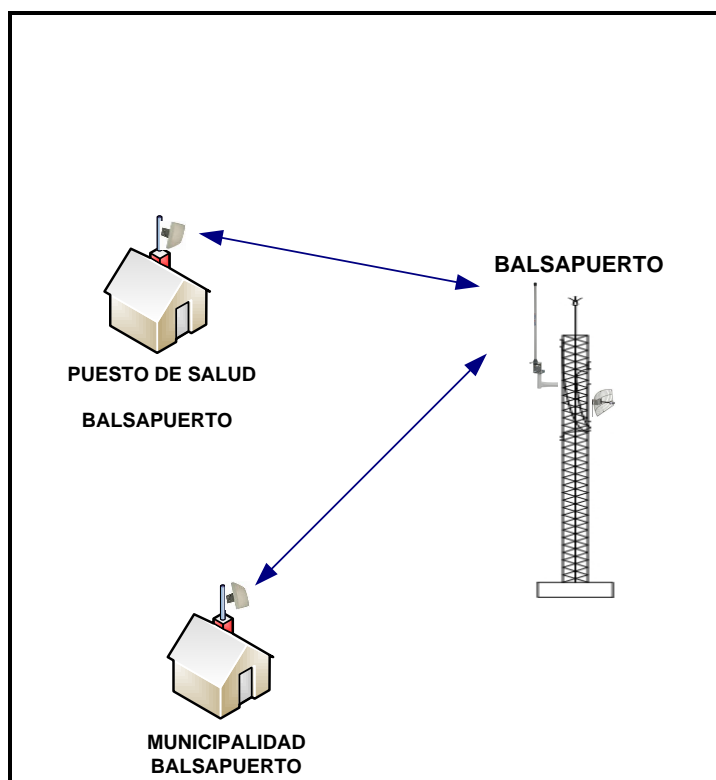


Ilustración 12: Red de distribución local – Repetidor Troncal Balsapuerto

El Repetidor Troncal de San Gabriel de Varadero (altura de la torre de 60 metros), descrito en la **Ilustración 13**, se comunica con el Repetidor Troncal de Balsapuerto tal como hemos comentado anteriormente.

También se comunica con el Repetidor Troncal ubicado en San Juan del Armanayacu (altura de la torre de 60 metros) a través de un enlace troncal empleando un sistema MIMO 2x2 con diversidad de polarización.

La utilización de este sistema se justifica en los valores superiores de throughput de datos obtenidos en un enlace inalámbrico de prueba de largas distancias, realizado en la ciudad de Lima, utilizando dos repetidores con la misma tecnología (MIMO 2x2) y empleando el mismo equipamiento que se ha utilizado en la red de telecomunicaciones del proyecto GTR – IEEE.

b) Características del enlace (troncal) inalámbrico que comunica San Gabriel de Varadero y San Juan del Armanayacu:

- ✓ Es un enlace inalámbrico IEEE802.11n punto a punto de largas distancias empleando un sistema MIMO 2x2 con diversidad de polarización.
- ✓ La distancia del enlace es de 19,47 Km.
- ✓ Ambos repetidores troncales utilizan antenas de Doble Polaridad de 29 dBi en la banda de 5.8 GHz.
- ✓ Respeta las regulaciones existentes.

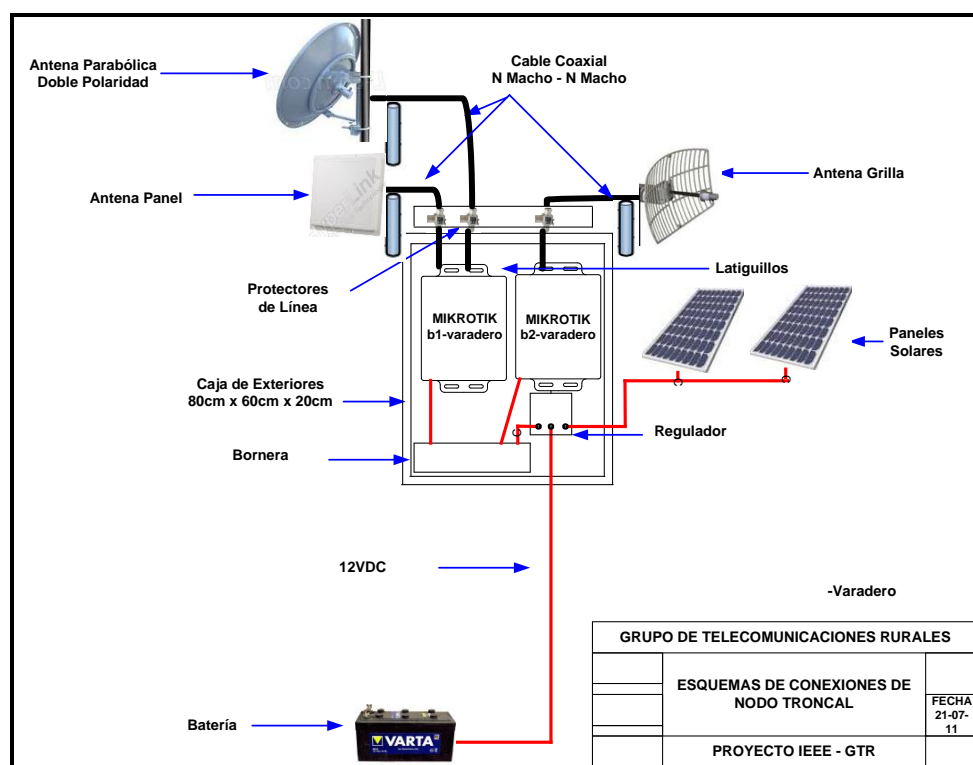


Ilustración 13: Esquema de conexiones – Repetidor Troncal Varadero

Para caso de la red de distribución local en este nodo, se utiliza una antena de panel instalada en la torre de comunicaciones del Repetidor Troncal de San Gabriel de Varadero, la cual permite comunicar un único cliente (puesto de salud).

En el futuro, se pretende comunicar también el colegio de la comunidad y otros posibles clientes para lo cual se decidirá utilizar apropiadamente una antena omnidireccional o sectorial según convenga, logrando distribuir la señal óptimamente a todos los clientes.

El Repetidor Troncal de San Juan del Armanayacu (altura de la torre de 60 metros), descrito en la *Ilustración 14*, se comunica con el Repetidor Troncal de Varadero tal como hemos comentado anteriormente. Además se comunica con el Repetidor Troncal ubicado en el Hospital Santa Gema de Yurimaguas (altura de la torre de 42 metros) a través de un enlace troncal empleando un sistema MIMO 2x2 con diversidad de polarización.

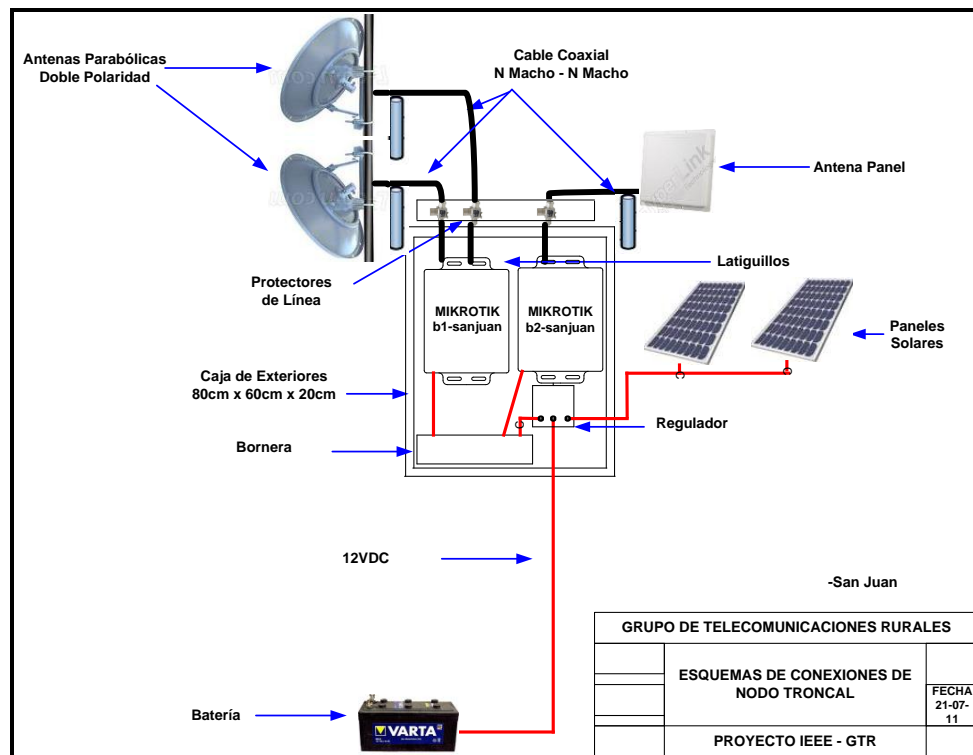


Ilustración 14: Esquema de conexiones – Repetidor Troncal San Juan

c) Características del enlace (troncal) inalámbrico que comunica San Juan del Armanayacu y el Hospital Santa Gema de Yurimaguas:

- ✓ Es un enlace inalámbrico IEEE802.11n punto a punto de largas distancias empleando un sistema MIMO 2x2 con diversidad de polarización.
- ✓ La distancia del enlace es de 28 Km.

- ✓ Ambos repetidores troncales utilizan antenas de Doble Polaridad de 29 dBi en la banda de 5.8 GHz.
- ✓ El enlace respeta las regulaciones existentes: el enlace cubre zonas urbanas, y no debe sobrepasar el PIRE de 36 dBm en cada nodo. La potencia de transmisión de la tarjeta inalámbrica está configurada a un valor menor al máximo permitido (< 30 dBm). Y el PIRE de cada antena será inferior al máximo permisible por radiaciones ionizantes (< 60.9 dBm).

Para caso de la red de distribución local en este nodo, se utiliza una antena de panel instalada en la torre de comunicaciones del Repetidor Troncal de San Juan del Armanayacu, la cual permite comunicar un único cliente (puesto de salud).

Al igual que en el enlace anterior, en el futuro se pretende comunicar otros posibles clientes considerando el uso de las antenas más apropiadas.

Finalmente, el Repetidor Troncal ubicado en el Hospital Santa Gema de Yurimaguas (altura de la torre de 42 metros), descrito en la *Ilustración 15*, se comunica con el Repetidor Troncal ubicado en San Juan del Armanayacu (altura de la torre de 60 metros) a través de un enlace troncal empleando un sistema MIMO 2x2 con diversidad de polarización.

Para el caso de la red de distribución local en este nodo, se utiliza una antena omnidireccional instalada en la torre de comunicaciones del Repetidor Troncal del Hospital Santa Gema, de igual forma que en la torre de Balsapuerto. Esta antena permite comunicar a dos clientes (Red de salud y una de las sedes de la Municipalidad del distrito) a través de un enlace punto a multipunto. Ambos clientes utilizan antenas panel de 17 dBi de ganancia.

Además, se ha implementado una conexión (utilizando cable UTP para exteriores y un switch) desde la torre de comunicaciones de este Repetidor, hasta el local ubicado en la sala de emergencias del Hospital y en la sala de conferencias del Hospital. La *Ilustración 16* e *Ilustración 17* describen la red de distribución local.

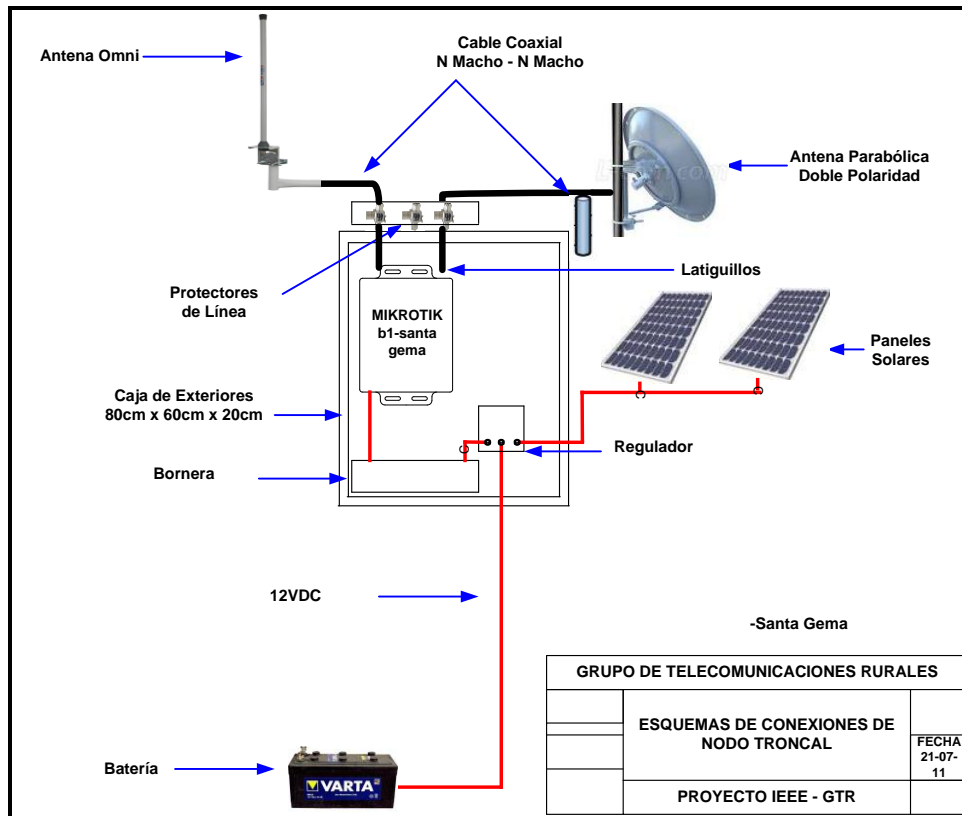


Ilustración 15: Esquema de conexiones – Repetidor Troncal Santa Gema

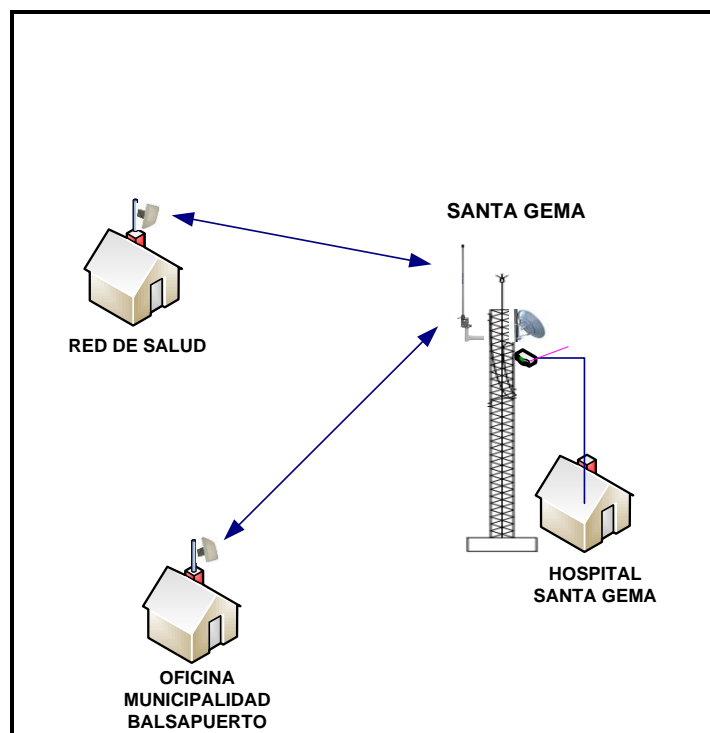


Ilustración 16: Red de distribución local – Repetidor Troncal Santa Gema

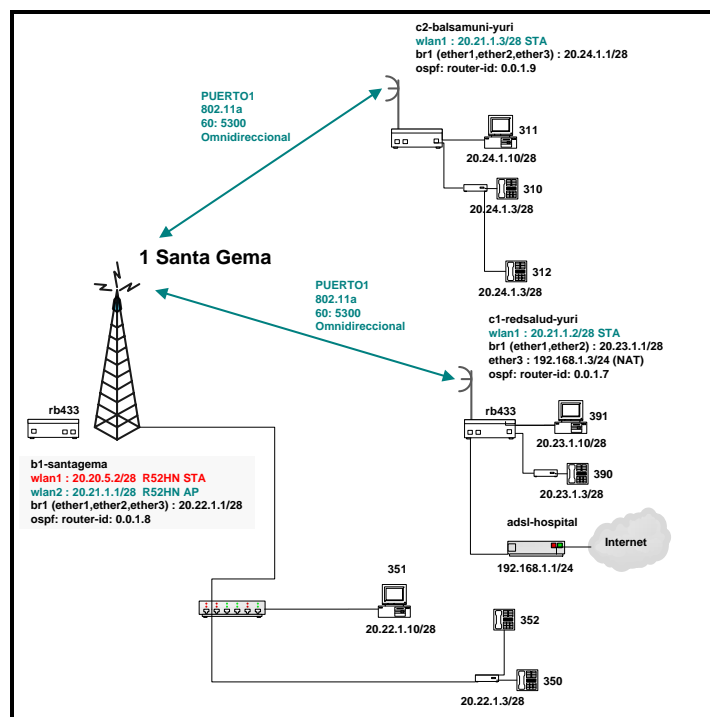


Ilustración 17: Red de distribución local – Repetidor Troncal Santa Gema (II)

4.3.1.1.3. Sistema de Energía de los Repetidores Troncales

En los repetidores troncales antes mencionados se empleó la energía suministrada por un sistema fotovoltaico. Este sistema está dimensionado para alimentar las placas Mikrotik RB 433AH las 24 horas del día con una autonomía de 3 días. El sistema fotovoltaico está constituido por los siguientes componentes:

Descripción de equipos del Sistema de Energía
Panel solar de 85 Wp – Marca SOLAR WORLD
Batería de 12 VDC – 100 A/h – Marca RITAR
Regulador fotovoltaico de 20 A – Marca STECA

Tabla 6: Equipamiento del Sistema de Energía de los Repetidores Troncales

4.3.1.1.4. Sistema de Protección Eléctrica de los Repetidores Troncales

El sistema de protección eléctrica consta de un sistema pararrayos montado en la torre de comunicaciones y está compuesta de los siguientes elementos:

- ✓ Tetrapuntal con base aislada

- ✓ Cable de cobre desnudo desde la cima de la torre hasta el fleje del pozo de tierra horizontal
- ✓ Brazos aisladores para la bajada del cable de cobre

El sistema de Energía está compuesto también por un pozo a tierra horizontal con fleje de 20 metros de longitud y una barra de cobre, ubicada en la caseta, para las conexiones de puesta a tierra de los equipos.

4.3.1.2. Red de Distribución Local

La red de distribución local se compone de dos partes:

- a) Repetidores Locales de Distribución
- b) Estaciones finales o clientes

En la *Tabla 7* se clasifica los clientes por repetidor local de distribución: (los clientes son dotados de servicios de telefonía y acceso a Internet)

ITEM	UBICACIÓN	TIPO
1	YURIMAGUAS	
1.1	Hospital Santa Gema	Repetidor local
1.2	Hospital	Cliente
1.3	Red de Salud	Cliente
1.3	Municipalidad de Balsapuerto	Cliente
2	SAN JUAN	
2.1	San Juan del Armanayacu	Repetidor local
2.2	Puesto de Salud	Cliente
3	VARADERO	
3.1	San Gabriel de Varadero	Repetidor local
3.2	Puesto de Salud	Cliente
4	BALSAPUERTO	
4.1	Balsapuerto	Repetidor local
4.2	Centro de Salud	Cliente
4.3	Municipalidad de Balsapuerto	Cliente

Tabla 7: *Cientes por repetidor local de distribución*

4.3.1.2.1. Repetidores Locales de Distribución

Como se ha comentado anteriormente, los repetidores troncales identificados anteriormente son además repetidores locales de distribución. Esto es debido a que estos cuatro repetidores

se encargan de repetir la señal que viaja a través de la red troncal y además distribuyen la señal a sus clientes finales.

Estos repetidores locales de distribución utilizan antenas omnidireccionales ó panel para comunicar a sus clientes finales.

Como se ha comentado anteriormente, los repetidores ubicados en Santa Gema y Balsapuerto, utilizan antenas omnidireccionales para establecer enlaces punto a multipunto con sus clientes finales, ubicados a una distancia de menos de 1 Km.

En el caso de los repetidores ubicados en Varadero y San Juan se utilizan antenas panel para establecer enlaces punto a punto con un único cliente final. Estos clientes finales son los centros o puestos de salud y las entidades municipales de los distritos beneficiarios.

En la *Ilustración 12: Red de distribución local – Repetidor Troncal Balsapuerto*, *Ilustración 16*, *Ilustración 17* y las correspondientes a los repetidores troncales, se observa las redes de distribución local de cada repetidor. También se explica sus enlaces inalámbricos de distribución.

Por lo tanto, los sistemas de telecomunicaciones, infraestructura, energía y protección eléctrica de los Repetidores Locales de Distribución son los mismos que hemos descrito anteriormente para el caso de los Repetidores Troncales.

4.3.1.2.2. Estaciones Finales o clientes

En este apartado se describen los sistemas de telecomunicaciones, infraestructura, energía y protección eléctrica pertenecientes a las estaciones finales o clientes.

4.3.1.2.2.1. Sistema de Telecomunicaciones de las Estaciones Finales

En la *Tabla 8: Equipamiento del Sistema de Telecomunicación* se especifican los equipos que conforman el sistema de telecomunicaciones, cada estación final dispone del equipamiento descrito a continuación. Los elementos principales son:

- ✓ Router Mikrotik modelo RB 433
- ✓ Router Mikrotik modelo RB 333
- ✓ Placa embebida modelo ALIX2D2 (servidor Asterisk)
- ✓ Tarjeta inalámbrica Mikrotik modelo R52Hn
- ✓ Tarjeta inalámbrica Mikrotik modelo R5H
- ✓ Antena panel

Descripción de equipos del Sistema de Telecomunicación
Antena Panel 5.8 Ghz 19 dbi (HG5819P) – Hyperlink
Cable coaxial N macho – N macho – X metros
Caja o Tablero metálico + plancha para equipos en torre CRN 600 x 400 x 200
Caja metálica + plancha para equipos en caseta CRN 800 x 600 x 200
Protector de línea 5.8 Ghz (1/4 onda) (N Macho –hembra)
Case para placa Mikrotik – Alix
Placa Mikrotik RB 433
Placa Mikrotik RB 333
Placa embebida ALIX2D2 para servidor Asterisk – PC Engines
Tarjeta Inalámbrica Mikrotik R52Hn
Tarjeta Inalámbrica Mikrotik R5H
Pigtail MMCX – N Hembra
Alimentación 12v – baterías – borneras
Fuente de Alimentación sobre Ethernet (PoE) - Ubiquiti
ATA Grandstream HT502 + cable de red
Teléfono Panasonic KX-TS500
MEMORIA CF de 2 GB
Computadora + Cámara Web

Tabla 8: Equipamiento del Sistema de Telecomunicación

4.3.1.2.2.2. Sistema de Infraestructura de las Estaciones Finales

La infraestructura de las estaciones finales está constituida básicamente por un ambiente adecuado en la institución beneficiaria.

Para tener una idea clara del equipamiento de telecomunicaciones y de infraestructura instalado en cada estación final, se describen a continuación los esquemas de conexión correspondientes a las cuatro estaciones finales; los cuales se detallan en la *Ilustración 18: esquema de conexión de una estación final con sistema fotovoltaico – Centro de Salud de Balsapuerto*, *Ilustración 19: Esquema de conexión de una estación final con sistema fotovoltaico – Puesto de Salud de Varadero*, *Ilustración 20: Esquema de conexión de una estación final con energía convencional – Municipalidad de Balsapuerto* e *Ilustración 21: Esquema de conexión de una estación final con energía convencional – Red de Salud de Yurimaguas*.

Tal como se observa en los esquemas de conexión, en los clientes finales se instalan antenas panel apuntadas convenientemente a la antena del repetidor local de distribución ubicada en la torre de comunicaciones.

La forma como se ha acondicionado la instalación de la antena panel ha sido en el tejado sin necesidad de la utilización de un mástil, esto es debido a la experiencia previa que se ha tenido instalando este tipo de redes en la selva amazónica.

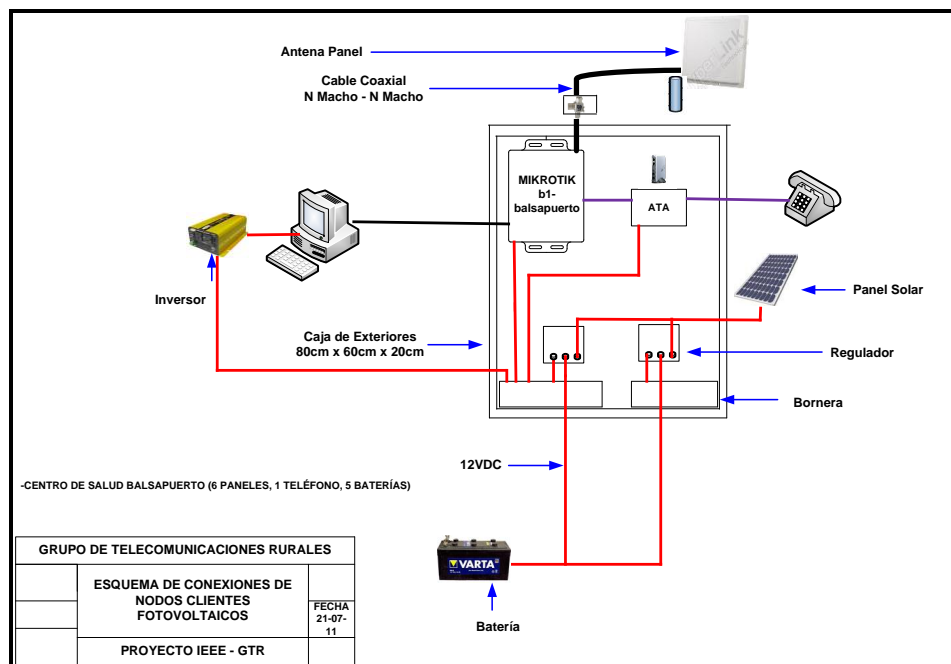


Ilustración 18: esquema de conexión de una estación final con sistema fotovoltaico – Centro de Salud de Balsapuerto

El esquema de conexión de la estación final del Centro de Salud de Balsapuerto es igual al implementado en el Puesto de Salud de San Juan.

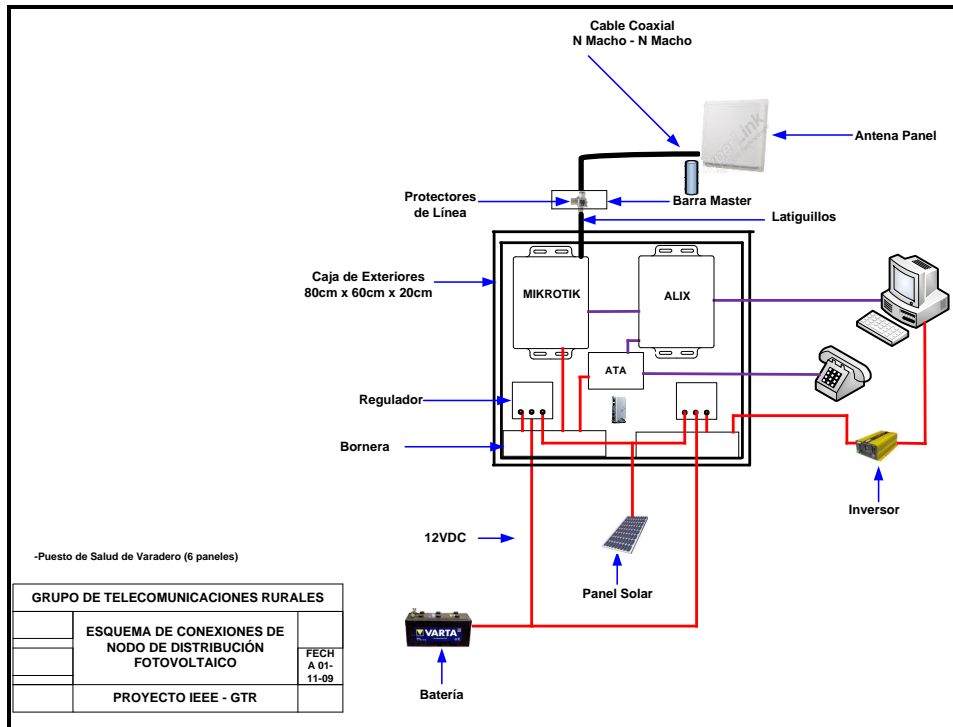


Ilustración 19: Esquema de conexión de una estación final con sistema fotovoltaico – Puesto de Salud de Varadero

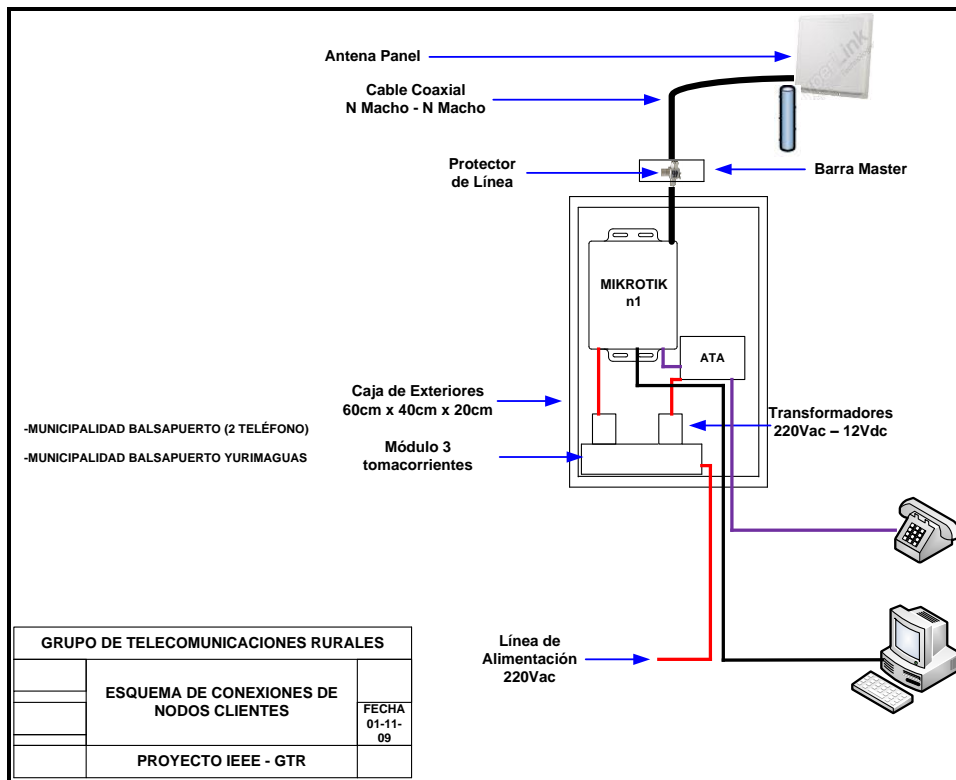


Ilustración 20: Esquema de conexión de una estación final con energía convencional – **Municipalidad de Balsapuerto**

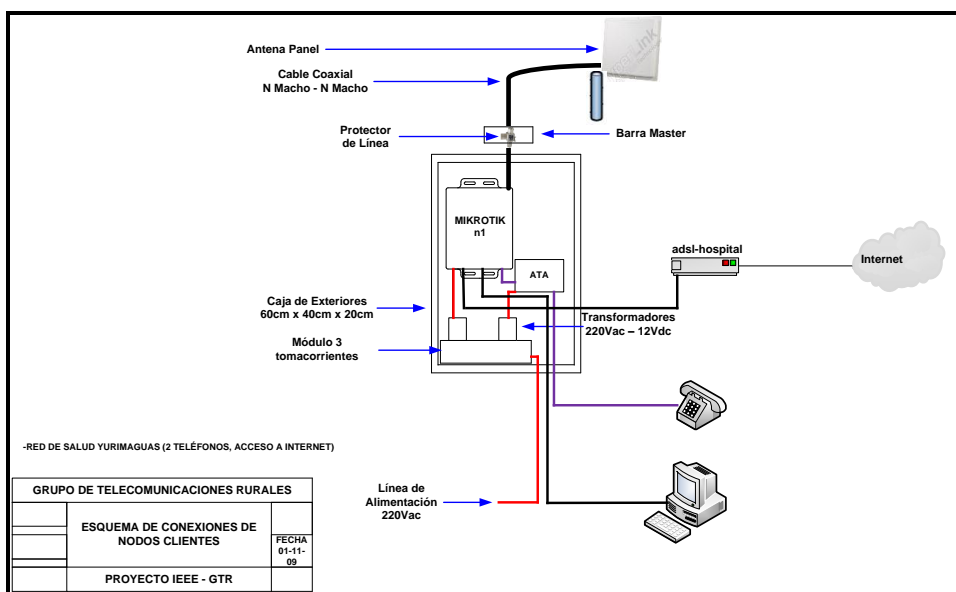


Ilustración 21: Esquema de conexión de una estación final con energía convencional – **Red de Salud de Yurimaguas**

Cada estación final está compuesta de un equipo de videoconferencia y su teléfono, estos equipos se conectan a una caja metálica que alberga las placas Mikrotik, la placa Alix, el ATA, los reguladores de corriente, borneras, etc.

La energía se obtiene a través de un sistema fotovoltaico constituido por paneles solares ubicados en el tejado que recargan el sistema utilizando baterías de 12V y un regulador. El ordenador o portátil se conecta a un inversor, el cual convierte la energía eléctrica continua (obtenida del sistema fotovoltaico) en alterna para permitir la alimentación de este equipo.

En el esquema de conexión de la estación final de la Red de Salud, descrita en la *Ilustración 21: Esquema de conexión de una estación final con energía convencional – Red de Salud de Yurimaguas*, se puede observar que este cliente se conecta al ADSL de Telefónica para salir a Internet. Además la configuración realizada permite que todos los nodos tengan salida a Internet a través de este cliente.

4.3.1.2.2.3. Sistema de Energía de las Estaciones Finales

Las estaciones finales ubicadas en la ciudad de Yurimaguas emplean la red eléctrica convencional para su funcionamiento.

La cantidad de paneles solares del sistema fotovoltaico varía según el diseño. El sistema fotovoltaico se diseña teniendo en cuenta su uso estimado en horas diarias y la autonomía de este sistema. La autonomía son los días que el sistema puede continuar funcionando, sin que exista generación de energía proveniente de los paneles solares, esto es debido a la acumulación de energía necesaria en las baterías.

En las estaciones finales restantes, San Juan del Armanayacu, San Gabriel de Varadero y Balsapuerto, se emplean sistemas fotovoltaicos para suministrar energía. Como hemos explicado anteriormente, estos sistemas están formados por paneles solares, baterías y reguladores fotovoltaicos.

A continuación se describe el uso y la autonomía de los tres sistemas fotovoltaicos empleados. Estos sistemas se utilizan en las tres estaciones finales antes mencionadas:

- a) **Sistema fotovoltaico para la alimentación de la placa MikroTik, la placa Alix de la estación final de Varadero y el ATA:** Este sistema se dimensiona con un panel, una batería y comparte un regulador de 20 A con el segundo sistema fotovoltaico, permitiendo un uso del sistema por 24 horas al día, y una autonomía de tres días.

- b) **Sistema fotovoltaico para la alimentación de una computadora:** Este sistema se dimensiona con dos paneles, una batería y comparte un regulador de 20 A con el primer sistema fotovoltaico, permitiendo un uso del sistema por 6 horas al día, y una autonomía de un día.
- c) **Sistema fotovoltaico para la alimentación de una computadora y dos luminarias:** Este sistema se dimensiona con cuatro paneles, cuatro baterías en un arreglo en paralelo, y un regulador de 30 A, permitiendo un uso del sistema por 24 horas al día, y una autonomía de tres días.

La *Tabla 9* describe el equipamiento del sistema de energía de las estaciones finales:

Descripción de equipos del Sistema de Energía
Panel solar de 85 Wp – Marca SOLAR WORLD
Batería de 12 VDC – 100 A/h – Marca RITAR
Regulador fotovoltaico de 20 A – Marca STECA
Regulador fotovoltaico de 30 A – Marca STECA

Tabla 9: Equipamiento del Sistema de Energía de las Estaciones Finales

4.3.1.2.2.4. Sistema de Protección Eléctrica de las Estaciones Finales

En el caso de las estaciones finales, todos cuentan con un pozo a tierra vertical, también una varilla de cobre de 2.4 metros enterrada con gel electrolítico, y una barra de cobre para las conexiones de puesta a tierra de los equipos.

En las siguientes ilustraciones se observa los sistemas de la red descritos anteriormente: en la *Ilustración 22* se observa la antena parabólica operando en la banda 5.8 GHz, consistente en dos antenas con diversidad de polarización para transmisión y recepción. Los enlaces 802.11n con sistemas MIMO 2x2 se implementan con este tipo de antenas en ambos repetidores del enlace troncal.

También se puede observar el panel solar que suministrará energía al sistema de telecomunicaciones del repetidor troncal.

En la *Ilustración 23* se observa el enrutador MikroTik ‘*RB 433*’ y la tarjeta inalámbrica ‘*RB R52Hn*’, se observa también, el conexionado y la configuración típica para un sistema de telecomunicación correspondiente a una estación final.



Ilustración 22: Fotografía Antena Parabólica 5.8 GHz



Ilustración 23: Placa MikroTik RB 433 y Tarjeta Inalámbrica R52Hn

En la *Ilustración 24: Fotografía de los enlaces Balsapuerto y Varadero* e *Ilustración 25: Fotografía de los enlaces Balsapuerto y Varadero*, se observan las fotografías con las torres de comunicaciones de los repetidores troncales de Varadero y Balsapuerto.

Las fotografías (de la izquierda) correspondientes a ambas ilustraciones, se corresponden a la torre de comunicaciones de Varadero, el cual es un repetidor troncal. Se observa que este se comunica con Balsapuerto utilizando una antena parabólica (MIMO 2x2) y además, se comunica con Varadero utilizando una antena de grilla (SISO 1x1).

En las fotografías se puede observar las cajas para equipos y en la fotografía de la *Ilustración 25: Fotografía de los enlaces Balsapuerto y Varadero* (derecha), se observa la caja para batería en la torre.

Por lo tanto, en las cuatro fotografías se puede observar los sistemas de: telecomunicación, infraestructura, energía y de protección eléctrica, correspondiente a los repetidores troncales de ambos nodos.

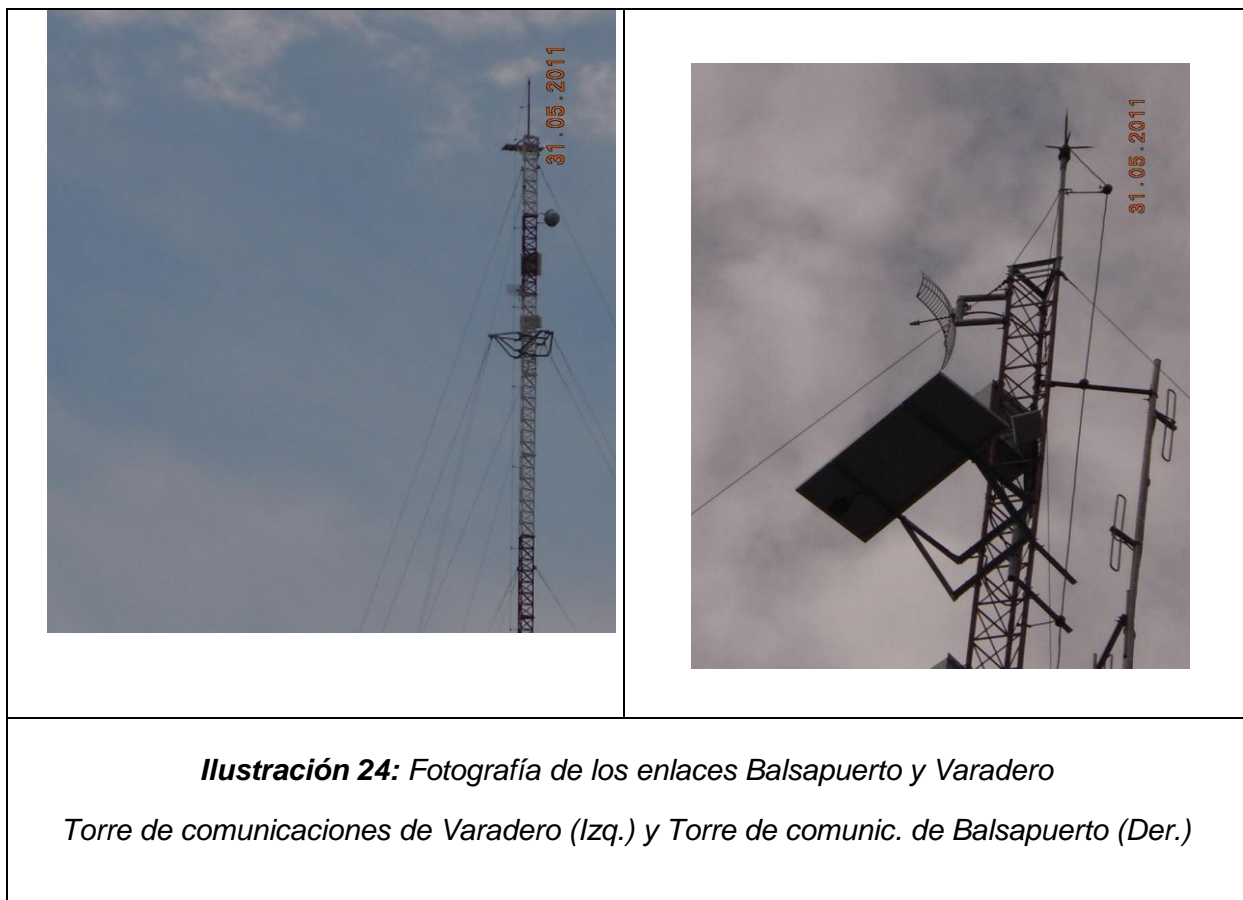










Ilustración 25: Fotografía de los enlaces Balsapuerto y Varadero

Torre de comunicaciones de Varadero (Izq.) y Torre de comunic. de Balsapuerto (Der.)

4.3.2. Equipos utilizados y especificaciones técnicas

En este apartado se describen los equipos utilizados, sus especificaciones técnicas y para qué fueron instalados en el presente proyecto.

 <p>Placa Mikrotik RB 433</p>	<p>Router empleado en las estaciones finales.</p> <ul style="list-style-type: none"> - CPU Atheros AR7130 300MHz - Memoria de 64/128MB DDR SDRAM - 64MB Almacenamiento de datos en tarjeta, chip de memoria NAND y microSD - Tres puertos Ethernet 10/100 Mbit/s con Auto-MDI/X - Tres slots MiniPCI Tipo IIIA/IIIB - Consumo de potencia ~3W sin tarjetas, máximo – 25 W POE 10..28V DC, 16W de salida a tarjetas - Sistema Operativo MikroTik RouterOS v3, Licencia nivel 5
 <p>Placa Mikrotik RB 433AH</p>	<p>Router empleado en los repetidores troncales, repetidores locales.</p> <ul style="list-style-type: none"> - CPU Atheros AR7161 680MHz - Memoria de 128MB DDR SDRAM - 128MB Almacenamiento de datos en tarjeta, chip de memoria NAND y microSD - Tres puertos Ethernet 10/100 Mbit/s con Auto-MDI/X - Tres slots MiniPCI Tipo IIIA/IIIB - Consumo de potencia ~3W sin tarjetas, máximo – 25 W POE 10..28V DC, 16W de salida a tarjetas - Sistema Operativo MikroTik RouterOS v3, Licencia nivel 5

 <p>Placa Mikrotik RB 333</p>	<p>Router empleado en la Red de Salud en Yurimaguas</p> <ul style="list-style-type: none"> - CPU MPC8231 333MHz - Memoria de 64 DDR SDRAM - 64MB Almacenamiento de datos en tarjeta, chip de memoria NAND - Tres puertos Ethernet 10/100 Mbit/s con Auto-MDI/X - Tres slots MiniPCI Tipo IIIA/IIIB - Consumo de potencia ~3W sin tarjetas, máximo – 25 W POE 10..28V DC, 16W de salida a tarjetas - Sistema Operativo MikroTik RouterOS v3, Licencia nivel 5
 <p>Placa ALIX 2D2</p>	<p>Computadora embebida empleada en una de las estaciones finales como servidor de telefonía.</p> <ul style="list-style-type: none"> - CPU 500 MHz AMD Geode LX800 - DRAM: 256MB DDR SDRAM - Socket para almacenamiento: CompactFlash - 2 puertos Ethernet - 2 slots MiniPCI slots - Conector para alimentación DC o POE, min. 7V a max. 20V - Puerto serial I/O: DB9, dual USB2.0
 <p>Memoria CF de 2GB</p>	<p>Memoria Compact Flash empleada como disco duro en las sistemas 'embedded' ALIX</p>
 <p>Tarjeta Inalámbrica R52Hn</p>	<p>Tarjeta inalámbrica empleada en los Routers Mikrotik</p> <ul style="list-style-type: none"> - 802.11 a, b, g,n - Operan en las bandas 2.4 y 5.8 Ghz. - Soporta Mikrotik Nstreme - Largas distancias y altas velocidades.

 <p>Antena Grilla 5.8GHz 27 dBi</p>	<p>Antena empleada en los repetidores troncales para enlaces con tecnología SISO</p> <ul style="list-style-type: none"> - Antena de Grilla de alta ganancia - Trabaja en la banda de 5.8GHz - Ganancia de la antena de 27 dBi
 <p>Antena Omnidireccional 12 dBi</p>	<p>Antena omnidireccional empleada en los repetidores locales para repartir la señal a las estaciones finales</p> <ul style="list-style-type: none"> - Trabaja en la banda de 5.8GHz - Ganancia de la antena de 12 dBi
 <p>Antena de Panel de 19 dBi</p>	<p>Antena de panel empleada en las estaciones finales</p> <ul style="list-style-type: none"> - Trabaja en la banda de 5.8GHz - Ganancia de la antena de 19 dBi
 <p>Protector de Línea 5.8 GHz</p>	<p>Protector de línea cuarto de onda – 5.8GHz – N hembra / N hembra</p> <ul style="list-style-type: none"> - Empleado en los repetidores troncales y locales para proteger los enrutadores inalámbricos contra las descargas eléctricas.
 <p>Protector de Línea 5.8 GHz</p>	<p>Protector de línea cuarto de onda – 5.8GHz – N Macho / N hembra</p> <ul style="list-style-type: none"> - Empleado en los repetidores troncales y locales para proteger los enrutadores inalámbricos contra las descargas eléctricas.

 <p>Pigtail MMCX – N Hembra</p>	<p>Cable coaxial tipo latiguillo</p> <ul style="list-style-type: none"> - Cable coaxial tipo latiguillo con extremos de conectores MMCX en un lado y N hembra en el otro lado. Por lo general miden 25 centímetros.
 <p>Cable Coaxial Heliax Super Flex</p>	<p>Cable coaxial de baja pérdida, se empleó en todas las conexiones de las antenas.</p> <ul style="list-style-type: none"> - Pérdida de 34 dB en 100 metros
 <p>ATA Grandstream HT502</p>	<p>Adaptador telefónico que se emplea en todos los puntos de instalación.</p> <ul style="list-style-type: none"> - 2 puertos FXS para 2 anexos - 1 puerto Ethernet.
 <p>Teléfono Panasonic KX-TS500</p>	<p>Teléfono analógico instalado en cada punto de la red GTR – IEEE de Telemedicina.</p>

 <p>Panel solar SOLAR WORLD</p>	<p>Panel solar</p> <ul style="list-style-type: none">- 85 Wp- Marca SOLAR WORLD
 <p>Controlador Solar STECA</p>	<p>Controlador Solar</p> <ul style="list-style-type: none">- Marca STECA- Modelo 20 Amperios- Modelo 30 Amperios
 <p>Batería RITAR</p>	<p>Batería de libre mantenimiento</p> <ul style="list-style-type: none">- Marca RITAR- 12 VDC – 100 A/h

4.4. Diseño de radioenlaces

En este documento, se describen los puntos generales que hay que tener en cuenta para el diseño de la red, ordenados por temas. Además se especifican los criterios de diseño y la justificación de mismos.

4.4.1. Estudio radioeléctrico

Previamente al diseño final, se realizó una visita a la zona, como hemos comentado al inicio de este capítulo. En esta visita se obtuvieron las coordenadas de todos los puntos a través de un GPS, se verificó la posibilidad de instalar torres en el terreno y se comprobaron las condiciones generales.

Con toda esta información y haciendo uso de las herramientas Radio Mobile y Google Earth se procedió a realizar el cálculo de los radioenlaces con Radio Mobile, Para lo cual se deben configurar los siguientes parámetros:

➤ Modo de Variabilidad

Hay cuatro opciones: Spot, Accidental, Mobile y Broadcast. Se escoge la opción Broadcast porque permite seleccionar porcentajes de tres opciones: tiempo, de localización y situación, los cuales son parámetros definidos por el modelo Longley-Rice.

Elevar los porcentajes de estos parámetros conlleva a aumentar las pérdidas añadidas al enlace. Para el presente diseño de la red de acceso de telecomunicación se escogió los valores:

- ✓ 60% del tiempo, 40% de localizaciones, 40% de situaciones.
- ✓ Clima: la opción que se ajusta a la zona de trabajo es “Ecuatorial”.

En la *Ilustración 26* se observa los parámetros de configuración para la red “San Juan – Santa Gema”, en la cual se coloca como frecuencia de operación el intervalo de 5725MHz – 5845 MHz; correspondiente a la banda de frecuencia de 5.8 GHz y admitida por el estándar 802.11n.

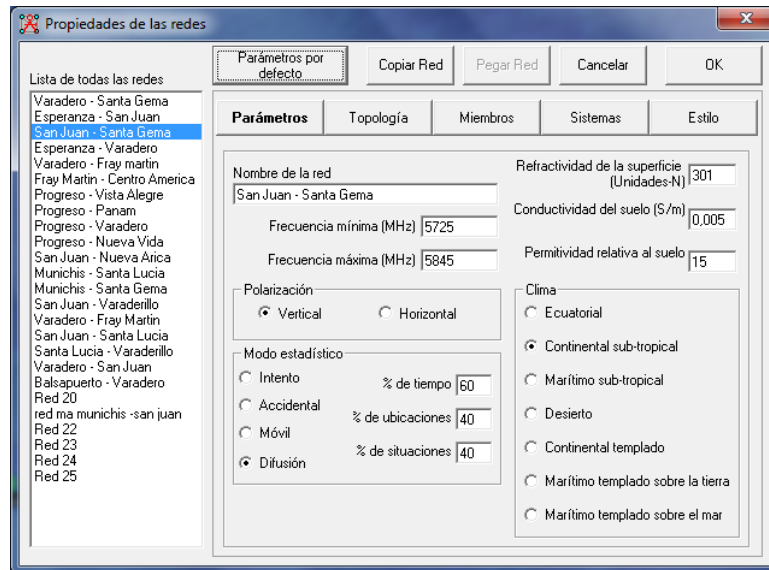


Ilustración 26: Parámetros de la configuración de las Redes

➤ **Selección de los miembros del enlace**

En la *Ilustración 27* incluimos a los miembros del enlace, configurando a la estación de Santa Gema como Maestro y la estación de San Juan como esclavo (topología estrella - “Master/Esclavo”).

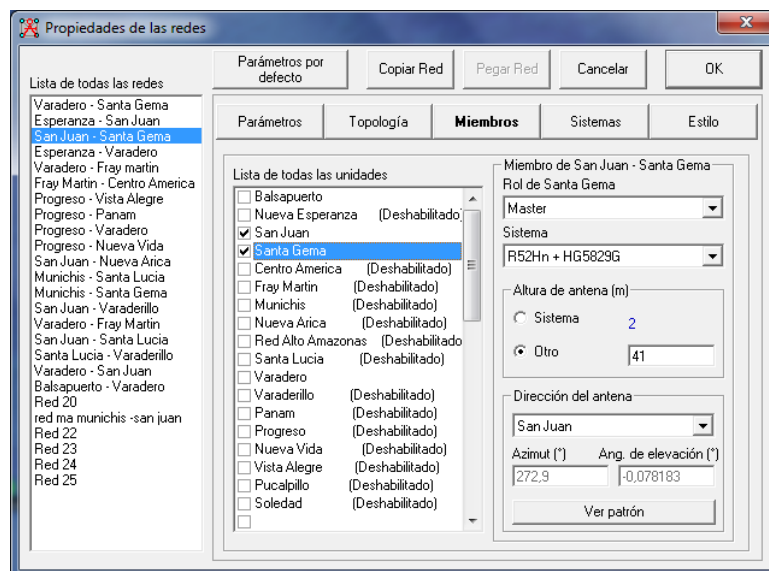


Ilustración 27: Parámetros de la configuración del nodo Santa Gema

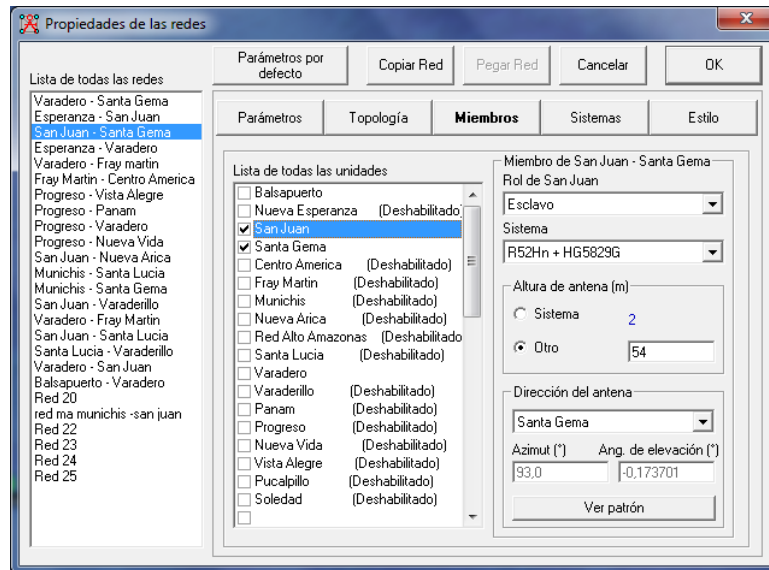


Ilustración 28: Parámetros de la configuración del nodo Santa Juan

➤ **Configuración de los sistemas en Radio Mobile**

Aquí se representan al conjunto de dispositivos de telecomunicaciones que funcionarán en las estaciones, incluyendo antenas y torres. Se ha creado un sistema correspondiente al enlace compuesto por la estación “Santa Gema” y la estación “San Juan”.

En el sistema se especifican los valores correspondientes a estos dispositivos para realizar el cálculo del presupuesto del enlace.

En la siguiente **Ilustración 29** observamos la ventana de configuración del sistema:

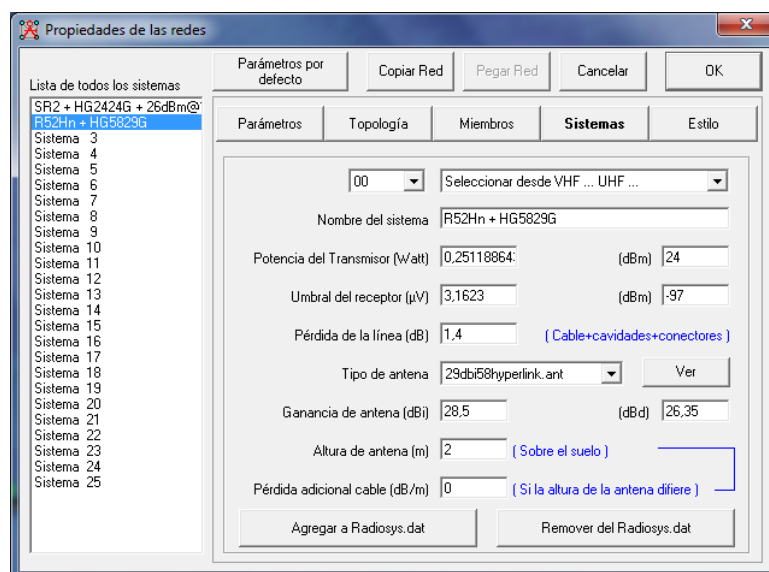


Ilustración 29: Configuración del sistema

En la *Ilustración 29*, se observa además, la configuración de nuestro sistema de acuerdo a las características de nuestros dispositivos de telecomunicación: la potencia de transmisión tiene un valor de 24 dBm, la pérdida de línea de transmisión es de 1,4 dB y la ganancia de la antena es de 28.5 dBi.

➤ **Perfil del enlace**

Se grafica el enlace en Radio Mobile y se recoge los parámetros relacionados con las características de propagación. Algunos de los resultados útiles para describir el enlace son: el margen relativo de señal recibida, azimut respecto del Norte, distancia entre ambos emplazamientos del enlace, sensibilidad de recepción, etc.

En la *Ilustración 30*, se observa la existencia de línea de vista entre los dos puntos (Santa Gema – San Juan), con una distancia de 28 km. El nivel de recepción captada es de -55.5 dBm, este valor es menor al obtenido en el cálculo del presupuesto enlace (-58.46 dBm), esto es debido a que el programa Radio Mobile considera las pérdidas que pueden aparecer por conceptos de la elección del clima, modo de variabilidad y tipo de área donde se desarrolla el enlace.

Son por estos motivos y para hacerle frente a las interferencias y multitrayecto que es preferible tener un margen superior a los 20 dB (margen obtenido = 41,5 dB) en el cálculo del presupuesto.

Por otro lado el valor del PIRE es de 128,82 W, Este PIRE ha sido utilizado para realizar un apuntamiento fino de la antena configurando la radio a su máxima potencia de transmisión. Posteriormente reducimos convenientemente este valor, consiguiendo un mayor throughput de datos, y logrando de esta forma el objetivo principal de este y de todos los enlaces troncales implementados en esta red.

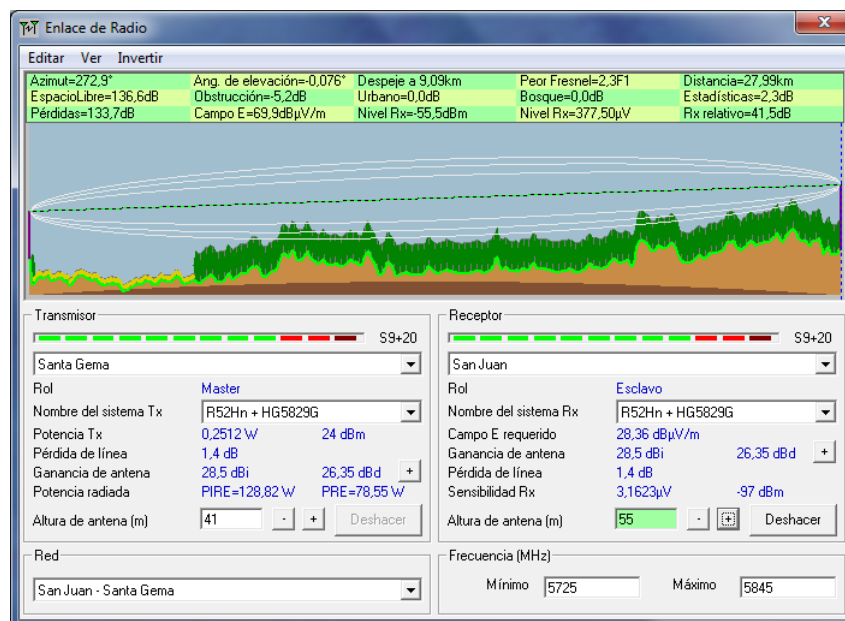


Ilustración 30: Perfil del enlace

Además considerando que la torre de Santa Gema tiene una altura de 41 metros, entonces en el programa Radio Mobile se coloca como dato este valor, y es a esta altura que se ha instalado la antena direccional (Parabólica de doble polaridad). De manera similar se ingresa el valor de 55 metros, como altura de la torre de San Juan.

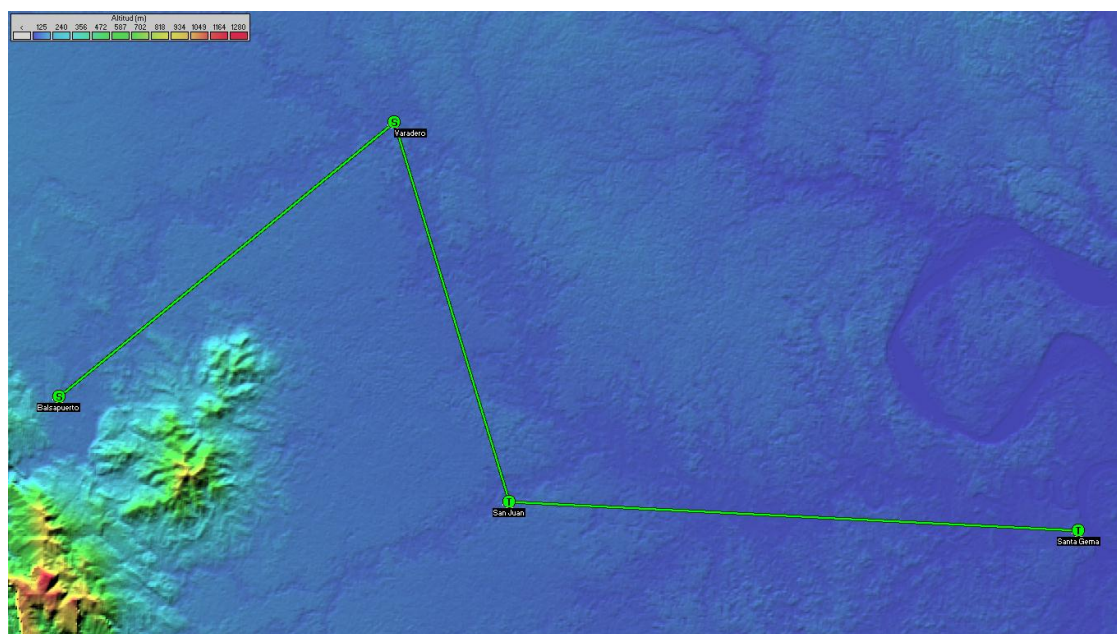


Ilustración 31: Mapa de Repetidores Troncales de la Red WiFi de Telemedicina de Balsapuerto

4.4.2. Resultados del diseño de Radioenlaces

En los resultados obtenidos en estos tres radioenlaces se observa la existencia de línea de vista, además se utilizó “*Landcover*” para simular una altura de árboles de aproximadamente 20 metros de altura y realizar una simulación más acorde con la realidad.

Con respecto al nivel de recepción captada en el receptor, este valor es ligeramente menor al obtenido en el presupuesto de potencia (especificado posteriormente en este capítulo), esto es debido a algunas pérdidas que considera este software.

El margen obtenido en los tres enlaces supera el valor de 38 dB, este es un valor muy conveniente para hacer frente a las interferencias y el multitrayecto.

En las siguientes ilustraciones, se muestra los resultados del diseño de los tres enlaces troncales de nuestra red:

1. Enlace: **Yurimaguas – San Juan del Armanayacu**

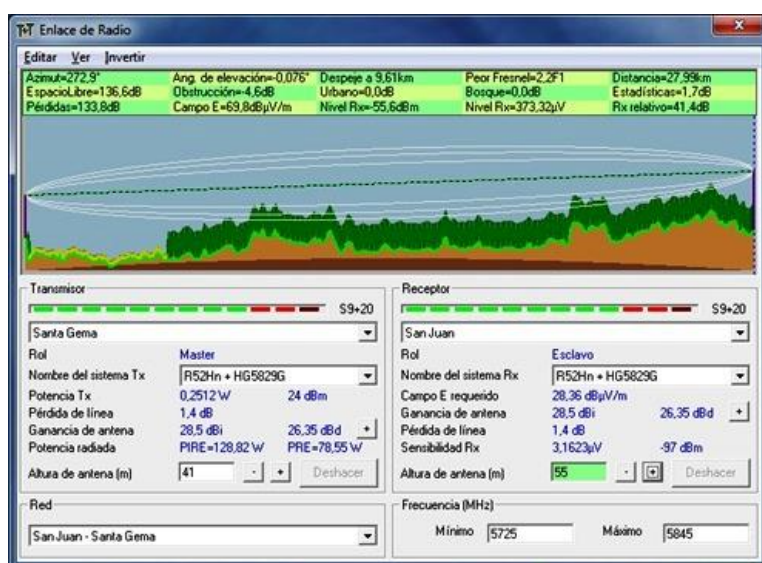


Ilustración 32: Perfil del radioenlace entre Santa Gema y San Juan

Resultados Radio Mobile	
Data Input / Output	1.0F1
San Juan	32.00m
Santa Gema	20.00m
Bosque	0.0dB
d1	19Km
% de tiempo	90%
% de situaciones	70%
Nivel RX	-66.4dBm
Cálculo de la Primera Zona de Fresnel	
d=	27.99Km
d1=	18.00Km
d2=	9.99Km
f=	5845.00Mhz
r1=	17.73m
0.6r1=	10.64m
Altura de los árboles	25.00m
Medida del Clearance	18.53m
Agregar	17.00m

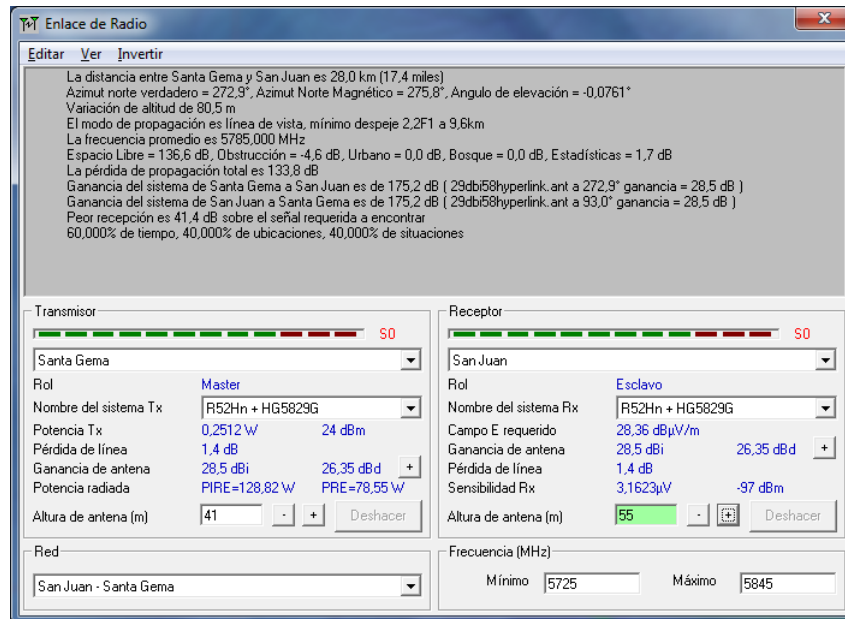


Ilustración 33: Detalles del radioenlace entre Santa Gema y San Juan

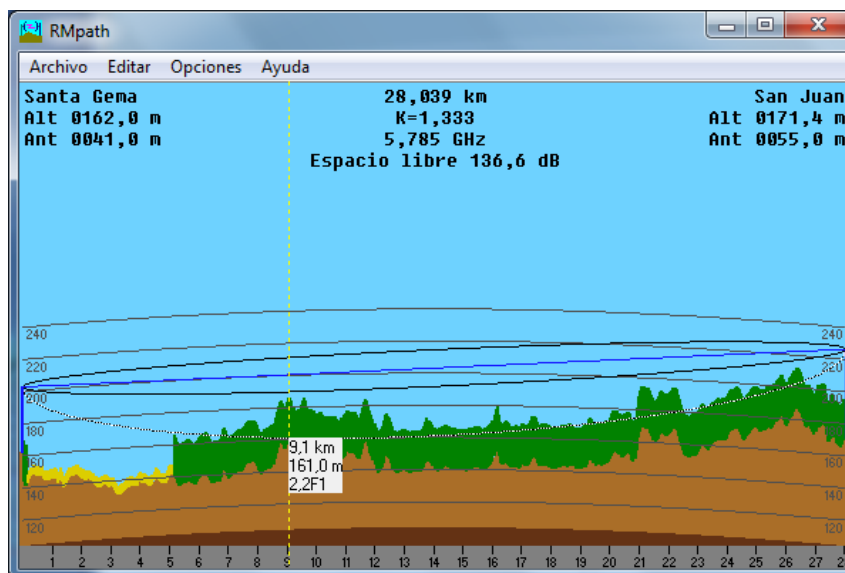


Ilustración 34: Resultados del radioenlace entre Santa Gema y San Juan

2. Enlace: **San Juan del Armanayacu – San Gabriel de Varadero**

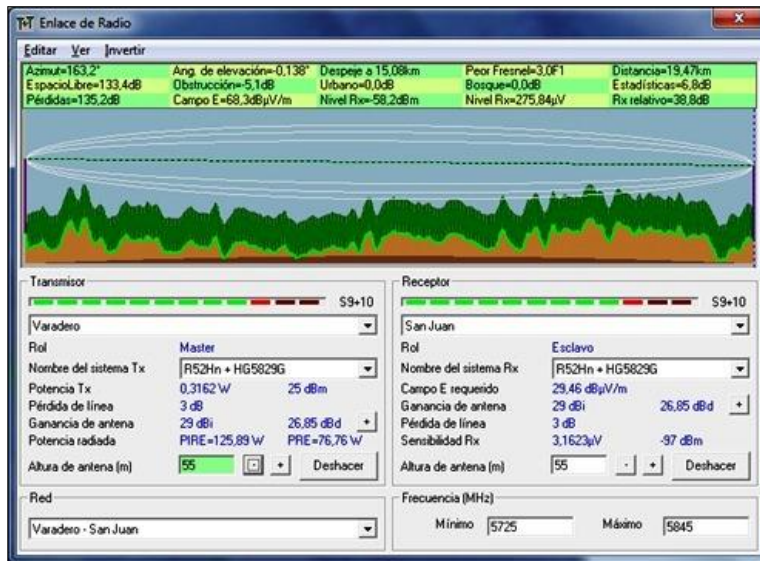


Ilustración 35: Perfil del radioenlace entre San Juan y Varadero

Resultados Radio Mobile	
Data Input / Output	1.0F1
Varadero	25.00m
San Juan	30.00m
Bosque	0.0dB
d1	10.35Km
% de tiempo	90%
% de situaciones	70%
Nivel RX	-64.9dBm
Cálculo de la Primera Zona de Fresnel	
d=	19.47Km
d1=	10.35Km
d2=	9.12Km
f=	5845.00Mhz
r1=	15.91m
0.6r1=	9.55m
Altura de los árboles	25.00m
Medida del Clearance	13.80m
Agregar	18.00m

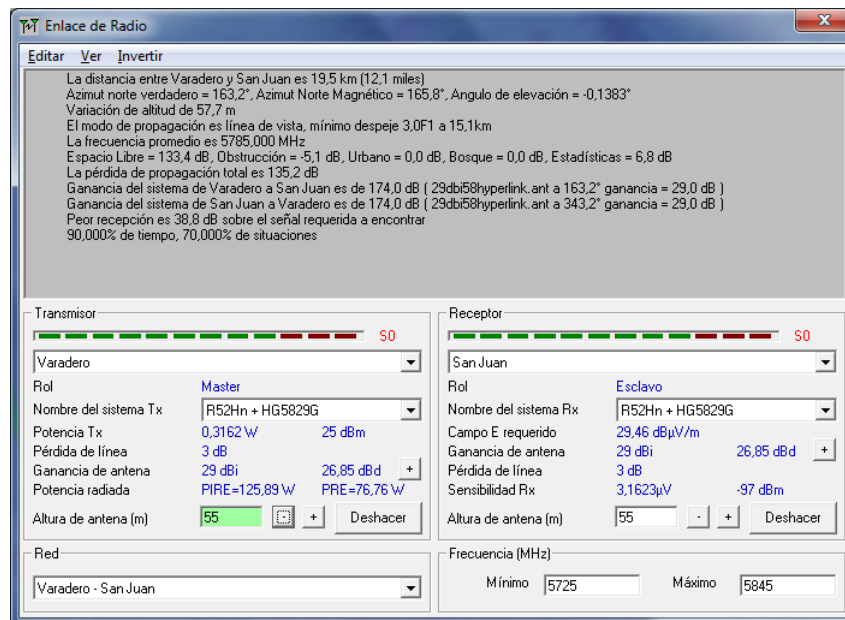


Ilustración 36: Detalles del radioenlace entre San Juan y Varadero

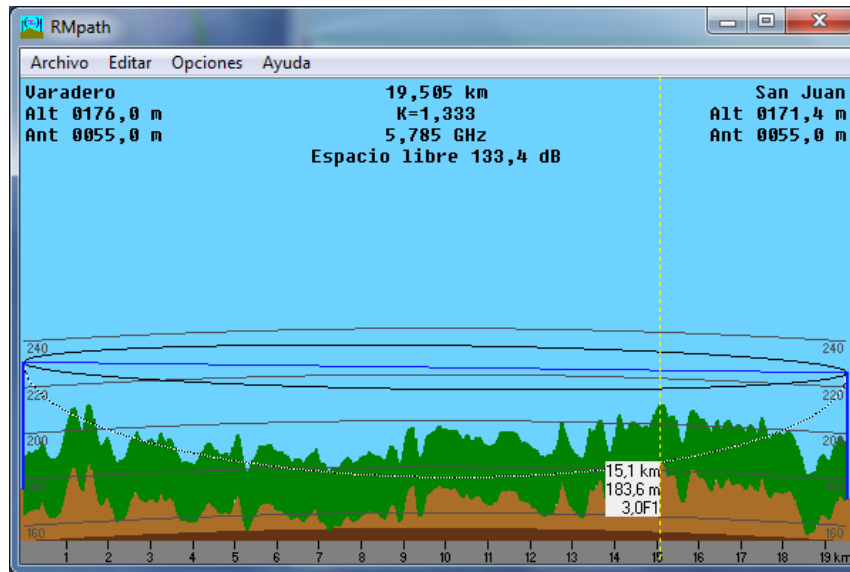
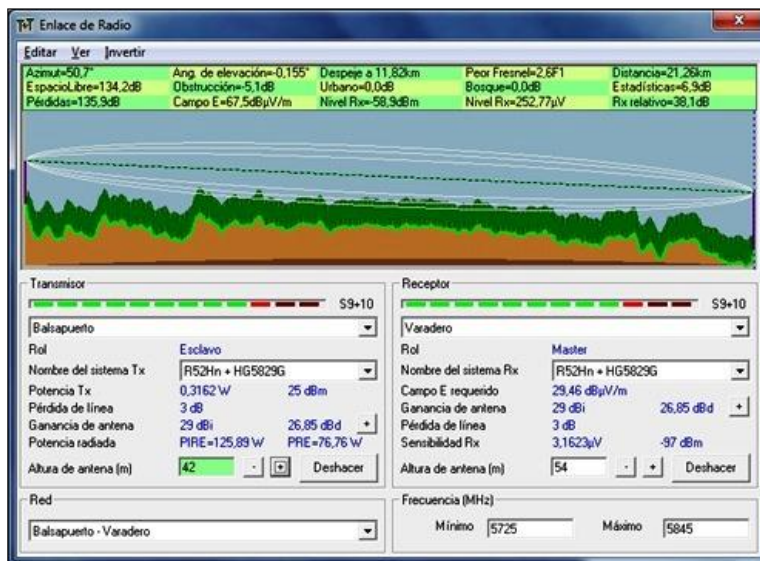


Ilustración 37: Resultado del radioenlace entre San Juan y Varadero

3. Enlace: San Gabriel de Varadero – Balsapuerto



Resultados Radio Mobile	
Data Input / Output	1.0F1
Balsapuerto	17.00m
Varadero	28.00m
Bosque	0.0Db
d1	10.35Km
% de tiempo	90%
% de situaciones	70%
Nivel RX	-67.70dBm
Cálculo de la Primera Zona de Fresnel	
d=	21.26Km
d1=	11.84Km
d2=	9.42Km
f=	5845.00Mhz
r1=	15.91M
0.6r1=	9.55M
Altura de los árboles	25.00m
Medida del Clearance	16.84m
Agregar	18.00m

Ilustración 38: Perfil del radioenlace entre S.G. de Varadero y Balsapuerto

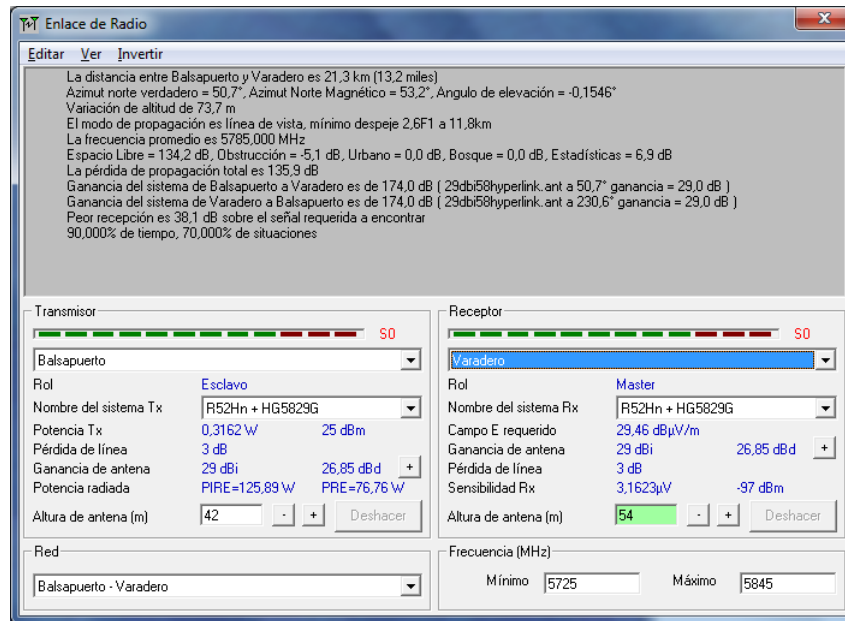


Ilustración 39: Detalles del radioenlace entre S.G. de Varadero y Balsapuerto

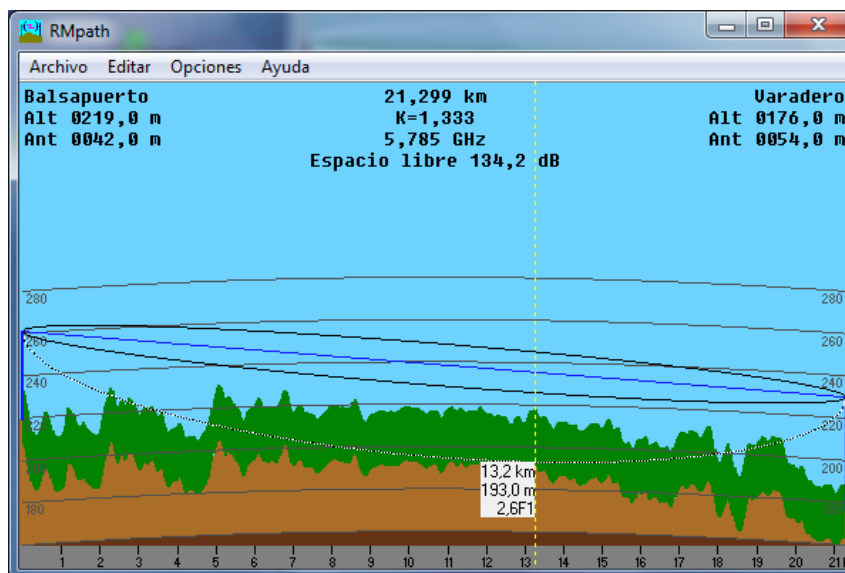


Ilustración 40: Resultado del radioenlace entre S.G. de Varadero y Balsapuerto

ALTURA DE TORRES FINALES

Nodo	Torre	Observaciones
San Juan	60.00m	Requiere una torre nueva
Santa Gema	42.00m	Existe una torre de 42m
Varadero	60.00m	Requiere una torre nueva
Balsapuerto	42.00m	Existe una torre de 42m

4.5. Direccionamiento IP y enrutamiento de la Red

En el diagrama de la Red de Telemedicina Balsapuerto 2011, expuesto anteriormente, se debe prestar atención al direccionamiento de las redes troncales y al direccionamiento interno de la red. En ella, se dispone de varias subredes con máscara “/28” (255.255.255.240). Con este enmascaramiento en cada subred disponemos de hasta 14 equipos ($2^4 - 2 = 14$), con lo cual se permite configurar 14 direcciones de Host en cada subred.

El criterio de diseño para el direccionamiento interno de la red, se justifica en la posibilidad de realizar una fase posterior de crecimiento de la red. Esta fase pretende comunicar equipos adicionales y además, la utilización de varios servidores Asterisk, con lo cual se mejoraría la disponibilidad de los servicios de VoIP y Videoconferencia.

Adicionalmente, se ha utilizado el enrutamiento dinámico con *OSPF*⁷. El criterio para la utilización de este tipo de enrutamiento OSPF se justifica en redes donde se esperan cambios en la topología o redes que manejan más de 15 saltos. De acuerdo al estudio de campo inicial, se ha supuesto que la red crecerá en el futuro, por lo que el uso de protocolos enrutados como OSPF nos facilitará esta expansión.

El enrutamiento estático se utiliza en casos donde el número de saltos es inferior a 15. Su uso también se justifica en redes donde no se esperan cambios en la topología, el uso de este tipo de enrutamiento reduce la sobrecarga de la red debido a que no se envían las actualizaciones de enrutamiento como sucede con OSPF.

Hay tres elementos básicos en la configuración del OSPF usando un Router MikroTik:

- a) Activar y configurar el sistema (instancia) OSPF.
- b) Configuración del área OSPF.
- c) Configuración de las redes e interfaces OSPF. Las redes OSPF se adicionan al enrutamiento OSPF y se especifica su área respectiva.

⁷ OSPF (**Open Shortest Path First**): Es un protocolo de enrutamiento jerárquico de pasarela interior o IGP (Interior Gateway Protocol), que usa el algoritmo Dijkstra enlace-estado (LSA – Link State Algorithm) para calcular la ruta más corta posible. Una *cost* como su medida de métrica. Además, construye una base de datos enlace-estado (*link-state database*, LSDB) idéntica en todos los enrutadores de la zona.

A continuación se detalla la configuración del OSPF en un Router Mikrotik:

```

OSPF
*****
[admin@b1-santagema] > routing ospf instance set router-id=0.0.1.8 metric-default=10
metric-connected=10 metric-static=10 metric-rip=0 metric-bgp=0 redistribute-connected=as-
type-1 redistribute-static=as-type-1 distribute-default=if-installed-as-type-1 numbers=0

[admin@b1-santagema] > routing ospf network add network=20.20.5.0/28 area=backbone
[admin@b1-santagema] > routing ospf network add network=20.21.1.0/28 area=backbone

[admin@b1-santagema] > routing ospf interface add interface=wlan1 cost=10

[admin@b1-santagema] > routing ospf interface add interface=wlan2 cost=10

```

Para verificar que el enrutamiento OSPF está correctamente configurado, realizamos la verificación sobre el sistema, interfaces y redes para que nos muestre los parámetros establecidos. La siguiente ilustración ejemplifica esta acción:

```

[admin@b1-santagema] > routing ospf instance print
Flags: X - disabled
0 name="default" router-id=0.0.1.8 distribute-default=if-installed-as-type-1 redistribute-
connected=as-type-1 redistribute-static=as-type-1 redistribute-rip=no redistribute-bgp=no
redistribute-other-ospf=no metric-default=10 metric-connected=10 metric-static=10 metric-
rip=0 metric-bgp=0 metric-other-ospf=auto in-filter=ospf-in out-filter=ospf-out

[admin@b1-santagema] > routing ospf interface print
Flags: X - disabled, I - inactive, D - dynamic, P - passive
# INTERFACE COST PRIORITY NETWORK-TYPE AUTHENTICATION
AUTHENTICATION-KEY
0 wlan1 10 1 default none
1 wlan2 10 1 default none

[admin@b1-santagema] > routing ospf network print
Flags: X - disabled, I - invalid
# NETWORK AREA
0 20.20.5.0/28 backbone
1 20.21.1.0/28 backbone

[admin@b1-santagema] > ip route print
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r - rip, b - bgp, o - ospf, m -
mme, B - blackhole, U - unreachable, P - prohibit
# DST-ADDRESS PREF-SRC GATEWAY DISTANCE
0 A S 0.0.0.0/0 20.21.1.2 1
1 ADC 20.20.5.0/28 20.20.5.2 wlan1 0
2 ADC 20.21.1.0/28 20.21.1.1 wlan2 0
3 ADC 20.22.1.0/28 20.22.1.1 br1 0

```

La primera línea de código de la tabla de enrutamiento representa el enrutamiento por defecto, para que se pueda navegar por Internet.

Una vez se hayan establecido las relaciones del router con sus vecinos OSPF, se importarán y exportarán todas las subredes correspondientes a toda la red. Finalmente, todas estas subredes aparecerán en la tabla de enrutamiento.

De la configuración del sistema (instancia) OSPF detallamos los siguientes parámetros:

```
[admin@b1-santagema] > routing ospf instance set router-id=0.0.1.8 metric-default=10 metric-connected=10 metric-static=10 metric-rip=0 metric-bgp=0 redistribute-connected=as-type-1 redistribute-static=as-type-1 distribute-default=if-installed-as-type-1 numbers=0
```

```
[admin@b1-santagema] > routing ospf instance print
```

```
Flags: X - disabled
```

```
0 name="default" router-id=0.0.1.8 distribute-default=if-installed-as-type-1 redistribute-connected=as-type-1 redistribute-static=as-type-1 redistribute-rip=no redistribute-bgp=no redistribute-other-ospf=no metric-default=10 metric-connected=10 metric-static=10 metric-rip=0 metric-bgp=0 metric-other-ospf=auto in-filter=ospf-in out-filter=ospf-out
```

- **router-id=0.0.1.8:** Es el identificador (ID) del 'router' OSPF. Si no es especificado, OSPF utiliza una de las direcciones IP del 'router'.
- **distribute-default=if-installed-as-type-1:** Asigna la ruta por defecto. En este caso la ruta por defecto es de métrica de 'tipo 1' o 'type 1', sólo para el caso en el que esta ruta haya sido instalada.
- **redistribute-connected=as-type-1:** Redistribuye directamente las rutas conectadas.
- **redistribute-static=as-type-1:** Redistribuye las rutas estáticas configuradas.
- **metric-default=10:** La ruta por defecto es distribuida con métrica igual a 10.
- **metric-connected=10:** Las rutas a redes directamente conectadas son distribuidas con métrica igual a 10.
- **metric-static=10:** Las rutas estáticas son distribuidas con métrica igual a 10.

Para realizar la configuración del área y las redes OSPF se deben añadir la red a un área determinada en el router. Además, se agregan también las redes que se desean compartir con sus respectivos vecinos OSPF, como vemos a continuación:

```
[admin@b1-santagema] > routing ospf network add network=20.20.5.0/28 area=backbone
```

```
[admin@b1-santagema] > routing ospf network add network=20.21.1.0/28 area=backbone
```

```
[admin@b1-santagema] > routing ospf network print
```

```
Flags: X - disabled, I - invalid
```

#	NETWORK	AREA
0	20.20.5.0/28	backbone
1	20.21.1.0/28	backbone

Cada vez que se agrega una interfaz a la configuración OSPF, se considera como un enlace, y se utiliza para generar una base de datos de enlaces. Como vemos a continuación, se han agregado las dos interfaces 'wlan1' y 'wlan2' con una métrica igual a 10.

```
[admin@b1-santagema] > routing ospf interface add interface=wlan1 cost=10
[admin@b1-santagema] > routing ospf interface add interface=wlan2 cost=10
[admin@b1-santagema] > routing ospf interface print
Flags: X - disabled, I - inactive, D - dynamic, P - passive
# INTERFACE COST PRIORITY NETWORK-TYPE AUTHENTICATION
AUTHENTICATION-KEY
0 wlan1 10 1 default none
1 wlan2 10 1 default none
```

4.6. Estudio de la viabilidad de los enlaces

El proceso de determinar si un enlace es viable se denomina '*Cálculo de presupuesto de potencia o balance de enlace*'. La potencia disponible en un sistema 802.11n puede caracterizarse por los siguientes parámetros:

- ✓ Mínimo de señal recibida
- ✓ Pérdida por atenuación en los cables y conectores
- ✓ Potencia de transmisión
- ✓ Ganancia de las antenas

Se desea estimar la viabilidad de los enlaces troncales que conforman la red, para ello se ha tenido en cuenta los parámetros antes mencionados.

A continuación se describe el cálculo de los tres enlaces troncales y se justifica las buenas prestaciones de estos enlaces.

4.6.1. Cálculo del presupuesto del enlace: Yurimaguas y San Juan del Armanayacu

Sumando todas las ganancias y pérdidas de lado de la estación transmisora se tiene:

	24 dBm	Potencia de transmisión	
+	28.5 dBi	Ganancia de la antena transmisora	
-	1.4 dB	Pérdida en los cables y conectores de transmisor	
	51.1 dBm	El PIRE < 52 dBm cumple lo especificado en la norma.	

Sumando todas las ganancias y pérdidas en la estación transmisora y receptora, y considerando la pérdida de propagación obtenemos la potencia recibida por el receptor:

	24 dBm	Potencia de transmisión
+	28.5 dBi	Ganancia de la antena transmisora
-	1.4 dB	Pérdida en los cables y conectores de transmisor
+	28.5 dBi	Ganancia de la antena receptora
-	1.4 dB	Pérdida en los cables y conectores del receptor
-	136.67 dB	Pérdida de propagación

-58.47 dBm = Potencia recibida por el receptor

Es sabido que basta con un margen de 10 a 15 dB para establecer la comunicación pero, la experiencia del grupo GTR-PUCP implementando este tipo de enlaces en zonas de selva, ha demostrado que para contrarrestar los efectos producidos por la atenuación y el multitrayecto en la señal de radio recibida, es preferible tener un margen de 20 a 25 dB.

Para el caso de una velocidad de transmisión mínima en un sistema MIMO 2x2 (MCS = 8 = 13 Mbit/s): debido a que **-58.47 dBm** es mayor que la sensibilidad del receptor para este caso (**-97 dBm**), se dispone de margen de **38.55 dBm** (97dBm - 58.45 dBm), este valor es muy satisfactorio y más que suficiente para la comunicación entre el transmisor y el receptor.

Para el caso de una velocidad de transmisión máxima en el mismo sistema (MCS = 15 = 130 Mbit/s): debido a que **-58.47 dBm** es mayor que la sensibilidad del receptor para este caso (**-77 dBm**), se dispone de un margen de **18.55 dBm** (77dBm - 58.45 dBm), este valor es cercano a los 20 dB que desearíamos obtener. Por lo tanto es un valor satisfactorio, y suficiente para la comunicación entre el transmisor y el receptor, con lo cual se garantiza teóricamente la velocidad de transmisión considerada.

Se ha decidió no configurar una velocidad (MCS =15) sino un valor menor que asegure estabilidad en el enlace y permita un enlace sin variaciones.

Sin embargo en la práctica se deberá tener en cuenta otros muchos aspectos que pueden influir para que no se obtenga la velocidad de transmisión deseada, por ejemplo: las condiciones climáticas en zonas de selva, las desventajas de utilizar la banda de 5.8 GHz frente a la banda de 2.4 GHz en zonas de lluvia intensa y algún desajuste en el apuntamiento de las antenas, entre otros.

4.6.2. Cálculo del presupuesto del enlace: San Gabriel de Varadero y Balsapuerto

Sumando todas las ganancias y pérdidas del lado de la estación transmisora tenemos:

	24 dBm	Potencia de transmisión
+	28.5 dBi	Ganancia de la antena transmisora
-	1.4 dB	Pérdida en los cables y conectores de transmisor
<hr/>		
	51.1 dBm	El PIRE < 52 dBm cumple lo especificado en la norma.

Sumando todas las ganancias y pérdidas en la estación transmisora y receptora, y considerando la pérdida de propagación obtenemos la potencia recibida por el receptor:

	24 dBm	Potencia de transmisión
+	28.5 dBi	Ganancia de la antena transmisora
-	1.4 dB	Pérdida en los cables y conectores de transmisor
+	28.5 dBi	Ganancia de la antena receptora
-	1.4 dB	Pérdida en los cables y conectores del receptor
-	133.52 dB	Pérdida de propagación
<hr/>		
	-55.32 dBm	= Potencia recibida por el receptor

Para el caso de una velocidad de transmisión mínima en un sistema MIMO 2x2 (MCS = 8 = 13 Mbit/s): obteniendo un margen de **41.68 dB (97dBm – 55.32 dBm)**, este valor es muy satisfactorio y más que suficiente para la comunicación entre el transmisor y el receptor.

Para el caso de una velocidad de transmisión máxima en este sistema (MCS = 15 = 130 Mbit/s): ya que **-55.32 dBm** es mayor que la sensibilidad del receptor (**-77 dBm**), se dispone de un margen de **21.68 dBm (77dBm - 55.32 dBm)**, el cual es mayor a los 20 dB que deseamos conseguir, este valor es satisfactorio, y suficiente para la comunicación entre el transmisor y el receptor, con lo cual se garantiza teóricamente la velocidad de transmisión considerada.

4.6.3. Cálculo del presupuesto del enlace: San Gabriel de Varadero y Balsapuerto

Sumando todas las ganancias y pérdidas en la estación transmisora tenemos:

	24 dBm	Potencia de transmisión
+	27 dBi	Ganancia de la antena transmisora
-	1.4 dB	Pérdida en los cables y conectores de transmisor
	<hr/>	
	49.6 dBm	El PIRE < 52 dBm cumple lo especificado en la norma.

Sumando todas las ganancias y pérdidas en la estación transmisora y receptora, y considerando la pérdida de propagación obtenemos la potencia recibida por el receptor:

	24 dBm	Potencia de transmisión
+	27 dBi	Ganancia de la antena transmisora
-	1.4 dB	Pérdida en los cables y conectores de transmisor
+	27 dBi	Ganancia de la antena receptora
-	1.4 dB	Pérdida en los cables y conectores del receptor
-	134.29 dB	Pérdida de propagación
	<hr/>	
	-59.09 dBm	= Potencia recibida por el receptor

A diferencia de los enlaces anteriores, este enlace utiliza un sistema SISO (Single Input Single Output) 1x1. Para el caso de una velocidad mínima (MCS = 0 = 6 Mbit/s): obtenemos un margen de **37.91 dB (97dBm – 59.09 dBm)**, este valor es muy satisfactorio y más que suficiente para la comunicación entre el transmisor y el receptor.

Para el caso de una velocidad de transmisión máxima en este sistema (MCS = 7 = 65 Mbit/s): ya que **-59.09 dBm** es mayor que la sensibilidad del receptor (**-77 dBm**), se dispone de un margen de **17.95 dBm (77dBm - 59.09 dBm)**, este valor es cercano a los 20 dB que deseáramos obtener. Por lo tanto es un valor satisfactorio, y suficiente para la comunicación entre el transmisor y el receptor, con lo cual se garantiza teóricamente la velocidad de transmisión considerada.

La tabla detalla los modos de funcionamiento del estándar (MCS0 al MCS15), para la tarjeta inalámbrica MikroTik RB R52Hn. Los valores siguientes nos han servido para realizar el cálculo del presupuesto del enlace y para el estudio radioeléctrico utilizando Radio Mobile.

802.11n (BW=20 MHz)			
MCS	Data rate (Mbps)	Potencia (dBm)	Sensibilidad (dBm)
0	6	24	-97
1	9	22	-95
2	12	22	-92
3	18	22	-89
4	24	22	-86
5	36	20	-83
6	48	19	-80
7	54	18	-77
8	13	24	-97
9	26	22	-95
10	39	22	-92
11	52	22	-89
12	78	22	-86
13	104	20	-83
14	117	19	-80
15	130	18	-77

Tabla 10: características de los equipos MikroTik RB R52Hn

4.7. Medición de las prestaciones de la red empleando la gestión avanzada de tráfico utilizando HTB en MikroTik para soporte de QoS

A continuación se explica las mediciones empíricas de las prestaciones obtenidas en la red utilizando la gestión avanzada de tráfico usando HTB para soportar QoS. Para ello, en primer lugar se define el ancho de banda repartido por cada tipo de tráfico, también se define el tráfico que queremos garantizar y el tráfico que queremos limitar.

En segundo lugar se justifica la razón del porqué se ha utilizado HTB.

Luego se detalla la configuración de la QoS usando HTB en la Mikrotik.

Y finalmente se describe y se discuten los resultados obtenidos, la cual muestra cómo es tratado cada tipo de tráfico por la red.

4.7.1. Criterios de diseño

Según lo explicado en el siguiente capítulo de ‘Resultados’, se dispone de los siguientes valores de ‘throughput’ de datos en los enlaces troncales:

<i>Enlaces troncales</i>	<i>‘throughput’ de datos (Mbit/s)</i>
<i>Balsapuerto y Varadero MIMO 2x2</i>	20
<i>Varadero y San Juan MIMO 2x2</i>	40
<i>San Juan y Santa Gema SISO 1x1</i>	63

Tabla 11: Valores de ‘throughput’ de datos (Mbit/s) en los enlaces troncales

Como podemos observar en la tabla anterior, se ha obtenido importantes valores de ‘throughput’ de datos en los dos enlaces troncales, con la utilización del estándar 802.11n y sistemas MIMO 2x2. Superando los 60 Mbit/s en el enlace desde el Hospital de Santa Gema a San Juan del Armanayacu.

Como ya se ha comentado anteriormente los enlaces locales de distribución también utilizan el estándar 802.11n, y superan los 100 Mbit/s.

En la *Ilustración 41* hay un ejemplo de este tipo de enlace local ‘San Juan’, el cual dispone de un solo cliente y se emplea antenas panel.

Para las siguientes mediciones utilizando la gestión avanzada de tráfico se ha considerado el entorno de la siguiente ilustración, se ha inyectado flujos de tráfico, desde el ordenador conectado al cliente de Santa Gema ‘**20.22.1.10/28**’ hacia otro ordenador conectado al cliente de San Juan ‘**20.23.5.10/28**’.

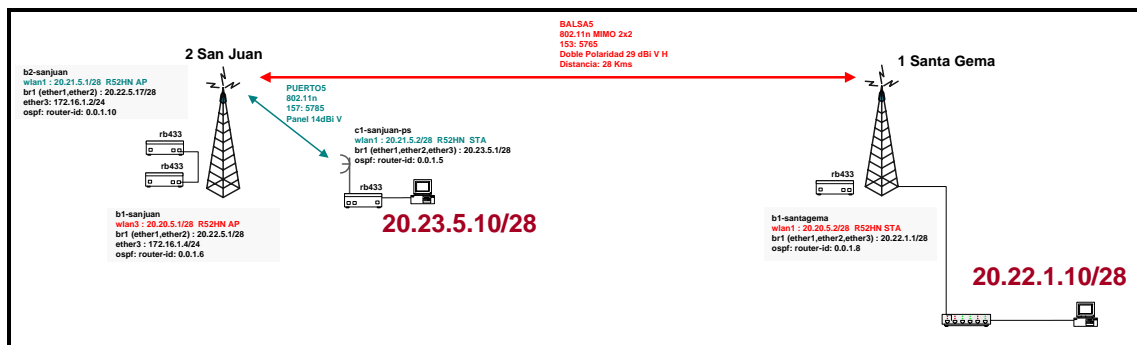


Ilustración 41: Esquema del entorno de prueba

Por lo tanto, para este entorno de prueba se ha utilizado, un ordenador conectado con cable de exteriores al repetidor troncal de Santa Gema, el cual se comunica con el repetidor troncal de San Juan, y este distribuye la señal al cliente de San Juan y al ordenador conectado a este cliente.

Se elaboró este entorno de pruebas para lograr un mejor entendimiento de los resultados obtenidos.

Sin embargo, en el anexo siguiente se ha adjuntado la configuración completa para soportar QoS en toda la Red, en la cual se detalla la necesidad de configurar cada uno de los enrutadores inalámbricos que componen la Red (incluyendo los repetidores troncales, los repetidores locales y los clientes), esto es debido a la necesidad de marcar los paquetes y también sus conexiones en todos los nodos de la red, comprendiendo a cabalidad el correcto flujo de estos paquetes.

Lograr mayores valores de ancho de banda, permiten realizar un mejor reparto por cada tipo de tráfico y mejores resultados. Sin embargo para lograr un funcionamiento óptimo en la gestión avanzada de tráfico, es importante además, que los valores de ancho de banda disponibles en el medio de transmisión no sean variables.

En este entorno de pruebas, según los resultados obtenidos ‘extremo a extremo’ utilizando la herramienta ‘*Bandwith Test*’ de Mikrotik (también ‘*IPERF*’), se obtiene un valor de ‘*throughput*’ de datos superior a los 40 Mbit/s. Sin embargo, se ha considerado que se dispone de un ancho de banda extremo a extremo de 10 Mbit/s, para contemplar el caso más pesimista debido a variaciones que puedan producirse en caso de lluvia intensa.

La siguiente ilustración muestra los resultados de *'throughput'* de datos o caudal total (extremo a extremo) correspondientes al entorno de prueba que se observa en la **Ilustración 63**, el valor obtenido es constante y superior a los 40 Mbit/s.

En esta ilustración se observa inyección de tráfico *'UDP'* con un tamaño de paquete *'MTU'* de 1500:

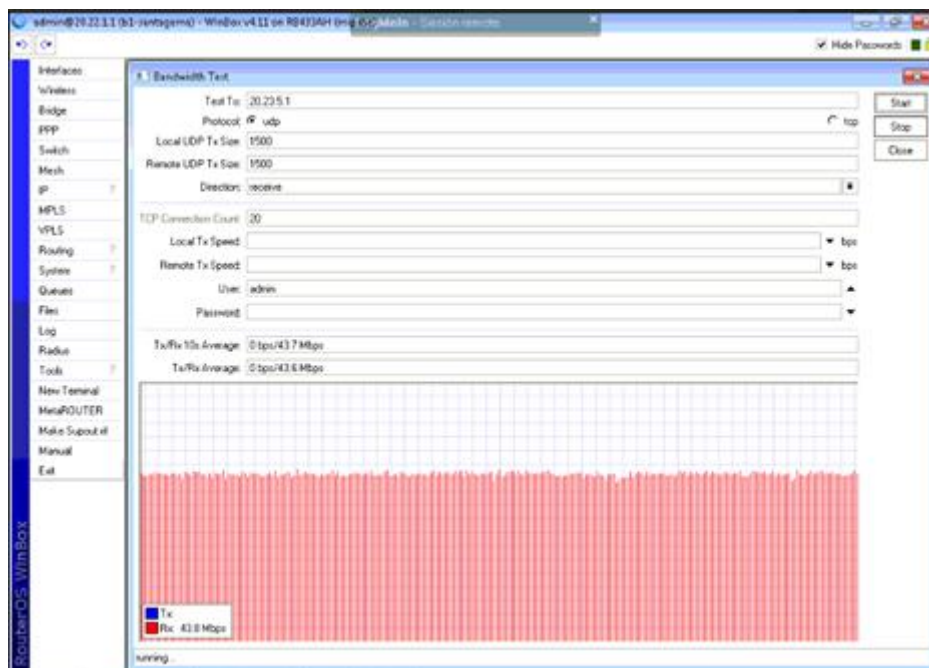


Ilustración 42: *'throughput'* de datos o caudal total (extremo a extremo) en el entorno de prueba

Una de las ventajas de HTB, es que si se dispone de mayor ancho de banda, entonces lo reparte jerárquicamente entre los tres tipos de tráfico respetando los que son más prioritarios. En la siguiente tabla se muestra la repartición de ancho de banda por tipo de tráfico prioritario:

<i>Tipos de Tráfico</i>	<i>Flujos</i>	<i>Prioridades (dscp)</i>	<i>Tasa constante (Kbit/s)</i>	<i>Ancho de banda (10 Mbit/s)</i>		
				<i>Doble limitación</i>		<i>Limitado (PCQ)</i>
				<i>(CIR)</i>	<i>(MIR)</i>	
<i>VoIP</i>	3	46→0xb8	200	1	10	-
<i>Videoconferencia</i>	1	38→0x98	2592	8	10	-
<i>BestEffort</i>	1	0→0x00	864	1	1	1

Tabla 12: Repartición del ancho de banda por tipo de tráfico usando HTB

Otra de las ventajas de HTB es la doble limitación que tiene cada cola. Es decir, cada cola dispone de un valor de CIR ‘*Committed Information Rate*’ o ‘*peor caso*’, esto significa que el flujo recibe esta cantidad de tráfico garantizado en todo momento. También dispone de un valor de MIR ‘*Maximal Information Rate*’ o ‘*mejor caso*’, es la tasa de flujo máxima que se puede llegar a conseguir si hay colas padres que tiene ancho de banda sobrante.

4.7.2. Simulación y preparación de flujos

Para las siguientes pruebas se ha utilizado el inyector de tráfico denominado D-ITG, el cual permite caracterizar flujos (para diferentes tipos de tráficos) de información con diferentes características para simular varias condiciones reales.

También se deberá sincronizar todos los enrutadores, debido a que para enlaces WiFi de 30 Km como en este caso se inyectará un valor de *delay igual a 100 useg*, conocido como tiempo de propagación (τ), a este valor también se sumará otro por latencia de los equipos. Para llevar a cabo la sincronización de los relojes de estos equipos se ha utilizado el protocolo Network Time Protocol (NTP).

➤ Preparación de flujos

Para las simulaciones se han definido cinco diferentes flujos de tráfico utilizando el D-ITG, tal como se muestra en el siguiente esquema:

```
-a 20.22.1.10 -b 0xb8 -rp 9000 -t 30000 VoIP -x G.711.1  
-a 20.22.1.10 -b 0xb8 -rp 9001 -t 30000 VoIP -x G.711.1  
-a 20.22.1.10 -b 0xb8 -rp 9002 -t 30000 VoIP -x G.711.1  
-a 20.22.1.10 -T TCP -b 0x00 -rp 9009 -t 30000 -c 540 -C 200  
-a 20.22.1.10 -T UDP -b 0x98 -rp 9010 -t 30000 -c 540 -C 600
```

De lo especificado en el esquema y la tabla anterior, se dispone de 3 flujos de tráfico de VoIP prioritarios. También 1 flujo de videoconferencia marcado como prioritario (representando a varias sesiones de videoconferencia) consistente en 600 paquetes, cada uno de un tamaño de 540 (igual a 2592 Kbps).

Y además 1 flujo de tráfico “besteffort” no prioritario consistente en 200 paquetes, cada uno de un tamaño de 540 (igual a 864 Kbps). Los flujos de tráfico de voz y videoconferencia son UDP, y el flujo de tráfico “besteffort” es TCP.

4.7.3. Justificación: ¿Por qué usamos HTB en MikroTik?

Se justifica la utilización de HTB debido a sus mayores ventajas en comparación con otras disciplinas de colas.

Características de HTB:

- ✓ Permite dividir una cantidad fija de ancho de banda entre diferentes tipos de tráfico. Para lo cual se tiene la posibilidad de conformar diferentes tamaños en las colas.
- ✓ Permite crear una estructura de colas jerárquica, y establece relaciones entre ellas, cada una con diferente prioridad
- ✓ Permite ordenar y darle forma a todo el tráfico saliente
- ✓ Cada cola de HTB permite una doble limitación

4.7.4. Configuración de HTB en MikroTik

A continuación procedemos a detallar la configuración de la QoS utilizando HTB (Hierarchical Token Bucket) en el enrutador Mikrotik RB433AH/RB433.

```
Mangle - Marcado de Paquetes
*****
[admin@b1-santagema] > ip firewall mangle add chain=forward action=mark-connection
new-connection-mark=voip-con passthrough=yes src-address=20.23.7.2 dst-
address=20.23.7.2 dscp=46

[admin@b1-santagema] > ip firewall mangle add chain=forward action=mark-packet
new-packet-mark=voip passthrough=no connection-mark=voip-con

[admin@b1-santagema] > ip firewall mangle add chain=forward action=mark-
connection new-connection-mark=voip-con passthrough=yes src-
address=20.22.1.0/28 dst-address=20.22.5.0/28 dscp=46

[admin@b1-santagema] > ip firewall mangle add chain=forward action=mark-
packet new-packet-mark=voip-con passthrough=no connection-
mark=voip-con
```

observar que marcamos los paquetes con su valor de DSCP=46, para la VoIP, con lo cual se le dará mayor prioridad. Además se deberá especificar la ruta que el paquete sigue, por lo tanto se ha especificado la dirección de la red de origen y destino (20.22.1.0/28 y 20.22.5.0/28).

También es importante comprender el correcto flujo del paquete (hay 5 lugares donde marcar: “Prerouting”, “Input”, “Forward”, “Output” y “Postrouting”) sin el cual no se podría efectuar el marcado de los paquetes y la priorización de los diferentes tipos de tráfico. La

siguiente ilustración establece las secuencias posibles que pueden seguir los flujos de paquetes:

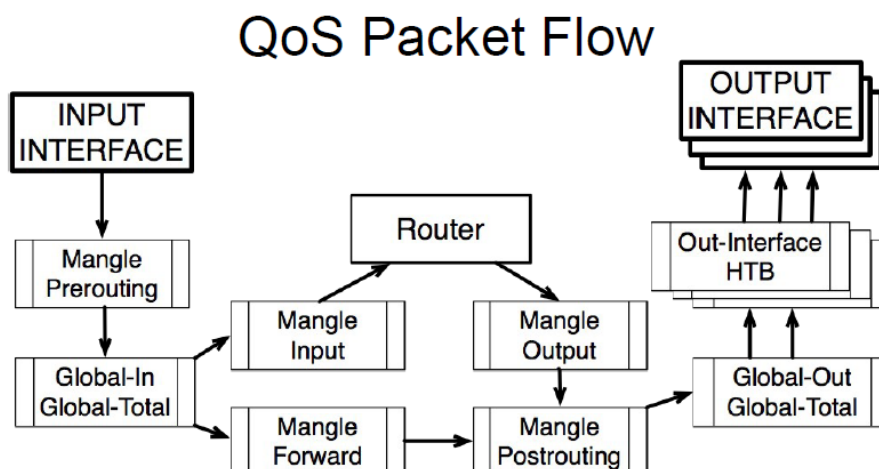


Ilustración 43: Diagrama de flujos de paquetes para soportar QoS

```

[admin@b1-santagema] > queue tree add name="trafico_total" parent=wlan1
limit-at=0 priority=8 max-limit=10485760 burst-limit=0 burst-threshold=0
burst-time=0s

[admin@b1-santagema] > queue tree add name="leaf_besteffort"
parent=trafico_total packet-mark=besteffort limit-at=1048576
queue=PCQ_besteffort priority=8 max-limit=10485760 burst-limit=0
burst-threshold=0 burst-time=0s

[admin@b1-santagema] > queue tree add name="leaf_video"
parent=trafico_total packet-mark=video limit-at=8388608
queue=SFQ_video priority=2 max-limit=10485760 burst-limit=0 burst-
threshold=0 burst-time=0s

[admin@b1-santagema] > queue tree add name="leaf_voip"
parent=trafico_total packet-mark=voip limit-at=1048576
queue=SFQ_VoIP priority=1 max-limit=10485760 burst-limit=0 burst-
threshold=0 burst-time=0s
  
```

En el esquema anterior se describe la configuración del árbol de colas de HTB, estas colas no dispone de ningún orden y todas se procesan simultáneamente. La topología de este árbol es de padre e hijos. Todas las colas hijas deberán tener sus paquetes marcados.

En la configuración siguiente se dispone de un padre, este padre es la interfaz “wlan1” y le hemos llamado “*trafico_total*”. El padre tiene una capacidad máxima de 10Mbps, una de las ventajas del HTB es que si se dispone de mayor ancho de banda, entonces HTB reparte jerárquicamente el ancho de banda respetando los tráficos que son más prioritarios.

En el esquema anterior se ha configurado tres hijos (voip, besteffort y video). Para el caso del tráfico de VoIP se observa que se tiene un padre llamado “*trafico_total*”, este tráfico está limitado a 1 Mbps ($1024 \times 1024 = 1048576$), con una capacidad máxima de uso (en caso de repartirse el ancho de banda sobrante) de hasta 10 Mbps, además la cola que utiliza este tipo de tráfico es “SFQ”.

```
[admin@b1-santagema] > queue type add name="SFQ_VoIP" kind=sfq sfq-
perturb=10 sfq-allot=1514

[admin@b1-santagema] > queue type add name="SFQ_video" kind=sfq sfq-
perturb=10 sfq-allot=1514

[admin@b1-santagema] > queue type add name="PCQ_besteffort" kind=pcq
pcq-rate=1048576 pcq-limit=50 pcq-classifier=dst-address pcq-total-limit=2000
```

En el esquema anterior se ha configurado los diferentes tipos de colas para los tres tipos de tráficos que tenemos en nuestra red.

Se dispone de una cola “SFQ” para los tráficos prioritarios (VoIP y Videoconferencia) y una cola “PCQ” para el caso del tráfico *besteffort* (BE), la cual está limitada a un máximo de 1Mbps con lo que se consigue no saturar el ancho de banda en caso de mal uso del acceso a Internet.

4.7.5. Discusión de los resultados

A continuación se discuten los resultados obtenidos correspondientes a los “logs” recibidos en el entorno de prueba descrito anteriormente.

La siguiente ilustración detalla los resultados obtenidos de “*Bitrate*”, el cual depende del número de paquetes enviados y sobre todo del ancho de banda que ofrezca la red.

En esta ilustración se puede observar que los cinco tipos de flujos enviados se pueden transmitir sin problemas, esto es debido a que las condiciones del medio inalámbrico permiten velocidades de transmisión de más de 40 Mbps, muy por encima de lo que se envía en promedio.

El resultado obtenido se traduce en un ancho de banda repartido, logrando un mejor uso de este, es decir se asegura un ancho de banda suficiente para los servicios de Videoconferencia y VoIP. Además se ha permitido priorizar estos dos tráficos frente al tráfico de Internet, es decir, estos tráficos tendrán un menor *delay* y *jitter*.

Además al disponer de un mayor throughput de datos, los resultados son mucho mejores, debido a que el tráfico menos prioritario (Internet) también se podrá cursar, permitiendo un óptimo funcionamiento de la Red.

Como ya se ha comentado HTB es una disciplina de colas con clases jerárquica, la cual permite utilizar disciplinas de colas simples para los diferentes tipos de tráfico.

En nuestro caso, se ha utilizado para los dos tráficos prioritarios (VoIP y Videoconferencia) una “SFQ”, debido a que el algoritmo estocástico que emplea permite dar igualdad a estos dos tráficos. Para el caso del tráfico no prioritario (Internet) se ha utilizado “PCQ”, la cual ha permitido especificar el tamaño máximo y mínimo de la cola, logrando limitar este tráfico menos prioritario.

4.7.5.1. Resultados

En la siguiente ilustración se puede observar que se cursan perfectamente los tráficos prioritarios correspondientes a la **Videoconferencia señalado con el color azul, igual a 2592 Mbps** y **VoIP**. Además también se cursa el tráfico menos prioritario de **Internet señalado con el color verde, y de valor igual a 864 Kbps**

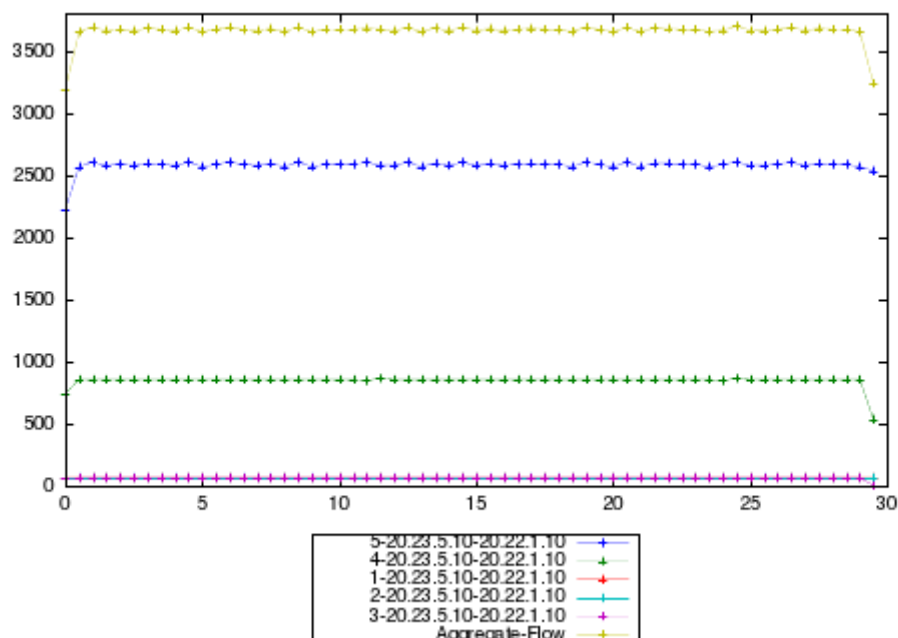


Ilustración 44: ‘Bitrate’ (Inyección de tráfico extremo a extremo Santa Gema y San Juan)

Tráfico Videoconferencia (color azul) y Tráfico Besteffort (color verde)

En la siguiente ilustración se puede comprobar que los valores de “*jitter*” y “*delay*” presentes en el tráfico de VoIP (TOS=0xb8, DSCP=46) y de Videoconferencia (TOS=0x98, DSCP=38) son menores que el del tráfico TCP – *Besteffort* (TOS=DSCP=0), debido a que estos dos primeros son mas prioritarios.

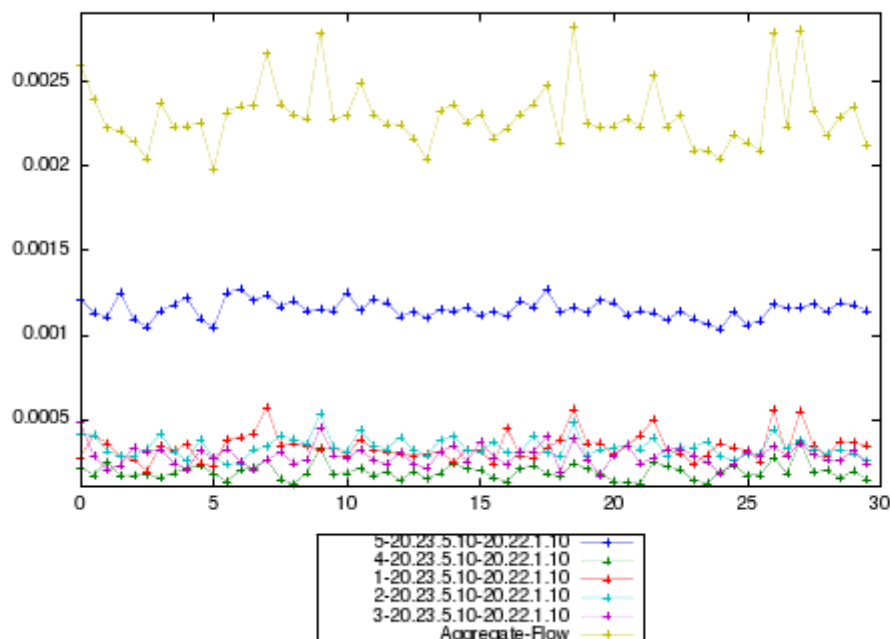


Ilustración 45: ‘*Jitter*’ (Inyección de tráfico extremo a extremo Santa Gema y San Juan)

Finalmente en la siguiente ilustración se puede observar que no existen paquetes perdidos

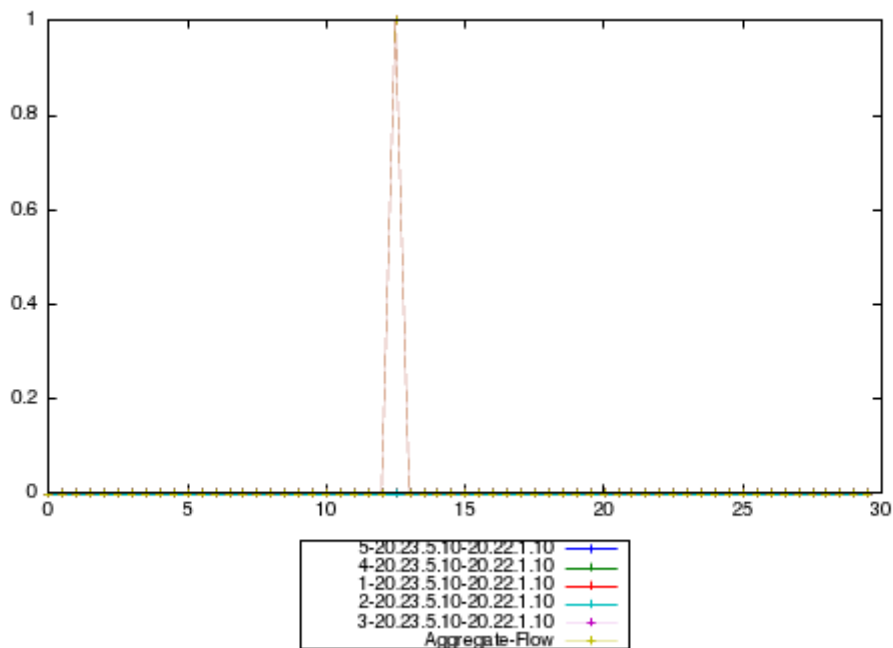


Ilustración 46: 'Paquetes perdidos' (Inyección de tráfico extremo a extremo Santa Gema y San Juan)

En la siguiente tabla se muestra los resultados de esta gestión avanzada de tráfico:

	<i>VoIP</i>	<i>Videoconferencia</i>	<i>BestEffort</i>
<i>DSCP</i>	46→0xb8	38→0x98	0→0x00
<i>Protocolo de transporte</i>	UDP	UDP	TCP
<i>Nro. Flujos</i>	3	1	1
<i>Jitter promedio [s]</i>	0.0003	0.0012	0.0002
<i>Bitrate promedio [Kbit/s]</i>	200	2592	864
<i>Paq. Perdidos</i>	0 (0.00 %)	0 (0.00 %)	0 (0.00 %)

Tabla 13: Resultados de la gestión avanzada de tráfico

Los resultados muestran que los tres tipos de tráfico se logran cursar, limitando siempre el tráfico de Internet con un máximo de 1 Mbit/s, es decir que nunca podrá conseguir una tasa mayor. También se consigue priorizar los tráficos de VoIP y Videoconferencia, asegurando siempre el valor de 'CIR' para ambos.

Además se consigue repartir el ancho de banda sobrante entre los dos tráficos prioritarios, esta repartición se hace teniendo en cuenta la cola que cursa la mayor cantidad de tráfico y el valor

de prioridad. En este caso, ambos tienen la posibilidad de conseguir la tasa de flujo máxima 'MIR'.

Capítulo V

Resultados

5.1. Introducción

Con la realización de un protocolo de pruebas se pretende demostrar y justificar los resultados obtenidos según las hipótesis formuladas en el diseño previo realizado en el laboratorio.

Estos resultados son fruto de una fase de monitoreo que se llevó a cabo al finalizar la instalación y puesta en marcha del sistema. En estas pruebas se analizaron parámetros como la potencia de la señal recibida, el caudal o *'throughput'* (*típicamente medido en un punto de referencia sobre la capa de red*) o los tiempos de transmisión en diferentes franjas horarias y condiciones atmosféricas.

Debido al corto tiempo de vida de la red implementada, estos resultados no dejan de ser orientativos ya que se continúan haciendo pruebas para tratar de optimizar todavía más los recursos de la red y dotarla, así, de una mayor eficiencia y estabilidad.

Este documento se compone de las siguientes partes:

- ✓ Pruebas y resultados: Se describen las pruebas correspondientes con el equipo instalado en la red, son las pruebas de escaneo de las señales que percibe el receptor y su análisis correspondiente. También el monitoreo del enlace para verificar que este funciona de manera óptima o considerar la utilización de otro canal en el caso de obtener valores incorrectos en el enlace.
- ✓ Capacidad del enlace: Se describen los resultados de *'throughput'* obtenido en los troncales y en las redes de distribución locales, especificando las características de los diferentes enlaces que tenemos en la red. También el *'throughput'* extremo a extremo que tenemos en la red.
- ✓ También se realizaran pruebas de transferencia de archivos, a estas pruebas se les conoce como *'Goodput'* o velocidad de transferencia de datos (se refiere al promedio

obtenido de velocidad de bit neto que es entregado a la capa de aplicación). Se dispone de la siguiente relación:

$$\textit{‘Goodput} \leq \textit{Throughput} \leq \textit{Maximum throughput} \leq \textit{Net bit rate} \textit{’}$$

- ✓ Finalmente los problemas encontrados y conclusiones.

5.2. Pruebas y resultados

Se realizaron las pruebas, instalando el equipo necesario en las redes troncales y en las redes locales. El equipamiento utilizado consiste en antenas directivas (Parabólicas, grilla), placas Mikrotik, tarjetas inalámbricas *MiniPCI*. En la siguiente ilustración se representa el equipamiento utilizado en la red.

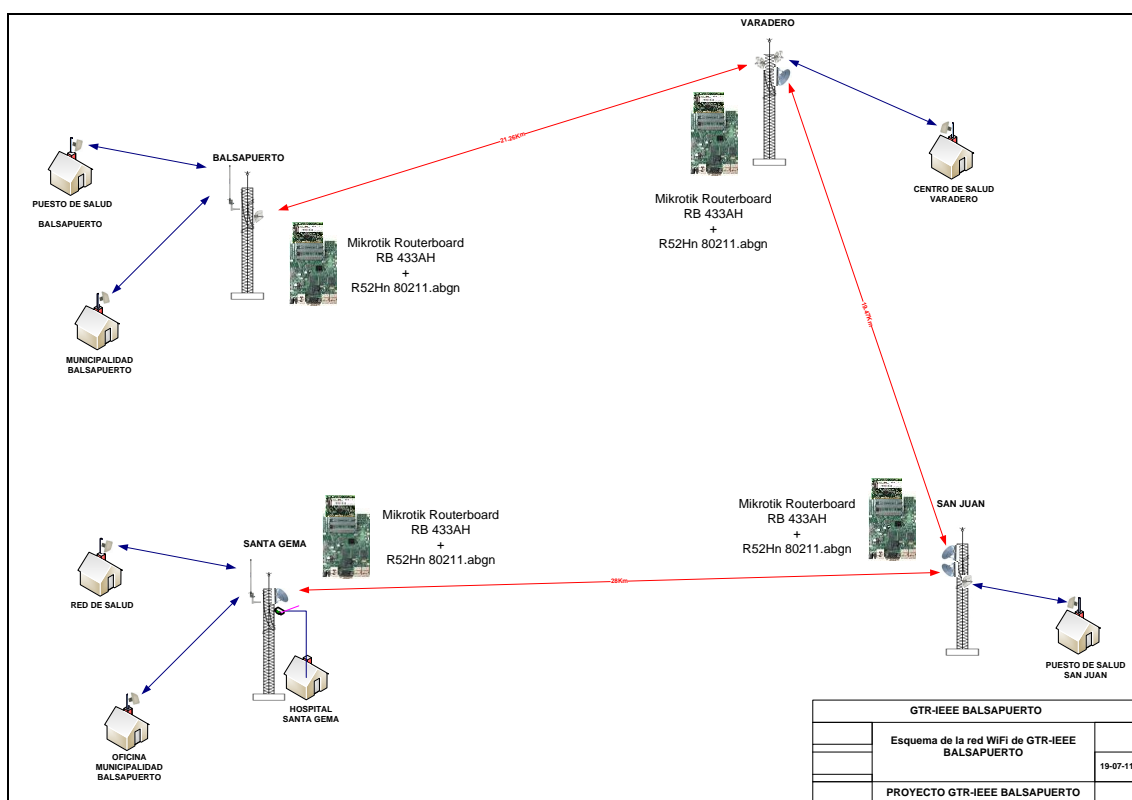


Ilustración 47: Redes Troncales y Redes Locales

5.2.1. Escaneo de la señal en la banda de 5.8 GHz

El objetivo de esta prueba es realizar un escaneo de las señales que percibe el receptor de la placa *Mikrotik*. Debido a que la placa está configurada para operar en la banda de 5.8 GHz, sólo captará señales que se encuentren dentro de ese rango.

Para ello, desde el Hospital de St. Gema, ubicado en la ciudad de Yurimaguas, realizamos un ‘scan’ sobre la interfaz ‘wlan1’. Como podemos ver en la Ilustración, el receptor capta la señal con SSID BALSAS, correspondiente al enlace troncal **802.11n con un sistema MIMO 2x2**. Este enlace une las poblaciones de Yurimaguas y San Juan del Armanayacu más concretamente.

Podemos ver las características de este enlace:

- Banda de frecuencia (**BAND**)
- Canal (Frequency – **FREQ**)
- Nivel de señal (Signal – **SIG**)
- Nivel de ruido (Noise Floor – **NF**)
- Relación señal a ruido (**SNR**)
- Dirección MAC de la tarjeta inalámbrica del AP (**RADIO-NAME**)

```
[admin@b1-santagema] > interface wireless scan wlan1
Flags: A - active, B - bss, P - privacy, R - routers-network, N - nstreme
ADDRESS          SSID          BAND    FREQ SIG NF SNR RADIO-NAME
AB R 00:0C:42:64:59:62 PUERTO1 5ghz-11n 5300 -46 -115 69 000C42645962
AB R 00:0C:42:64:5F:F9 BALSAS 5ghz-11n 5765 -66 -115 49 000C42645FF9
ABPR 00:15:6D:FE:11:CC AUCCOOP 2010 5ghz-11n 5805 -53 -115 62 AP - Sta Gema
ABPR 00:15:6D:68:0B:8E computelhugo 5ghz-11n 5200 -86 -115 29 00156D680B8E
```

Según los parámetros obtenidos escaneando este enlace, y considerando una sensibilidad en recepción es de -83 dBm correspondiente a una velocidad (MCS = 12 = 78 Mbps), se observa que el nivel de ruido es de -115 dBm y el nivel de señal recibida es de -66 dBm; lo que ofrece un excelente valor de SNR igual a 49 dB (valor que servirá de ‘colchón’ permitiendo un enlace de buenas condiciones).

Estos resultados justifican que utilizar un sistema MIMO aumenta el valor de SNR. Además, se obtiene un margen de 17 dB (83dBm - 66dBm), este valor es suficiente para comunicarse, sin embargo se debe evaluar considerar un margen mayor o igual a 20 dB (para zona de selva).

Si los resultados no reflejan un comportamiento estable en el enlace, se deberá configurar un valor de MCS menor a 12, para lograr un margen mayor o igual a 20 dB. Es necesario estimar una velocidad que permita lograr un enlace estable, sin cortes y poco variable.

Realizamos, también, una prueba de conectividad a los equipos ubicados en la torre de San Juan y a Internet a través del comando de testeo '*ping*'. De esta manera, comprobamos que hay conexión y podemos analizar el retardo de ida y vuelta de un paquete ('*Round Trip delay Time* o *RTT*').

```
[admin@b1-santagema] > ping address=20.20.5.1
20.20.5.1 64 byte ping: ttl=64 time=14 ms
20.20.5.1 64 byte ping: ttl=64 time=10 ms
20.20.5.1 64 byte ping: ttl=64 time=10 ms
20.20.5.1 64 byte ping: ttl=64 time=10 ms
20.20.5.1 64 byte ping: ttl=64 time=10 ms
20.20.5.1 64 byte ping: ttl=64 time=10 ms
42 packets transmitted, 42 packets received, 0% packet loss
round-trip min/avg/max = 2/9.1/14 ms

[admin@b1-santagema] > ping google.es
74.125.229.52 64 byte ping: ttl=249 time=315 ms
74.125.229.52 64 byte ping: ttl=249 time=514 ms
74.125.229.52 64 byte ping: ttl=249 time=432 ms
74.125.229.52 64 byte ping: ttl=249 time=490 ms
74.125.229.52 64 byte ping: ttl=249 time=220 ms
35 packets transmitted, 35 packets received, 0% packet loss
round-trip min/avg/max = 113/314.1/539 ms
```

5.2.2. Monitoreo del enlace con SSID: 'Balsa5'

Igual que el escaneo, el monitoreo se realiza únicamente desde la estación cliente. Al teclear el comando '*interface wireless monitor wlan1*' se monitoriza la interfaz inalámbrica número 1, donde se obtienen los valores representados en la siguiente ilustración.

Los parámetros que más nos interesan son los siguientes:

- Estado o STATUS: Indica si nos encontramos conectados con el AP
- Banda
- Frecuencia
- Tasa de transmisión y recepción
- SSID (Service Set Identifier): Nombre de la red inalámbrica
- BSSID (Basic Service Set Identifier): Identificador de la dirección MAC de la tarjeta inalámbrica del AP
- Nivel de señal (Signal – strength)

- Nivel de ruido (Noise – floor)
- Relación señal a ruido (Signal – to – noise)

```
[admin@b1-santagema] > interface wireless monitor wlan1

status: connected-to-ess
band: 5ghz-11n
frequency: 5765MHz
tx-rate: "104.0Mbps-HT"
rx-rate: "104.0Mbps-HT"
ssid: "BALSA5"
bssid: 00:0C:42:64:5F:F9
radio-name: "000C42645FF9"
signal-strength: -64dBm
tx-signal-strength: -64dBm
noise-floor: -109dBm
signal-to-noise: 45dB
tx-ccq: 84%
rx-ccq: 91%
p-throughput: 82638
overall-tx-ccq: 84%
authenticated-clients: 1
current-ack-timeout: 207
wds-link: no
nstreme: no
framing-mode: none
routeros-version: "4.11"
last-ip: 20.23.7.10
802.1x-port-enabled: yes
compression: no
wmm-enabled: yes
current-tx-powers:
6Mbps:24(24/27),9Mbps:22(22/25),12Mbps:22(22/25),18Mbps:22(22/25),24Mbps:22(22/25),36Mbps:20(20/23),48Mbps:19(19/22),54Mbps:18(18/21),HT20-0:24(24/27),HT20-1:20(20/23),HT20-2:19(19/22),HT20-3:18(18/21),HT20-4:17(17/20),HT20-5:16(16/19),HT20-6:15(15/18),HT20-7:14(14/17)
notify-external-fdb: no
```

Del monitoreo de este enlace, lo que podemos concluir es un funcionamiento y establecimiento del enlace. Si observamos el nivel de señal (-64 dBm) y la relación señal a ruido (45 dB) podemos observar que se está transmitiendo con un buen nivel de potencia sin demasiado nivel de ruido, permitiendo conectividad.

Los parámetros ‘tx-ccq’ y ‘rx-ccq’, evalúan la calidad del enlace tanto en transmisión y en recepción correspondientemente. Estos parámetros se expresan en porcentaje y representan la cantidad efectiva de ancho de banda transmitido y recibido. Por eso nos interesa que esté cerca del 100%, que equivaldría a un enlace perfecto.

En nuestro caso ronda una proporción del 84% en este caso (en otras pruebas superaba el 90%), lo que equivale a una calidad de enlace casi excelente.

Los parámetros ‘**tx-rate**’ y ‘**rx-rate**’, representan la velocidad de transmisión de datos a las que podemos funcionar, estas se configuran en el equipo.

En nuestro caso hemos configurado una velocidad (MCS = 12 = 78 Mbps), esta es la velocidad máxima de funcionamiento. Sin embargo como se ha comentado anteriormente, y teniendo en cuenta los valores de margen, relación señal a ruido, la cantidad de bits erróneos recibidos (Bit Error Rate – BER) y la zona de trabajo; esta velocidad deberá ser una que permita estabilidad y poca variabilidad del enlace.

También observamos cómo el sistema *Mikrotik*, fijando su parámetro ‘**ack-timeout = dynamic**’, resuelve, en este caso, el ACKTimeout a 207 μ s. De manera inteligente, en base a los parámetros y a la distancia del enlace, calcula qué ACKTimeout es el adecuado en cada caso, cosa que nos facilita la labor en enlaces de larga distancia como los nuestros. Recordemos que:

$$ACKTimeou = SIFS + 2 \cdot t_{prop} + PLCPpreamble + PLCPHeader + SlotTime + ACK$$

Donde, en un enlace de 28 Km como es en este caso, el tiempo de propagación sería:

$$t_{prop} = \frac{28 \text{ Km}}{3 \cdot 10^5 \left(\frac{\text{Km}}{\text{s}}\right)} = 93.3 \mu\text{s}$$

Si analizamos un poco más la configuración que se ha realizado para controlar este enlace, podemos ver que se ha programado un intervalo de guarda variable ‘**ht-guard-interval = any**’.

```
[admin@b1-santagema] > interface wireless set wlan1 ack-timeout=dynamic
band=5ghz-onlyn frequency=5765 mode=station ssid=BALSA5 disable-running-
check=yes rate-set=configured tx-power=24 tx-power-mode=card-rates disabled=no ht-
extension-channel=disabled ht-guard-interval=any ht-basic-mcs=mcs-15 ht-supported-
mcs=mcs-0,mcs-1,mcs-2,mcs-3, mcs-4,mcs-5,mcs-6,mcs-7,mcs-8,mcs-9,mcs-10,mcs-
11,mcs-12,mcs-13,mcs-14,mcs-15 ht-txchains=0,1 ht-rxchains=0,1
```

Recordemos que el intervalo de guarda equivale a una porción de tiempo en la que se deja de transmitir información para poder canalizar interferencias, como pueden ser las producidas por los efectos multicamino. Los efectos multicamino se traducen en interferencias entre símbolos (ISI, Interferencia Inter Simbólica) y en la consiguiente destrucción de la información.

Como sabemos, el estándar 802.11n permite elegir qué intervalo de guarda queremos, si el largo, que es de **800 ns**, o el corto, que sería de **400 ns**. Con este parámetro configurado a *'any'*, el sistema elige cuál es el adecuado en cada momento. En condiciones donde no existe una elevada probabilidad de interferencias o en escenarios de interiores, nos interesa que el intervalo de guarda sea mínimo, de 400 ns, para poder transmitir el máximo tiempo posible y aumentar, así, la tasa de transferencia de datos.

5.3. Capacidad del enlace

La red de Telemedicina implementada, como hemos descrito en apartados anteriores, está formada por tres enlaces troncales y cuatro de distribución.

Dos de los enlaces troncales, los que enlazan Yurimaguas – San Juan y San Juan – Varadero, están gobernados bajo la tecnología **MIMO (Multiple-Input Multiple-Output) - 2x2**, mientras que el tercero y último enlace troncal, el que enlaza Varadero – Balsapuerto, funciona con tecnología **SISO (Simple-Input Simple-Output, 1x1)**.

Esta dicotomía se debe a que, inicialmente, se iba a establecer sólo un enlace piloto entre las comunidades de Balsapuerto y Varadero.

Por esta razón, se decidió utilizar tecnología SISO para analizar y observar cómo funcionaba en la zona y, posteriormente, se aumentaría la capacidad del enlace agregando tráfico con una antena de doble polaridad (sistema MIMO).

Al sumar dos puntos más a la red, se decidió probar la tecnología MIMO para poder compararla, sobre las mismas condiciones orográficas y climáticas, con la tecnología del enlace piloto.

Como hemos explicado en el capítulo de *'Fundamentos Teóricos'*, la tecnología MIMO aprovecha fenómenos físicos, como la propagación multicamino, para incrementar la tasa de transmisión y reducir la tasa de error. En breves palabras, MIMO aumenta la eficiencia espectral de un sistema de comunicación inalámbrica por medio de la utilización del dominio espacial.

Lo que supone añadir una dimensión espacial adicional es que puede aprovechar la formación de canales estadísticamente independientes originados por el *multitrayecto*⁸ y mitigar el efecto del mismo, consiguiendo un incremento sustancial de la eficiencia espectral.

5.3.1. Enlaces con tecnología MIMO

En nuestro caso, los enlaces implementados con tecnología MIMO nos ofrecen tasas de transferencia de datos mucho mayor de lo que habíamos estimado en el laboratorio.

Como podemos observar, el caudal o *throughput* del enlace MIMO 2x2 desde el Hospital de Santa Gema a San Juan del Armanayacu, supera los 60 Mbps (tráfico UDP) y se encuentra estable en la actualidad.

En este enlace, los equipos están configurados con un intervalo de guarda variable *any* y un índice MCS básico máximo para una tecnología de doble polaridad (*mcs-basic = mcs-15*) y soporta velocidades menores.

Bajo estas condiciones y a corta distancia, se podrían llegar a conseguir 130 Mbps de tasa de transferencia. En nuestro caso (largas distancias) el equipo ha fijado su velocidad automáticamente para funcionar con velocidades menores o iguales a: $MCS = 13 = 104$ Mbps. En la siguiente ilustración se muestra que la velocidad real de funcionamiento varía entre *MCS = 12 y MCS = 13* (78 y 52 Mbps).

Sin embargo, si este enlace fuera variable. Se deberá cambiar su configuración, considerando un índice MCS básico menor y óptimo; y además con velocidades soportadas adecuadas que permitan un enlace sin variaciones.

Realizando un *tool bandwidth-test* sobre el enlace obtenemos los siguientes resultados:

⁸ Multitrayecto: la **propagación multicamino o multitrayecto** hace referencia al hecho de que múltiples versiones de la señal transmitida llegan a la antena receptora desplazadas una respecto de otra en términos de tiempo y de orientación espacial.

Hospital Santa Gema (Yurimaguas) – San Juan del Armanayacu

```

20.22.7.1 64 byte ping: ttl=63 time=17 ms
20.22.7.1 64 byte ping: ttl=63 time=10 ms
20.22.7.1 64 byte ping: ttl=63 time=10 ms
20.22.7.1 64 byte ping: ttl=63 time=10 ms
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 10/11.7/17 ms
[admin@b1-santagema] > tool bandwidth-test 20.20.5.1
status: running
duration: 59s
rx-current: 63.5Mbps
rx-10-second-average: 62.9Mbps
rx-total-average: 59.1Mbps
lost-packets: 65
random-data: no
direction: receive
rx-size: 1500
[Q quit|D dump|C-z pause]

```

Ilustración 48: Throughput del enlace MIMO 2x2 'BALSA5'

```

[admin@b1-santagema] > tool bandwidth-test address=20.22.5.1
status: running
duration: 1m15s
rx-current: 64.8Mbps
rx-10-second-average: 63.1Mbps
rx-total-average: 59.1Mbps
lost-packets: 51
random-data: no
direction: receive
rx-size: 1500

```

Ilustración 49: Throughput del enlace MIMO 2x2 'BALSA5'

Al día de hoy, se realizaron mediciones en diferentes condiciones, días y horarios. Para lograr comprender el comportamiento real de la red.

El resultado de la última medición obtenida desde el repetidor de Santa Gema hasta la interfaz 'wlan3' del repetidor de San Juan (considerando tráfico UDP) se muestra en la [Ilustración 50](#), con un throughput de datos promedio de 74.8 Mbps (dirección = transmisión) y 70.6 Mbps (dirección = recepción).

La [Ilustración 51](#) presenta la medición gráfica de este enlace (dirección = transmisión) con un resultado de throughput de datos promedio ('tx-total-average') igual a 76.4 Mbps:

- ✓ Fecha y hora de las mediciones: 20/05/2012 a las 5 am.
- ✓ Dirección: transmisión y recepción
- ✓ Protocolo: tráfico UDP.
- ✓ Tiempo: 7 minutos.

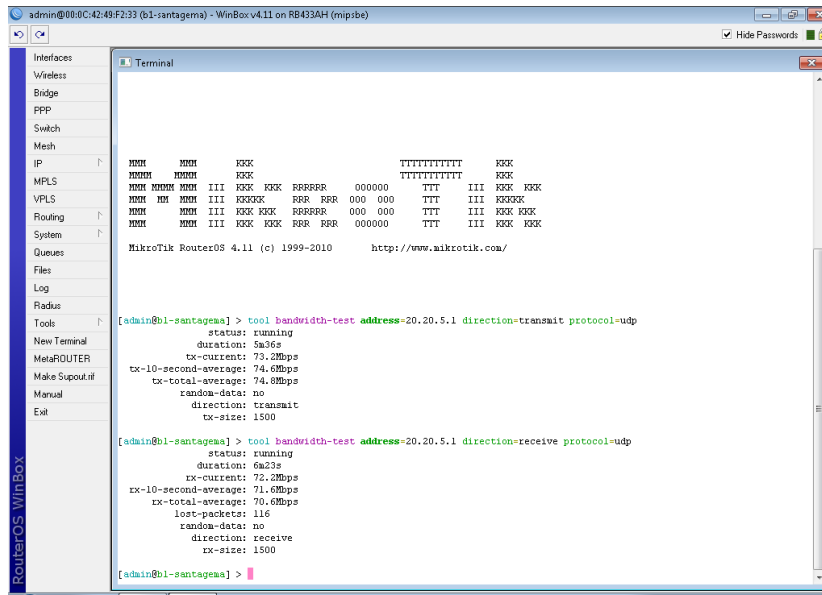


Ilustración 50: Throughput del enlace MIMO 2x2 'BALSA5'

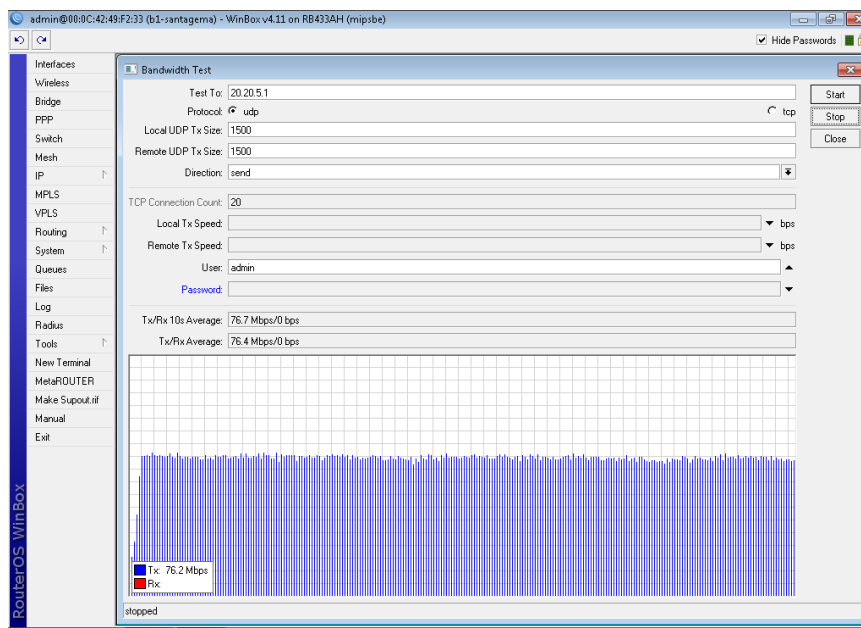


Ilustración 51: Throughput del enlace MIMO 2x2 'BALSA5'

El segundo enlace MIMO 2x2 implementado es, como hemos dicho en varias ocasiones, el que une las comunidades de San Gabriel de Varadero y San Juan del Armanayacu.

Este enlace es de una distancia menor al anterior, la configuración empleada se realizó teniendo en cuenta sus prestaciones, el resultado obtenido es un caudal menos elevado al anterior pero el enlace se encuentra totalmente estable en la actualidad. El resultado obtenido se describe en las siguientes ilustraciones:

San Gabriel de Varadero – San Juan del Armanayacu

```

[admin@bl-varadero] > ping 20.22.1.10
20.22.1.10 ping timeout
2 packets transmitted, 0 packets received, 100% packet loss
[admin@bl-varadero] > ping 20.22.1.3
20.22.1.3 64 byte ping: ttl=62 time=12 ms
20.22.1.3 64 byte ping: ttl=62 time=3 ms
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 3/7.5/12 ms
[admin@bl-varadero] > tool bandwidth-test address=20.22.1.2
status: running
duration: 34m38s
rx-current: 48.4Mbps
rx-10-second-average: 38.4Mbps
rx-total-average: 34.9Mbps
lost-packets: 00
random-data: no
direction: receive
rx-size: 1500
-- [Q quit|D dump|C-z pause]

```

Ilustración 52: Throughput del enlace MIMO 2x2 'Balsa7'

```

[admin@bl-sanjuan] > tool bandwidth-test address=20.20.7.1
status: running
duration: 1m6s
rx-current: 40.4Mbps
rx-10-second-average: 40.3Mbps
rx-total-average: 37.2Mbps
lost-packets: 47
random-data: no
direction: receive
rx-size: 1500

```

Ilustración 53: Throughput del enlace MIMO 2x2 'Balsa7'

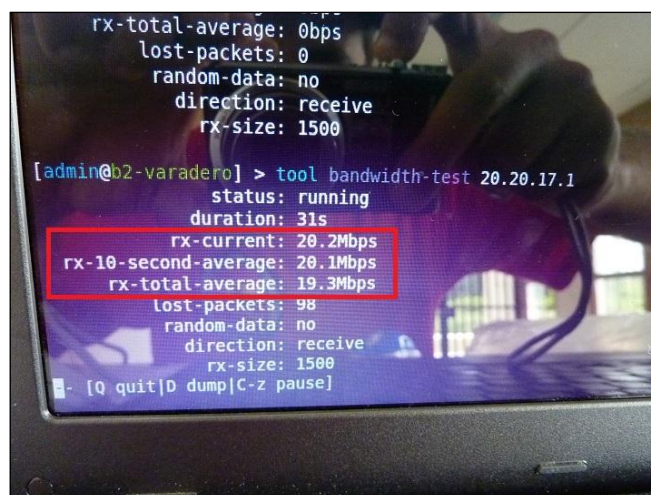
Las peores prestaciones de un enlace son debidos a varios factores, como el canal utilizado y el apuntamiento fino de las antenas.

En la actualidad se siguen haciendo pruebas al respecto. Se pretende cambiar el canal para encontrar uno, dentro de la banda, que funcione libre de interferencias y con una calidad mucho mejor. Algunos canales no funcionan igual en las comunicaciones inalámbricas, debido a la orografía del terreno, a los factores climáticos, etc., por esa razón se deberá elegir uno que permita una calidad óptima y un menor porcentaje de paquetes perdidos.

5.3.2. Enlaces con tecnología SISO

Como hemos explicado antes, el enlace SISO emplea sólo una antena en transmisión y otra en recepción. Aun así, como podemos observar en la figura, conseguimos un caudal de aproximadamente 20 Mbps, dato que nos asegura un funcionamiento estable.

San Gabriel de Varadero – Balsapuerto



```

rx-total-average: 0bps
lost-packets: 0
random-data: no
direction: receive
rx-size: 1500

[admin@b2-varadero] > tool bandwidth-test 20.20.17.1
status: running
duration: 31s
rx-current: 20.2Mbps
rx-10-second-average: 20.1Mbps
rx-total-average: 19.3Mbps
lost-packets: 98
random-data: no
direction: receive
rx-size: 1500
[Q quit|D dump|C-z pause]

```

Ilustración 54: Throughput del enlace SISO 1x1 'BALSA17'

Es importante destacar que con un enlace SISO 802.11n de largas distancias se consigue un *'throughput'* de datos mucho mayor a los obtenidos por el Grupo de Telecomunicaciones Rurales (GTR-PUCP) en otras zonas del país con tecnologías 802.11 a/b/g/n.

5.3.3. Enlaces locales

Para comunicar los clientes finales se utiliza una antena panel (en el caso de Varadero y San Juan), o una antena omnidireccional (en el caso de Santa Gema y Balsapuerto), estas antenas están ubicadas en la cima de la torre de comunicaciones. Todos los clientes finales usan antenas panel de 17 dBi.

Para el caso de los enlaces locales de Varadero y San Juan, son enlaces SISO 802.11n de cortas distancias, en estos enlaces se consigue un *'throughput'* de datos mayor a 100 Mbps. Y también son enlaces totalmente estables (ver [Ilustración 55](#)).

```

[admin@b2-sanjuan] > tool bandwidth-test address=20.23.5.1
status: running
duration: 1m7s
rx-current: 125.6Mbps
rx-10-second-average: 125.4Mbps
rx-total-average: 113.9Mbps
lost-packets: 42
random-data: no
direction: receive
rx-size: 1500

```

Ilustración 55: Throughput del enlace SISO 1x1 'BALSA17'

Este enlace está configurado con un intervalo de guarda mínimo de 400 ns y un índice MCS básico máximo para una tecnología SISO, *'mcs-basic = mcs-7'*.

Además se ha configurado un ancho de banda de 40 Mhz teniendo en cuenta usar canales que no se interfieran entre sí, y la tasa de transferencia se incrementa en valores correspondientes con los especificados en los rangos de velocidad de datos de enlaces 1x1 con 802.11n.

Es importante valorar el uso de un ancho de banda de 40 Mhz ó 20 Mhz para estos enlaces, debido a la interferencia que se puede ocasionar. Se deberá asegurar que no exista ninguna interferencia con los enlaces troncales si se decide utilizar un ancho de banda de 40 Mhz.

Para el caso del enlace local de Santa Gema, son enlaces 802.11a (punto – multipunto), de cortas distancias (máximo 300 metros), en estos enlaces se consigue un *'throughput'* de datos estable, igual a 11 Mbps. También se tiene una conexión con cable UTP, utilizando cable de exteriores apropiado, desde la torre de comunicaciones hasta el local de emergencias de Hospital.

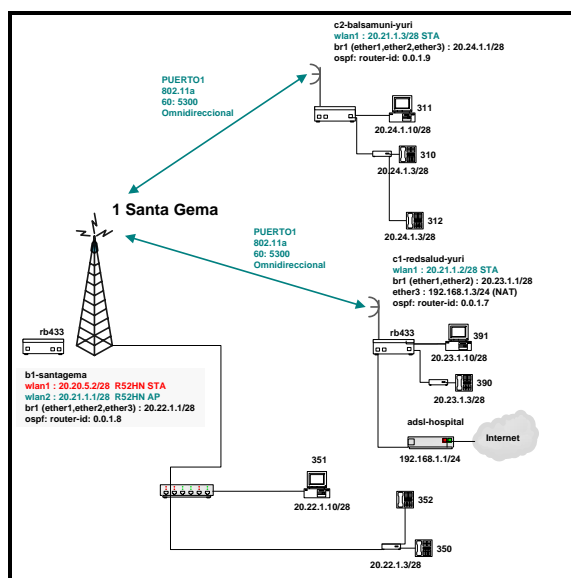


Ilustración 56: Red Local Hospital Santa Gema

En el caso del enlace local de Balsapuerto, la topología es similar al de Santa Gema. La diferencia es que se trata de enlaces 802.11n (punto – multipunto) de cortas distancias, y el *'throughput'* de datos conseguido es mucho mayor.

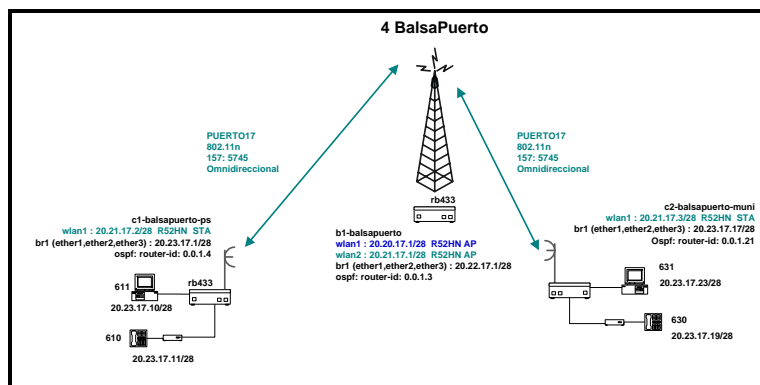


Ilustración 57: Red Local Balsapuerto

5.3.4. Capacidad extremo a extremo

Gracias a la aplicación *iperf*⁹ y *tool bandwidth-test* de Mikrotik, podemos saber la capacidad extremo a extremo de la red.

5.3.4.1. Santa Gema (hospital) a cliente de San Juan

Como se ha comentado antes, se han realizado mediciones en diferentes días y horarios. A continuación se presenta el resultado de la última medición (considerando tráfico UDP) obtenida desde el cliente en el hospital de Santa Gema hasta el cliente en San Juan.

La *Ilustración 58* muestra un *'throughput'* de datos promedio de 60.2 Mbps (dirección = transmisión) y la *Ilustración 59* un *'throughput'* de datos promedio de 60 Mbps (dirección = recepción). Se debe resaltar la importancia de lograr *'throughputs'* (cliente a cliente) superiores a los 60 Mbps considerando un enlace troncal de 29 Kms de distancia y sus clientes.

- ✓ Fecha y hora de las mediciones: 20/05/2012 a las 5 am.
- ✓ Dirección: transmisión y recepción
- ✓ Protocolo: tráfico UDP.
- ✓ Tiempo: 5 minutos.

⁹ *iperf*: *'iperf'* es una aplicación de software que nos permite saber el caudal o *'throughput'* entre dos puntos o extremos de una red

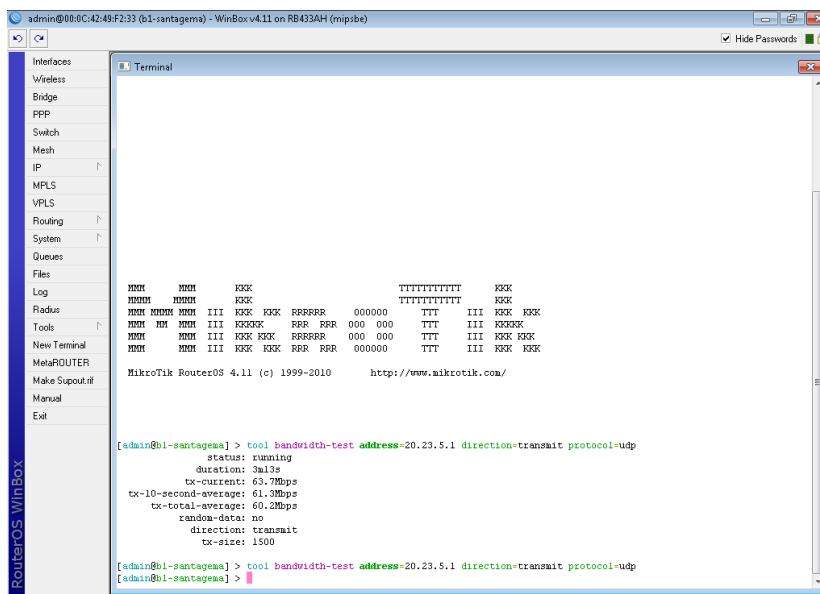


Ilustración 58: Throughput cliente Santa Gema - cliente San Juan (dirección = transmisión)

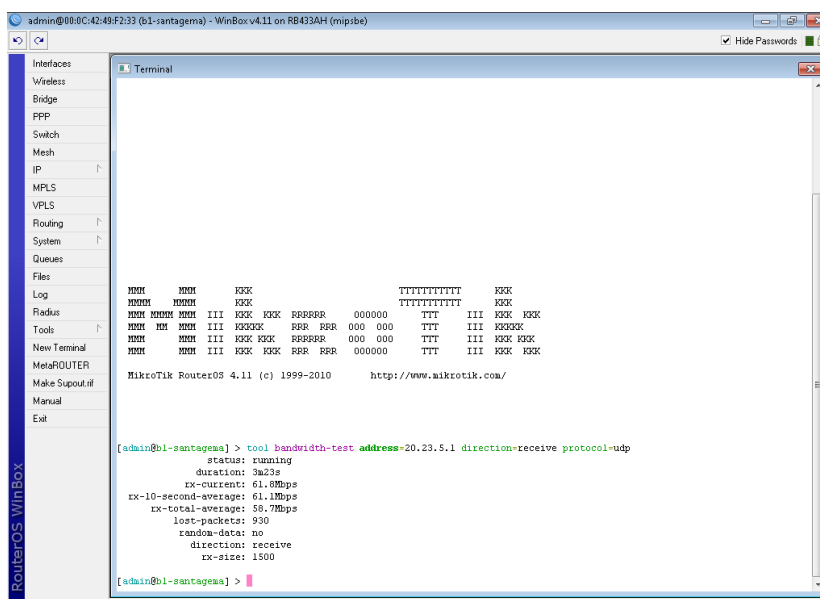


Ilustración 59: Throughput cliente Santa Gema - cliente San Juan (dirección = recepción)

5.3.4.2. Santa Gema (hospital) a cliente de Varadero

A continuación se presenta el resultado de la última medición realizada (considerando tráfico UDP) obtenida desde el cliente en el hospital de Santa Gema hasta el cliente en Varadero.

La *Ilustración 60* muestra un 'throughput' de datos promedio de 12.2 Mbps (dirección = transmisión) y un 'throughput' de datos promedio de 10.2 Mbps (dirección = recepción).

Estos resultados se realizaron luego del cambio de canal (frecuencia del canal = 5765) que realizamos en el enlace de distribución local que comunica al cliente de Varadero por motivo de caída del enlace. Los resultados de estos enlaces son menores a los obtenidos en mediciones anteriores, lo cual nos obliga a hacer una revisión en la planificación de las frecuencias y mejorar su rendimiento:

- ✓ Fecha y hora de las mediciones: 20/05/2012 a las 5 am.
- ✓ Dirección: transmisión y recepción
- ✓ Protocolo: tráfico UDP.
- ✓ Tiempo: 7 minutos.

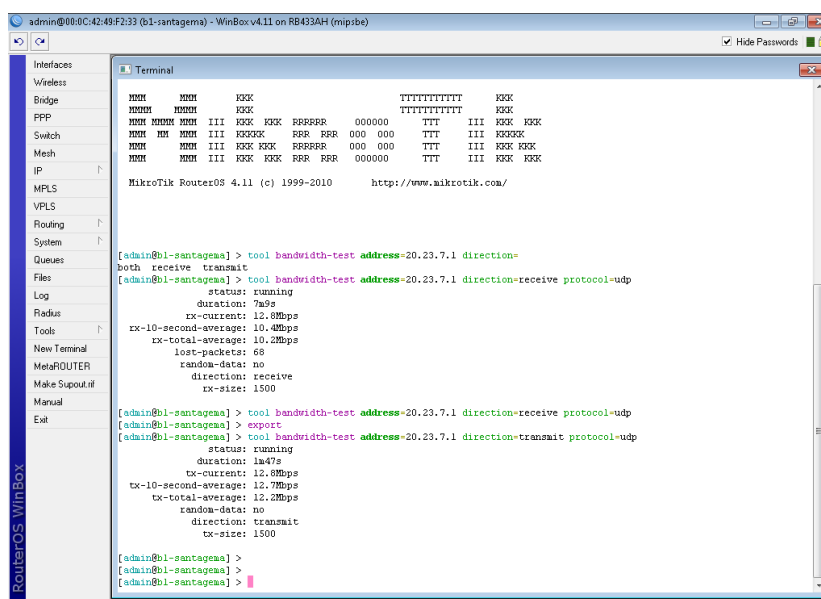


Ilustración 60: Throughput cliente Santa Gema - cliente Varadero

Será necesario mejorar la calidad de los enlaces, eliminando las interferencias, logrando una óptima planificación de frecuencias y las pérdidas de paquetes.

Se deberá ensayar las correcciones en la utilización de los canales. Considerando además la posibilidad de sustituir canales de 40 Mhz por canales de 20 Mhz en los enlaces de distribución local para evitar posibles interferencias.

La *Ilustración 61* muestra los resultados que se obtuvieron en la medición realizada (antes de cambiar el canal) desde el Hospital de Santa Gema hasta el repetidor de Varadero. En esta ilustración se observa un *'throughput'* de datos (tráfico UDP) promedio de 21 Mbps (que aseguraba un *'throughput'* de datos extremo a extremo mayor a los 12 Mbps obtenidos

recientemente), la última medición de estos tramos daba como resultado un *'throughput'* promedio de 14.5 Mbps.

- ✓ Fecha y hora de las mediciones: 12/10/2011 a las 6 pm.
- ✓ Dirección: transmisión
- ✓ Protocolo: tráfico UDP.

```

MMM      MMM      KKK                      TTTTTTTTTT      KKK
MMMM     MMMM     KKK                      TTTTTTTTTT      KKK
MMM MMMM MMM  III  KKK  KKK  RRRRRR      000000      TTT      III  KKK  KKK
MMM MM  MMM  III  KKKKK  RRR  RRR  000  000      TTT      III  KKKKK
MMM      MMM  III  KKK  KKK  RRRRRR      000  000      TTT      III  KKK  KKK
MMM      MMM  III  KKK  KKK  RRR  RRR  000000      TTT      III  KKK  KKK

MikroTik RouterOS 4.11 (c) 1999-2010      http://www.mikrotik.com/

[admin@bl-santagema] >
[admin@bl-santagema] >
[admin@bl-santagema] > tool bandwidth-test address=20.22.7.1
      status: running
      duration: 42s
      rx-current: 21.4Mbps
rx-10-second-average: 21.2Mbps
rx-total-average: 20.6Mbps
      lost-packets: 91
      random-data: no
      direction: receive
      rx-size: 1500
-- [0 quit|D dump|C-z pause]

```

Ilustración 61: Throughput cliente Santa Gema - Repetidor Varadero

5.3.4.3. Santa Gema (hospital) a cliente de Balsapuerto

A continuación se presenta el resultado de la medición realizada (considerando tráfico UDP) obtenida desde el cliente en el hospital de Santa Gema hasta el cliente en Balsapuerto.

Estos enlaces disponen de un enlace *'SISO 1x1'* que comunica el reptidor de Varadero con el repetidor de Balsapuerto. También dispone de un Repetidor de distribución local con una antena omnidireccional que comunica con sus dos clientes.

La *Ilustración 62* muestra un *'throughput'* de datos promedio de 11 Mbps (dirección = transmisión).

- ✓ Fecha y hora de las mediciones: 12/10/2011 a las 6 pm.
- ✓ Dirección: transmisión.

```
-----
MMMM  MMMM  KKK
MMM  MMMM  III  KKK  KKK  RRRRRR  000000  TTT  III  KKK  KKK
MMM  MM  MMM  III  KKKKK  RRR  RRR  000  000  TTT  III  KKKKK
MMM  MMM  III  KKK  KKK  RRRRRR  000  000  TTT  III  KKK  KKK
MMM  MMM  III  KKK  KKK  RRR  RRR  000000  TTT  III  KKK  KKK

MikroTik RouterOS 4.11 (c) 1999-2010      http://www.mikrotik.com/

[admin@bl-santagema] > tool bandwidth-test address=20.23.17.1
      status: running
      duration: 19s
      rx-current: 12.2Mbps
rx-10-second-average: 10.6Mbps
rx-total-average: 10.8Mbps
lost-packets: 13
random-data: no
direction: receive
rx-size: 1500
-- [Q quit|D dump|C-z pause]
```

Ilustración 62: Throughput cliente Santa Gema - cliente Balsapuerto

5.3.4.4. Mediciones de tráfico TCP utilizando la aplicación *iperf*

Si ejecutamos la aplicación *iperf* (considerando tráfico TCP) entre los equipos de videoconferencia del equipo en el Hospital de Santa Gema ubicado en Yurimaguas, y del P.S. San Gabriel de Varadero (“**c1-varadero-ps**”), obtenemos los siguientes resultados:

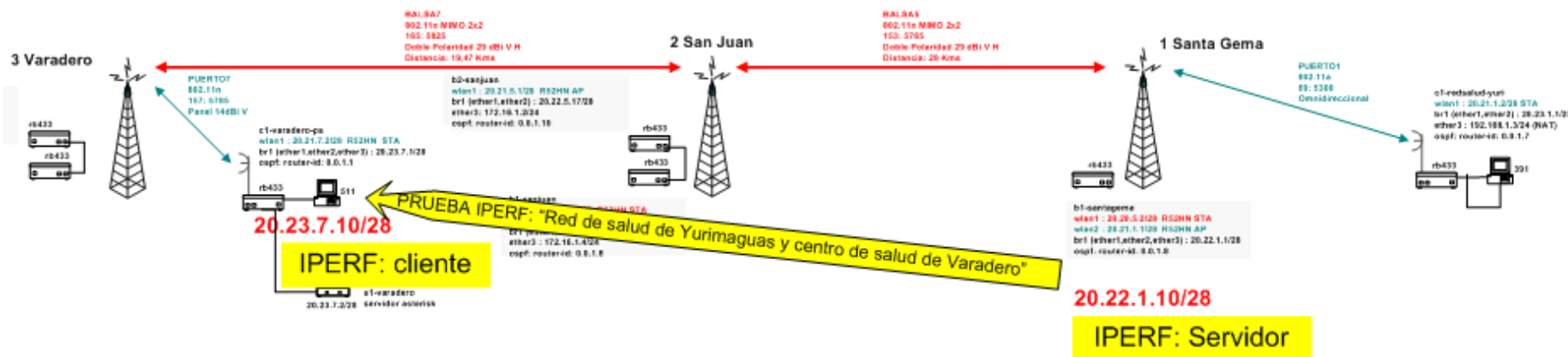
```
root@ubuntu:/home/cdga# iperf -s
-----
Server listening on TCP port 5001
TCP window size: 85.3 KByte (default)
-----
[ 4] local 20.22.1.10 port 5001 connected with 20.23.7.10 port 2545
[ 4] 0.0-30.9 sec 24.24 MBytes 9.44 Mbits/sec
```

```
root@ubuntu:/home/osantos# iperf -c 20.22.1.10 -i 5 -t 30
-----
Client connecting to 20.22.1.10, TCP port 5001
TCP window size: 16.0 KByte (default)
-----
[ 3] local 20.23.7.10 port 2545 connected with 20.22.1.10 port 5001
[ 3] 0.0- 5.0 sec 4.59 MBytes 8.69 Mbits/sec
[ 3] 5.0-10.0 sec 3.82 MBytes 9.41 Mbits/sec
[ 3] 10.0-15.0 sec 4.08 MBytes 9.84 Mbits/sec
[ 3] 15.0-20.0 sec 3.83 MBytes 9.42 Mbits/sec
[ 3] 20.0-25.0 sec 3.83 MBytes 9.42 Mbits/sec
[ 3] 25.0-30.0 sec 4.09 MBytes 9.86 Mbits/sec
[ 3] 0.0-30.3 sec 24.24 MBytes 9.44 Mbits/sec
```

Los resultados mejorarán luego de llevar a cabo la revisión que hemos comentado, para mejorar el rendimiento de estos enlaces.

En el esquema siguiente podemos ver una aproximación gráfica del escenario de medición empleando la herramienta *iperf*:

Prueba de capacidad extremo a extremo entre el cliente del Hospital y el P.S. Varadero



Realizamos ahora un 'iperf' nuevamente desde el equipo en el Hospital de Santa Gema ubicado en Yurimaguas pero ahora hasta el equipo de videoconferencia del C.S. Balsapuerto ("c1-balsapuerto-ps"):

- ✓ Fecha y hora de las mediciones: 12/10/2011 a las 18 pm.
- ✓ Protocolo: tráfico TCP.

```
C:\Windows>iperf -s
-----
Server listening on TCP port 5001
TCP window size: 8.00 KByte (default)
-----
OpenSCManager failed - Acceso denegado. (0x5)
[276] local 20.22.1.10 port 5001 connected with 20.23.17.10 port 53855
[ ID] Interval      Transfer      Bandwidth
[276]  0.0-30.0 sec  27.2 MBytes  7.61 Mbits/sec
```

```
C:\Windows>iperf -c 20.22.1.10 -i 5 -t 30
-----
Client connecting to 20.22.1.10, TCP port 5001
TCP window size: 8.00 KByte (default)
-----
[160] local 20.23.17.10 port 53855 connected with 20.22.1.10 port 5001
[ ID] Interval      Transfer      Bandwidth
[160]  0.0- 5.0 sec   4.49 MBytes   7.54 Mbits/sec
[160]  5.0-10.0 sec  4.84 MBytes   8.11 Mbits/sec
[160] 10.0-15.0 sec  4.85 MBytes   8.14 Mbits/sec
[160] 15.0-20.0 sec  4.49 MBytes   7.54 Mbits/sec
[160] 20.0-25.0 sec  4.55 MBytes   7.63 Mbits/sec
[160] 25.0-30.0 sec  4.02 MBytes   6.74 Mbits/sec
[160]  0.0-30.0 sec  27.2 MBytes   7.61 Mbits/sec
```

Ilustración 63: Medición de capacidad extremo a extremo real de la red (incluyendo el enlace SISO) a través de 'iperf'

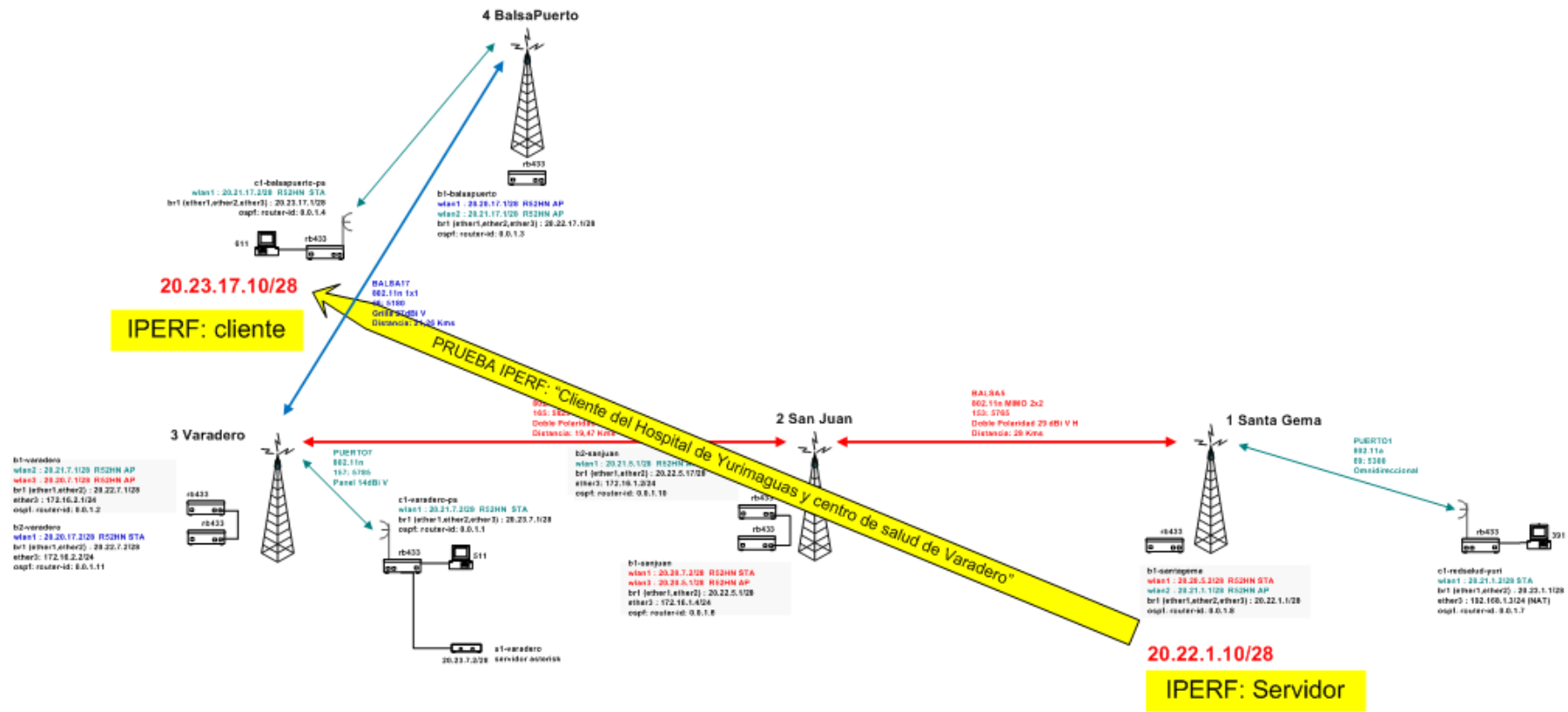
En los repetidores troncales de San Juan y Varadero, se han instalado dos enrutadores inalámbricos en cada repetidor, cada enrutador se une al otro en el mismo repetidor a través de cable de red.

Esta medida es eventual y ha sido debido a un fallo de los equipos que ya ha sido solucionado, posteriormente se procederá a realizar la configuración y la instalación de los equipos para disponer de uno solo enrutador en cada repetidor.

Esta es una de las razones por las que se han obtenido valores de capacidad extremo a extremo debajo de los valores que esta red es capaz de brindar.

A continuación, se observa el diagrama correspondiente a la medición con la herramienta 'iperf':

Prueba de capacidad extremo a extremo entre el hospital Santa Gema y el C.S. Balsapuerto



5.4. Problemas encontrados

Han sido muchos los problemas con los que nos hemos encontrado a la hora de implementar estos enlaces.

Una de las primeras cosas que se ha llevado a cabo, son las pruebas realizadas en corta y larga distancia, para lo cual se ha debido elaborar una plantilla de configuración para las placas ‘Mikrotik’, teniendo en cuenta el uso del estándar 802.11n y la tecnología MIMO; logrando compactar todas sus funciones para optimizar los enlaces correctamente.

De todas maneras, los principales problemas han sido físicos:

- Mal funcionamiento del cableado
- Vulcanización deficiente de los conectores

Una vez solucionados estos problemas físicos, los requisitos principales del éxito han sido las pruebas o ‘tests’ que hemos ido realizando para conseguir:

- El mejor canal de funcionamiento
- Seleccionar los índices MCS adecuados para lograr estabilidad en los enlaces
- Una buena elección del intervalo de guarda

De esta manera, hemos ido observando y analizando cómo funcionan cada uno de esos parámetros, relacionándolos entre ellos y extrayendo lo mejor de cada uno. Los resultados, pese a todos los problemas, han sido y son satisfactorios.

Capítulo VI

Conclusiones

Según el estudio de los resultados obtenidos, se ha logrado que el comportamiento de esta red sea estable.

La tecnología 802.11n con un sistema básico MIMO (2x2) con diversidad de polarización es útil para zonas rurales y para largas distancias, además es una implementación que no se había realizado anteriormente.

El uso de esta tecnología en el diseño e implementación de la red ha permitido comprender algunos aspectos que se deberá tener en cuenta:

- ✓ Se ha podido comprobar que en enlaces de largas distancias, es posible incrementar el *'throughput'* de datos o mejorar la cobertura, con sistemas MIMO; para lo cual será necesario adaptar mejor los transceptores MIMO. Con el propósito de que, utilizando sus diferentes modos, este sistema sea aprovechado lo mejor posible; y finalmente se consiga un aumento de capacidad de transmisión (*'throughput'* de datos), o un mejoramiento del enlace según sea el caso.
- ✓ Esta adaptación o rediseño del trancceptor tiene que tener en cuenta el tipo de zona, con el propósito de mejorar el rendimiento del sistema MIMO. Logrando contrarrestar la pérdida de eficacia en largas distancias.

Lograr *'throughputs'* de más de 60 Mbit/s en enlaces de hasta 30 Km de distancia, es un aspecto importante a tener en cuenta. Sin embargo, en largas distancias se deberá en primer lugar asegurar un funcionamiento óptimo de los enlaces, esto quiere decir que según sus prestaciones, se debe emplear una correcta configuración de los equipos que asegure una estabilidad en su funcionamiento.

La banda de 5.8 GHz no está saturada en comparación a la de 2.4 GHz, pero es muy sensible a los cambios climáticos, hecho que debería ser objeto de estudio en el futuro para poder mitigar esas variaciones que sufren nuestros enlaces bajo precipitaciones incontroladas típicas de climas tropicales.

Estas tasas de transferencias superiores, han permitido dotar Calidad de Servicio (QoS) a la red con mejor eficiencia, además un buen funcionamiento de los servicios de VoIP y Videoconferencia; y también la posibilidad de utilizar en el futuro, diferentes aplicaciones para el servicio de Telemedicina, como son: Sistema de Teleestetoscopia, transmisión de electrocardiogramas digitalizados, imágenes médicas, etc.

El éxito de los resultados ha sido debido a aspectos relevantes, como son: Seguir las recomendaciones para una correcta instalación de los equipos, vulcanización de los dispositivos, una correcta alineación y apuntamiento fino de las antenas.

Documentar este trabajo y los resultados obtenidos tiene como objetivo contribuir en la implementación de redes similares utilizando estos aportes.

Según los resultados logrados hasta el día de hoy, la tecnología WIFI es una solución muy importante y de bajo costo para la comunicación de comunidades aisladas como es el caso del distrito de Balsapuerto, se ha conseguido acercarlos a recursos que siempre han sido imposibles de alcanzar.

Luego de una segunda visita, y después de entrevistar al personal de salud, se pudo comprobar la utilidad de la red. Además, se comprobó un descenso considerable en la tasa de mortalidad.

La telefonía y la videoconferencia contribuyeron con una diagnóstico eficaz en casos graves. Permitiendo una mejor coordinación en el caso del traslado de los pacientes, se posibilitó diagnosticar correctamente casos como por ejemplo, mordedura de serpiente; y se pudo capacitar a distancia a través de la videoconferencia.

La red de Telemedicina de Balsapuerto ha logrado brindar conexión a Internet, servicio de Telefonía IP y Videoconferencia de alta calidad, que ha permitido mejorar el sistema público de asistencia de salud. Este es un buen ejemplo de un uso apropiado de las nuevas Tecnologías de la Información y las Comunicaciones (TIC).

Anexos

Anexo A: Configuración de las Placas MikroTik

1. YURIMAGUAS

1.1. Repetidor Santa Gema (Torre)

Placa Mikrotik Routerboard 433AH – Placa 1 (Torre)

```
*****  
* RouterOS 4.5 *  
*****
```

```
Password  
*****  
[admin@MikroTik] > password  
gtrehasisf
```

```
Nombre de la Placa  
*****  
[admin@MikroTik] > system identity set name=b1-santagema
```

```
Interface Wireless  
*****  
[admin@b1-santagema] > interface wireless security-profiles add name=psk2-ieee  
  
[admin@b1-santagema] > interface wireless security-profiles set psk2-ieee  
authentication-types=wpa2-psk group-ciphers=aes-ccm unicast-ciphers=aes-ccm wpa2-  
pre-shared-key=gtr0ehas0isf mode=dynamic-keys  
[admin@b1-santagema] > interface wireless set wlan1 security-profile=psk2-ieee  
[admin@b1-santagema] > interface wireless set wlan2 security-profile=psk2-ieee  
  
[admin@b1-santagema] > interface wireless set wlan1 ack-timeout=dynamic band=5ghz-  
onlyn frequency=5765 mode=station ssid=BALSA5 disable-running-check=yes rate-  
set=configured tx-power=24 tx-power-mode=card-rates disabled=no ht-extension-  
channel=disabled ht-guard-interval=any ht-basic-mcs=mcs-15 ht-supported-mcs=mcs-  
0,mcs-1,mcs-2,mcs-3, mcs-4,mcs-5,mcs-6,mcs-7,mcs-8,mcs-9,mcs-10,mcs-11,mcs-12,mcs-  
13,mcs-14,mcs-15 ht-txchains=0,1 ht-rxchains=0,1  
  
[admin@b1-santagema] > interface wireless set wlan2 ack-timeout=dynamic antenna-  
mode=ant-a band=5ghz frequency=5300 mode=ap-bridge ssid=PUERTO1 disable-running-  
check=yes basic-rates-a/g=6Mbps supported-rates-a/g=6Mbps,9Mbps,12Mbps,18Mbps rate-  
set=configured tx-power=25 tx-power-mode=card-rates disabled=no
```

```
Direcciones IP  
*****  
[admin@b1-santagema] > interface bridge add name=br1  
[admin@b1-santagema] > interface bridge port add interface=ether1 bridge=br1  
[admin@b1-santagema] > interface bridge port add interface=ether2 bridge=br1  
[admin@b1-santagema] > interface bridge port add interface=ether3 bridge=br1  
  
[admin@b1-santagema] > ip address add address=20.20.5.2/28 interface=wlan1  
[admin@b1-santagema] > ip address add address=20.21.1.1/28 interface=wlan2
```

```
[admin@b1-santagema] > ip address add address=20.22.1.1/28 interface=br1

OSPF
****
[admin@b1-santagema] > routing ospf instance set router-id=0.0.1.8 metric-
default=10 metric-connected=10 metric-static=10 metric-rip=0 metric-bgp=0
redistribute-connected=as-type-1 redistribute-static=as-type-1 distribute-
default=if-installed-as-type-1 numbers=0

[admin@b1-santagema] > routing ospf network add network=20.20.5.0/28 area=backbone
[admin@b1-santagema] > routing ospf network add network=20.21.1.0/28 area=backbone

[admin@b1-santagema] > routing ospf interface add interface=wlan1 cost=10
[admin@b1-santagema] > routing ospf interface add interface=wlan2 cost=10
```

1.2. Cliente: Oficina de coordinación de la Municipalidad de Balsapuerto

Placa Mikrotik Routerboard 433

```
*****
* RouterOS 4.5 *
*****

Password
*****
[admin@MikroTik] > password
gtrehasisf

Nombre de la Placa
*****
[admin@MikroTik] > system identity set name=c2-balsamuni-yuri

Interface Wireless
*****
[admin@c2-balsamuni-yuri] > interface wireless security-profiles add name=psk2-ieee

[admin@c2-balsamuni-yuri] > interface wireless security-profiles set psk2-ieee
authentication-types=wpa2-psk group-ciphers=aes-ccm unicast-ciphers=aes-ccm wpa2-
pre-shared-key=gtr0ehas0isf mode=dynamic-keys
[admin@c2-balsamuni-yuri] > interface wireless set wlan1 security-profile=psk2-ieee

[admin@c2-balsamuni-yuri] > interface wireless set wlan1 ack-timeout=dynamic
antenna-mode=ant-a band=5ghz frequency=5300 mode=station ssid=PUERTO1 disable-
running-check=yes basic-rates-a/g=6Mbps supported-rates-
a/g=6Mbps, 9Mbps, 12Mbps, 18Mbps rate-set=configured tx-power=23 tx-power-mode=card-
rates disabled=no

Direcciones IP
*****
[admin@c2-balsamuni-yuri] > interface bridge add name=br1
[admin@c2-balsamuni-yuri] > interface bridge port add interface=ether1 bridge=br1
[admin@c2-balsamuni-yuri] > interface bridge port add interface=ether2 bridge=br1
[admin@c2-balsamuni-yuri] > interface bridge port add interface=ether3 bridge=br1
[admin@c2-balsamuni-yuri] > ip address add address=20.21.1.3/28 interface=wlan1
[admin@c2-balsamuni-yuri] > ip address add address=20.24.1.1/28 interface=br1

OSPF
****
```

```
[admin@c2-balsamuni-yuri] > routing ospf instance set router-id=0.0.1.9 metric-
default=10 metric-connected=10 metric-static=10 metric-rip=0 metric-bgp=0
redistribute-connected=as-type-1 redistribute-static=as-type-1 distribute-default=
if-installed-as-type-1 numbers=0

[admin@c2-balsamuni-yuri] > routing ospf network add network=20.21.1.0/28
area=backbone

[admin@c2-balsamuni-yuri] > routing ospf interface add interface=wlan1 cost=10
```

1.3. Cliente: Red de Salud de Alto Amazonas

Placa Mikrotik Routerboard 433

```
*****
* RouterOS 4.5 *
*****
```

```
Password
*****
[admin@MikroTik] > password
gtr0ehasisf
```

```
Nombre de la Placa
*****
[admin@MikroTik] > system identity set name= c1-redsalud-yuri
```

```
Interface Wireless
*****
[admin@c1-redsalud-yuri] > interface wireless security-profiles add name=psk2-ieee

[admin@c1-redsalud-yuri] > interface wireless security-profiles set psk2-ieee
authentication-types=wpa2-psk group-ciphers=aes-ccm unicast-ciphers=aes-ccm wpa2-
pre-shared-key=gtr0ehasisf mode=dynamic-keys
[admin@c1-redsalud-yuri] > interface wireless set wlan1 security-profile=psk2-ieee

[admin@c1-redsalud-yuri] > interface wireless set wlan1 ack-timeout=dynamic
antenna-mode=ant-a band=5ghz frequency=5300 mode=station ssid=PUERTO1 disable-
running-check=yes basic-rates-a/g=6Mbps supported-rates-
a/g=6Mbps,9Mbps,12Mbps,18Mbps rate-set=configured tx-power=25 tx-power-mode=card-
rates disabled=no
```

```
Direcciones IP
*****
[admin@c1-redsalud-yuri] > interface bridge add name=br1
[admin@c1-redsalud-yuri] > interface bridge port add interface=ether1 bridge=br1
[admin@c1-redsalud-yuri] > interface bridge port add interface=ether2 bridge=br1
[admin@c1-redsalud-yuri] > ip address add address=20.21.1.2/28 interface=wlan1
[admin@c1-redsalud-yuri] > ip address add address=192.168.1.2/24 interface=ether3
[admin@c1-redsalud-yuri] > ip address add address=20.23.1.1/28 interface=br1
```

```
OSPF
****
[admin@c1-redsalud-yuri] > routing ospf instance set router-id=0.0.1.7 metric-
default=10 metric-connected=10 metric-static=10 metric-rip=0 metric-bgp=0
redistribute-connected=as-type-1 redistribute-static=as-type-1 distribute-
default=always-as-type-1 numbers=0

[admin@c1-redsalud-yuri] > routing ospf network add network=20.21.1.0/28
area=backbone
```

```
[admin@c1-redsalud-yuri] > routing ospf interface add interface=wlan1 cost=10
```

```
Rutas  
*****
```

```
[admin@c1-redsalud-yuri] > ip route add gateway=192.168.1.1
```

2. SAN JUAN

2.1. Repetidor San Juan (Torre)

Placa Mikrotik Routerboard 433AH – Placa 1 (Torre)

```
*****  
* RouterOS 4.5 *  
*****
```

```
Password  
*****  
[admin@MikroTik] > password  
gtrehasisf
```

```
Nombre de la Placa  
*****  
[admin@MikroTik] > system identity set name=b1-sanjuan
```

```
Interface Wireless  
*****  
[admin@b1-sanjuan] > interface wireless security-profiles add name=psk2-ieee  
  
[admin@b1-sanjuan] > interface wireless security-profiles set psk2-ieee  
authentication-types=wpa2-psk group-ciphers=aes-ccm unicast-ciphers=aes-ccm wpa2-  
pre-shared-key=gtr0ehas0isf mode=dynamic-keys  
[admin@b1-sanjuan] > interface wireless set wlan1 security-profile=psk2-ieee  
[admin@b1-sanjuan] > interface wireless set wlan3 security-profile=psk2-ieee  
  
[admin@b1-sanjuan] > interface wireless set wlan1 ack-timeout=dynamic band=5ghz-  
onlyn frequency=5825 mode=ap-bridge ssid=BALSA7 disable-running-check=yes rate-  
set=configured tx-power=24 tx-power-mode=card-rates disabled=no ht-extension-  
channel=disabled ht-guard-interval=long ht-basic-mcs=mcs-8 ht-supported-mcs=mcs-  
0,mcs-1,mcs-2,mcs-3, mcs-4,mcs-5,mcs-6,mcs-7,mcs-8 ht-txchains=0,1 ht-rxchains=0,1  
  
[admin@b1-sanjuan] > interface wireless set wlan3 ack-timeout=dynamic band=5ghz-  
onlyn frequency=5765 mode=ap-bridge ssid=BALSA5 disable-running-check=yes rate-  
set=configured tx-power=24 tx-power-mode=card-rates disabled=no ht-extension-  
channel=disabled ht-guard-interval=any ht-basic-mcs=mcs-15 ht-supported-mcs=mcs-  
0,mcs-1,mcs-2,mcs-3, mcs-4,mcs-5,mcs-6,mcs-7,mcs-8,mcs-9,mcs-10,mcs-11,mcs-12,mcs-  
13,mcs-14,mcs-15 ht-txchains=0,1 ht-rxchains=0,1
```

```
Direcciones IP  
*****  
[admin@b1-sanjuan] > interface bridge add name=br1  
[admin@b1-sanjuan] > interface bridge port add interface=ether1 bridge=br1  
[admin@b1-sanjuan] > interface bridge port add interface=ether2 bridge=br1
```

```
[admin@b1-sanjuan] > ip address add address=20.20.7.2/28 interface=wlan1  
[admin@b1-sanjuan] > ip address add address=20.20.5.1/28 interface=wlan3  
[admin@b1-sanjuan] > ip address add address=172.16.1.4/24 interface=ether3
```

Configuración de las placas Mikrotik

```
[admin@b1-sanjuan] > ip address add address=20.22.5.1/28 interface=br1

OSPF
****
[admin@b1-sanjuan] > routing ospf instance set router-id=0.0.1.6 metric-default=10
metric-connected=10 metric-static=10 metric-rip=0 metric-bgp=0 redistribute-
connected=as-type-1 redistribute-static=as-type-1 distribute-default=if-installed-
as-type-1 numbers=0

[admin@b1-sanjuan] > routing ospf network add network=20.20.7.0/28 area=backbone
[admin@b1-sanjuan] > routing ospf network add network=20.20.5.0/28 area=backbone

[admin@b1-sanjuan] > routing ospf interface add interface=wlan1 cost=10
[admin@b1-sanjuan] > routing ospf interface add interface=wlan3 cost=10
```

Placa Mikrotik Routerboard 433AH – Placa 2 (Torre)

```
*****
* RouterOS 4.5 *
*****

Password
*****
[admin@MikroTik] > password
gtrehasisf

Nombre de la Placa
*****
[admin@MikroTik] > system identity set name=b2-sanjuan

Interface Wireless
*****
[admin@b2-sanjuan] > interface wireless security-profiles add name=psk2-ieee

[admin@b2-sanjuan] > interface wireless security-profiles set psk2-ieee
authentication-types=wpa2-psk group-ciphers=aes-ccm unicast-ciphers=aes-ccm wpa2-
pre-shared-key=gtr0ehas0isf mode=dynamic-keys
[admin@b2-sanjuan] > interface wireless set wlan1 security-profile=psk2-ieee

[admin@b2-sanjuan] > interface wireless set wlan1 ack-timeout=dynamic antenna-
mode=ant-a band=5ghz-onlyn frequency=5785 mode=ap-bridge ssid=PUERTO5 disable-
running-check=yes rate-set=configured tx-power=17 tx-power-mode=card-rates
disabled=no ht-extension-channel=disabled ht-guard-interval=long ht-basic-mcs=mcs-0
ht-supported-mcs=mcs-0,mcs-1,mcs-2,mcs-3

Direcciones IP
*****
[admin@b2-sanjuan] > interface bridge add name=br1
[admin@b2-sanjuan] > interface bridge port add interface=ether1 bridge=br1
[admin@b2-sanjuan] > interface bridge port add interface=ether2 bridge=br1
[admin@b2-sanjuan] > ip address add address=20.21.5.1/28 interface=wlan1
[admin@b2-sanjuan] > ip address add address=172.16.1.2/24 interface=ether3
[admin@b2-sanjuan] > ip address add address=20.22.5.17/28 interface=br1

OSPF
****
[admin@b2-sanjuan] > routing ospf instance set router-id=0.0.1.10 metric-default=10
metric-connected=10 metric-static=10 metric-rip=0 metric-bgp=0 redistribute-
```

```
connected=as-type-1 redistribute-static=as-type-1 distribute-default=if-installed-
as-type-1 numbers=0
```

```
[admin@b2-sanjuan] > routing ospf network add network=20.21.5.0/28 area=backbone
[admin@b2-sanjuan] > routing ospf network add network=172.16.1.0/24 area=backbone
```

```
[admin@b2-sanjuan] > routing ospf interface add interface=wlan1 cost=10
[admin@b2-sanjuan] > routing ospf interface add interface=ether3 cost=10
```

2.2. Cliente: Puesto de Salud de San Juan

Placa Mikrotik Routerboard 433 – Placa 1

```
*****
* RouterOS 4.5 *
*****
```

```
Password
*****
[admin@MikroTik] > password
gtrehasisf
```

```
Nombre de la Placa
*****
[admin@MikroTik] > system identity set name=c1-sanjuan-ps
```

```
Interface Wireless
*****
[admin@c1-sanjuan-ps] > interface wireless security-profiles add name=psk2-ieee

[admin@c1-sanjuan-ps] > interface wireless security-profiles set psk2-ieee
authentication-types=wpa2-psk group-ciphers=aes-ccm unicast-ciphers=aes-ccm wpa2-
pre-shared-key=gtr0ehas0isf mode=dynamic-keys
[admin@c1-sanjuan-ps] > interface wireless set wlan1 security-profile=psk2-ieee

[admin@c1-sanjuan-ps] > interface wireless set wlan1 ack-timeout=dynamic antenna-
mode=ant-a band=5ghz-onlyn frequency=5785 mode=ap-bridge ssid=PUERTO5 disable-
running-check=yes rate-set=configured tx-power=17 tx-power-mode=card-rates
disabled=no ht-extension-channel=disabled ht-guard-interval=long ht-basic-mcs=mcs-0
ht-supported-mcs=mcs-0,mcs-1,mcs-2,mcs-3
```

```
Direcciones IP
*****
[admin@c1-sanjuan-ps] > interface bridge add name=br1
[admin@c1-sanjuan-ps] > interface bridge port add interface=ether1 bridge=br1
[admin@c1-sanjuan-ps] > interface bridge port add interface=ether2 bridge=br1
[admin@c1-sanjuan-ps] > interface bridge port add interface=ether3 bridge=br1
[admin@c1-sanjuan-ps] > ip address add address=20.21.5.2/28 interface=wlan1
[admin@c1-sanjuan-ps] > ip address add address=20.23.5.1/28 interface=br1
```

```
OSPF
****
[admin@c1-sanjuan-ps] > routing ospf instance set router-id=0.0.1.5 metric-
default=10 metric-connected=10 metric-static=10 metric-rip=0 metric-bgp=0
redistribute-connected=as-type-1 redistribute-static=as-type-1 distribute-
default=if-installed-as-type-1 numbers=0
```

```
[admin@c1-sanjuan-ps] > routing ospf network add network=20.21.5.0/28 area=backbone
```



```
[admin@c1-sanjuan-ps] > routing ospf network add network=20.23.5.0/28 area=backbone
```

```
[admin@c1-sanjuan-ps] > routing ospf interface add interface=wlan1 cost=10
```

3. VARADERO

3.1. Repetidor Varadero (Torre)

Placa Mikrotik Routerboard 433AH – Placa 1

```
*****  
* RouterOS 4.5 *  
*****
```

Password

```
*****
```

```
[admin@MikroTik] > password  
gtrehasisf
```

Nombre de la Placa

```
*****
```

```
[admin@MikroTik] > system identity set name=b1-varadero
```

Interface Wireless

```
*****
```

```
[admin@b1-varadero] > interface wireless security-profiles add name=psk2-ieee
```

```
[admin@b1-varadero] > interface wireless security-profiles set psk2-ieee  
authentication-types=wpa2-psk group-ciphers=aes-ccm unicast-ciphers=aes-ccm wpa2-  
pre-shared-key=gtr0ehas0isf mode=dynamic-keys
```

```
[admin@b1-varadero] > interface wireless set wlan2 security-profile=psk2-ieee
```

```
[admin@b1-varadero] > interface wireless set wlan3 security-profile=psk2-ieee
```

```
[admin@b1-varadero] > interface wireless set wlan2 ack-timeout=dynamic antenna-  
mode=ant-a band=5ghz-onlyn frequency=5765 mode=ap-bridge ssid=PUERTO7 disable-  
running-check=yes rate-set=configured tx-power=17 tx-power-mode=card-rates  
disabled=no ht-extension-channel=above-control ht-guard-interval=any ht-basic-  
mcs=mcs-0 ht-supported-mcs=mcs-0,mcs-1,mcs-2,mcs-3
```

```
[admin@b1-varadero] > interface wireless set wlan3 ack-timeout=dynamic band=5ghz-  
onlyn frequency=5825 mode=station ssid=BALSA7 disable-running-check=yes rate-  
set=configured tx-power=24 tx-power-mode=card-rates disabled=no ht-extension-  
channel=disabled ht-guard-interval=long ht-basic-mcs=mcs-8 ht-supported-mcs=mcs-  
0,mcs-1,mcs-2,mcs-3, mcs-4,mcs-5,mcs-6,mcs-7,mcs-8 ht-txchains=0,1 ht-rxchains=0,1
```

Direcciones IP

```
*****
```

```
[admin@b1-varadero] > interface bridge add name=br1
```

```
[admin@b1-varadero] > interface bridge port add interface=ether1 bridge=br1
```

```
[admin@b1-varadero] > interface bridge port add interface=ether2 bridge=br1
```

```
[admin@b1-varadero] > ip address add address=20.21.7.1/28 interface=wlan2
```

```
[admin@b1-varadero] > ip address add address=20.20.7.1/28 interface=wlan3
```

```
[admin@b1-varadero] > ip address add address=172.16.2.1/24 interface=ether3
```

```
[admin@b1-varadero] > ip address add address=20.22.7.1/28 interface=br1
```

```
OSPF
****
[admin@b1-varadero] > routing ospf instance set router-id=0.0.1.2 metric-default=10
metric-connected=10 metric-static=10 metric-rip=0 metric-bgp=0 redistribute-
connected=as-type-1 redistribute-static=as-type-1 distribute-default=if-installed-
as-type-1 numbers=0

[admin@b1-varadero] > routing ospf network add network=20.21.7.0/28 area=backbone
[admin@b1-varadero] > routing ospf network add network=20.20.7.0/28 area=backbone
[admin@b1-varadero] > routing ospf network add network=172.16.2.0/24 area=backbone

[admin@b1-varadero] > routing ospf interface add interface=wlan2 cost=10
[admin@b1-varadero] > routing ospf interface add interface=wlan3 cost=10
[admin@b1-varadero] > routing ospf interface add interface=ether3 cost=10
```

Placa Mikrotik Routerboard 433AH – Placa 2 (Torre)

```
*****
* RouterOS 4.5 *
*****

Password
*****
[admin@MikroTik] > password
gtrehasisf

Nombre de la Placa
*****
[admin@MikroTik] > system identity set name=b2-varadero

Interface Wireless
*****
[admin@b2-varadero] > interface wireless security-profiles add name=psk2-ieee

[admin@b2-varadero] > interface wireless security-profiles set psk2-ieee
authentication-types=wpa2-psk group-ciphers=aes-ccm unicast-ciphers=aes-ccm wpa2-
pre-shared-key=gtr0ehas0isf mode=dynamic-keys
[admin@b2-varadero] > interface wireless set wlan1 security-profile=psk2-ieee

[admin@b2-varadero] > interface wireless set wlan1 ack-timeout=dynamic antenna-
mode=ant-a band=5ghz-onlyn frequency=5180 mode=station ssid=BALSA17 disable-
running-check=yes rate-set=configured tx-power=24 tx-power-mode=card-rates
disabled=no ht-extension-channel=disabled ht-guard-interval=long ht-basic-mcs=mcs-0
ht-supported-mcs=mcs-0,mcs-1,mcs-2,mcs-3

Direcciones IP
*****
[admin@b2-varadero] > interface bridge add name=br1
[admin@b2-varadero] > interface bridge port add interface=ether1 bridge=br1
[admin@b2-varadero] > interface bridge port add interface=ether2 bridge=br1
[admin@b2-varadero] > ip address add address=20.20.17.2/28 interface=wlan1
[admin@b2-varadero] > ip address add address=172.16.2.2/24 interface=ether3
[admin@b2-varadero] > ip address add address=20.22.7.2/28 interface=br1

OSPF
****
[admin@b2-varadero] > routing ospf instance set router-id=0.0.1.11 metric-
default=10 metric-connected=10 metric-static=10 metric-rip=0 metric-bgp=0
redistribute-connected=as-type-1 redistribute-static=as-type-1 distribute-
default=if-installed-as-type-1 numbers=0
```

```
[admin@b2-varadero] > routing ospf network add network=20.20.17.0/28 area=backbone
[admin@b2-varadero] > routing ospf network add network=172.16.2.0/24 area=backbone

[admin@b2-varadero] > routing ospf interface add interface=wlan1 cost=10
[admin@b2-varadero] > routing ospf interface add interface=ether3 cost=10
```

3.2. Cliente: Puesto de Salud de Varadero

Placa Mikrotik Routerboard 433 – Placa 1

```
<*****
* RouterOS 4.5 *
*****
```

```
Password
*****
```

```
[admin@MikroTik] > password
gtrehasisf
```

```
Nombre de la Placa
*****
```

```
[admin@MikroTik] > system identity set name=c1-varadero-ps
```

```
Interface Wireless
*****
```

```
[admin@c1-varadero-ps] > interface wireless security-profiles add name=psk2-ieee
```

```
[admin@c1-varadero-ps] > interface wireless security-profiles set psk2-ieee
authentication-types=wpa2-psk group-ciphers=aes-ccm unicast-ciphers=aes-ccm wpa2-
pre-shared-key=gtr0ehas0isf mode=dynamic-keys
```

```
[admin@c1-varadero-ps] > interface wireless set wlan1 security-profile=psk2-ieee
```

```
[admin@c1-varadero-ps] > interface wireless set wlan1 ack-timeout=dynamic antenna-
mode=ant-a band=5ghz-onlyn frequency=5765 mode=station ssid=PUERTO7 disable-
running-check=yes rate-set=configured tx-power=17 tx-power-mode=card-rates
disabled=no ht-extension-channel=above-control ht-guard-interval=any ht-basic-
mcs=mcs-0 ht-supported-mcs=mcs-0,mcs-1,mcs-2,mcs-3
```

```
Direcciones IP
*****
```

```
[admin@c1-varadero-ps] > interface bridge add name=br1
```

```
[admin@c1-varadero-ps] > interface bridge port add interface=ether1 bridge=br1
```

```
[admin@c1-varadero-ps] > interface bridge port add interface=ether2 bridge=br1
```

```
[admin@c1-varadero-ps] > interface bridge port add interface=ether3 bridge=br1
```

```
[admin@c1-varadero-ps] > ip address add address=20.21.7.2/28 interface=wlan1
```

```
[admin@c1-varadero-ps] > ip address add address=20.23.7.1/28 interface=br1
```

```
OSPF
****
```

```
[admin@c1-varadero-ps] > routing ospf instance set router-id=0.0.1.1 metric-
default=10 metric-connected=10 metric-static=10 metric-rip=0 metric-bgp=0
redistribute-connected=as-type-1 redistribute-static=as-type-1 distribute-
default=if-installed-as-type-1 numbers=0
```

```
[admin@c1-varadero-ps] > routing ospf network add network=20.21.7.0/28 area=backbone
```

```
[admin@c1-varadero-ps] > routing ospf network add network=20.23.7.0/28
area=backbone
```

```
[admin@c1-varadero-ps] > routing ospf interface add interface=wlan1 cost=10
```

3.3. Servidor Asterisk

a) Configuración ASTERIX

```
s1-varadero:~# cat /etc/default/asterisk  
RUNASTERISK=yes
```

b) Configuración ASTERIX - SIP.CONF

```
s1-varadero:~# cat /etc/asterisk/sip.conf  
#####  
; sip.conf  
#####  
;  
[general]  
;  
;tos=0xb8  
bindport=5060  
disallow=all  
allow=gsm  
allow=g726aal2  
allow=ulaw  
allow=alaw  
;allow=g729a  
;allow=g722.1/C  
;  
;[360]  
;type=friend  
;host=dynamic  
;language=es  
;context=center  
;secret=passwd  
;username=360  
;callerid=360  
;fromuser=<360>  
;dtmfmode=rfc2833  
;videosupport=yes  
;allow=h261  
;allow=h263  
;allow=h263p  
;allow=h264  
;maxcallbitrate=2048  
;qualify=yes  
;  
[610]  
type=friend  
host=dynamic  
language=es  
context=center  
secret=passwd  
username=610  
callerid=610  
;fromuser=<610>  
dtmfmode=rfc2833  
;videosupport=yes  
;allow=h261  
;allow=h263  
;allow=h263p  
;allow=h264  
;maxcallbitrate=2048  
qualify=yes
```

```
;  
[611]  
type=friend  
host=dynamic  
language=es  
context=center  
secret=passwd  
username=611  
callerid=611  
;fromuser=<611>  
dtmfmode=rfc2833  
videosupport=yes  
;allow=h261  
allow=h263  
allow=h263p  
allow=h264  
maxcallbitrate=2048  
qualify=yes  
;  
[612]  
type=friend  
host=dynamic  
language=es  
context=center  
secret=passwd  
username=612  
callerid=612  
;fromuser=<612>  
dtmfmode=rfc2833  
videosupport=yes  
;allow=h261  
allow=h263  
allow=h263p  
allow=h264  
maxcallbitrate=2048  
qualify=yes  
;  
[630]  
type=friend  
host=dynamic  
language=es  
context=center  
secret=passwd  
username=630  
callerid=630  
;fromuser=<630>  
dtmfmode=rfc2833  
videosupport=yes  
;allow=h261  
allow=h263  
allow=h263p  
allow=h264  
maxcallbitrate=2048  
qualify=yes  
;  
[631]  
type=friend  
host=dynamic  
language=es  
context=center  
secret=passwd  
username=631  
callerid=631  
;fromuser=<631>  
dtmfmode=rfc2833  
videosupport=yes  
;allow=h261`  
allow=h263
```

```
allow=h263p
allow=h264
maxcallbitrate=2048
qualify=yes
;
[632]
type=friend
host=dynamic
language=es
context=center
secret=passwd
username=632
callerid=632
;fromuser=<632>
dtmfmode=rfc2833
videosupport=yes
;allow=h261
allow=h263
allow=h263p
allow=h264
maxcallbitrate=2048
qualify=yes
;
[510]
type=friend
host=dynamic
language=es
context=center
secret=passwd
username=510
callerid=510
;fromuser=<510>
dtmfmode=rfc2833
videosupport=yes
;allow=h261
allow=h263
allow=h263p
allow=h264
maxcallbitrate=2048
qualify=yes
;
[511]
type=friend
host=dynamic
language=es
context=center
secret=passwd
username=511
callerid=511
;fromuser=<511>
dtmfmode=rfc2833
videosupport=yes
;allow=h261
allow=h263
allow=h263p
allow=h264
maxcallbitrate=2048
qualify=yes
;
[512]
type=friend
host=dynamic
language=es
context=center
secret=passwd
username=512
callerid=512
;fromuser=<512>
```

```
dtmfmode=rfc2833
videosupport=yes
;allow=h261
allow=h263
allow=h263p
allow=h264
maxcallbitrate=2048
qualify=yes
;
[530]
type=friend
host=dynamic
language=es
context=center
secret=passwd
username=530
callerid=530
;fromuser=<530>
dtmfmode=rfc2833
videosupport=yes
;allow=h261
allow=h263
allow=h263p
allow=h264
maxcallbitrate=2048
qualify=yes
;
[531]
type=friend
host=dynamic
language=es
context=center
secret=passwd
username=531
callerid=531
;fromuser=<531>
dtmfmode=rfc2833
videosupport=yes
;allow=h261
allow=h263
allow=h263p
allow=h264
maxcallbitrate=2048
qualify=yes
;
[532]
type=friend
host=dynamic
language=es
context=center
secret=passwd
username=532
callerid=532
;fromuser=<532>
dtmfmode=rfc2833
videosupport=yes
;allow=h261
allow=h263
allow=h263p
allow=h264
maxcallbitrate=2048
qualify=yes
;
[470]
type=friend
host=dynamic
language=es
context=center
```

```
secret=passwd
username=470
callerid=470
;fromuser=<470>
dtmfmode=rfc2833
videosupport=yes
;allow=h261
allow=h263
allow=h263p
allow=h264
maxcallbitrate=2048
qualify=yes
;
[471]
type=friend
host=dynamic
language=es
context=center
secret=passwd
username=471
callerid=471
;fromuser=<471>
dtmfmode=rfc2833
videosupport=yes
;allow=h261
allow=h263
allow=h263p
allow=h264
maxcallbitrate=2048
qualify=yes
;
[472]
type=friend
host=dynamic
language=es
context=center
secret=passwd
username=472
callerid=472
;fromuser=<472>
dtmfmode=rfc2833
videosupport=yes
;allow=h261
allow=h263
allow=h263p
allow=h264
maxcallbitrate=2048
qualify=yes
;
[390]
type=friend
host=dynamic
language=es
context=center
secret=passwd
username=390
callerid=390
;fromuser=<390>
dtmfmode=rfc2833
videosupport=yes
;allow=h261
allow=h263
allow=h263p
allow=h264
maxcallbitrate=2048
qualify=yes
;
[391]
```



```
type=friend
host=dynamic
language=es
context=center
secret=passwd
username=391
callerid=391
;fromuser=<391>
dtmfmode=rfc2833
videosupport=yes
;allow=h261
allow=h263
allow=h263p
allow=h264
maxcallbitrate=2048
qualify=yes
;
[392]
type=friend
host=dynamic
language=es
context=center
secret=passwd
username=392
callerid=392
;fromuser=<392>
dtmfmode=rfc2833
videosupport=yes
;allow=h261
allow=h263
allow=h263p
allow=h264
maxcallbitrate=2048
qualify=yes
;
[310]
type=friend
host=dynamic
language=es
context=center
secret=passwd
username=310
callerid=310
;fromuser=<310>
dtmfmode=rfc2833
videosupport=yes
;allow=h261
allow=h263
allow=h263p
allow=h264
maxcallbitrate=2048
qualify=yes
;
[311]
type=friend
host=dynamic
language=es
context=center
secret=passwd
username=311
callerid=311
;fromuser=<311>
dtmfmode=rfc2833
videosupport=yes
;allow=h261
allow=h263
allow=h263p
allow=h264
```

```
maxcallbitrate=2048
qualify=yes
;
[312]
type=friend
host=dynamic
language=es
context=center
secret=passwd
username=312
callerid=312
;fromuser=<312>
dtmfmode=rfc2833
videosupport=yes
;allow=h261
allow=h263
allow=h263p
allow=h264
maxcallbitrate=2048
qualify=yes
;
[350]
type=friend
host=dynamic
language=es
context=center
secret=passwd
username=350
callerid=350
;fromuser=<350>
dtmfmode=rfc2833
videosupport=yes
;allow=h261
allow=h263
allow=h263p
allow=h264
maxcallbitrate=2048
qualify=yes
;
[351]
type=friend
host=dynamic
language=es
context=center
secret=passwd
username=351
callerid=351
;fromuser=<351>
dtmfmode=rfc2833
videosupport=yes
;allow=h261
allow=h263
allow=h263p
allow=h264
maxcallbitrate=2048
qualify=yes
;
[352]
type=friend
host=dynamic
language=es
context=center
secret=passwd
username=352
callerid=352
;fromuser=<352>
dtmfmode=rfc2833
videosupport=yes
```

```
;allow=h261
allow=h263
allow=h263p
allow=h264
maxcallbitrate=2048
qualify=yes
```

c) Configuración ASTERIX - EXTENSIONS.CONF

```
s1-varadero:~# cat /etc/asterisk/extensions.conf
#####
; extensions.conf
; dialplan
#####
; parametros general
;
[general]
;
static=yes
writeprotect=no
autofallthrough=no
clearglobalvars=no
;priorityjumping=yes
;
=====
; variables globales
;
[globals]
;
IP-SERVER200=
IP-SERVER300=20.20.20.13
IP-SERVER800=
IP-SERVER900=
;
IP-SERVER-PSTN=
;
PHONE-DEFAULT=
;
=====
; macros
;
[macro-dial-svlocal]
exten => s,1,Dial(${ARG1}/${ARG2},26)
exten => s,2,Hangup
exten => s,3,Macroexit()
exten => s,102,Hangup
exten => s,103,Macroexit()
;
1:38 PM [macro-sounds-record]
exten => s,1,Set(CHANNEL(language)=es)
exten => s,n,Wait(2)
exten => s,n,Record(/root/mensaje-pbx%d:${ARG1})
exten => s,n,Wait(2)
exten => s,n,Playback(${RECORDED_FILE})
exten => s,n,Hangup
exten => s,n,Macroexit()
;
[macro-dial-svred]
exten => s,1,Dial(IAX2/iaxuser:passwd@${ARG1}/${ARG2},28)
exten => s,2,Hangup
exten => s,3,Macroexit()
exten => s,102,Hangup
exten => s,103,Macroexit()
;
[macro-call-svlocal]
exten => s,1,Set(CHANNEL(language)=es)
exten => s,n,Playback(xservidor)
```

```
exten => s,n,Saydigits(${ARG1})
exten => s,n,Wait(1)
exten => s,n,Hangup
exten => s,n,Macroexit()
;
[macro-dial-pstn]
exten => s,1,Dial(SIP/${ARG1}@${ARG2},30)
exten => s,2,Hangup
exten => s,3,Macroexit()
exten => s,102,Hangup
exten => s,103,Macroexit()
;
;=====
;contexto principal
;
[center]
;
;prueba de llamada al servidor
exten => 200,1,Macro(call-svlocal,200)
;
;grabacion de archivos de sonido gsm
exten => 170,1,Macro(sounds-record,gsm)
;
;llamar area local
;exten => _3[67]X,1,Macro(dial-svlocal,SIP,${EXTEN})
;exten => _6[23]X,1,Macro(dial-svlocal,SIP,${EXTEN})
;exten => _4[23]X,1,Macro(dial-svlocal,SIP,${EXTEN})
exten => _61X,1,Macro(dial-svlocal,SIP,${EXTEN})
exten => _63X,1,Macro(dial-svlocal,SIP,${EXTEN})
exten => _51X,1,Macro(dial-svlocal,SIP,${EXTEN})
exten => _53X,1,Macro(dial-svlocal,SIP,${EXTEN})
exten => _47X,1,Macro(dial-svlocal,SIP,${EXTEN})
exten => _39X,1,Macro(dial-svlocal,SIP,${EXTEN})
exten => _31X,1,Macro(dial-svlocal,SIP,${EXTEN})
exten => _35X,1,Macro(dial-svlocal,SIP,${EXTEN})
;
;llamar a clientes de otros servidores
;exten => _8XX,1,Macro(dial-svred,${IP-SERVER800},${EXTEN})
;exten => _9XX,1,Macro(dial-svred,${IP-SERVER900},${EXTEN})
;
;llamar a la PSTN
:exten => 0147,1,Macro(dial-svred,${IP-SERVER-PSTN},${EXTEN})
;exten => _0.,1,Macro(dial-svred,${IP-SERVER-PSTN},${EXTEN})
;exten => 0147,1,Macro(dial-pstn,${EXTEN:1},10)
;exten => _0.,1,Macro(dial-pstn,${EXTEN:1},10)
;
;llamadas provenientes de la PSTN
exten => 11,1,Goto(ivr,s,1)
;
```

A continuación explicamos con detalle los archivos de configuración "SIP.CONF" y "EXTENSIONS.CONF":

Configuración ASTERIX - SIP.CONF

Es el archivo de configuración donde tenemos que definir nuestras extensiones, nuestros proveedores VoIP y todo lo relacionado con el protocolo SIP¹⁰. El archivo de configuración "*sip.conf*" está estructurado en tres bloques. **La parte general** donde hay que definir la configuración general de nuestras extensiones, **el bloque central** donde configuraremos la registración a nuestros proveedores VoIP y

¹⁰ SIP (Session Initiation Protocol o Protocolo de Inicio de Sesiones): Es un protocolo desarrollado por el grupo de trabajo *MMUSIC* del *IETF* con la intención de ser el estándar para la iniciación, modificación y finalización de sesiones interactivas de usuario donde intervienen elementos multimedia como el video, voz, mensajería instantánea, juegos en línea y realidad virtual.

la parte final del archivo donde configuraremos todas nuestras extensiones internas y externas.

Con las extensiones configuradas podremos llamar de una a otra, enrutar las llamadas a teléfonos fijos o celulares, hacia nuestros proveedores VoIP y utilizar los típicos servicios de *centralita* como llamadas en espera, desvío de llamadas, llamadas a tres, contestador, etc.

A continuación describimos la configuración del archivo de configuración "*sip.conf*"; cada línea del archivo viene acompañada de una breve explicación después del punto y coma. La versión instalada de nuestro servidor Asterisk (ubicada en el centro de salud de San Gabriel de Varadero) es la 1.6, pero la mayoría de las opciones son validas también para las versiones anteriores. Este servidor Asterisk es el único del que dispone esta red y es el que permite que las extensiones de VoIP y Videoconferencia puedan hacer llamadas SIP, y también establecer sesiones SIP de Videoconferencia. En el archivo de configuración "*sip.conf*" solamente se ha configurado la parte general y no se han considerado extensiones internas y externas.

```
s1-varadero:~# cat /etc/asterisk/sip.conf
;#####
; sip.conf
;#####
;
[general] ; Etiqueta que introduce la parte general de la configuración.
;
;tos=0xb8 ; Habilitada el marcado de paquetes con valor 0xb8 en el Asterisk.
bindport=5060 ; El puerto utilizado para conectar las extensiones SIP al servidor
Asterisk (protocolo UDP).
disallow=all ; Deshabilitar todos los codecs (Audio y video).
allow=gsm ; Habilita el códec audio "gsm" para todas las extensiones.
allow=g726aal2 ; Igual que arriba para el códec "g726".
allow=ulaw ; Igual que arriba para el códec "ulaw".
allow=alaw ; Igual que arriba para el códec "alaw".
;allow=g729a ; Igual que arriba para el códec "g729a".
;allow=g722.1/C ; Igual que arriba para el códec "g722".
;
[610] ; número de la extensión
type=friend ; Tipo de extensión. Puede ser friend, user o peer. Friend puede hacer
y recibir llamadas, user solo recibir y peer solo puede hacer (En el caso de
proveedores VoIP que usamos solo para hacer llamadas).
host=dynamic ; Si la extensión se conecta remotamente, cambiando continuamente su
dirección IP, entonces este parámetro debe ser configurado de esta manera.
language=es ; Si hemos instaladas locuciones en más de un idioma, entonces aquí
podemos definir cual idioma usará la extensión.
context=center ; El contexto que usará la extensión.
secret=passwd ; La clave o contraseña de la extensión.
username=610 ; Nombre de usuario de la extensión.
callerid=610 ; El nombre y el número de identificación de la extensión.
;fromuser=<610> ; Los datos que nos pide el proveedor para conectarnos (Usuario y
contraseña).
dtmfmode=rfc2833 ; El protocolo para enviar los tonos DTMF.
;videosupport=yes ; Para permitir videollamadas.
;allow=h261 ; Habilita el códec audio h261 (el primero que se intentará utilizar a
lo largo de una llamada).
;allow=h263 ; Habilita el códec audio h263.
;allow=h263p ; Habilita el códec audio h263p.
;allow=h264 ; Habilita el códec audio h264.
;maxcallbitrate=2048
```

qualify=yes ; Para saber el tiempo de respuesta de una extensión, y si está alcanzable o no.

Configuración ASTERIX - EXTENSIONS.CONF

El archivo de configuración "**extensions.conf**" es muy importante para la puesta en marcha de nuestra centralita (servidor Asterisk). En él se define todo lo relacionado con el plan de numeración. Cualquier número marcado desde una extensión, será procesado dentro de este archivo. Al igual que el "**sip.conf**", también está dividido en tres bloques:

- **La parte general** donde se configuran algunos parámetros generales
- **La parte global** donde se definen las variables globales que se van a utilizar en el servidor Asterisk
- **Una última parte** donde queda toda la configuración de las llamadas (**Contexto Principal - "center"**)

```
sl-varadero:~# cat /etc/asterisk/extensions.conf
;#####
; extensions.conf
; dialplan
;#####
; parametros general
;
[general]
;
static=yes ; Si es static es yes, y writeprotect es no, para guardar los cambios
hechos desde la consola de asterisk tendremos que escribir el comando dialplan
reload.
writeprotect=no ; En caso contrario se actualizará automáticamente pero
perderemos todos los comentarios presentes en el archivo.
autofallthrough=no ; Si es yes, cuando alguna llamada, por algún motivo se sale
del plan se terminará.
clearglobalvars=no
;priorityjumping=yes ; Algunas aplicaciones y/o funciones tienen la capacidad,
bajo algunas circunstancias de "saltar" desde la prioridad donde se encuentran, a
una prioridad que normalmente es "n+=101", donde n es el número de la línea que se
está ejecutando. Si está en yes, hará ese salto sino no.
;
;=====
; variables globales
;
[globals]
;
IP-SERVER200=
IP-SERVER300=20.20.20.13
IP-SERVER800=
IP-SERVER900=
;
IP-SERVER-PSTN=
;
PHONE-DEFAULT=
; En "globals" configuramos las variables que queremos usar en el dialplan, por
ejemplo si llamamos a menudo a un número y queremos configurarlo con una sigla o un
nombre, es en esta parte del archivo que lo podemos configurar.
;=====
; macros
;
[macro-dial-svlocal]
exten => s,1,Dial(${ARG1}/${ARG2},26)
exten => s,2,Hangup ; Con esta línea de comando la llamada se terminará y además
el número "2" indica la prioridad de la línea de comando.
```

```

exten => s,3,Macroexit()
exten => s,102,Hangup
exten => s,103,Macroexit()
;
1:38 PM [macro-sounds-record]
exten => s,1,Set(CHANNEL(language)=es)
exten => s,n,Wait(2)
exten => s,n,Record(/root/mensaje-pbx%d:${ARG1})
exten => s,n,Wait(2)
exten => s,n,Playback(${RECORDED_FILE})
exten => s,n,Hangup
exten => s,n,Macroexit()
;
[macro-dial-svred]
exten => s,1,Dial(IAX2/iaxuser:passwd@${ARG1}/${ARG2},28)
exten => s,2,Hangup
exten => s,3,Macroexit()
exten => s,102,Hangup
exten => s,103,Macroexit()
;
[macro-call-svlocal]
exten => s,1,Set(CHANNEL(language)=es)
exten => s,n,Playback(xservidor)
exten => s,n,Saydigits(${ARG1})
exten => s,n,Wait(1)
exten => s,n,Hangup
exten => s,n,Macroexit()
;
[macro-dial-pstn]
exten => s,1,Dial(SIP/${ARG1}@${ARG2},30)
exten => s,2,Hangup
exten => s,3,Macroexit()
exten => s,102,Hangup
exten => s,103,Macroexit()
;
;=====
; Es en esta parte donde vamos a configurar el verdadero plan de numeración
(dialplan). El plan de numeración se compone de contextos y dentro de cada
contexto, extensiones y prioridades. En este caso se va a definir un solo contexto
para realizar las llamadas VoIP y sesiones de Videoconferencia.
;
;contexto principal
[center]
;
;llamar area local
;exten => _3[67]X,1,Macro(dial-svlocal,SIP,${EXTEN})
;exten => _6[23]X,1,Macro(dial-svlocal,SIP,${EXTEN})
;exten => _4[23]X,1,Macro(dial-svlocal,SIP,${EXTEN})
exten => _61X,1,Macro(dial-svlocal,SIP,${EXTEN})
exten => _63X,1,Macro(dial-svlocal,SIP,${EXTEN})
exten => _51X,1,Macro(dial-svlocal,SIP,${EXTEN})
exten => _53X,1,Macro(dial-svlocal,SIP,${EXTEN})
exten => _47X,1,Macro(dial-svlocal,SIP,${EXTEN})
exten => _39X,1,Macro(dial-svlocal,SIP,${EXTEN})
exten => _31X,1,Macro(dial-svlocal,SIP,${EXTEN})
exten => _35X,1,Macro(dial-svlocal,SIP,${EXTEN})
;

```

La línea del contexto principal (resaltada con color azul), le dice a Asterisk que para todos los número marcados que empiecen por "**_61X**" deberá usar esta parte del plan de numeración. El "**_**", se pone cuando no indicamos el número exacto sino solamente una parte. El "**63X**" indica que después del "63" puede haber cualquier número que puede ser desde del tipo "36X". Dial es la aplicación que se utiliza para hacer una llamada (en nuestro caso se utiliza una

"macro: [macro-dial-svlocal]" que contiene a la aplicación Dial y Hungup).

Además "\${EXTEN}" es una variable interna de Asterisk, donde este servidor guarda el número al que se está llamando.

Finalmente con las líneas de comando del contexto principal se configurara las llamadas entre todas las extensiones, todas con prioridad igual a 1.

e) Configuración De Interfaces

```
s1-varadero:~# cat /etc/network/interfaces
# Used by ifup(8) and ifdown(8). See the interfaces(5) manpage or
# /usr/share/doc/ifupdown/examples for more information.

auto lo
iface lo inet loopback

#auto eth0
#iface eth0 inet static
# address 20.23.7.2
# netmask 255.255.255.240

#auto eth1
#iface eth1 inet static
# address 11.11.12.1
# netmask 255.255.255.0

#auto eth2
#iface eth2 inet static
#address 11.11.12.1
#netmask 255.255.255.0

auto br0
iface br0 inet static
# address 192.168.1.40
address 20.23.7.2
# netmask 255.255.255.0
netmask 255.255.255.240
bridge_ports eth0 eth1
bridge_stp off
bridge_maxwait 5

s1-varadero:~# cat /etc/network/nat-static-routes
# Configuración de rutas estáticas, max 100 rutas
# Configuración de nat, max 100 redes
# Configuración de nat para todas las redes por medio de una interfaz
#
#ROUTENAT_VERBOSITY=0

DEFAULT_GW="20.23.7.1"
#DEFAULT_GW="192.168.1.1"

#ROUTE1="10.10.12.0/24 10.10.1.2 10"
#ROUTE2="10.10.13.0/24 10.10.1.2 10"

#NAT1="10.10.1.0/24 ath1 172.16.6.33"
#NAT2="10.10.10.0/24 ath1 172.16.6.33"

#DEFAULT_NAT="eth1"
```


4. BALSAPUERTO

4.1. Repetidor Balsapuerto (Torre)

Placa Mikrotik Routerboard 433AH – Placa 1 (Torre)

```
*****
* RouterOS 4.5 *
*****

Password
*****
[admin@MikroTik] > password
gtrehasisf

Nombre de la Placa
*****
[admin@MikroTik] > system identity set name=b1-balsapuerto

Interface Wireless
*****
[admin@b1-balsapuerto] > interface wireless security-profiles add name=psk2-ieee

[admin@b1-balsapuerto] > interface wireless security-profiles set psk2-ieee
authentication-types=wpa2-psk group-ciphers=aes-ccm unicast-ciphers=aes-ccm wpa2-
pre-shared-key=gtr0ehas0isf mode=dynamic-keys
[admin@b1-balsapuerto] > interface wireless set wlan1 security-profile=psk2-ieee
[admin@b1-balsapuerto] > interface wireless set wlan2 security-profile=psk2-ieee

[admin@b1-balsapuerto] > interface wireless set wlan1 ack-timeout=dynamic antenna-
mode=ant-a band=5ghz-onlyn frequency=5180 mode=ap-bridge ssid=BALSA17 disable-
running-check=yes rate-set=configured tx-power=24 tx-power-mode=card-rates
disabled=no ht-extension-channel=disabled ht-guard-interval=long ht-basic-mcs=mcs-0
ht-supported-mcs=mcs-0,mcs-1,mcs-2,mcs-3

[admin@b1-balsapuerto] > interface wireless set wlan2 ack-timeout=dynamic antenna-
mode=ant-a band=5ghz-onlyn frequency=5745 mode=ap-bridge ssid=PUERTO17 disable-
running-check=yes rate-set=configured tx-power=17 tx-power-mode=card-rates
disabled=no ht-extension-channel=disabled ht-guard-interval=long ht-basic-mcs=mcs-0
ht-supported-mcs=mcs-0,mcs-1,mcs-2,mcs-3

Direcciones IP
*****
[admin@b1-balsapuerto] > interface bridge add name=br1
[admin@b1-balsapuerto] > interface bridge port add interface=ether1 bridge=br1
[admin@b1-balsapuerto] > interface bridge port add interface=ether2 bridge=br1
[admin@b1-balsapuerto] > interface bridge port add interface=ether3 bridge=br1

[admin@b1-balsapuerto] > ip address add address=20.20.17.1/28 interface=wlan1
[admin@b1-balsapuerto] > ip address add address=20.21.17.1/28 interface=wlan2
[admin@b1-balsapuerto] > ip address add address=20.22.17.1/28 interface=br1

OSPF
****
[admin@b1-balsapuerto] > routing ospf instance set router-id=0.0.1.3 metric-
default=10 metric-connected=10 metric-static=10 metric-rip=0 metric-bgp=0
```

```
redistribute-connected=as-type-1 redistribute-static=as-type-1 distribute-
default=if-installed-as-type-1 numbers=0

[admin@b1-balsapuerto] > routing ospf network add network=20.20.17.0/28
area=backbone
[admin@b1-balsapuerto] > routing ospf network add network=20.21.17.0/28
area=backbone

[admin@b1-balsapuerto] > routing ospf interface add interface=wlan1 cost=10
[admin@b1-balsapuerto] > routing ospf interface add interface=wlan2 cost=10
```

4.2. Cliente: Municipalidad de Balsapuerto

Placa Mikrotik Routerboard 433

```
*****
* RouterOS 4.5 *
*****
```

```
Password
*****
[admin@MikroTik] > password
gtrehasisf
```

```
Nombre de la Placa
*****
[admin@MikroTik] > system identity set name=c2-balsapuerto-muni
```

```
Interface Wireless
*****
[admin@c2-balsapuerto-muni] > interface wireless security-profiles add name=psk2-
ieee
```

```
[admin@c2-balsapuerto-muni] > interface wireless security-profiles set psk2-ieee
authentication-types=wpa2-psk group-ciphers=aes-ccm unicast-ciphers=aes-ccm wpa2-
pre-shared-key=gtr0ehas0isf mode=dynamic-keys
[admin@c2-balsapuerto-muni] > interface wireless set wlan1 security-profile=psk2-
ieee
```

```
[admin@c2-balsapuerto-muni] > interface wireless set wlan1 ack-timeout=dynamic
antenna-mode=ant-a band=5ghz-onlyn frequency=5745 mode=station ssid=PUERTO17
disable-running-check=yes rate-set=configured tx-power=17 tx-power-mode=card-rates
disabled=no ht-extension-channel=above-control ht-guard-interval=any ht-basic-
mcs=mcs-7 ht-supported-mcs=mcs-0,mcs-1,mcs-2,mcs-3,mcs-4,mcs-5,mcs-6,mcs7
```

```
Direcciones IP
*****
[admin@c2-balsapuerto-muni] > interface bridge add name=br1
[admin@c2-balsapuerto-muni] > interface bridge port add interface=ether1 bridge=br1
[admin@c2-balsapuerto-muni] > interface bridge port add interface=ether2 bridge=br1
[admin@c2-balsapuerto-muni] > interface bridge port add interface=ether3 bridge=br1
[admin@c2-balsapuerto-muni] > ip address add address=20.21.17.3/28 interface=wlan1
[admin@c2-balsapuerto-muni] > ip address add address=20.23.17.17/28 interface=br1
```

```
OSPF
****
[admin@c2-balsapuerto-muni] > routing ospf instance set router-id=0.0.1.21 metric-
default=10 metric-connected=10 metric-static=10 metric-rip=0 metric-bgp=0
redistribute-connected=as-type-1 redistribute-static=as-type-1 distribute-default=
if-installed-as-type-1 numbers=0
```

```
[admin@c2-balsapuerto-muni] > routing ospf network add network=20.21.17.0/28
area=backbone

[admin@c2-balsapuerto-muni] > routing ospf interface add interface=wlan1 cost=10
```

4.3. Cliente: Centro de Salud de Balsapuerto

Placa Mikrotik Routerboard 433

```
*****
* RouterOS 4.5 *
*****
```

```
Password
*****
[admin@MikroTik] > password
gtrehasisf
```

```
Nombre de la Placa
*****
[admin@MikroTik] > system identity set name=c1-balsapuerto-ps
```

```
Interface Wireless
*****
[admin@c1-balsapuerto-ps] > interface wireless security-profiles add name=psk2-ieee

[admin@c1-balsapuerto-ps] > interface wireless security-profiles set psk2-ieee
authentication-types=wpa2-psk group-ciphers=aes-ccm unicast-ciphers=aes-ccm wpa2-
pre-shared-key=gtr0ehas0isf mode=dynamic-keys
[admin@c1-balsapuerto-ps] > interface wireless set wlan1 security-profile=psk2-ieee

[admin@c1-balsapuerto-ps] > interface wireless set wlan1 ack-timeout=dynamic
antenna-mode=ant-a band=5ghz-onlyn frequency=5745 mode=station ssid=PUERTO17
disable-running-check=yes rate-set=configured tx-power=17 tx-power-mode=card-rates
disabled=no ht-extension-channel=disabled ht-guard-interval=long ht-basic-mcs=mcs-0
ht-supported-mcs=mcs-0,mcs-1,mcs-2,mcs-3
```

```
Direcciones IP
*****
[admin@c1-balsapuerto-ps] > interface bridge add name=br1
[admin@c1-balsapuerto-ps] > interface bridge port add interface=ether1 bridge=br1
[admin@c1-balsapuerto-ps] > interface bridge port add interface=ether2 bridge=br1
[admin@c1-balsapuerto-ps] > interface bridge port add interface=ether3 bridge=br1
[admin@c1-balsapuerto-ps] > ip address add address=20.21.17.2/28 interface=wlan1
[admin@c1-balsapuerto-ps] > ip address add address=20.23.17.1/28 interface=br1
```

```
OSPF
****
[admin@c1-balsapuerto-ps] > routing ospf instance set router-id=0.0.1.4 metric-
default=10 metric-connected=10 metric-static=10 metric-rip=0 metric-bgp=0
redistribute-connected=as-type-1 redistribute-static=as-type-1 distribute-
default=always-as-type-1 numbers=0
```

```
[admin@c1-balsapuerto-ps] > routing ospf network add network=20.21.17.0/28
area=backbone

[admin@c1-balsapuerto-ps] > routing ospf interface add interface=wlan1 cost=10
```


Anexo B: Configuración de HTB en las Placas MikroTik

1. YURIMAGUAS

1.1. Repetidor Santa Gema (Torre)

Placa Mikrotik Routerboard 433AH – (Torre)

```
*****  
* RouterOS 4.5 *  
*****
```

```
Password  
*****  
[admin@MikroTik] > password  
gtrehasisf
```

```
Mangle - Marcado de Paquetes  
*****
```

```
[admin@b1-santagema] > ip firewall mangle add chain=forward action=mark-connection  
new-connection-mark=voip-con passthrough=yes src-address=20.23.7.2 dst-  
address=20.23.7.2 dscp=46
```

```
[admin@b1-santagema] > ip firewall mangle add chain=forward action=mark-packet new-  
packet-mark=voip passthrough=no connection-mark=voip-con
```

```
[admin@b1-santagema] > ip firewall mangle add chain=forward action=mark-connection  
new-connection-mark=voip-con passthrough=yes src-address=20.22.1.0/28 dst-  
address=20.22.5.0/28 dscp=46
```

```
[admin@b1-santagema] > ip firewall mangle add chain=forward action=mark-packet new-  
packet-mark=voip-con passthrough=no connection-mark=voip-con
```

```
[admin@b1-santagema] > ip firewall mangle add chain=forward action=mark-connection  
new-connection-mark=video-con passthrough=yes src-address=20.23.7.2 dst-  
address=20.23.7.2 dscp=38
```

```
[admin@b1-santagema] > ip firewall mangle add chain=forward action=mark-packet new-  
packet-mark=video passthrough=no connection-mark=video-con
```

```
[admin@b1-santagema] > ip firewall mangle add chain=forward action=mark-connection  
new-connection-mark=video-con passthrough=yes src-address=20.22.1.0/28 dst-  
address=20.22.5.0/28 dscp=38
```

```
[admin@b1-santagema] > ip firewall mangle add chain=forward action=mark-packet new-  
packet-mark=video passthrough=no connection-mark=video-con
```

```
[admin@b1-santagema] > ip firewall mangle add chain=forward action=mark-connection  
new-connection-mark=besteffort-con passthrough=yes src-address=20.22.1.0/28 dst-  
address=20.22.5.0/28 dscp=0
```

Configuración de HTB en las placas Mikrotik

```
[admin@b1-santagema] > ip firewall mangle add chain=forward action=mark-packet new-  
packet-mark=besteffort passthrough=no connection-mark=besteffort-con
```

Queue Tree - Arbol de colas

```
[admin@b1-santagema] > queue tree add name="trafico_total" parent=wlan1 limit-at=0  
priority=8 max-limit=10485760 burst-limit=0 burst-threshold=0 burst-time=0s
```

```
[admin@b1-santagema] > queue tree add name="leaf_besteffort" parent=trafico_total  
packet-mark=besteffort limit-at=1048576 queue=PCQ_besteffort priority=8 max-  
limit=10485760 burst-limit=0 burst-threshold=0 burst-time=0s
```

```
[admin@b1-santagema] > queue tree add name="leaf_video" parent=trafico_total  
packet-mark=video limit-at=8388608 queue=SFQ_video priority=2 max-limit=10485760  
burst-limit=0 burst-threshold=0 burst-time=0s
```

```
[admin@b1-santagema] > queue tree add name="leaf_voip" parent=trafico_total packet-  
mark=voip limit-at=1048576 queue=SFQ_VoIP priority=1 max-limit=10485760 burst-  
limit=0 burst-threshold=0 burst-time=0s
```

Queue Type - Tipos de colas

```
[admin@b1-santagema] > queue type add name="SFQ_VoIP" kind=sfq sfq-perturb=10 sfq-  
allot=1514
```

```
[admin@b1-santagema] > queue type add name="SFQ_video" kind=sfq sfq-perturb=10 sfq-  
allot=1514
```

```
[admin@b1-santagema] > queue type add name="PCQ_besteffort" kind=pcq pcq-  
rate=1048576 pcq-limit=50 pcq-classifier=dst-address pcq-total-limit=2000
```

1.3. Cliente: Red de Salud de Alto Amazonas

Placa Mikrotik Routerboard 433

```
*****  
* RouterOS 4.5 *  
*****
```

Password

```
[admin@MikroTik] > password  
gtrehasisf
```

Mangle - Marcado de Paquetes

```
[admin@c1-redsalud-yuri] > ip firewall mangle add chain=prerouting action=mark-  
connection new-connection-mark=voip-con passthrough=yes src-address=20.23.7.2 dst-  
address=20.23.7.2 dscp=46
```

```
[admin@c1-redsalud-yuri] > ip firewall mangle add chain=prerouting action=mark-  
packet new-packet-mark=voip passthrough=no connection-mark=voip-con
```

Configuración de HTB en las placas Mikrotik

```
[admin@c1-redsalud-yuri] > ip firewall mangle add chain=prerouting action=mark-connection new-connection-mark=voip-con passthrough=yes src-address=20.23.1.0/28 dst-address=20.23.5.0/28 dscp=46

[admin@c1-redsalud-yuri] > ip firewall mangle add chain=prerouting action=mark-packet new-packet-mark=voip-con passthrough=no connection-mark=voip-con

[admin@c1-redsalud-yuri] > ip firewall mangle add chain=prerouting action=mark-connection new-connection-mark=video-con passthrough=yes src-address=20.23.7.2 dst-address=20.23.7.2 dscp=38

[admin@c1-redsalud-yuri] > ip firewall mangle add chain=prerouting action=mark-packet new-packet-mark=video passthrough=no connection-mark=video-con

[admin@c1-redsalud-yuri] > ip firewall mangle add chain=prerouting action=mark-connection new-connection-mark=video-con passthrough=yes src-address=20.23.1.0/28 dst-address=20.23.5.0/28 dscp=38

[admin@c1-redsalud-yuri] > ip firewall mangle add chain=prerouting action=mark-packet new-packet-mark=video passthrough=no connection-mark=video-con

[admin@c1-redsalud-yuri] > ip firewall mangle add chain=prerouting action=mark-connection new-connection-mark=besteffort-con passthrough=yes src-address=20.23.1.0/28 dst-address=20.23.5.0/28 dscp=0

[admin@c1-redsalud-yuri] > ip firewall mangle add chain=prerouting action=mark-packet new-packet-mark=besteffort passthrough=no connection-mark=besteffort-con
```

Queue Tree - Arbol de colas

```
[admin@c1-redsalud-yuri] > queue tree add name="trafico_total" parent=br1 limit-at=0 priority=8 max-limit=10485760 burst-limit=0 burst-threshold=0 burst-time=0s

[admin@c1-redsalud-yuri] > queue tree add name="leaf_besteffort" parent=trafico_total packet-mark=besteffort limit-at=1048576 queue=PCQ_besteffort priority=8 max-limit=10485760 burst-limit=0 burst-threshold=0 burst-time=0s

[admin@c1-redsalud-yuri] > queue tree add name="leaf_video" parent=trafico_total packet-mark=video limit-at=8388608 queue=SFQ_video priority=2 max-limit=10485760 burst-limit=0 burst-threshold=0 burst-time=0s

[admin@c1-redsalud-yuri] > queue tree add name="leaf_voip" parent=trafico_total packet-mark=voip limit-at=1048576 queue=SFQ_VoIP priority=1 max-limit=10485760 burst-limit=0 burst-threshold=0 burst-time=0s
```

Queue Type - Tipos de colas

```
[admin@c1-redsalud-yuri] > queue type add name="SFQ_VoIP" kind=sfq sfq-perturb=10 sfq-allot=1514

[admin@c1-redsalud-yuri] > queue type add name="SFQ_video" kind=sfq sfq-perturb=10 sfq-allot=1514

[admin@c1-redsalud-yuri] > queue type add name="PCQ_besteffort" kind=pcq pcq-rate=1048576 pcq-limit=50 pcq-classifier=dst-address pcq-total-limit=2000
```

2. SAN JUAN

2.1. Repetidor San Juan (Torre)

Placa Mikrotik Routerboard 433AH – Placa 1 (Torre)

```
*****  
* RouterOS 4.5 *  
*****
```

```
Password  
*****  
[admin@MikroTik] > password  
gtrehasisf
```

```
Mangle - Marcado de Paquetes  
*****
```

```
[admin@b1-sanjuan] > ip firewall mangle add chain=forward action=mark-connection  
new-connection-mark=voip-con passthrough=yes src-address=20.23.7.2 dst-  
address=20.23.7.2 dscp=46
```

```
[admin@b1-sanjuan] > ip firewall mangle add chain=forward action=mark-packet new-  
packet-mark=voip passthrough=no connection-mark=voip-con
```

```
[admin@b1-sanjuan] > ip firewall mangle add chain=forward action=mark-connection  
new-connection-mark=voip-con passthrough=yes src-address=20.22.5.0/28 dst-  
address=20.22.1.0/28 dscp=46
```

```
[admin@b1-sanjuan] > ip firewall mangle add chain=forward action=mark-packet new-  
packet-mark=voip-con passthrough=no connection-mark=voip-con
```

```
[admin@b1-sanjuan] > ip firewall mangle add chain=forward action=mark-connection  
new-connection-mark=video-con passthrough=yes src-address=20.23.7.2 dst-  
address=20.23.7.2 dscp=38
```

```
[admin@b1-sanjuan] > ip firewall mangle add chain=forward action=mark-packet new-  
packet-mark=video passthrough=no connection-mark=video-con
```

```
[admin@b1-sanjuan] > ip firewall mangle add chain=forward action=mark-connection  
new-connection-mark=video-con passthrough=yes src-address=20.22.5.0/28 dst-  
address=20.22.1.0/28 dscp=38
```

```
[admin@b1-sanjuan] > ip firewall mangle add chain=forward action=mark-packet new-  
packet-mark=video passthrough=no connection-mark=video-con
```

```
[admin@b1-sanjuan] > ip firewall mangle add chain=forward action=mark-connection  
new-connection-mark=besteffort-con passthrough=yes src-address=20.22.5.0/28 dst-  
address=20.22.1.0/28 dscp=0
```

```
[admin@b1-sanjuan] > ip firewall mangle add chain=forward action=mark-packet new-  
packet-mark=besteffort passthrough=no connection-mark=besteffort-con
```

```
[admin@b1-sanjuan] > ip firewall mangle add chain=forward action=mark-connection  
new-connection-mark=video-con passthrough=yes src-address=20.22.5.0/28 dst-  
address=20.22.1.0/28 dscp=38
```

```
[admin@b1-sanjuan] > ip firewall mangle add chain=forward action=mark-packet new-  
packet-mark=video passthrough=no connection-mark=video-con
```

```
[admin@b1-sanjuan] > ip firewall mangle add chain=forward action=mark-connection  
new-connection-mark=voip-con passthrough=yes src-address=20.22.5.0/28 dst-  
address=20.22.7.0/28 dscp=46
```


Configuración de HTB en las placas Mikrotik

```
[admin@b1-sanjuan] > ip firewall mangle add chain=forward action=mark-packet new-packet-mark=voip-con passthrough=no connection-mark=voip-con
```

```
[admin@b1-sanjuan] > ip firewall mangle add chain=forward action=mark-connection new-connection-mark=video-con passthrough=yes src-address=20.22.5.0/28 dst-address=20.22.7.0/28 dscp=38
```

```
[admin@b1-sanjuan] > ip firewall mangle add chain=forward action=mark-packet new-packet-mark=video passthrough=no connection-mark=video-con
```

```
[admin@b1-sanjuan] > ip firewall mangle add chain=forward action=mark-connection new-connection-mark=besteffort-con passthrough=yes src-address=20.22.5.0/28 dst-address=20.22.7.0/28 dscp=0
```

```
[admin@b1-sanjuan] > ip firewall mangle add chain=forward action=mark-packet new-packet-mark=besteffort passthrough=no connection-mark=besteffort-con
```

Queue Tree - Arbol de colas

```
[admin@b1-sanjuan] > queue tree add name="trafico_total" parent=wlan1 limit-at=0 priority=8 max-limit=10485760 burst-limit=0 burst-threshold=0 burst-time=0s
```

```
[admin@b1-sanjuan] > queue tree add name="leaf_besteffort" parent=trafico_total packet-mark=besteffort limit-at=1048576 queue=PCQ_besteffort priority=8 max-limit=10485760 burst-limit=0 burst-threshold=0 burst-time=0s
```

```
[admin@b1-sanjuan] > queue tree add name="leaf_video" parent=trafico_total packet-mark=video limit-at=8388608 queue=SFQ_video priority=2 max-limit=10485760 burst-limit=0 burst-threshold=0 burst-time=0s
```

```
[admin@b1-sanjuan] > queue tree add name="leaf_voip" parent=trafico_total packet-mark=voip limit-at=1048576 queue=SFQ_VoIP priority=1 max-limit=10485760 burst-limit=0 burst-threshold=0 burst-time=0s
```

Queue Type - Tipos de colas

```
[admin@b1-sanjuan] > queue type add name="SFQ_VoIP" kind=sfq sfq-perturb=10 sfq-allot=1514
```

```
[admin@b1-sanjuan] > queue type add name="SFQ_video" kind=sfq sfq-perturb=10 sfq-allot=1514
```

```
[admin@b1-sanjuan] > queue type add name="PCQ_besteffort" kind=pcq pcq-rate=1048576 pcq-limit=50 pcq-classifier=dst-address pcq-total-limit=2000
```

2.2. Cliente: Puesto de Salud de San Juan

Placa Mikrotik Routerboard 433

```
*****  
* RouterOS 4.5 *  
*****
```

```
Password  
*****  
[admin@MikroTik] > password  
gtrehasisf
```

Mangle - Marcado de Paquetes

```
[admin@c1-sanjuan-ps] > ip firewall mangle add chain=prerouting action=mark-  
connection new-connection-mark=voip-con passthrough=yes src-address=20.23.7.2 dst-  
address=20.23.7.2 dscp=46
```

```
[admin@c1-sanjuan-ps] > ip firewall mangle add chain=prerouting action=mark-packet  
new-packet-mark=voip passthrough=no connection-mark=voip-con
```

```
[admin@c1-sanjuan-ps] > ip firewall mangle add chain=prerouting action=mark-  
connection new-connection-mark=voip-con passthrough=yes src-address=20.23.5.0/28  
dst-address=20.23.1.0/28 dscp=46
```

```
[admin@c1-sanjuan-ps] > ip firewall mangle add chain=prerouting action=mark-packet  
new-packet-mark=voip-con passthrough=no connection-mark=voip-con
```

```
[admin@c1-sanjuan-ps] > ip firewall mangle add chain=prerouting action=mark-  
connection new-connection-mark=video-con passthrough=yes src-address=20.23.7.2 dst-  
address=20.23.7.2 dscp=38
```

```
[admin@c1-sanjuan-ps] > ip firewall mangle add chain=prerouting action=mark-packet  
new-packet-mark=video passthrough=no connection-mark=video-con
```

```
[admin@c1-sanjuan-ps] > ip firewall mangle add chain=prerouting action=mark-  
connection new-connection-mark=video-con passthrough=yes src-address=20.23.5.0/28  
dst-address=20.23.1.0/28 dscp=38
```

```
[admin@c1-sanjuan-ps] > ip firewall mangle add chain=prerouting action=mark-packet  
new-packet-mark=video passthrough=no connection-mark=video-con
```

```
[admin@c1-sanjuan-ps] > ip firewall mangle add chain=prerouting action=mark-  
connection new-connection-mark=besteffort-con passthrough=yes src-  
address=20.23.5.0/28 dst-address=20.23.1.0/28 dscp=0
```

```
[admin@c1-sanjuan-ps] > ip firewall mangle add chain=prerouting action=mark-packet  
new-packet-mark=besteffort passthrough=no connection-mark=besteffort-con
```

Queue Tree - Arbol de colas

```
[admin@c1-sanjuan-ps] > queue tree add name="trafico_total" parent=br1 limit-at=0
priority=8 max-limit=10485760 burst-limit=0 burst-threshold=0 burst-time=0s
```

```
[admin@c1-sanjuan-ps] > queue tree add name="leaf_besteffort" parent=trafico_total
packet-mark=besteffort limit-at=1048576 queue=PCQ_besteffort priority=8 max-
limit=10485760 burst-limit=0 burst-threshold=0 burst-time=0s
```

```
[admin@c1-sanjuan-ps] > queue tree add name="leaf_video" parent=trafico_total
packet-mark=video limit-at=8388608 queue=SFQ_video priority=2 max-limit=10485760
burst-limit=0 burst-threshold=0 burst-time=0s
```

```
[admin@c1-sanjuan-ps] > queue tree add name="leaf_voip" parent=trafico_total
packet-mark=voip limit-at=1048576 queue=SFQ_VoIP priority=1 max-limit=10485760
burst-limit=0 burst-threshold=0 burst-time=0s
```

Queue Type - Tipos de colas

```
[admin@c1-sanjuan-ps] > queue type add name="SFQ_VoIP" kind=sfq sfq-perturb=10 sfq-
allot=1514
```

```
[admin@c1-sanjuan-ps] > queue type add name="SFQ_video" kind=sfq sfq-perturb=10
sfq-allot=1514
```

```
[admin@c1-sanjuan-ps] > queue type add name="PCQ_besteffort" kind=pcq pcq-
rate=1048576 pcq-limit=50 pcq-classifier=dst-address pcq-total-limit=2000
```

3. VARADERO

3.1. Repetidor Varadero (Torre)

Placa Mikrotik Routerboard 433AH – Placa 1

* RouterOS 4.5 *

```
Password
*****
[admin@MikroTik] > password
gtrehasisf
```

Mangle - Marcado de Paquetes

```
[admin@b1-varadero] > ip firewall mangle add chain=forward action=mark-connection
new-connection-mark=voip-con passthrough=yes src-address=20.23.7.2 dst-
address=20.23.7.2 dscp=46
```

```
[admin@b1-varadero] > ip firewall mangle add chain=forward action=mark-packet new-
packet-mark=voip passthrough=no connection-mark=voip-con
```

```
[admin@b1-varadero] > ip firewall mangle add chain=forward action=mark-connection
new-connection-mark=voip-con passthrough=yes src-address=20.22.7.0/28 dst-
address=20.22.5.0/28 dscp=46
```

Configuración de HTB en las placas Mikrotik

```
[admin@b1-varadero] > ip firewall mangle add chain=forward action=mark-packet new-  
packet-mark=voip-con passthrough=no connection-mark=voip-con
```

```
[admin@b1-varadero] > ip firewall mangle add chain=forward action=mark-connection  
new-connection-mark=video-con passthrough=yes src-address=20.23.7.2 dst-  
address=20.23.7.2 dscp=38
```

```
[admin@b1-varadero] > ip firewall mangle add chain=forward action=mark-packet new-  
packet-mark=video passthrough=no connection-mark=video-con
```

```
[admin@b1-varadero] > ip firewall mangle add chain=forward action=mark-connection  
new-connection-mark=video-con passthrough=yes src-address=20.22.7.0/28 dst-  
address=20.22.5.0/28 dscp=38
```

```
[admin@b1-varadero] > ip firewall mangle add chain=forward action=mark-packet new-  
packet-mark=video passthrough=no connection-mark=video-con
```

```
[admin@b1-varadero] > ip firewall mangle add chain=forward action=mark-connection  
new-connection-mark=besteffort-con passthrough=yes src-address=20.22.7.0/28 dst-  
address=20.22.5.0/28 dscp=0
```

```
[admin@b1-varadero] > ip firewall mangle add chain=forward action=mark-packet new-  
packet-mark=besteffort passthrough=no connection-mark=besteffort-con
```

Queue Tree - Arbol de colas

```
[admin@b1-varadero] > queue tree add name="trafico_total" parent=wlan3 limit-at=0  
priority=8 max-limit=10485760 burst-limit=0 burst-threshold=0 burst-time=0s
```

```
[admin@b1-varadero] > queue tree add name="leaf_besteffort" parent=trafico_total  
packet-mark=besteffort limit-at=1048576 queue=PCQ_besteffort priority=8 max-  
limit=10485760 burst-limit=0 burst-threshold=0 burst-time=0s
```

```
[admin@b1-varadero] > queue tree add name="leaf_video" parent=trafico_total packet-  
mark=video limit-at=8388608 queue=SFQ_video priority=2 max-limit=10485760 burst-  
limit=0 burst-threshold=0 burst-time=0s
```

```
[admin@b1-varadero] > queue tree add name="leaf_voip" parent=trafico_total packet-  
mark=voip limit-at=1048576 queue=SFQ_VoIP priority=1 max-limit=10485760 burst-  
limit=0 burst-threshold=0 burst-time=0s
```

Queue Type - Tipos de colas

```
[admin@b1-varadero] > queue type add name="SFQ_VoIP" kind=sfq sfq-perturb=10 sfq-  
allot=1514
```

```
[admin@b1-varadero] > queue type add name="SFQ_video" kind=sfq sfq-perturb=10 sfq-  
allot=1514
```

```
[admin@b1-varadero] > queue type add name="PCQ_besteffort" kind=pcq pcq-  
rate=1048576 pcq-limit=50 pcq-classifier=dst-address pcq-total-limit=2000
```

Placa Mikrotik Routerboard 433AH – Placa 2 (Torre)

Configuración de HTB en las placas Mikrotik

```
* RouterOS 4.5 *  
*****
```

```
Password  
*****  
[admin@MikroTik] > password  
gtrehasisf
```

```
Mangle - Marcado de Paquetes  
*****
```

```
[admin@b2-varadero] > ip firewall mangle add chain=forward action=mark-connection  
new-connection-mark=voip-con passthrough=yes src-address=20.23.7.2 dst-  
address=20.23.7.2 dscp=46
```

```
[admin@b2-varadero] > ip firewall mangle add chain=forward action=mark-packet new-  
packet-mark=voip passthrough=no connection-mark=voip-con
```

```
[admin@b2-varadero] > ip firewall mangle add chain=forward action=mark-connection  
new-connection-mark=voip-con passthrough=yes src-address=20.22.7.0/28 dst-  
address=20.22.17.0/28 dscp=46
```

```
[admin@b2-varadero] > ip firewall mangle add chain=forward action=mark-packet new-  
packet-mark=voip-con passthrough=no connection-mark=voip-con
```

```
[admin@b2-varadero] > ip firewall mangle add chain=forward action=mark-connection  
new-connection-mark=video-con passthrough=yes src-address=20.23.7.2 dst-  
address=20.23.7.2 dscp=38
```

```
[admin@b2-varadero] > ip firewall mangle add chain=forward action=mark-packet new-  
packet-mark=video passthrough=no connection-mark=video-con
```

```
[admin@b2-varadero] > ip firewall mangle add chain=forward action=mark-connection  
new-connection-mark=video-con passthrough=yes src-address=20.22.7.0/28 dst-  
address=20.22.17.0/28 dscp=38
```

```
[admin@b2-varadero] > ip firewall mangle add chain=forward action=mark-packet new-  
packet-mark=video passthrough=no connection-mark=video-con
```

```
[admin@b2-varadero] > ip firewall mangle add chain=forward action=mark-connection  
new-connection-mark=besteffort-con passthrough=yes src-address=20.22.7.0/28 dst-  
address=20.22.17.0/28 dscp=0
```

```
[admin@b2-varadero] > ip firewall mangle add chain=forward action=mark-packet new-  
packet-mark=besteffort passthrough=no connection-mark=besteffort-con
```

```
Queue Tree - Arbol de colas  
*****
```

```
[admin@b2-varadero] > queue tree add name="trafico_total" parent=wlan1 limit-at=0  
priority=8 max-limit=10485760 burst-limit=0 burst-threshold=0 burst-time=0s
```

```
[admin@b2-varadero] > queue tree add name="leaf_besteffort" parent=trafico_total  
packet-mark=besteffort limit-at=1048576 queue=PCQ_besteffort priority=8 max-  
limit=10485760 burst-limit=0 burst-threshold=0 burst-time=0s
```

```
[admin@b2-varadero] > queue tree add name="leaf_video" parent=trafico_total packet-  
mark=video limit-at=8388608 queue=SFQ_video priority=2 max-limit=10485760 burst-  
limit=0 burst-threshold=0 burst-time=0s
```

```
[admin@b2-varadero] > queue tree add name="leaf_voip" parent=trafico_total packet-  
mark=voip limit-at=1048576 queue=SFQ_VoIP priority=1 max-limit=10485760 burst-  
limit=0 burst-threshold=0 burst-time=0s
```

Queue Type - Tipos de colas

```
[admin@b2-varadero] > queue type add name="SFQ_VoIP" kind=sfq sfq-perturb=10 sfq-allot=1514
```

```
[admin@b2-varadero] > queue type add name="SFQ_video" kind=sfq sfq-perturb=10 sfq-allot=1514
```

```
[admin@b2-varadero] > queue type add name="PCQ_besteffort" kind=pcq pcq-rate=1048576 pcq-limit=50 pcq-classifier=dst-address pcq-total-limit=2000
```

3.2. Cliente: Puesto de Salud de Varadero

Placa Mikrotik Routerboard 433

* RouterOS 4.5 *

Password

```
[admin@MikroTik] > password  
gtrehasisf
```

Mangle - Marcado de Paquetes

```
[admin@c1-varadero-ps] > ip firewall mangle add chain=prerouting action=mark-connection new-connection-mark=voip-con passthrough=yes src-address=20.23.7.2 dst-address=20.23.7.2 dscp=46
```

```
[admin@c1-varadero-ps] > ip firewall mangle add chain=prerouting action=mark-packet new-packet-mark=voip passthrough=no connection-mark=voip-con
```

```
[admin@c1-varadero-ps] > ip firewall mangle add chain=prerouting action=mark-connection new-connection-mark=voip-con passthrough=yes src-address=20.23.7.0/28 dst-address=20.23.17.0/28 dscp=46
```

```
[admin@c1-varadero-ps] > ip firewall mangle add chain=prerouting action=mark-packet new-packet-mark=voip-con passthrough=no connection-mark=voip-con
```

```
[admin@c1-varadero-ps] > ip firewall mangle add chain=prerouting action=mark-connection new-connection-mark=video-con passthrough=yes src-address=20.23.7.2 dst-address=20.23.7.2 dscp=38
```

```
[admin@c1-varadero-ps] > ip firewall mangle add chain=prerouting action=mark-packet new-packet-mark=video passthrough=no connection-mark=video-con
```

```
[admin@c1-varadero-ps] > ip firewall mangle add chain=prerouting action=mark-connection new-connection-mark=video-con passthrough=yes src-address=20.23.7.0/28 dst-address=20.23.17.0/28 dscp=38
```

```
[admin@c1-varadero-ps] > ip firewall mangle add chain=prerouting action=mark-packet new-packet-mark=video passthrough=no connection-mark=video-con
```

```
[admin@c1-varadero-ps] > ip firewall mangle add chain=prerouting action=mark-connection new-connection-mark=besteffort-con passthrough=yes src-address=20.23.7.0/28 dst-address=20.23.17.0/28 dscp=0
```

```
[admin@c1-varadero-ps] > ip firewall mangle add chain=prerouting action=mark-packet
new-packet-mark=besteffort passthrough=no connection-mark=besteffort-con
```

Queue Tree - Arbol de colas

```
[admin@c1-varadero-ps] > queue tree add name="trafico_total" parent=br1 limit-at=0
priority=8 max-limit=10485760 burst-limit=0 burst-threshold=0 burst-time=0s
```

```
[admin@c1-varadero-ps] > queue tree add name="leaf_besteffort" parent=trafico_total
packet-mark=besteffort limit-at=1048576 queue=PCQ_besteffort priority=8 max-
limit=10485760 burst-limit=0 burst-threshold=0 burst-time=0s
```

```
[admin@c1-varadero-ps] > queue tree add name="leaf_video" parent=trafico_total
packet-mark=video limit-at=8388608 queue=SFQ_video priority=2 max-limit=10485760
burst-limit=0 burst-threshold=0 burst-time=0s
```

```
[admin@c1-varadero-ps] > queue tree add name="leaf_voip" parent=trafico_total
packet-mark=voip limit-at=1048576 queue=SFQ_VoIP priority=1 max-limit=10485760
burst-limit=0 burst-threshold=0 burst-time=0s
```

Queue Type - Tipos de colas

```
[admin@c1-varadero-ps] > queue type add name="SFQ_VoIP" kind=sfq sfq-perturb=10
sfq-allot=1514
```

```
[admin@c1-varadero-ps] > queue type add name="SFQ_video" kind=sfq sfq-perturb=10
sfq-allot=1514
```

```
[admin@c1-varadero-ps] > queue type add name="PCQ_besteffort" kind=pcq pcq-
rate=1048576 pcq-limit=50 pcq-classifier=dst-address pcq-total-limit=2000
```

4. BALSAPUERTO

4.1. Repetidor Balsapuerto (Torre)

Placa Mikrotik Routerboard 433AH – (Torre)

```
*****
* RouterOS 4.5 *
*****
```

Password

```
[admin@MikroTik] > password
gtrehasisf
```

Mangle - Marcado de Paquetes

```
[admin@b1-balsapuerto] > ip firewall mangle add chain=forward action=mark-
connection new-connection-mark=voip-con passthrough=yes src-address=20.23.7.2 dst-
address=20.23.7.2 dscp=46
```

```
[admin@b1-balsapuerto] > ip firewall mangle add chain=forward action=mark-packet
new-packet-mark=voip passthrough=no connection-mark=voip-con
```

Configuración de HTB en las placas Mikrotik

```
[admin@b1-balsapuerto] > ip firewall mangle add chain=forward action=mark-connection new-connection-mark=voip-con passthrough=yes src-address=20.22.17.0/28 dst-address=20.22.7.0/28 dscp=46

[admin@b1-balsapuerto] > ip firewall mangle add chain=forward action=mark-packet new-packet-mark=voip-con passthrough=no connection-mark=voip-con

[admin@b1-balsapuerto] > ip firewall mangle add chain=forward action=mark-connection new-connection-mark=video-con passthrough=yes src-address=20.23.7.2 dst-address=20.23.7.2 dscp=38

[admin@b1-balsapuerto] > ip firewall mangle add chain=forward action=mark-packet new-packet-mark=video passthrough=no connection-mark=video-con

[admin@b1-balsapuerto] > ip firewall mangle add chain=forward action=mark-connection new-connection-mark=video-con passthrough=yes src-address=20.22.17.0/28 dst-address=20.22.7.0/28 dscp=38

[admin@b1-balsapuerto] > ip firewall mangle add chain=forward action=mark-packet new-packet-mark=video passthrough=no connection-mark=video-con

[admin@b1-balsapuerto] > ip firewall mangle add chain=forward action=mark-connection new-connection-mark=besteffort-con passthrough=yes src-address=20.22.17.0/28 dst-address=20.22.7.0/28 dscp=0

[admin@b1-balsapuerto] > ip firewall mangle add chain=forward action=mark-packet new-packet-mark=besteffort passthrough=no connection-mark=besteffort-con
```

Queue Tree - Arbol de colas

```
[admin@b1-balsapuerto] > queue tree add name="trafico_total" parent=wlan1 limit-at=0 priority=8 max-limit=10485760 burst-limit=0 burst-threshold=0 burst-time=0s

[admin@b1-balsapuerto] > queue tree add name="leaf_besteffort" parent=trafico_total packet-mark=besteffort limit-at=1048576 queue=PCQ_besteffort priority=8 max-limit=10485760 burst-limit=0 burst-threshold=0 burst-time=0s

[admin@b1-balsapuerto] > queue tree add name="leaf_video" parent=trafico_total packet-mark=video limit-at=8388608 queue=SFQ_video priority=2 max-limit=10485760 burst-limit=0 burst-threshold=0 burst-time=0s

[admin@b1-balsapuerto] > queue tree add name="leaf_voip" parent=trafico_total packet-mark=voip limit-at=1048576 queue=SFQ_VoIP priority=1 max-limit=10485760 burst-limit=0 burst-threshold=0 burst-time=0s
```

Queue Type - Tipos de colas

```
[admin@b1-balsapuerto] > queue type add name="SFQ_VoIP" kind=sfq sfq-perturb=10 sfq-allot=1514

[admin@b1-balsapuerto] > queue type add name="SFQ_video" kind=sfq sfq-perturb=10 sfq-allot=1514

[admin@b1-balsapuerto] > queue type add name="PCQ_besteffort" kind=pcq pcq-rate=1048576 pcq-limit=50 pcq-classifier=dst-address pcq-total-limit=2000
```

4.3. Cliente: Centro de Salud de Balsapuerto

Placa Mikrotik Routerboard 433

Configuración de HTB en las placas Mikrotik

```
*****  
* RouterOS 4.5 *  
*****
```

```
Password  
*****  
[admin@MikroTik] > password  
gtrehasisf
```

```
Mangle - Marcado de Paquetes  
*****
```

```
[admin@c1-balsapuerto-ps] > ip firewall mangle add chain=prerouting action=mark-connection new-connection-mark=voip-con passthrough=yes src-address=20.23.7.2 dst-address=20.23.7.2 dscp=46
```

```
[admin@c1-balsapuerto-ps] > ip firewall mangle add chain=prerouting action=mark-packet new-packet-mark=voip passthrough=no connection-mark=voip-con
```

```
[admin@c1-balsapuerto-ps] > ip firewall mangle add chain=prerouting action=mark-connection new-connection-mark=voip-con passthrough=yes src-address=20.23.17.0/28 dst-address=20.23.7.0/28 dscp=46
```

```
[admin@c1-balsapuerto-ps] > ip firewall mangle add chain=prerouting action=mark-packet new-packet-mark=voip-con passthrough=no connection-mark=voip-con
```

```
[admin@c1-balsapuerto-ps] > ip firewall mangle add chain=prerouting action=mark-connection new-connection-mark=video-con passthrough=yes src-address=20.23.7.2 dst-address=20.23.7.2 dscp=38
```

```
[admin@c1-balsapuerto-ps] > ip firewall mangle add chain=prerouting action=mark-packet new-packet-mark=video passthrough=no connection-mark=video-con
```

```
[admin@c1-balsapuerto-ps] > ip firewall mangle add chain=prerouting action=mark-connection new-connection-mark=video-con passthrough=yes src-address=20.23.17.0/28 dst-address=20.23.7.0/28 dscp=38
```

```
[admin@c1-balsapuerto-ps] > ip firewall mangle add chain=prerouting action=mark-packet new-packet-mark=video passthrough=no connection-mark=video-con
```

```
[admin@c1-balsapuerto-ps] > ip firewall mangle add chain=prerouting action=mark-connection new-connection-mark=besteffort-con passthrough=yes src-address=20.23.17.0/28 dst-address=20.23.7.0/28 dscp=0
```

```
[admin@c1-balsapuerto-ps] > ip firewall mangle add chain=prerouting action=mark-packet new-packet-mark=besteffort passthrough=no connection-mark=besteffort-con
```

```
Queue Tree - Arbol de colas  
*****
```

```
[admin@c1-balsapuerto-ps] > queue tree add name="trafico_total" parent=br1 limit-at=0 priority=8 max-limit=10485760 burst-limit=0 burst-threshold=0 burst-time=0s
```

```
[admin@c1-balsapuerto-ps] > queue tree add name="leaf_besteffort" parent=trafico_total packet-mark=besteffort limit-at=1048576 queue=PCQ_besteffort priority=8 max-limit=10485760 burst-limit=0 burst-threshold=0 burst-time=0s
```

```
[admin@c1-balsapuerto-ps] > queue tree add name="leaf_video" parent=trafico_total packet-mark=video limit-at=8388608 queue=SFQ_video priority=2 max-limit=10485760 burst-limit=0 burst-threshold=0 burst-time=0s
```

```
[admin@c1-balsapuerto-ps] > queue tree add name="leaf_voip" parent=trafico_total packet-mark=voip limit-at=1048576 queue=SFQ_VoIP priority=1 max-limit=10485760 burst-limit=0 burst-threshold=0 burst-time=0s
```

Configuración de HTB en las placas Mikrotik

Queue Type - Tipos de colas

```
[admin@c1-balsapuerto-ps] > queue type add name="SFQ_VoIP" kind=sfq sfq-perturb=10  
sfq-allot=1514
```

```
[admin@c1-balsapuerto-ps] > queue type add name="SFQ_video" kind=sfq sfq-perturb=10  
sfq-allot=1514
```

```
[admin@c1-balsapuerto-ps] > queue type add name="PCQ_besteffort" kind=pcq pcq-  
rate=1048576 pcq-limit=50 pcq-classifier=dst-address pcq-total-limit=2000
```

Bibliografía

- [IEE07] IEEE. *IEEE 802.11-2007 Standard (Revision of IEEE Std 802.11-1999): Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. IEEE Computer Society, Nov 2007.
- [IEE09n] IEEE. *IEEE 802.11n-2009 Standard (Amendment to IEEE Std 802.11-2007): Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput*. IEEE Computer Society, Oct 2009.
- [Sim07] Javier Simo. *Modelado y optimización de IEEE 802.11 para su aplicación en el despliegue de redes extensas en zonas rurales aisladas de países en desarrollo*. Tesis Doctoral de Ingeniería de Telecomunicación, Universidad Politécnica de Madrid, Madrid, Ene 2007.
- [Lud11] Patricia Ludeña. *Estudio de aplicabilidad del estándar 802.11n para redes de larga distancia para entornos rurales en América Latina*, Parte II(3,4): 11-31. Proyecto Fin de Máster. Universidad Rey Juan Carlos, Madrid, 2011.
- [Lag11] José Luis lagunas. *Signal detection and cannel estimation over undetermined MIMO channels*. PhD thesis, Laval University, Québec, Abr 2011.
- [VY03] Branka Vucetic, Jinhong Yuan. *Space-Time Coding*, 2003
- [ACC08] Gerson Araujo, Luis Camacho, David Chavéz, César Córdova, David Espinoza, Renato Honda, Leopoldo Liñan, Jesús Margarito, Andrés Martinez, Eva Juliana Maya, Pablo Osuna, Yuri Pacheco, Juan Paco, Yvanna Quijandria, River Quispe, Carlos Rey, Sandra Salmerón, Arnau Sánchez, Paola Sanoni, Joaquín Seoane, Javier Simó y Jaime Vera. *Redes Inalámbricas para Zonas Rurales*. GTR-PUCP, 2008.
- [CQC09] Luis Camacho, River Quispe, César Córdova, Leopoldo Liñán, David Chávez. *WiLD (WiFi Based Long Distance)*, Capítulo 3: 41-53. GTR_PUCP, 2009.

- [Gas02] Matthew Gast. 802.11 Wireless Network: The Definitive Guide. 2002.
- [Fli07] Rob Flickenger. Redes Inalámbricas en los Países en Desarrollo, Capítulo 1, 2007.
- [Wil03] Jhon Wiley & Sons. Space Time Coding, Capítulo 3, 2003.
- [SMR10] Javier Simó, Andrés Martínez, Javier Ramos, Joaquín Seoane. Modeling and optimizing IEEE 802.11 DCF for long-distances links. IEEE Transactions on Mobile Computing. 2010.
- [Sal06] Sandra Salmerón. Parametrización de IEEE 802.11e EDCA para la priorización del tráfico VoIP en redes extensas para zonas rurales de países en vías de desarrollo. Tesis de Maestría en Telecomunicaciones. 2006.
- [IEE05e] IEEE. *IEEE 802.11e-2005 IEEE Standard for Information Technology – Medium Access Method (MAC) Quality of Service Enhancements*. IEEE Computer Society, 2005.
- [MBC06] MikroTik. Bandwidht Control. URL: http://wiki.mikrotik.com/wiki/Package_Flow, Feb 2006.
- [WCW06] MikroTik. Wireless Client and Wireless Access Point. URL: <http://www.mikrotik.com/testdocs/ros/3.0/interface/wireless.php>, Jan 2008.
- [MMP11] MikroTik. Manual: Packet Flow. URL: http://wiki.mikrotik.com/wiki/Package_Flow, Feb 2011.
- [MMH11] MikroTik. Manual: HTB. URL: <http://wiki.mikrotik.com/wiki/HTB>, Oct 2011.
- [Val05] Valens Riyadi. HTB Implementation on RouterOS QoS. URL: <http://mum.mikrotik.com/presentations/US09/Valens-MUM2009USA.pdf>, 2005
- [Meg09] Janis Megis, MikroTik RouterOS Workshop QoS Best Practice. URL: http://mum.mikrotik.com/presentations/US09/megis_qos.pdf, MUM USA, 2009
- [Cle05] Mario Clep. Implementación de un Sistema de QoS en RouterOS. URL: http://mum.mikrotik.com/presentations/AR09/mario_clep.pdf, Nov 2009.

- [Hub04] Bert Hubert. Enrutamiento avanzado y control de tráfico en Linux. URL: <http://www.gulic.org/almacen/lartc/lartc.pdf>, Dic 2004.
- [Ehw] Ehas Wiki. Página de ayuda de la Fundación EHAS. EHAS: Enlace Hispanoamericano de la Salud. URL: <http://wiki.ehas.org/index.php?title=Portada>
- [Dit] D-ITG. Página de la plataforma del generador de tráfico. URL: <http://www.grid.unina.it/software/ITG/>
- [MMW11] MikroTik. Manual: Winbox. URL: <http://wiki.mikrotik.com/wiki/Manual:Winbox>, May 2011.