



UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACSISTEL

INGENIERÍA EN TELECOMUNICACIONES

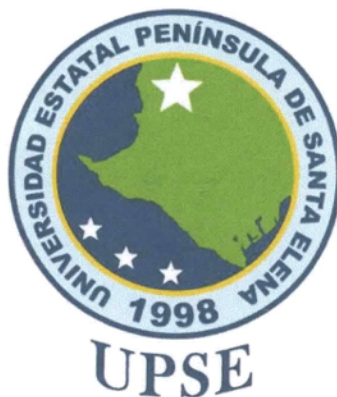
TRABAJO DE INTEGRACIÓN CURRICULAR

**Diseño y simulación de parámetros de prueba para
análisis en redes WISP aplicando virtualización en
entornos simulados**

Elvin Fabricio Pozo Ortega

Dirigido por:

Ing. Luis Amaya Fariño, Mgr.



**UNIVERSIDAD ESTATAL PENÍNSULA
DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES**

TRIBUNAL DE SUSTENTACIÓN

Ing. Ronald Rovira Jurado, Ph. D.
DIRECTOR DE LA CARRERA

Ing. Luis Amaya Fariño, Mgti.
TUTOR

Ing. Fernando Chamba
DOCENTE ESPECIALISTA

Ing. Luis Amaya Fariño, Mgti.
DOCENTE GUÍA UIC

Ing. Corina Gonzabay De La A, Mgtr.
SECRETARIA



**UNIVERSIDAD ESTATAL PENÍNSULA
DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES**

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por la cual apruebo en todas sus partes el presente trabajo de integración curricular que fue realizado en su totalidad por **Pozo Ortega Elvin Fabricio**, como requerimiento para la obtención del título de Ingeniero en Telecomunicaciones.

La Libertad, a los 03 días del mes de agosto del año 2026

TUTOR



Ing. Luis Amaya Fariño Mgti.



**UNIVERSIDAD ESTATAL PENÍNSULA
DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES**

DECLARACIÓN DE RESPONSABILIDAD

Yo, POZO ORTEGA ELVIN FABRICIO

DECLARO QUE:

El trabajo de integración curricular, **“Diseño y simulación de parámetros de prueba para análisis en redes WISP aplicando virtualización en entornos simulados”**, previo a la obtención del título de Ingeniero en Telecomunicaciones, ha sido desarrollado respetando derechos intelectuales de terceros conforme a las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente, este trabajo es de mi total autoría. En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Integración Curricular referido.

La Libertad, a los 03 días del mes de agosto del año 2026

EL AUTOR

Elvin Fabricio Pozo Ortega



**UNIVERSIDAD ESTATAL PENÍNSULA
DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES**

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de integración curricular denominado **Diseño y simulación de parámetros de prueba para análisis en redes WISP aplicando virtualización en entornos simulados**, presentado por el estudiante, **Pozo Ortega Elvin Fabricio**, fue enviado al Sistema Antiplagio, presentando un porcentaje de similitud correspondiente al 06%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.



Certificado de análisis
Compilatio Magister+ | UPSE-ECU

CAPITULO 1,2,3 y 4

ID : ca8eb70defcbd7ed3e54347dbc49b1093c8b46a7



6%

Textos sospechosos

Nombre del fichero : CAPITULO 1,2,3 y 4 .txt
Tamaño del archivo original : 63,59 MB
Número de palabras : 77.466

Depositante : AMAYA FARIÑO LUIS MIGUEL
Fecha de depósito : 20 de agosto de 2026
Tipo de carga : interface
fecha de fin de análisis : 20 de agosto de 2026

TUTOR

Ing. Luis Amaya Fariño Mgti.



**UNIVERSIDAD ESTATAL PENÍNSULA
DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES**

AUTORIZACIÓN

Yo, Pozo Ortega Elvin Fabricio

Autorizo a la Universidad Estatal Península de Santa Elena para que haga de este trabajo de integración curricular o parte de él un documento disponible para su lectura, consulta y procesos de investigación, según las normas de la Institución.[1]

Cedo los derechos en línea patrimoniales del artículo profesional de alto nivel con fines de difusión pública. Además, apruebo la reproducción de este artículo académico dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor.

Santa Elena, a los 03 días del mes de agosto del año 2026

EL AUTOR

Elvin Fabricio Pozo Ortega

AGRADECIMIENTO

Quiero dar gracias, en primer lugar, a Dios, pues soy un devoto creyente en Él. Gracias por ser la luz que iluminó cada paso de este camino, por darme la fuerza para no rendirme en los momentos más difíciles y por permitirme alcanzar esta meta que hoy se hace realidad.

Agradezco también a todos los maestros que me acompañaron durante la carrera por cada uno de los aprendizajes que serán fundamentales en mi vida profesional. De manera especial, al Ing. Carlos Andrade, por ser el impulso para ser mejor y por las oportunidades de aprendizaje que me brindó, tanto a nivel nacional como internacional; y a mi tutor, el Ing. Luis Amaya, por guiar cada paso del desarrollo de este trabajo de integración curricular.

Gracias, asimismo, a cada uno de los compañeros que conocí a lo largo de esta grandiosa etapa, quienes fueron un pilar fundamental durante todo el proceso. Y, por supuesto, a mis padres, por su ayuda y por darme el aliento que me motivó a salir adelante, a dar cada paso y a no rendirme.

Elvin Fabricio Pozo Ortega

DEDICATORIA

Dedico este logro, en primer lugar, a Dios, por ser esa luz que cada mañana me permite levantarme y me da la fuerza para seguir adelante.

A mis padres, por su apoyo incondicional, por los valores que me inculcaron desde pequeño y por enseñarme a levantarme en cada tropiezo y a superar cada obstáculo. A mis hermanos, abuelos, tíos y primos, que me alentaron a seguir adelante y celebraron conmigo cada meta alcanzada.

Dedico también este trabajo a todas las personas que estuvieron pendientes y me ayudaron en esta etapa: este logro no es solo mío, sino de cada una de ellas.

Y, por supuesto, a mi compañera de vida, alguien muy especial para mí. Gracias por tu apoyo y por tus palabras de aliento, por acompañarme en cada paso, por celebrar mis logros y ayudarme a levantarme en los momentos difíciles. Gracias por quedarte conmigo y por todo.

Elvin Fabricio Pozo Ortega

Índice general

TRIBUNAL DE SUSTENTACIÓN	II
CERTIFICACIÓN.....	III
DECLARACIÓN DE RESPONSABILIDAD	IV
DECLARO QUE:	IV
CERTIFICACIÓN DE ANTIPLAGIO	V
AUTORIZACIÓN	VI
AGRADECIMIENTO	VII
DEDICATORIA	VIII
Índice general	IX
Índice de figuras	XIV
Índice de tablas	XXI
Resumen	23
Abstract	24
Introducción	25
Capítulo 1: Aspectos introductorios	27
1.1. Antecedentes	27
1.2. Descripción del proyecto	28
1.3. Objetivos.....	30
1.3.1. Objetivo general	30
1.3.2. Objetivos específicos	31
1.4. Justificación	31
1.5. Problemática	32
1.6. Alcance del proyecto	36
1.7. Metodología	37

1.7.1. Enfoque experimental-aplicado	37
1.7.2. Enfoque documental-descriptivo.....	38
Capítulo 2: Marco teórico y conceptual de tecnologías de simulación de redes WISP	39
2.1. Introducción	39
2.2. Marco teórico.....	40
2.2.1. Virtualización, rendimiento, cobertura y seguridad en redes WISP	40
2.2.2. Emulación y simulación de redes híbridas WISP	56
2.2.3. Fortalecer la formación en redes inalámbricas mediante simulación	68
2.3. Simuladores de tráfico en redes	82
2.3.1. Tecnologías de simulación para generación de tráfico en redes	82
2.3.2. Estudio técnico de factibilidad en sistemas de propagación	97
2.4. Redes WISP.....	102
2.4.1. Técnicas de implementación de redes WISP	103
2.4.2. Tipos de redes WISP y su arquitectura.....	109
2.4.3. Calidad de servicio en redes WISP	113
2.4.4. Características técnicas en redes WISP	117
2.4.5. Justificación de las redes WISP en entornos académicos	118
2.5. Equipos de red simulados	120
2.5.1. Equipos MikroTik.....	120
2.5.2. MikroTik vs otros equipos WISP	122
2.5.3. Justificación técnica de la selección de equipos simulados	123
Capítulo 3: Diseño y desarrollo de la red WISP	124
3.1. Introducción del capítulo	124
3.2. Metodología de desarrollo del prototipo	125
3.2.1. Herramientas utilizadas en el desarrollo	126

3.2.2. Flujo de trabajo del diseño de la red	132
3.3. Diseño de la red WISP propuesta.....	133
3.3.1. Descripción de los componentes de red.....	134
3.3.2. Plan de direccionamiento IPv4	139
3.3.3. Diseño lógico de comunicación	147
3.4. Desarrollo de la simulación en GNS3	154
3.4.1. Instalación e integración de GNS3 con VMware Workstation	154
3.4.2. Integración de GNS3 con la máquina virtual GNS3 VM	166
3.4.3. Instalación de dispositivos MikroTik en GNS3	168
3.4.4. Selección de dispositivos para el prototipo WISP	170
3.4.5. Configuración del Router_Core (Gateway Central)	170
3.4.6. Configuración del Switch_Administrable.....	177
3.4.7. Configuración de Antena_Sectorial_Principal (Sector Rural)	183
3.4.8. Configuración del CPE_Rural (Sector Rural – VLAN 10)	189
3.4.9. Configuración del Router_Cliente_Rural.....	194
3.4.10. Configuración de dispositivos finales (PC1 y Windows-10).....	199
3.4.11. Configuración de los sectores Urbano y Empresas.....	205
3.4.12. Configuración del Backup_Rural.....	209
3.4.13. Configuración de los nodos de respaldo Urbano y Empresas.....	217
3.4.14. Topología final de la infraestructura WISP implementada	217
3.5. Desarrollo de la simulación en Atoll.....	219
3.5.1. Configuración inicial del proyecto.....	219
3.5.2. Configuración del canal y ancho de banda	220
3.5.3. Obtención e importación de datos geográficos	221
3.5.4. Configuración del proyecto en Atoll e importación de mapas	234

3.5.5. Configuración de las clases de obstáculos (Clutter Classes)	239
3.5.6. Colocación y configuración de antenas	242
3.5.7. Creación de los enlaces punto a multipunto (PTMP)	253
3.6. Resumen del capítulo	255
Capítulo 4: Resultados y validación de la red WISP propuesta	256
4.1. Introducción	256
4.2. Resultados de la simulación de la red WISP en GNS3	256
4.2.1. Validación del direccionamiento IP	256
4.2.2. Validación del servicio DHCP	260
4.2.3. Validación de la segmentación mediante VLAN	264
4.2.4. Verificación del acceso a internet	270
4.2.5. Análisis de transmisión y recepción de paquetes	274
4.2.6. Análisis estadístico de latencia	278
4.2.7. Evaluación del rendimiento de transferencia de datos	282
4.2.8. Validación de enlaces redundantes	286
4.2.9. Validación integral de la topología propuesta	288
4.3. Resultados de la planificación y cobertura en Atoll	289
4.3.1. Análisis de viabilidad de los enlaces inalámbricos	290
4.3.2. Resultados del modelo de propagación seleccionado	296
4.3.3. Análisis de niveles de señal recibida	298
4.3.4. Mapas de cobertura de la red WISP	301
4.3.5. Análisis de capacidad de transmisión de la red	303
4.3.6. Análisis de cobertura por transmisor	306
4.3.7. Análisis de nivel de ruido e interferencia	307
4.3.8. Validación tridimensional de los enlaces	309

4.3.9. Evaluación global de la cobertura proyectada	312
Conclusiones	313
Recomendaciones	315
Referencias	317
Anexo. Procedimiento de configuración completa de la red WISP	325

Índice de figuras

Figura 1. Evolución del acceso a internet en Ecuador (2014–2025).....	34
Figura 2. Mapa de virtualización de redes WISP	42
Figura 3. Métricas de rendimiento en redes WISP	46
Figura 4. Modelos de cobertura en redes WISP con simulación en Atoll.....	52
Figura 5. Seguridad de las redes WISP y mecanismos de protección.....	56
Figura 6. Emulación de redes híbridas con GNS3 y VMware Workstation	60
Figura 7. Evaluación de rendimiento en GNS3.....	64
Figura 8. Simulación de cobertura WISP en Atoll	67
Figura 9. Simulación educativa en redes WISP.....	72
Figura 10. Integración de Atoll y GNS3 para la evaluación de redes WISP.....	75
Figura 11. Metodologías activas para la enseñanza en redes inalámbricas	78
Figura 12. Estandarización de simulación en redes WISP.....	82
Figura 13. Diseño de una red en un entorno de simulación	83
Figura 14. Características de GNS3 para la simulación de redes	86
Figura 15. Captura de paquetes en Wireshark.....	96
Figura 16. Justificación de GNS3 para la simulación de redes.....	97
Figura 17. Factores que se pueden determinar en una simulación.....	98
Figura 18. Ventajas de los enlaces PTP	104
Figura 19. Limitaciones de los enlaces PTP.....	105
Figura 20. Ventajas de los enlaces punto a multipunto (PTMP).....	106
Figura 21. Desventajas de los enlaces punto a multipunto (PTMP)	106
Figura 22. Ventajas de las redes malladas.....	107
Figura 23. Desventajas de las redes malladas.....	108
Figura 24. Ventajas de las topologías híbridas	108
Figura 25. Características de redes WISP en zonas rurales.....	110
Figura 26. Características de redes WISP en zonas urbanas	111
Figura 27. Características técnicas destacadas del router MikroTik	121
Figura 28. Características técnicas destacadas del switch MikroTik CRS328-24P-4S+	121
Figura 29. Entorno de simulación de la topología WISP en GNS3.....	127
Figura 30. Entorno de modelado radioeléctrico en Atoll	128
Figura 31. Obtención de información topográfica mediante EarthExplorer.....	129
Figura 32. Información de cobertura terrestre obtenida mediante ESA WorldCover	130

Figura 33. Procesamiento de datos de cobertura terrestre de ESA WorldCover en Global Mapper.....	131
Figura 34. Modelo digital del terreno obtenido de EarthExplorer en Global Mapper	131
Figura 35. Flujo de trabajo del diseño del prototipo de red WISP.....	133
Figura 36. Diseño esquemático de la red WISP.....	134
Figura 37. Router principal implementado mediante MikroTik CHR en GNS3.....	135
Figura 38. Switch administrable implementado en la red WISP simulada	136
Figura 39. Representación lógica de la antena sectorial en GNS3	136
Figura 40. Antena sectorial Ubiquiti LiteAP LAP-120 utilizada como referencia en Atoll	136
Figura 41. Representación lógica de los clientes inalámbricos en GNS3	137
Figura 42. Antena Ubiquiti NanoStation Loco5AC utilizada como referencia en Atoll.....	138
Figura 43. Routers cliente implementados en GNS3.....	138
Figura 44. Topología lógica de la red WISP simulada en GNS3	140
Figura 45. Arquitectura de segmentación VLAN de la red WISP	148
Figura 46. Flujo de tráfico por segmento de red	150
Figura 47. Topología lógica del plano de gestión y administración (VLAN 100).....	153
Figura 48. Apertura de la máquina virtual GNS3 VM en VMware Workstation	155
Figura 49. Error de virtualización durante el arranque de GNS3 VM.....	156
Figura 50. Ejecución del comando msinfo32 desde Windows.....	157
Figura 51. Verificación del estado de seguridad basada en virtualización	157
Figura 52. Descarga del archivo dgreediness_v3.6.zip desde el portal oficial de Microsoft.....	158
Figura 53. Extracción del archivo dgreediness_v3.6.zip	159
Figura 54. Ejecución de Windows PowerShell como administrador	159
Figura 55. Desactivación del hipervisor mediante PowerShell.....	160
Figura 56. Navegación hacia la carpeta Downloads mediante PowerShell.....	161
Figura 57. Acceso a la carpeta Downloads desde PowerShell.....	162
Figura 58. Acceso a la carpeta dgreediness_v3.6	163
Figura 59. Error de permisos de ejecución en PowerShell	163
Figura 60. Modificación temporal de la política de ejecución en PowerShell	164
Figura 61. Ejecución exitosa del script DG_Readiness_Tool_v3.6.ps1	165
Figura 62. Verificación de seguridad basada en virtualización deshabilitada.....	166
Figura 63. Configuración del enlace entre GNS3 y GNS3 VM	167
Figura 64. Instalación del router MikroTik CHR en GNS3.....	169
Figura 65. Instalación del switch MikroTik CRS en GNS3	169
Figura 66. Configuración de identidad y conectividad WAN del Router_Core	172

Figura 67. Configuración de VLAN en el Router_Core.....	174
Figura 68. Configuración de direccionamiento IPv4 en el Router_Core.....	176
Figura 69. Configuración de servicios DNS y NAT en el Router_Core.....	177
Figura 70. Configuración inicial del Switch_Administrable.....	179
Figura 71. Configuración de la interfaz de gestión del Switch_Administrable.....	180
Figura 72. Configuración de enlaces troncales mediante VLAN en el Switch_Administrable.....	182
Figura 73. Activación del filtrado de VLAN en el Switch_Administrable.....	183
Figura 74. Configuración inicial de la Antena_Sectorial_Principal.....	185
Figura 75. Configuración de la interfaz de gestión de la Antena_Sectorial_Principal.....	187
Figura 76. Configuración de canales troncales y filtrado VLAN de la Antena_Sectorial_Principal.....	189
Figura 77. Configuración inicial del CPE_Rural y asociación de interfaces al bridge.....	190
Figura 78. Configuración de la interfaz de gestión del CPE_Rural.....	192
Figura 79. Configuración de VLAN y filtrado de tráfico del CPE_Rural.....	194
Figura 80. Configuración del enlace WAN del Router_Cliente_Rural.....	196
Figura 81. Configuración del segmento LAN y servicio DHCP del Router_Cliente_Rural.....	198
Figura 82. Configuración del protocolo NAT en el Router_Cliente_Rural.....	199
Figura 83. Configuración y validación de conectividad en dispositivos finales del sector rural.....	201
Figura 84. Configuración del adaptador virtual VMnet10 en VMware Workstation.....	203
Figura 85. Configuración de hardware y red de Windows 10.....	204
Figura 86. Configuración de la máquina virtual Windows 10 en GNS3.....	205
Figura 87. Configuración de integración del Backup_Rural en la Antena_Sectorial_Principal.....	210
Figura 88. Configuración estructural del BACKUP_ZONAL_1.....	213
Figura 89. Configuración de gestión y filtrado del BACKUP_ZONAL_1.....	214
Figura 90. Configuración del anillo de respaldo RSTP en el CPE_Rural.....	216
Figura 91. Topología final de la infraestructura WISP implementada.....	218
Figura 92. Selección de la plantilla de proyecto Wi-Fi en Atoll.....	219
Figura 93. Tabla de bandas de frecuencia en Atoll (Radio Network Settings > Frequency > Bands).....	220
Figura 94. Selección del dataset SRTM 1 Arc-Second Global en USGS EarthExplorer.....	222
Figura 95. Definición del área de búsqueda mediante coordenadas sobre la península de Santa Elena en EarthExplorer.....	222
Figura 96. Identificación del tile SRTM correcto sobre la península de Santa Elena en la pestaña Results.....	223
Figura 97. Opciones de descarga del tile SRTM en formato GeoTIFF.....	224
Figura 98. Archivos GeoTIFF descargados desde USGS EarthExplorer para la zona de Santa Elena.....	224
Figura 99. Carga de archivos GeoTIFF en Global Mapper.....	225

Figura 100. Visualización del relieve de la península de Santa Elena en Global Mapper tras cargar los archivos SRTM	226
Figura 101. Configuración de la proyección UTM Zona 17S (WGS84) en Global Mapper para exportar el relieve en metros.....	227
Figura 102. Selección del formato de exportación Vertical Mapper Grid File en Global Mapper	228
Figura 103. Activación de la generación del archivo de proyección (.prj) en Global Mapper	228
Figura 104. Visualización de la capa ESA WorldCover V2 2021 sobre la península de Santa Elena	229
Figura 105. Definición del Bounding Box y opciones de descarga en ESA WorldCover para la zona de Santa Elena	230
Figura 106. Archivos descargados de ESA WorldCover.....	231
Figura 107. Configuración de proyección UTM Zona 17S en Global Mapper para los archivos de cobertura ESA WorldCover.....	232
Figura 108. Selección del formato Vertical Mapper Classified/Clutter Grid File en Global Mapper	232
Figura 109. Configuración de archivos complementarios de exportación en Global Mapper	233
Figura 110. Configuración de límites de exportación en Global Mapper (Export Bounds).....	234
Figura 111. Asignación del nombre y guardado del archivo de exportación en Global Mapper	234
Figura 112. Configuración del sistema de coordenadas WGS84 / UTM Zone 17S (EPSG: 32717) en las propiedades del proyecto Atoll.....	235
Figura 113. Ventana de importación del archivo de elevación (.grd) en Atoll.....	236
Figura 114. Mapa de elevación del terreno de la península de Santa Elena correctamente cargado en Atoll.....	237
Figura 115. Ventana de importación del archivo de Clutter (.grc) en Atoll.....	238
Figura 116. Mapa de uso de suelo (ESA WorldCover) cargado en Atoll sobre la península de Santa Elena	238
Figura 117. Configuración del servidor de mapa satelital (Google Satellite) en la opción Online Maps de Atoll	239
Figura 118. Ventana de propiedades de Clutter Classes en Atoll mostrando la configuración de alturas e Indoor Loss por tipo de cobertura.....	241
Figura 119. Verificación visual de la capa de Clutter en Atoll, confirmando la correcta asignación de colores por tipo de cobertura	242
Figura 120. Distribución de las antenas de la red WISP sobre el mapa satelital de la península de Santa Elena en Atoll.....	243
Figura 121. Parámetros reales de antenas configurados en el simulador Atoll.....	245
Figura 122. Configuración de la pestaña Cell de la antena principal en Atoll	246
Figura 123. Configuración de la pestaña Transmitter de la antena principal en Atoll.....	247
Figura 124. Configuración de la pestaña Cell de la antena CPE-Urbano en Atoll	248
Figura 125. Configuración de la pestaña Transmitter de la antena CPE-Urbano en Atoll.....	249
Figura 126. Configuración de la pestaña Cell de la antena CPE-Empresas en Atoll.....	250

Figura 127. Configuración de la pestaña Transmitter de la antena CPE-Empresas en Atoll.....	251
Figura 128. Configuración de la pestaña Cell de la antena CPE-Rural en Atoll.....	252
Figura 129. Configuración de la pestaña Transmitter de la antena CPE-Rural en Atoll.....	253
Figura 130. Selección de la opción Hub with links en el menú New PMP de la barra de herramientas de Atoll	254
Figura 131. Vista final de los enlaces PTMP establecidos entre la antena principal y las antenas CPE sobre el mapa de la península de Santa Elena en Atoll.....	254
Figura 132. Verificación del direccionamiento IP en el Router_Core.....	258
Figura 133. Verificación del direccionamiento IP en la antena sectorial principal.....	258
Figura 134. Verificación del direccionamiento IP en el Router_Cliente_Rural.....	259
Figura 135. Verificación del direccionamiento IP en el Router_Cliente_Urbano	259
Figura 136. Verificación del direccionamiento IP en el Router_Empresas	259
Figura 137. Asignación dinámica de dirección IP mediante DHCP en PC1 de la VLAN 10 Rural	261
Figura 138. Configuración completa de red en la máquina virtual Windows 10 de la VLAN 10 Rural.....	261
Figura 139. Asignación DHCP exitosa en PC2 de la VLAN 20 Urbana	262
Figura 140. Verificación de los parámetros DHCP en la máquina virtual Ubuntu de la VLAN 20 Urbana.....	263
Figura 141. Asignación DHCP y verificación de conectividad en PC3 de la VLAN 30 Empresas	263
Figura 142. Verificación de la configuración DHCP en la máquina virtual Kali Linux de la VLAN 30 Empresas	264
Figura 143. Pruebas de conectividad ICMP desde el Router_Core hacia todos los nodos de infraestructura a través de la VLAN 100 de gestión.....	265
Figura 144. Verificación de conectividad desde el Router_Core hacia los routers de acceso Rural, Urbano y Empresas mediante ping a través de sus respectivas VLAN.....	266
Figura 145. Verificación de conectividad desde el Router_Core hacia los dispositivos de respaldo de las zonas Rural, Urbana y Empresarial a través de la VLAN 100 de gestión.....	266
Figura 146. Prueba de ping desde PC1 de la VLAN 10 Rural hacia el gateway 10.0.10.1, mostrando respuestas exitosas y tiempos de latencia estables sin pérdida de paquetes.....	267
Figura 147. Verificación de conectividad en la VLAN 10 Rural desde la máquina virtual Windows 10.....	267
Figura 148. Prueba de ping desde PC2 hacia el gateway de la VLAN 20 Urbana	268
Figura 149. Verificación de conectividad en la VLAN 20 Urbana desde la máquina virtual Ubuntu	268
Figura 150. Prueba de ping desde PC3 de la VLAN 30 Empresas hacia el gateway 10.0.30.1	269
Figura 151. Verificación de la segmentación VLAN 30 Empresas desde la máquina virtual Kali Linux	269
Figura 152. Verificación del acceso a internet desde PC1 de la VLAN 10 Rural mediante ping a google.com.....	270
Figura 153. Navegación web exitosa desde la máquina virtual Windows 10 de la VLAN 10 Rural.....	271
Figura 154. Verificación del acceso a internet desde PC2 de la VLAN 20 Urbana mediante ping a google.com	272
Figura 155. Navegación web desde la máquina virtual Ubuntu de la VLAN 20 Urbana	272

Figura 156. Verificación del acceso a internet desde PC3 de la VLAN 30 Empresas mediante ping a google.com ...	273
Figura 157. Navegación web exitosa desde la máquina virtual Kali Linux de la VLAN 30 Empresas	273
Figura 158. Captura de tráfico local en la VLAN 10 Rural (VMnet10)	274
Figura 159. Captura de tráfico de salida en la VLAN 10 Rural (VMnet10)	275
Figura 160. Captura de tráfico local en la VLAN 20 Urbana (VMnet11).....	276
Figura 161. Captura de tráfico de salida en la VLAN 20 Urbana.....	276
Figura 162. Captura de tráfico local en la VLAN 30 Empresas (VMnet12)	277
Figura 163. Captura de tráfico externo en la VLAN 30 Empresas (VMnet12)	278
Figura 164. Análisis estadístico de latencia en la VLAN 10 Rural desde Windows 10	279
Figura 165. Análisis estadístico de latencia en la VLAN 20 Urbana desde Ubuntu.....	280
Figura 166. Análisis estadístico de latencia en la VLAN 30 Empresas desde Kali Linux.....	281
Figura 167. Resultado del Bandwidth Test desde el Router_Core hacia el Router_Cliente_Rural (10.0.10.254) mediante WinBox.....	283
Figura 168. Resultado del Bandwidth Test desde el Router_Core hacia el Router_Cliente_Urbano (10.0.20.254) mediante WinBox.....	284
Figura 169. Resultado del Bandwidth Test desde el Router_Core hacia el Router_Empresas (10.0.30.254) mediante WinBox.....	285
Figura 170. Simulación de fallo del enlace principal hacia CPE_Rural mediante inhabilitación de ether2 en la antena sectorial principal.....	287
Figura 171. Simulación de fallo del enlace hacia CPE_Urbano mediante inhabilitación de ether3 en la antena sectorial principal.....	287
Figura 172. Simulación de fallo del enlace hacia CPE_Empresas mediante inhabilitación de ether4 en la antena sectorial principal.....	288
Figura 173. Perfil topográfico del enlace inalámbrico entre la antena principal y el CPE-Rural (VLAN 10).....	291
Figura 174. Perfil topográfico del enlace inalámbrico entre la antena principal y el CPE-Urbano (VLAN 20).....	292
Figura 175. Perfil topográfico del enlace inalámbrico entre la antena principal y el CPE-Empresas (VLAN 30).....	293
Figura 176. Análisis de la primera zona de Fresnel en el enlace antena principal – CPE-Rural (VLAN 10).....	294
Figura 177. Análisis de la primera zona de Fresnel en el enlace antena principal – CPE-Urbano (VLAN 20).....	295
Figura 178. Análisis de la primera zona de Fresnel en el enlace antena principal – CPE-Empresas (VLAN 30).....	296
Figura 179. Configuración del modelo de propagación ITU-R P.526 en la ventana de predicciones de Atoll para la red WISP de la provincia de Santa Elena	297
Figura 180. Mapa de calor de niveles de señal recibida (RSSI) generado por la predicción Effective Signal Analysis (DL) en Atoll para la red WISP de Santa Elena	299

Figura 181. Mapa de cobertura por niveles de señal (Coverage by Signal Level DL) generado en Atoll para la red WISP.....	302
Figura 182. Mapa de capacidad de transmisión (Coverage by Throughput DL) generado en Atoll para la red WISP de Santa Elena.....	304
Figura 183. Mapa de cobertura por transmisor (Coverage by Transmitter, DL)	306
Figura 184. Mapa de predicción de nivel total de ruido e interferencia (Coverage by Total Noise (I+N) Level DL) generado en Atoll.....	308
Figura 185. Validación tridimensional de los enlaces de la red WISP en Google Earth Pro	310

Índice de tablas

Tabla 1. Análisis del uso de simuladores en redes WISP en universidades ecuatorianas	33
Tabla 2. Evolución del acceso a internet en Ecuador (2014–2025) [13].....	34
Tabla 3. Comparación de características entre GNS3 y SEED	62
Tabla 4. Ventajas y desventajas del uso de simuladores en redes inalámbricas.....	71
Tabla 5. Comparativa técnica de GNS3 vs otros simuladores.....	87
Tabla 6. Análisis comparativo de capturadores y analizadores de tráfico de red	88
Tabla 7. Tipos de análisis de tráfico en herramientas de monitoreo.....	89
Tabla 8. Comparativa de interfaz de usuario en herramientas de análisis de tráfico.....	90
Tabla 9. Comparativa de niveles de protocolo soportados por herramientas de análisis	91
Tabla 10. Comparativa de captura de tráfico en tiempo real.....	92
Tabla 11. Comparativa de exportación y análisis forense.....	93
Tabla 12. Comparativa de costo y licenciamiento.....	94
Tabla 13. Características del simulador Atoll.....	99
Tabla 14. Modelos de propagación en el simulador Atoll.....	100
Tabla 15. Comparativa técnica entre Atoll, Radio Mobile e iBwave	101
Tabla 16. Comparativa entre redes WISP rurales y urbanas	111
Tabla 17. Comparativa entre redes WISP, FTTH, LTE y satelitales	113
Tabla 18. Parámetros técnicos de calidad de servicio en redes WISP	115
Tabla 19. Comparativa de características técnicas en arquitecturas de redes WISP.....	117
Tabla 20. Comparativa técnica entre MikroTik y otros equipos virtuales en GNS3	122
Tabla 21. Características técnicas de la antena sectorial utilizada como referencia en Atoll	137
Tabla 22. Características técnicas de la antena CPE utilizada como referencia en Atoll	138
Tabla 23. Esquema general de direccionamiento IPv4.....	141
Tabla 24. Resumen de enlaces troncales entre el Router_Core y cada segmento de red.....	141
Tabla 25. Direccionamiento IPv4 de la VLAN 100 — segmento de gestión y administración	142
Tabla 26. Detalle de conexiones entre dispositivos de la topología lógica	143
Tabla 27. Direccionamiento IPv4 del segmento rural (VLAN 10).....	144
Tabla 28. Conexiones de dispositivos — segmento rural (VLAN 10).....	144
Tabla 29. Direccionamiento IPv4 del segmento urbano (VLAN 20).....	145
Tabla 30. Conexiones de dispositivos — segmento urbano (VLAN 20)	145
Tabla 31. Direccionamiento IPv4 del segmento empresarial (VLAN 30).....	146
Tabla 32. Conexiones de dispositivos — segmento empresarial (VLAN 30).....	146

Tabla 33. VLAN implementadas en la red WISP propuesta	147
Tabla 34. Subinterfaces y rutas del Router_Core.....	151
Tabla 35. Jerarquía de caminos RSTP por sector	154
Tabla 36. Equivalencia de dispositivos implementados en GNS3	170
Tabla 37. Parámetros comparativos de configuración de los sectores Rural, Urbano y Empresas.....	207
Tabla 38. Parámetros diferenciales de los nodos de respaldo por sector.....	217
Tabla 39. Configuración de clases de obstáculos (Clutter Classes) en Atoll para la península de Santa Elena	240
Tabla 40. Parámetros de antena Ubiquiti LiteAP LAP-120.....	244
Tabla 41. Parámetros de antena NanoStation Loco5AC para las CPE	244
Tabla 42. Parámetros de celda configurados para la antena principal en Atoll.....	245
Tabla 43. Parámetros de transmisor configurados para la antena principal en Atoll	246
Tabla 44. Parámetros de celda configurados para la antena CPE-Urbano en Atoll	247
Tabla 45. Parámetros de transmisor configurados para la antena CPE-Urbano en Atoll.....	248
Tabla 46. Parámetros de celda configurados para la antena CPE-Empresas en Atoll	249
Tabla 47. Parámetros de transmisor configurados para la antena CPE-Empresas en Atoll	250
Tabla 48. Parámetros de celda configurados para la antena CPE-Rural en Atoll.....	251
Tabla 49. Parámetros de transmisor configurados para la antena CPE-Rural en Atoll.....	252
Tabla 50. Resumen comparativo de latencia por VLAN para tráfico local (gateway) y tráfico externo (8.8.8.8) en la red WISP simulada.....	281
Tabla 51. Niveles de señal recibida (RSSI) máximo y mínimo estimados por sector mediante Effective Signal Analysis (DL).....	300
Tabla 52. Velocidades estimadas de descarga (Throughput DL) en cada sector analizado	305
Tabla 53. Relación C/(I+N) estimada por sector a partir del RSSI y el Total Noise (I+N)	309

Resumen

En un ambiente controlado, la presente propuesta de tesis desarrolla el diseño y la simulación de una red WISP orientada a brindar servicio de internet inalámbrico en la provincia de Santa Elena, mediante la implementación de parámetros de prueba estandarizados aplicados sobre dos entornos complementarios: GNS3 para la topología lógica de la red y Atoll para el análisis de propagación radioeléctrica, con el fin de evaluar el rendimiento, la cobertura y la viabilidad técnica de la infraestructura propuesta.

Se plantea una topología punto a multipunto (PTMP), en la cual una antena principal ubicada en las instalaciones de la universidad actúa como transmisor central, mientras que tres antenas CPE representan los sectores rural, urbano y empresarial. En GNS3 se configuran el enrutamiento, la segmentación mediante VLAN, la traducción de direcciones NAT y el protocolo de redundancia RSTP, mientras que en Atoll se parametrizan los equipos de radiofrecuencia, las alturas de instalación y las condiciones de terreno, con el fin de generar mapas de cobertura ajustados a la zona de estudio. Todo ello se organiza en etapas de planificación, diseño, implementación y evaluación.

Con ello se logra un entorno de simulación funcional y replicable, capaz de representar el comportamiento de una red WISP real. Esta propuesta constituye, además, un recurso pedagógico que facilita el aprendizaje práctico en telecomunicaciones y contribuye a disminuir la brecha entre la formación académica y las necesidades del entorno laboral.

Palabras clave: WISP, GNS3, Atoll, simulación, propagación radioeléctrica, cobertura, VLAN, RSTP.

Abstract

In a controlled environment, this thesis proposal develops the design and simulation of a WISP network intended to provide wireless internet service in the province of Santa Elena, through the implementation of standardized test parameters applied to two complementary environments: GNS3 for the logical topology of the network and Atoll for radio propagation analysis, in order to evaluate the performance, coverage, and technical feasibility of the proposed infrastructure.

A point-to-multipoint (PTMP) topology is proposed, in which a main antenna located at the university facilities acts as the central transmitter, while three CPE antennas represent the rural, urban and business sectors. In GNS3, routing, VLAN segmentation, network address translation (NAT) and the RSTP redundancy protocol are configured, whereas in Atoll the radio frequency equipment, installation heights and terrain conditions are parameterized in order to generate coverage maps adjusted to the study area. All of this is organized into planning, design, implementation, and evaluation stages.

As a result, a functional and replicable simulation environment is achieved, capable of representing the behavior of a real WISP network. This proposal also constitutes a pedagogical resource that facilitates practical learning in telecommunications and helps to reduce the gap between academic training and the needs of the professional environment.

Keywords: WISP, GNS3, Atoll, simulation, radio propagation, coverage, VLAN, RSTP.

Introducción

En la era digital actual, el acceso a internet se ha convertido en un servicio esencial que incide directamente en los ámbitos educativo, laboral, económico y social. La conectividad ha dejado de ser un privilegio para convertirse en un derecho fundamental, reconocido como un habilitador del desarrollo individual y colectivo. Sin embargo, en muchas regiones del mundo, particularmente en zonas rurales o de difícil acceso, persisten serias limitaciones para garantizar un acceso confiable y de calidad a servicios de telecomunicaciones. Esta situación plantea la necesidad urgente de explorar e implementar soluciones innovadoras y sostenibles que permitan ampliar la cobertura de redes y cerrar la brecha digital.

En este contexto, las redes WISP (Wireless Internet Service Provider) emergen como una alternativa eficaz y de bajo costo para llevar conectividad a sectores desatendidos. Un WISP es un proveedor de servicios de internet que utiliza tecnologías inalámbricas para distribuir conectividad desde un punto central hacia múltiples usuarios finales. Estas redes hacen uso de enlaces punto a punto y punto a multipunto, así como de tecnologías de radiofrecuencia (RF) y antenas direccionales, para alcanzar áreas donde las redes cableadas como la fibra óptica o el cobre resultan poco viables por razones económicas, geográficas o logísticas [1].

El presente proyecto de tesis se centra en el diseño y simulación de una red WISP, con el propósito de desarrollar un modelo funcional y replicable que pueda ser utilizado en entornos académicos y profesionales. La propuesta tiene una doble finalidad: por un lado, busca demostrar la viabilidad técnica y operativa de una red WISP mediante simulación lógica y física; por otro lado, pretende constituirse en una herramienta pedagógica que contribuya a la formación de futuros profesionales en telecomunicaciones, redes e ingeniería [1].

Para lograr este objetivo, se han empleado dos plataformas de simulación ampliamente reconocidas: GNS3 (Graphical Network Simulator-3) para el diseño lógico y la simulación de protocolos de red, y Atoll para la simulación de cobertura y propagación de señal inalámbrica en un entorno geográfico realista. Estas herramientas permiten construir una representación integral del funcionamiento de una red WISP, desde su arquitectura básica hasta los parámetros técnicos que afectan la calidad del servicio (QoS) [2].

La metodología adoptada combina un enfoque experimental-aplicado, que permite diseñar, simular, probar y optimizar una red en un entorno virtual, con un enfoque documental-descriptivo, que respalda el proceso mediante una revisión exhaustiva de literatura técnica, normativa y científica. Esta combinación metodológica garantiza un proceso sistemático, fundamentado y orientado a resultados, permitiendo no solo validar técnicamente el sistema propuesto, sino también documentar y sistematizar el procedimiento para su reutilización en contextos educativos o de formación técnica [3].

El proyecto se desarrolla en cuatro fases principales:

- Diseño lógico de la red en GNS3, donde se configura una topología que incluye un router principal (simulando el NOC), enlaces punto a punto, un router central de distribución, un switch gestionable y varios usuarios finales conectados a través de routers individuales.
- Diseño físico de cobertura en Atoll, en el que se simula un entorno geográfico real, incluyendo torres, obstáculos, distancia entre nodos y condiciones de propagación, con el objetivo de generar mapas de cobertura y evaluar la calidad de la señal.
- Pruebas de validación técnica, utilizando métricas como latencia, throughput, jitter y disponibilidad de los enlaces, para comprobar la funcionalidad y desempeño de la red bajo distintas condiciones simuladas.
- Optimización de la red, ajustando parámetros de configuración, ubicación de nodos y protocolos, con el fin de maximizar la eficiencia, cobertura y calidad del servicio.

Este trabajo adquiere especial relevancia dentro del ámbito educativo, ya que responde a una problemática identificada en el proceso de enseñanza-aprendizaje de asignaturas como redes de datos, comunicaciones inalámbricas y planificación de redes. A menudo, los estudiantes carecen de recursos físicos para practicar la implementación de redes inalámbricas reales, y la simulación se presenta como una alternativa viable para suplir estas limitaciones. Al mismo tiempo, el proyecto contribuye a la formación de competencias técnicas, analíticas y metodológicas en el diseño, configuración, monitoreo y optimización de redes, lo que los prepara para su inserción en el campo laboral con un enfoque práctico y actualizado [3].

En definitiva, la tesis busca demostrar que es posible diseñar y validar una red WISP completamente funcional mediante herramientas de simulación, documentando cada paso del proceso de forma detallada, para que sirva de modelo pedagógico y profesional. La propuesta no solo promueve la innovación en la enseñanza de redes y telecomunicaciones, sino que también propone una solución concreta a la brecha digital, especialmente en zonas donde el acceso a internet sigue siendo limitado. Así, se plantea una contribución académica con impacto real, al servicio de la educación, la tecnología y el desarrollo social [1].

Capítulo 1: Aspectos introductorios

1.1. Antecedentes

En la actualidad, la creciente demanda de conectividad en áreas urbanas y rurales ha impulsado el desarrollo de soluciones innovadoras en el ámbito de las telecomunicaciones. Los Proveedores de Servicios de Internet Inalámbrico (WISP) han emergido como una alternativa viable para ofrecer acceso a internet en zonas donde las infraestructuras tradicionales son limitadas o inexistentes. Diversos estudios han abordado la implementación y simulación de redes WISP, destacando la importancia de herramientas como GNS3 y Atoll para su análisis y diseño.

En 2018, Patricio Germánico Caisaguano Pérez desarrolló un estudio enfocado en el diseño y simulación de una red WISP para la ciudad de Pedernales, en la provincia de Manabí, Ecuador. El objetivo principal fue proporcionar acceso a internet mediante una red inalámbrica, considerando las características geográficas y demográficas de la región. El estudio incluyó la selección de equipos, análisis de cobertura y evaluación de costos, utilizando herramientas de simulación para validar la viabilidad del proyecto [1].

En 2021, Andrés Wladimir Párraga Lara y Juan Carlos Aspiazu Rovira llevaron a cabo un proyecto en la Universidad Politécnica Salesiana que consistió en el análisis, diseño e implementación de un módulo WISP como herramienta práctica para el laboratorio de telecomunicaciones. El propósito fue proporcionar a los estudiantes una plataforma para comprender y experimentar con redes inalámbricas, facilitando la adquisición de habilidades prácticas en el manejo de equipos y configuraciones de redes WISP [4].

Carlos William Suárez González, en 2022, realizó un estudio en la Universidad Estatal Península de Santa Elena sobre la implementación de redes comunitarias WISP en la comuna Bellavista del Cerro. El proyecto tuvo como objetivo brindar un servicio de internet inalámbrico en una zona rural con limitada infraestructura tecnológica. Se consideraron aspectos técnicos, sociales y económicos para diseñar una red eficiente y sostenible que beneficiara a la comunidad [5].

En un estudio realizado por Manuel Alejandro Ponce Monterrosas en la Universidad Nacional Autónoma de México (UNAM), se evaluó el uso de GNS3 como herramienta educativa para la simulación de redes. La investigación demostró que GNS3 permite emular dispositivos reales, facilitando el desarrollo de prácticas de laboratorio sin necesidad de hardware físico. El autor propuso su integración en la enseñanza de redes para mejorar la comprensión y el dominio de conceptos técnicos, destacando su utilidad en la formación de competencias prácticas aplicables al entorno profesional [6].

En 2020, en la Universidad Politécnica Salesiana, se desarrolló un proyecto titulado “Diseño e implementación de un banco de pruebas para simulación de redes”, cuyo objetivo fue abordar los desafíos actuales en la administración y seguridad de redes mediante la creación de un banco de pruebas innovador y realista, empleando herramientas de software libre disponibles en la plataforma GNS3. Este estudio destaca la importancia de la simulación en entornos controlados para la formación académica y la optimización de redes [7].

Por tanto, se espera que este proyecto no solo contribuya al desarrollo de una red de pruebas virtual sólida, sino que también sirva como referencia para futuras investigaciones y aplicaciones prácticas orientadas al despliegue eficiente de redes WISP. A través de esta iniciativa se busca fortalecer la capacidad técnica de los estudiantes y profesionales del sector, al mismo tiempo que se impulsa el uso de tecnologías digitales para reducir la brecha de conectividad en zonas tradicionalmente desatendidas.

1.2. Descripción del proyecto

La implementación de este parámetro controlado, relacionado con entornos virtuales, se establece dentro de la descripción del proyecto como una evidencia de la necesidad educativa de

fomentar en los estudiantes de la carrera de Telecomunicaciones el uso de herramientas de simulación. Esto permite desarrollar un adecuado control y comprensión sobre los recursos necesarios para la implementación física de este tipo de proyectos. En este contexto, la presente investigación surge como una propuesta técnica y formativa dentro del campo de las telecomunicaciones, específicamente enfocada en la planificación, análisis y validación de redes WISP (Wireless Internet Service Provider). El proyecto busca responder a una problemática recurrente dentro del ámbito educativo y profesional: la brecha existente entre la teoría impartida en el aula y la realidad práctica a la que se enfrentan los futuros ingenieros al momento de implementar redes inalámbricas en entornos reales [8].

En muchos casos, al hablar de redes inalámbricas, se tiende a considerar únicamente la instalación física de equipos, sin tomar en cuenta que todo diseño de red debería estar precedido por un análisis técnico profundo que permita anticipar errores, reducir pérdidas económicas y garantizar un desempeño óptimo del sistema. En este sentido, el proyecto plantea una alternativa eficiente y educativamente valiosa: el uso de entornos simulados para la validación de parámetros críticos en redes WISP, utilizando herramientas ampliamente reconocidas como GNS3 y Atoll [8].

El enfoque principal se centra en la implementación y estandarización de un conjunto de parámetros de prueba que puedan ser utilizados como base para evaluar el rendimiento de redes WISP en escenarios virtuales. Este conjunto incluirá indicadores como la intensidad de señal, la relación señal/ruido (SNR), el comportamiento del tráfico bajo diferentes condiciones de carga, la latencia, la pérdida de paquetes, el jitter, entre otros. Dichos parámetros permitirán medir de forma objetiva el desempeño de una red antes de ser implementada en el terreno, lo que representa una ventaja significativa tanto para proyectos académicos como para soluciones reales en zonas donde el acceso a internet por medios tradicionales es limitado o costoso [9].

La propuesta contempla el diseño de un entorno de simulación estructurado en dos fases. En primer lugar, se trabajará con GNS3, una herramienta que permite emular el comportamiento de routers, switches, firewalls y otros dispositivos de red, facilitando la construcción de topologías similares a las utilizadas por proveedores reales de servicios inalámbricos. A través de esta plataforma se desarrollarán escenarios donde se pondrán a prueba configuraciones típicas de redes

WISP, incluyendo la administración del ancho de banda, el enrutamiento, las políticas de seguridad y la segmentación de red [9].

En la segunda fase, se utilizará Atoll, un software de planificación radioeléctrica especializado en el análisis de propagación de señales inalámbricas. Este programa permite simular condiciones reales del entorno (como la orografía, obstáculos físicos, interferencias, densidad de usuarios, entre otros) para evaluar el comportamiento de la red en términos de cobertura, interferencia y calidad del enlace. Al integrar GNS3 y Atoll en un mismo proceso de simulación, se logrará una visión completa y detallada de cómo se comportaría la red WISP en condiciones reales, sin necesidad de invertir en costosos equipos físicos ni de realizar pruebas directamente en campo [10].

Un componente clave de este trabajo será la elaboración de una guía metodológica, pensada como un recurso de apoyo tanto para estudiantes como para docentes y profesionales del área. Esta guía incluirá un paso a paso para la configuración de entornos de simulación, recomendaciones sobre qué parámetros observar y cómo interpretarlos, ejemplos de topologías y sugerencias para la mejora del rendimiento de las redes. Se busca así aportar no solo un producto académico, sino una herramienta didáctica útil y replicable en otros contextos educativos.

En definitiva, este proyecto no pretende ser únicamente una simulación técnica, sino una propuesta integral que combina la innovación educativa con la solución de una necesidad real en el diseño de redes inalámbricas. El uso de herramientas como GNS3 y Atoll, integradas dentro de una metodología clara y con parámetros definidos, permitirá generar conocimientos aplicables y formar profesionales mejor preparados para enfrentar los desafíos del mundo laboral en el ámbito de las telecomunicaciones [10].

1.3. Objetivos

1.3.1. Objetivo general

Implementar un conjunto de parámetros de prueba estandarizados para el análisis y validación de redes WISP en entornos simulados mediante GNS3 y Atoll, con el propósito de

mejorar la precisión en el diseño, la optimización y la planificación de infraestructuras inalámbricas.

1.3.2. Objetivos específicos

- Diseñar un ambiente controlado con parámetros de prueba más relevantes para evaluar el rendimiento, cobertura y seguridad de redes WISP.
- Diseñar un escenario de prueba en GNS3 para la implementación y configuración de dispositivos que conforman la red WISP.
- Diseñar un escenario de prueba en Atoll para analizar el rendimiento de la red WISP bajo diferentes condiciones de enlace, interferencia y cobertura.
- Desarrollar una guía metodológica para la aplicación de la simulación en la formación académica y optimización de redes WISP, incluyendo mejores prácticas, herramientas y ajustes de configuración.

1.4. Justificación

La presente investigación cobra relevancia en un momento donde la eficiencia y precisión en el diseño de redes inalámbricas son factores críticos para asegurar una conectividad estable, escalable y de bajo costo. En este marco, la integración de herramientas de simulación como GNS3 y Atoll en los procesos de análisis y validación técnica constituye una estrategia clave para la formación de profesionales altamente capacitados y la optimización de recursos en el ámbito de las telecomunicaciones [11].

GNS3, al permitir emular topologías completas con routers, switches, firewalls y otros dispositivos de red, facilita el desarrollo de competencias en configuración, enrutamiento, segmentación de redes y gestión del tráfico. Por su parte, Atoll permite simular variables físicas como el entorno geográfico, interferencias, niveles de señal y pérdida por obstáculos, lo cual aporta una visión más realista y técnica sobre la viabilidad de una red inalámbrica en condiciones específicas. La combinación de ambas herramientas permite una evaluación holística de una red WISP, integrando aspectos lógicos y físicos en un entorno controlado [11].

La estandarización de parámetros de prueba, como la latencia, throughput, pérdida de paquetes y cobertura efectiva, facilitará la construcción de modelos predictivos robustos, los cuales permitirán simular el comportamiento de una red antes de su implementación, reduciendo así los riesgos técnicos y económicos. Además, esta estandarización constituye un aporte metodológico valioso tanto para el ámbito académico como para el empresarial, ya que permitirá replicar experimentos, validar resultados y construir buenas prácticas de diseño [12].

Desde el punto de vista formativo, el proyecto busca cerrar la brecha entre teoría y práctica, promoviendo una educación basada en la experimentación y la resolución de problemas reales, lo cual incrementa la empleabilidad de los egresados y eleva la calidad de los programas de estudio. En el ámbito profesional, se potencia la eficiencia en la implementación de redes, se reduce la posibilidad de errores en campo y se mejora la planificación a largo plazo.

En definitiva, esta investigación representa una contribución significativa al fortalecimiento del ecosistema de redes inalámbricas, al brindar un marco técnico y práctico que impulse la innovación, la eficiencia y la calidad tanto en la formación académica como en el ejercicio profesional del diseño e implementación de redes WISP.

1.5. Problemática

La expansión del acceso a internet en Ecuador ha experimentado un notable avance en la última década. Si bien, como se observa en la Tabla 1, algunas universidades han desarrollado tesis relacionadas con telecomunicaciones y simuladores, los trabajos específicos sobre redes WISP en entornos simulados son escasos y poco sistematizados. Esta brecha evidencia la necesidad de incorporar entornos virtuales como GNS3 y Atoll con metodologías estandarizadas que fortalezcan la enseñanza-aprendizaje, garanticen la calidad de los diseños y preparen adecuadamente a los futuros profesionales del sector, especialmente en zonas rurales, donde la cobertura ha pasado del 14,6 % en 2014 al 45 % en 2025, como se evidencia en la Tabla 2. Este crecimiento ha sido impulsado en gran medida por el desarrollo de redes WISP (Wireless Internet Service Provider), que han permitido superar las limitaciones de infraestructura en áreas de difícil acceso. A pesar de este progreso, la formación práctica en el diseño y despliegue de estas redes aún presenta desafíos importantes dentro del ámbito académico.

Tabla 1. *Análisis del uso de simuladores en redes WISP en universidades ecuatorianas*

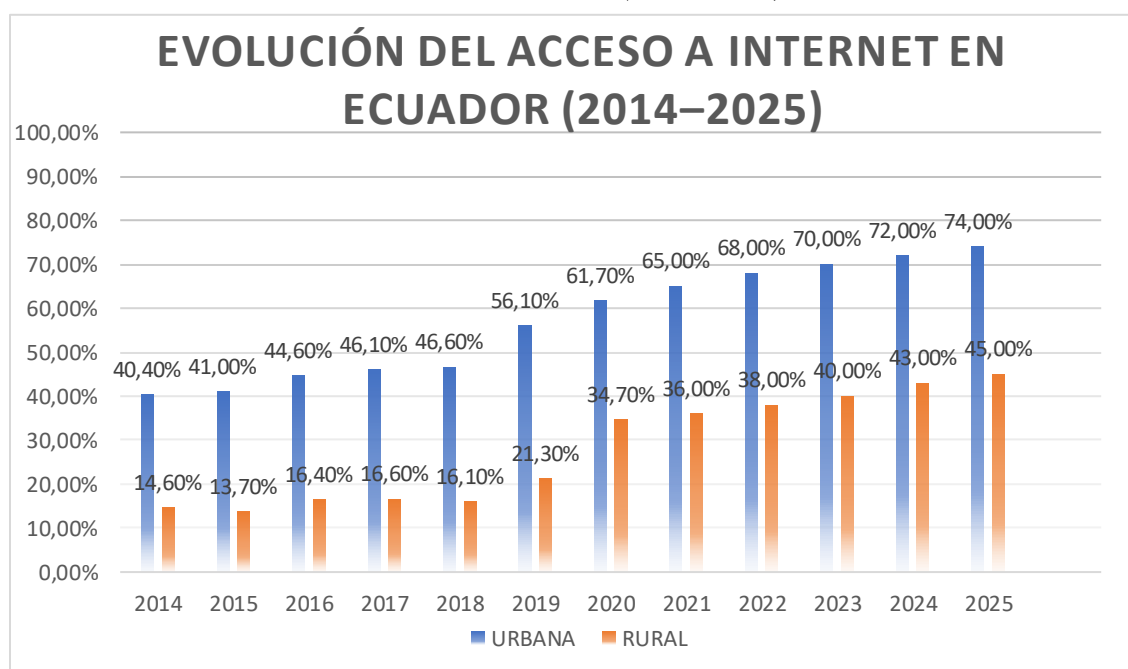
Universidades	Tipos de tesis	Tesis sobre redes WISP en entornos simulados
ESPOL	Implementación de una herramienta didáctica de redes Bluetooth. Simulación de redes inteligentes para telefonía fija. Seguridad en redes de comunicación para laboratorios. Simulación de servicios de red inteligente para telefonía. Simulación de sistemas de cancelación ciega en sistemas DMT.	Ninguna.
Universidad Politécnica Salesiana (UPS)	Modelamiento de redes para medición inteligente. Sistema de alarma inalámbrica con respuesta WAP.	Diseño y simulación de un WISP para la ciudad de Pedernales. Red ISP gratuita en espacios públicos.
Pontificia Universidad Católica del Ecuador (PUCE)	Proveedor de servicios de internet en la Ciudad Borbón. WISP para la comunidad de Pulinguí. ISP para Guangopolo. ISP en Lago San Pablo. VoD, VoIP e internet en la ciudad de Ibarra. WLAN con IoT para el Hotel Río Suites.	Análisis y diseño de redes WISP para zonas rurales.

Tabla 2. *Evolución del acceso a internet en Ecuador (2014–2025)* [13]

Año	Población total estimada	Hogares con acceso a internet en zonas urbanas (%)	Aproximado de personas con internet (zona urbana)	Hogares con acceso a internet en zonas rurales (%)	Aproximado de personas con internet (zona rural)
2014	16 000 000	40,4 %	4 078 784	14,6 %	861 984
2015	16 300 000	41,0 %	4 216 973	13,7 %	824 013
2016	16 510 000	44,6 %	4 646 343	16,4 %	999 119
2017	16 760 000	46,1 %	4 875 333	16,6 %	1 026 617
2018	17 050 000	46,6 %	5 013 484	16,1 %	1 012 923
2019	17 340 000	56,1 %	6 138 203	21,6 %	1 382 067
2020	17 550 000	61,7 %	6 832 688	34,7 %	2 247 154
2021	17 680 000	65,0 %	7 251 452	36,0 %	2 348 611
2022	17 820 000	68,0 %	7 646 205	38,0 %	2 498 720
2023	17 980 000	70,0 %	7 941 766	40,0 %	2 653 848
2024	18 190 492	72,0 %	8 264 304	43,0 %	2 886 285
2025	19 000 000	74,0 %	8 871 860	45,0 %	3 154 950

Población urbana 63,1 % y rural 36,9 %

Representación gráfica

Figura 1. *Evolución del acceso a internet en Ecuador (2014–2025)*

En el contexto actual de crecimiento acelerado de las telecomunicaciones en Ecuador, la implementación de redes WISP (Wireless Internet Service Provider) se ha consolidado como una solución eficiente para extender el acceso a internet, especialmente en zonas rurales o de difícil acceso. Según DataReportal (2025), el porcentaje de acceso a internet en áreas rurales ha aumentado de apenas un 14,6 % en 2014 a un estimado del 45 % en 2025, evidenciando un progreso significativo en la conectividad digital fuera de los núcleos urbanos. Este crecimiento ha sido posible, en gran medida, gracias a tecnologías inalámbricas como las redes WISP, que permiten superar las limitaciones de infraestructura propias del entorno rural [14].

No obstante, este tipo de redes exige un diseño detallado y una validación rigurosa de parámetros técnicos como línea de vista, interferencia espectral, pérdidas de enlace y capacidad de cobertura, ya que su descuido puede comprometer seriamente la calidad del servicio y la viabilidad del despliegue en campo. Uno de los principales desafíos que enfrentan tanto instituciones educativas como empresas emergentes del sector tecnológico es la brecha existente entre el conocimiento teórico impartido y su aplicación práctica en entornos reales.

Este problema se agrava en muchos programas de instituciones educativas superiores, donde la incorporación de entornos de simulación especializados es limitada o inexistente. Una de las razones principales es el alto costo asociado a la implementación de laboratorios físicos de telecomunicaciones, lo cual limita significativamente las oportunidades de aprendizaje práctico para los estudiantes. Ante esta realidad, se vuelve fundamental contar con sistemas simulados adecuados, que permitan generar distintos entornos de trabajo virtuales en los que se puedan aplicar y validar conceptos técnicos clave.

Herramientas como GNS3, que permite emular dispositivos de red y realizar pruebas en entornos controlados, y Atoll, que facilita la planificación detallada de redes inalámbricas mediante análisis de cobertura, topografía y propagación de señal, representan una alternativa eficaz para complementar la formación académica. Sin embargo, estas plataformas suelen ser subutilizadas o aplicadas sin una estructura metodológica clara, lo que limita su impacto formativo [15].

La consecuencia de esta situación es una preparación deficiente para enfrentar retos técnicos en el campo profesional. Un uso inadecuado o insuficiente de estas plataformas puede

derivar en errores en la proyección, dimensionamiento y ejecución de infraestructuras WISP, impactando negativamente en la calidad del servicio, los costos de implementación y la sostenibilidad del proyecto. A esto se suma la falta de estandarización de parámetros de prueba en los entornos virtuales, lo que dificulta la comparación objetiva de resultados, la repetibilidad de pruebas y la generación de buenas prácticas en el diseño de redes inalámbricas [4].

Por tanto, se identifica una necesidad urgente de establecer un conjunto de parámetros de prueba estandarizados que sirvan de guía en la simulación y análisis de redes WISP. Esto permitirá no solo fortalecer el aprendizaje aplicado, sino también preparar profesionales más competentes, capaces de diseñar, evaluar y optimizar infraestructuras inalámbricas desde la simulación hasta la ejecución real, garantizando su eficiencia, seguridad y cobertura [1].

1.6. Alcance del proyecto

El presente proyecto tiene como objetivo el diseño, simulación, validación y documentación de una red inalámbrica del tipo WISP (Wireless Internet Service Provider) utilizando herramientas especializadas como GNS3 y Atoll. La iniciativa contempla la creación de un entorno virtual que permita emular con precisión los distintos componentes de una red WISP, incluyendo enlaces troncales, routers de distribución, enlaces punto a punto, antenas sectoriales y equipos de cliente final [16].

Mediante GNS3, se desarrollarán topologías funcionales de red que simulen el comportamiento lógico y operativo de la infraestructura, tales como el enrutamiento, la asignación de direcciones IP, la gestión de tráfico y la seguridad a nivel de capa de red. Paralelamente, con el software Atoll se llevará a cabo la simulación del diseño físico, enfocándose en la cobertura de señal, interferencias, pérdidas por obstáculos, análisis de línea de vista (LoS) y otros aspectos esenciales para garantizar la eficiencia de la propagación de la señal en el terreno [17].

El alcance técnico del proyecto incluye la elaboración de un conjunto de parámetros estandarizados de prueba que permitan evaluar el rendimiento de la red virtualizada, tales como latencia, ancho de banda, pérdida de paquetes, jitter y calidad de la cobertura. Estos parámetros servirán como base para validar el diseño previo a una posible implementación física, contribuyendo a reducir riesgos y errores en el despliegue real de una red WISP [18].

En términos de formación profesional, el proyecto busca beneficiar a estudiantes y técnicos en telecomunicaciones mediante el desarrollo de una guía metodológica que pueda ser utilizada como referencia para prácticas de laboratorio, proyectos de titulación o entrenamiento en simulación de redes. Asimismo, se proyecta que los resultados puedan ser adaptables a escenarios empresariales reales, ofreciendo una herramienta útil para pequeños y medianos proveedores de internet (ISP) que requieran optimizar sus procesos de diseño y planificación sin incurrir inicialmente en altos costos de infraestructura [4].

Finalmente, el alcance del proyecto también comprende la elaboración de un documento técnico que consolide las configuraciones, resultados, análisis y recomendaciones obtenidos durante el proceso. Este documento servirá como base para futuras investigaciones, mejoras sucesivas del modelo simulado y la implementación de sistemas de monitoreo y seguridad que puedan integrarse en fases posteriores del desarrollo de redes WISP [4].

1.7. Metodología

La metodología adoptada en este proyecto combina un enfoque experimental-aplicado y un enfoque documental-descriptivo, con el objetivo de garantizar un proceso sistemático, reproducible y riguroso para el diseño y simulación de una red WISP (Wireless Internet Service Provider). Esta combinación metodológica permite abordar tanto la validación técnica del entorno simulado como la sistematización de los procedimientos empleados, con miras a generar un modelo replicable en contextos académicos y profesionales.

1.7.1. Enfoque experimental-aplicado

Este enfoque se centra en la construcción, simulación y validación de una red WISP a través de entornos virtuales. El desarrollo sigue las siguientes etapas:

Diseño lógico de red en GNS3: Se plantea una topología de red que incluye el router principal (simulando el NOC o punto de salida hacia internet), enlaces punto a punto, router central, switch administrable, clientes con routers y subredes diferenciadas. Se configuran protocolos de enrutamiento, direccionamiento IP, firewall básico y gestión de tráfico [19].

Diseño físico de cobertura en Atoll: Se selecciona una zona geográfica representativa para simular las condiciones reales de propagación de señal inalámbrica. Se modelan elementos como torres, obstáculos físicos, distancia entre nodos y se genera el mapa de cobertura RF. Se evalúan parámetros como línea de vista, pérdidas por trayectoria y nivel de señal recibido (RSRP) [20].

Pruebas y validación: Se definen parámetros de prueba estandarizados (latencia, throughput, jitter) y se ejecutan escenarios simulados para evaluar el comportamiento de la red bajo distintas condiciones. Se documentan los resultados y se comparan con valores esperados en un entorno real [12].

Optimización: Con base en los resultados obtenidos, se realizan ajustes en la topología, protocolos o distribución de nodos con el fin de optimizar la eficiencia y el rendimiento del sistema.

1.7.2. Enfoque documental-descriptivo

Este enfoque respalda la parte teórica del proyecto, permitiendo estructurar una base sólida de conocimientos y referencias mediante las siguientes actividades:

Revisión bibliográfica: Se recopila información actualizada sobre redes WISP, metodologías de simulación, herramientas como GNS3 y Atoll, estándares de calidad de servicio (QoS) y parámetros técnicos recomendados por la literatura y las normas internacionales. Las fuentes incluyen tesis, artículos académicos, manuales técnicos y documentación de fabricantes [11].

Análisis comparativo: Se analizan proyectos similares para identificar buenas prácticas, errores comunes, herramientas más eficaces y formas de validar resultados. Esto permite construir un marco de referencia sólido para la propuesta metodológica propia.

Sistematización del procedimiento: Se documentan detalladamente todas las fases del proceso experimental (desde la planificación hasta el análisis de resultados), con el propósito de generar una guía metodológica replicable que pueda ser utilizada como referencia en entornos educativos, de investigación o empresariales [21].

Capítulo 2: Marco teórico y conceptual de tecnologías de simulación de redes WISP

2.1. Introducción

En el desarrollo de soluciones inalámbricas como las redes WISP (Wireless Internet Service Provider), la planificación adecuada y la simulación previa de escenarios posibles no solo son recomendables, sino fundamentales. Antes de cualquier despliegue físico, es necesario comprender a fondo el comportamiento de la red bajo diferentes condiciones técnicas, topológicas y geográficas; esto permite reducir fallos, optimizar recursos y asegurar una experiencia de conectividad satisfactoria para los usuarios finales [1].

Este capítulo tiene como propósito analizar las tecnologías de simulación más relevantes para el diseño y estudio de redes WISP, enfocándose tanto en herramientas de tráfico como en sistemas de propagación de señales. A través de este análisis se busca establecer cuáles son las plataformas más adecuadas para modelar redes de acceso inalámbrico desde una perspectiva técnica, educativa y práctica [1].

Se parte del estudio de simuladores de tráfico como GNS3, Cisco Packet Tracer y EVE-NG, evaluando sus ventajas, limitaciones, compatibilidad con equipos reales y su capacidad para emular entornos de red complejos. Posteriormente, se profundiza en simuladores de propagación como Atoll, Radio Mobile e iBwave, fundamentales para predecir la cobertura de la señal en distintos tipos de terreno [22].

Además, se examina cómo estas tecnologías permiten evaluar la viabilidad técnica de diferentes arquitecturas de redes WISP como los enlaces punto a punto, punto a multipunto y redes malladas, comparando su rendimiento frente a otras tecnologías de acceso como FTTH, LTE o satelital [1].

Esta revisión también incluye un estudio detallado de los equipos de red utilizados en un entorno físico real, destacando sus capacidades, protocolos soportados, rendimiento y aplicabilidad dentro de proyectos WISP. Aunque la implementación del proyecto se desarrolla en un entorno de simulación, se realiza un análisis basado en especificaciones técnicas reales, a fin de reflejar con mayor precisión los desafíos, ventajas y limitaciones que estos equipos

representarían en una instalación física. Este análisis resulta especialmente útil en contextos académicos, ya que facilita una aproximación práctica al hardware profesional y su vinculación con escenarios de aprendizaje técnico [1].

Gracias a este enfoque, no solo se justifica la selección de cada herramienta y tecnología, sino que se aporta una visión integral que combina teoría, simulación práctica y pertinencia en contextos educativos, como el de una universidad o centro de formación técnica.

2.2.Marco teórico

2.2.1. Virtualización, rendimiento, cobertura y seguridad en redes WISP

Este apartado se centra en el análisis integral de las redes inalámbricas WISP, abordando aspectos clave tanto técnicos como operativos. En primer lugar, se explora el uso de la virtualización en entornos de laboratorio como una herramienta efectiva para simular escenarios reales de red y facilitar pruebas controladas. A continuación, se identifican y aplican métricas fundamentales que permiten evaluar el rendimiento de estas redes, considerando variables como la latencia y el throughput. Posteriormente, se introducen modelos de cobertura desarrollados con simuladores de propagación, los cuales permiten prever el comportamiento del enlace inalámbrico en distintas condiciones geográficas. Finalmente, se examinan las principales amenazas de seguridad en redes WISP, junto con los protocolos y soluciones actuales que permiten mitigar riesgos y proteger la integridad de la red y sus usuarios.

Virtualización de redes en entornos de laboratorio para pruebas WISP

La virtualización de redes ha emergido como una herramienta fundamental en el desarrollo, implementación y validación de tecnologías inalámbricas, especialmente en el contexto de redes WISP (Wireless Internet Service Provider). Este enfoque consiste en crear réplicas funcionales de componentes de red mediante software, sin necesidad de utilizar infraestructura física real. Esta capacidad permite simular entornos de red complejos, evaluar su comportamiento bajo condiciones controladas y realizar pruebas exhaustivas sin los altos costos asociados al hardware tradicional [23].

En el ámbito académico y profesional, la virtualización representa una ventaja significativa, ya que permite a los estudiantes, técnicos e ingenieros diseñar y validar arquitecturas de red de forma económica, segura y escalable. Esto es especialmente valioso para las redes WISP, que operan en contextos de conectividad inalámbrica punto a punto o multipunto, en zonas urbanas, periurbanas y rurales, donde es necesario planificar cuidadosamente la cobertura, la capacidad y la interferencia [23].

Entre las herramientas más utilizadas para la virtualización de redes se encuentra GNS3 (Graphical Network Simulator-3), una plataforma que permite simular arquitecturas de red avanzadas en un entorno gráfico interactivo. GNS3 es ampliamente adoptado en el ámbito de las telecomunicaciones debido a su capacidad para emular dispositivos reales como routers, switches gestionables y firewalls, utilizando imágenes reales de sistemas operativos de red como Cisco IOS, MikroTik RouterOS o Juniper JunOS. Una de sus principales ventajas es la posibilidad de integrarse con software de virtualización como VirtualBox o VMware, ampliando su funcionalidad para incluir servidores, estaciones de monitoreo, generadores de tráfico o clientes finales [24].

Por su parte, VMware Workstation, desarrollado por VMware, es una herramienta de virtualización de código abierto que permite ejecutar múltiples sistemas operativos invitados sobre un mismo sistema anfitrión. En el contexto de pruebas para redes WISP, VMware Workstation facilita la creación de entornos virtuales que simulan el funcionamiento de clientes (como estaciones base o CPE), servidores web, sistemas de autenticación (Radius), herramientas de análisis de tráfico (como Wireshark o NetFlow Analyzer), y hasta sistemas de seguridad como firewalls con pfSense o IDS como Snort [25].

La combinación de GNS3 y VMware Workstation permite construir laboratorios virtuales altamente realistas y funcionales, que replican con precisión los escenarios presentes en implementaciones reales de redes WISP. En estos entornos virtuales es posible interconectar routers, switches y otros dispositivos dentro de un entorno virtualizado, así como puntos de acceso, estaciones base, enlaces backhaul y nodos de distribución. Además, se pueden integrar servidores DNS, DHCP, Radius y herramientas de monitoreo, lo que posibilita un control total sobre las variables técnicas de la red [26].

Este tipo de arquitectura híbrida ofrece un entorno ideal para estudiar y evaluar aspectos clave del diseño y operación de redes inalámbricas, tales como el rendimiento de enlaces (mediante métricas como throughput, latencia y jitter), la gestión de la interferencia entre canales, la optimización de rutas para el transporte eficiente de datos y la implementación de estrategias de seguridad como segmentación de red, firewalling y control de acceso. Asimismo, permite reproducir escenarios de falla y recuperación, congestión de tráfico, actualizaciones de firmware, e incluso ataques controlados para probar la resiliencia de la red [3].

La virtualización también posibilita la replicabilidad de las pruebas, un factor crucial en entornos académicos, donde se requiere que los estudiantes puedan replicar procedimientos y resultados como parte del proceso de aprendizaje. Adicionalmente, las instituciones pueden documentar las configuraciones y escenarios simulados en forma de guías de laboratorio, lo que enriquece los programas de formación técnica en telecomunicaciones [27].

En conclusión, la virtualización de redes en laboratorios para pruebas WISP no solo optimiza recursos y permite una exploración técnica profunda, sino que también representa una herramienta pedagógica de alto valor. Su adopción fomenta el aprendizaje práctico, el pensamiento crítico y la innovación en el diseño de redes inalámbricas, siendo una base sólida para el desarrollo de capacidades profesionales en el campo de las telecomunicaciones modernas. En la Figura 2 se presenta un mapa mental que resume los componentes esenciales abordados en este apartado respecto a la virtualización de redes WISP.

Figura 2. Mapa de virtualización de redes WISP



Métricas clave para evaluar el rendimiento de redes inalámbricas

La evaluación del rendimiento de redes inalámbricas, especialmente en entornos WISP (Wireless Internet Service Provider), constituye un componente fundamental para garantizar la calidad del servicio (QoS) y la experiencia del usuario final. A diferencia de las redes cableadas, las redes WISP están sujetas a diversas condiciones ambientales, topográficas y de interferencia que pueden afectar directamente su eficiencia. Por ello, se requiere un monitoreo constante y riguroso de ciertas métricas clave que permiten diagnosticar problemas, optimizar configuraciones y validar las estrategias de diseño e implementación de la red.

Entre las principales métricas utilizadas para evaluar el rendimiento de una red inalámbrica se encuentran:

1. Throughput (rendimiento efectivo)

El throughput es la cantidad de datos que son transmitidos exitosamente desde un emisor a un receptor en un tiempo determinado, expresada generalmente en bits por segundo (bps). Esta métrica difiere del ancho de banda teórico, ya que refleja el rendimiento real teniendo en cuenta pérdidas, retransmisiones y retrasos. En una red WISP, el throughput puede verse afectado por factores como interferencia entre estaciones, congestión del canal, eficiencia del protocolo y calidad de la señal [28].

Importancia: Un throughput bajo puede indicar problemas de saturación, interferencia o equipos mal configurados. Mediante herramientas de simulación o monitoreo real, los administradores pueden establecer umbrales y diseñar topologías que maximicen este parámetro [28].

2. Latencia (delay)

La latencia representa el tiempo que tarda un paquete de datos en viajar desde el origen hasta el destino y se mide generalmente en milisegundos (ms). En aplicaciones como VoIP, videoconferencias o juegos en línea, una latencia baja es indispensable para mantener una comunicación fluida [29].

Factores que afectan la latencia: distancia física entre nodos, procesamiento en los dispositivos intermedios (routers, firewalls), congestión de red, calidad de los enlaces y presencia de retransmisiones por errores [29].

Umbrales típicos: una latencia menor a 50 ms se considera buena en redes locales, aunque en redes WISP puede variar dependiendo de la topografía y los equipos utilizados [29].

3. Jitter

El jitter es la variación en el tiempo de llegada de los paquetes de datos. Es especialmente crítico en aplicaciones en tiempo real, como voz y video, ya que una alta variabilidad puede generar interrupciones perceptibles, como audio entrecortado o video pixelado [30].

Causas del jitter: cambios en la ruta de los paquetes, congestión de red, buffers mal configurados, interferencia y colisiones en el canal inalámbrico [30].

Solución común: uso de búferes de jitter o priorización de tráfico mediante QoS.

4. Pérdida de paquetes (packet loss)

Se refiere al porcentaje de paquetes que se pierden durante la transmisión y no llegan a su destino. La pérdida de paquetes puede deberse a errores de transmisión, interferencia, saturación del canal o fallos en los equipos de red [16].

Impacto: afecta negativamente la calidad del servicio, sobre todo en aplicaciones en tiempo real. Además, puede generar retransmisiones automáticas (como en TCP), reduciendo el throughput y aumentando la latencia [16].

Valor ideal: lo más cercano a 0 %. Valores superiores al 1 % o 2 % pueden generar degradaciones notables [16].

5. Relación señal/ruido (SNR – Signal to Noise Ratio)

La relación señal/ruido (SNR) es una métrica fundamental en telecomunicaciones que mide la calidad de una señal en comparación con el nivel de ruido presente en el canal de transmisión. Se expresa en decibelios (dB), y un valor alto de SNR indica que la señal es mucho más fuerte que el ruido, lo cual se traduce en una transmisión más confiable y con menos errores [31].

Valores típicos de SNR y su interpretación:

- SNR > 20 dB: excelente calidad de señal.
- SNR entre 13 y 20 dB: aceptable, pero puede haber errores.
- SNR < 13 dB: problemas frecuentes de transmisión.

Relación matemática entre SNR y BER

En comunicaciones digitales, la tasa de error de bits (BER) está relacionada con la calidad de la señal recibida y la presencia de ruido en el canal. En particular, para canales con ruido aditivo gaussiano blanco (AWGN), la BER puede expresarse en función de la relación señal/ruido (SNR) mediante funciones estadísticas asociadas a la distribución normal [31].

Para modulaciones binarias en canales AWGN, una forma general de estimar la BER es:

$$BER \approx \frac{1}{2} * erfc(\sqrt{SNR})$$

donde:

- $erfc(\cdot)$ es la función complemento del error, que se usa para calcular probabilidades relacionadas con la dispersión gaussiana del ruido.
- $\sqrt{SNR}$ se refiere a la raíz cuadrada del SNR expresado en escala lineal (no en dB).

Función erfc(x)

La función complemento del error, $erfc(x)$, se define como:

$$erfc(x) = 1 - \operatorname{erf}(x)$$

donde $\operatorname{erf}(x)$ (*función error*) está definida como:

$$\operatorname{erf}(x) = \frac{2}{\sqrt{\pi}} \int_0^x e^{-t^2} dt$$

Estas funciones son comunes en la teoría de la probabilidad y la estadística, especialmente cuando se trabaja con ruido gaussiano, ya que permiten estimar la probabilidad de error en la detección de símbolos transmitidos [31].

La función erfc mide el área bajo la curva de una distribución gaussiana estándar a partir de un punto x hasta el infinito. A mayor x , menor es el valor de $\text{erfc}(x)$, y, por ende, menor la BER [31].

Conversión de SNR a escala lineal

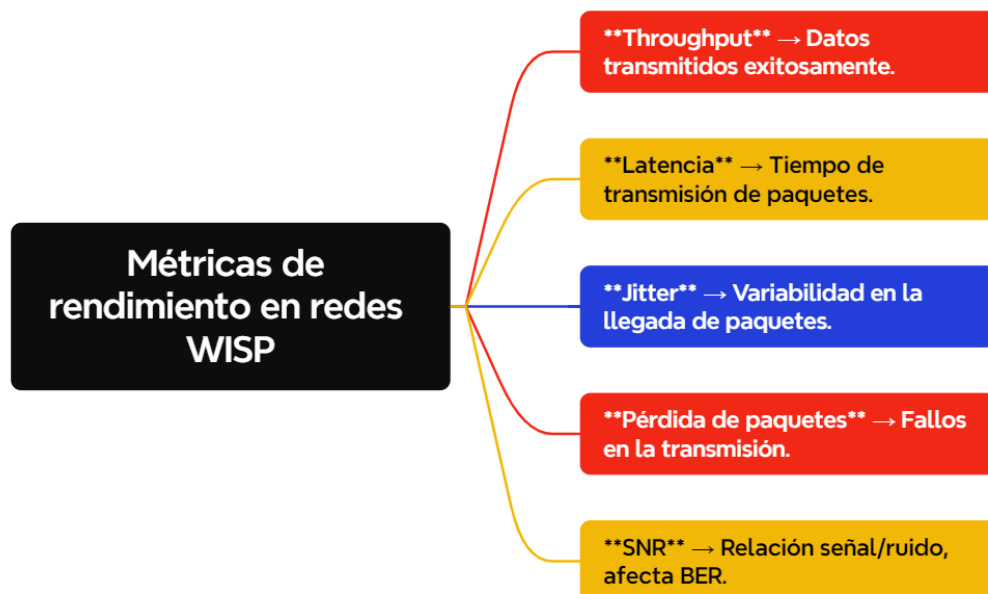
Para aplicar la expresión anterior, la SNR debe expresarse en escala lineal:

$$\text{SNR}(\text{lineal}) = 10^{\frac{\text{SNR}(\text{db})}{10}}$$

Relevancia de estas métricas en redes WISP

Estas métricas permiten evaluar el desempeño de enlaces inalámbricos en redes WISP, ya que están directamente relacionadas con la calidad de la transmisión y la confiabilidad del servicio. En entornos de simulación, su análisis permite comparar diferentes configuraciones de red bajo condiciones variables de propagación, interferencia y carga de tráfico. En la Figura 3 se muestra un resumen del apartado de métricas de rendimiento de las redes WISP.

Figura 3. Métricas de rendimiento en redes WISP



Modelos de cobertura en redes WISP usando simuladores de propagación

En el ámbito de las redes WISP (Wireless Internet Service Provider), la planificación de cobertura representa un aspecto crítico que influye directamente en la calidad del servicio ofrecido a los usuarios finales. Una cobertura adecuada no solo garantiza la disponibilidad del enlace inalámbrico en las áreas objetivo, sino que también minimiza la interferencia, mejora la eficiencia del espectro, optimiza el rendimiento de la red y reduce los costos de infraestructura [1].

Para lograr una planificación efectiva, es indispensable utilizar herramientas que permitan modelar con precisión el comportamiento de las ondas electromagnéticas en escenarios reales. En este contexto, los simuladores de propagación, como Atoll, se consolidan como recursos esenciales para el diseño, análisis y optimización de redes inalámbricas, especialmente en entornos geográficamente complejos o densamente urbanizados [1].

Importancia de los modelos de propagación en redes WISP

Los modelos de propagación son representaciones matemáticas del comportamiento de las ondas de radio al atravesar distintos tipos de entornos. Permiten estimar parámetros fundamentales como [1]:

- La pérdida de trayectoria (Path Loss)
- El nivel de señal recibida (RSSI)
- La interferencia entre nodos
- La cobertura geográfica esperada
- La calidad del enlace (SNR)

En redes WISP, que comúnmente operan en bandas no licenciadas como 2.4 GHz y 5.8 GHz, y en zonas rurales, suburbanas o semiurbanas, la correcta elección y aplicación de modelos de propagación es fundamental para evitar zonas de sombra, enlaces inestables y problemas de saturación [1].

Modelos de propagación más utilizados en Atoll y redes WISP

1. Modelo de Okumura-Hata (urbano, suburbano y rural)

Este modelo empírico es ampliamente utilizado para predecir pérdidas de trayectoria en áreas urbanas. Es aplicable en frecuencias de 150 MHz a 1500 MHz, aunque sus extensiones permiten utilizarlo también hasta 2 GHz con ajustes [32].

$$L_u(dB) = 69.55 + 26.16 \log_{10}(f) \\ - 13.82 \log_{10}(ht) - a(h_r) + [44.9 - 6.55 \log_{10}(h_t)] \log_{10}(d)$$

Donde:

- f : frecuencia en MHz
- h_t : altura de la antena transmisora (m)
- h_r : altura de la antena receptora (m)
- d : distancia entre transmisor y receptor (km)
- $a(h_r)$: corrección por altura del receptor, que varía si el entorno es urbano, suburbano o rural.

Corrección para entorno suburbano:

$$L_{sub} = L_u - 2(\log_{10}\left(\frac{f}{28}\right))^2 - 5.4$$

Corrección para entorno rural:

$$L_{rul} = L_u - 4.78 (\log_{10}(f))^2 + 18.33 \log_{10}(f) - 40.94$$

Este modelo es especialmente útil en zonas rurales y suburbanas, típicas de los despliegues WISP.

2. Modelo COST-231 Hata (entorno urbano/densamente urbano)

Es una extensión del modelo de Hata para frecuencias más altas, entre 1500 MHz y 2000 MHz, y se aplica en áreas urbanas o densamente edificadas [33].

$$\begin{aligned}
L_{COST}(dB) = & 46.3 \\
& + 33.9 (\log_{10}(f)) \\
& - 13.82 \log_{10}(ht) - a(h_r) + [44.9 - 6.55 \log_{10}(h_t) \log_{10}(h_t)] \log_{10}(d) + c]
\end{aligned}$$

Donde:

- $c = 0$ (suburbano) o 3 (urbano denso)
- El resto de las variables son iguales al modelo anterior.

Este modelo es ideal para simulaciones en zonas urbanizadas, como las áreas centrales de pequeñas ciudades o pueblos donde los WISP también ofrecen servicio.

3. Modelo ITU-R P.525 / P.1546 (espacios abiertos y propagación terrestre)

El modelo ITU-R es una recomendación de la Unión Internacional de Telecomunicaciones para estimar la propagación en sistemas inalámbricos sobre terreno abierto o costero. Es útil en zonas rurales planas o costeras y funciona bien hasta los 30 GHz [34].

Su ecuación es compleja y depende de curvas predefinidas, pero en su forma básica incluye la pérdida libre más factores de corrección [34]:

Fórmula básica (Pérdida de espacio libre):

$$L_{FS}(dB) = 20 \log_{10}(d) + 20 \log_{10}(f) + 32.45$$

Donde:

- d : distancia en km
- f : frecuencia en MHz

Este modelo se adapta bien a zonas costeras, rurales planas o áreas despejadas, donde muchos WISP operan sin obstrucciones significativas.

Uso de simuladores de propagación: el caso de Atoll

Uno de los simuladores más avanzados y reconocidos a nivel profesional para la planificación de redes inalámbricas es Atoll, desarrollado por la empresa francesa Forsk. Atoll se

ha consolidado como una herramienta estándar para operadores de redes móviles, redes IoT, enlaces de microondas y servicios WISP, ya que integra potentes funcionalidades de simulación, análisis y optimización [35].

Atoll permite realizar simulaciones de cobertura sobre mapas digitales detallados, los cuales pueden incluir tanto información topográfica (curvas de nivel, elevaciones) como datos satelitales y cartografía vectorial (edificios, calles, ríos, zonas boscosas). Esta capacidad es vital para proyectar cómo las señales se propagan en el mundo real y cómo interactúan con obstáculos físicos [35].

Entre sus características más relevantes, Atoll ofrece:

- Aplicación de modelos de propagación reconocidos internacionalmente como Okumura-Hata, COST-231, ITU-R, Erceg-Greenstein y otros, adaptables a distintos entornos (urbanos, suburbanos, rurales, interiores).
- Parámetros configurables, tales como:
 - Altura de antenas transmisoras y receptoras.
 - Potencia de transmisión.
 - Ganancia y apertura de los haces de las antenas.
 - Tipo de terreno y obstrucciones.
 - Frecuencia de operación.
- Capacidad de simular tanto enlaces punto a punto (backhaul) entre estaciones o torres como enlaces punto a multipunto hacia usuarios finales.
- Importación de Modelos Digitales de Elevación (DEM) y datos GIS, lo que mejora la exactitud de los cálculos y permite una planificación contextualizada con el entorno real.
- Análisis de interferencias entre celdas o enlaces superpuestos, lo cual es fundamental en redes densas o con varios nodos de distribución cercanos.

- Simulación de capacidades de canal, estimando el ancho de banda disponible según el nivel de señal, tipo de modulación empleada y condiciones del canal inalámbrico.

Aplicación específica de Atoll en redes WISP

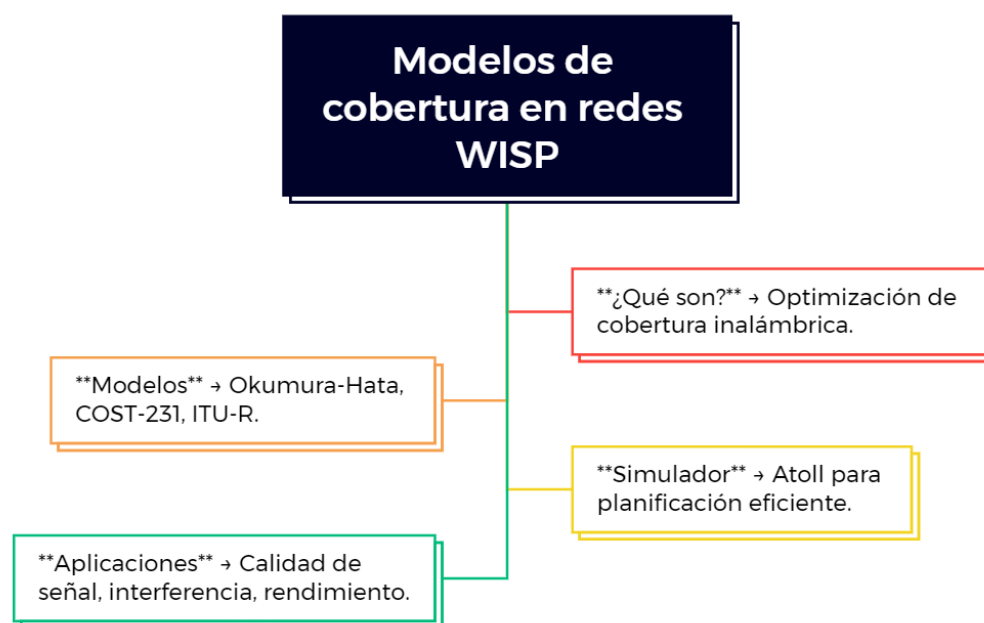
En el contexto de redes WISP, donde las estaciones base suelen instalarse en ubicaciones estratégicas como cerros, torres de telecomunicaciones o postes elevados, Atoll permite una planificación precisa que responde a los requerimientos del proveedor de internet inalámbrico. Las principales aplicaciones prácticas de Atoll en redes WISP incluyen [35]:

- Cálculo de la zona de cobertura efectiva de un nodo distribuidor (como un Access Point), permitiendo visualizar gráficamente hasta dónde llega la señal útil bajo condiciones reales.
- Detección de zonas de sombra o cobertura deficiente, lo cual ayuda a definir si es necesario reubicar equipos, aumentar la altura de las antenas o implementar estaciones repetidoras.
- Optimización de la ubicación y orientación de las antenas, maximizando el rendimiento del enlace y minimizando pérdidas por reflexión, difracción o dispersión.
- Evaluación de la interferencia entre enlaces y el solapamiento de frecuencias, crucial para evitar degradaciones en el servicio causadas por colisiones de señal o saturación del canal.
- Cálculo de parámetros como la relación señal/ruido (SNR) y el margen de enlace, que determinan la calidad de conexión en distintas ubicaciones del mapa.
- Estimación de capacidad del enlace, prediciendo el throughput disponible para cada usuario o nodo en función del tipo de modulación (BPSK, QPSK, 16-QAM, etc.) y la intensidad de la señal recibida.

En resumen, los modelos de cobertura son fundamentales para garantizar un diseño técnico y eficiente de redes WISP. La utilización de simuladores de propagación como Atoll no solo

permite prever el comportamiento real de la señal en diferentes escenarios, sino que también facilita la toma de decisiones estratégicas relacionadas con la ubicación de torres, selección de equipos, planificación de frecuencias y optimización de recursos. Al combinar el conocimiento teórico de los modelos de propagación con herramientas profesionales de simulación, los diseñadores de redes inalámbricas pueden asegurar un despliegue robusto, escalable y orientado a la calidad del servicio, lo cual resulta clave en entornos rurales o de difícil acceso donde las redes WISP cumplen un rol esencial en la democratización del acceso a internet. La Figura 4 muestra el resumen del apartado de modelos de cobertura desarrollado en esta sección.

Figura 4. Modelos de cobertura en redes WISP con simulación en Atoll



Seguridad en redes inalámbricas WISP: amenazas, protocolos y soluciones

La seguridad en redes inalámbricas WISP (Wireless Internet Service Provider) es un pilar fundamental para garantizar la integridad y confiabilidad del servicio ofrecido a los usuarios. Debido a la naturaleza abierta del medio inalámbrico, estas redes están expuestas a múltiples vulnerabilidades que pueden ser explotadas por actores maliciosos si no se aplican mecanismos de protección adecuados. A diferencia de las redes cableadas, donde el acceso físico a la infraestructura representa una barrera natural, las redes WISP emiten señales que pueden ser

captadas desde grandes distancias, lo que incrementa el riesgo de interceptación, manipulación o sabotaje [36].

El crecimiento de la demanda de conectividad, especialmente en zonas rurales o de difícil acceso donde los WISP son protagonistas, ha provocado que la seguridad se convierta en un aspecto crítico no solo desde el punto de vista técnico, sino también regulatorio y comercial. Los proveedores deben proteger no solo la infraestructura de red, sino también la privacidad y los datos de los usuarios, cumpliendo con normativas de protección de datos y asegurando la continuidad del servicio frente a ataques cibernéticos [36].

Amenazas comunes en redes WISP

Las amenazas a las redes inalámbricas pueden clasificarse en varios tipos, y cada una representa un riesgo específico para la operación segura del servicio. A continuación, se describen las amenazas más relevantes [36]:

- **Intercepción de tráfico (Sniffing):** Consiste en capturar el tráfico que circula por la red. Si los datos no están cifrados, los atacantes pueden acceder a información confidencial como credenciales, direcciones IP, configuraciones de red o incluso datos personales de los usuarios.
- **Rogue Access Points:** También conocidos como puntos de acceso falsos, son dispositivos maliciosos configurados para imitar la red legítima. Engañan a los usuarios para que se conecten a ellos, permitiendo al atacante interceptar credenciales y tráfico sensible.
- **Ataques de fuerza bruta:** Este tipo de ataque busca descubrir contraseñas débiles a través de múltiples intentos automatizados. Los equipos de red mal configurados, con contraseñas por defecto o débiles, son especialmente vulnerables a este tipo de ataques.
- **Denegación de servicio (DoS/DDoS):** Consiste en sobrecargar deliberadamente los servidores, routers o estaciones base para provocar la caída del servicio. Un ataque

distribuido puede saturar completamente el canal inalámbrico o el backbone IP del WISP.

- Acceso no autorizado a la red troncal: Si los mecanismos de segmentación de red (como VLAN, firewalls o túneles VPN) no están debidamente implementados, los atacantes pueden acceder directamente a la infraestructura principal, modificar configuraciones o interceptar tráfico de múltiples usuarios.

Protocolos y buenas prácticas de seguridad

Para contrarrestar las amenazas mencionadas, los WISP deben adoptar una combinación de protocolos estándar, mecanismos de autenticación y políticas de administración seguras. Algunas de las estrategias más efectivas incluyen [36]:

- WPA3 (Wi-Fi Protected Access 3): Es el estándar más reciente en cifrado inalámbrico. Ofrece cifrado individualizado para cada conexión y protección reforzada contra ataques de diccionario, que son comunes en redes WPA2 mal configuradas.
- IEEE 802.11i (WPA2 Enterprise): Utilizado principalmente en entornos corporativos o de alta seguridad. Emplea servidores RADIUS y métodos de autenticación EAP (como EAP-TLS) para ofrecer un nivel superior de control sobre los dispositivos autorizados.
- TLS y HTTPS: Es obligatorio que las interfaces de administración de los routers, APs y firewalls estén protegidas mediante protocolos seguros. TLS y HTTPS evitan que las credenciales de acceso sean expuestas durante la gestión remota.
- VPNs (Virtual Private Networks): Las redes privadas virtuales permiten establecer túneles seguros entre sedes o dispositivos remotos y la infraestructura del WISP. Son ideales para acceder a routers distribuidos geográficamente sin exponer puertos vulnerables a internet.
- Firewalls físicos y control de accesos: El uso de dispositivos de seguridad dedicados permite filtrar el tráfico de entrada y salida. La segmentación de la red

con reglas de acceso específicas (por IP, puerto, protocolo) limita las oportunidades de intrusión y permite un monitoreo más eficaz.

Adaptación de tecnologías avanzadas a redes WISP

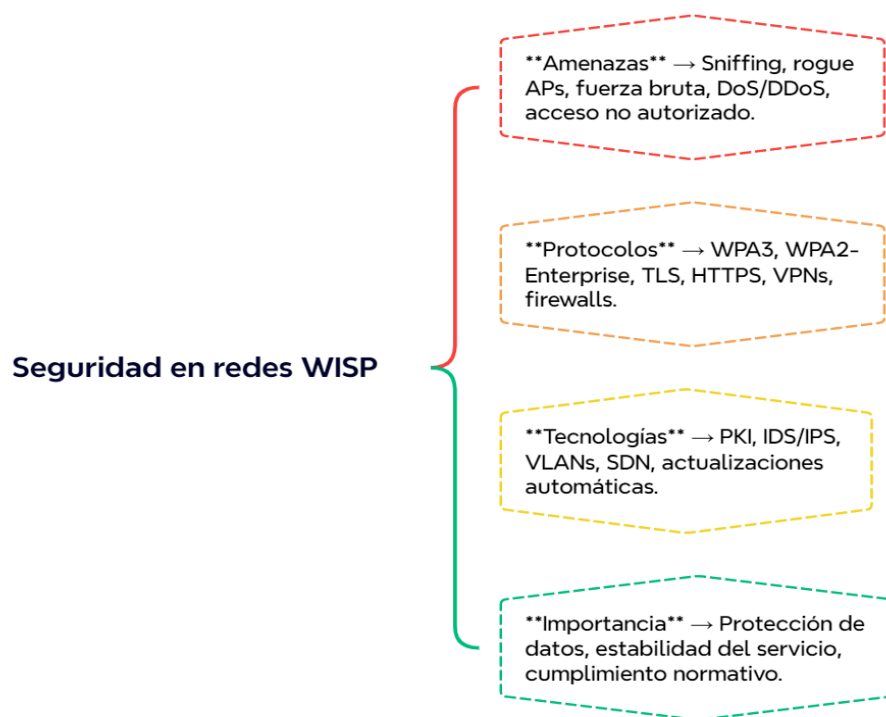
Aunque los WISP suelen operar en bandas no licenciadas y tecnologías distintas de las redes móviles como LTE o 5G, muchas de las técnicas de seguridad aplicadas en estos entornos pueden ser adaptadas con éxito. La incorporación de tecnologías emergentes permite a los WISP estar mejor preparados frente a amenazas complejas [36]:

- Autenticación basada en certificados (PKI): Sustituye el uso de contraseñas por certificados digitales que autentican a los dispositivos de manera más segura y automatizada.
- Sistemas IDS/IPS (Intrusion Detection/Prevention Systems): Analizan el tráfico en tiempo real en busca de patrones anómalos o comportamientos maliciosos. Al detectar una amenaza, pueden bloquearla automáticamente o alertar a los administradores.
- Segmentación de red con VLAN o SDN: Separar los diferentes tipos de tráfico (clientes residenciales, empresariales, administración, etc.) mejora el control, la seguridad y el rendimiento general de la red. El uso de redes definidas por software (SDN) permite una gestión centralizada y dinámica de las políticas de seguridad.
- Actualizaciones automáticas de firmware: Mantener todos los equipos con el firmware actualizado cierra vulnerabilidades conocidas que podrían ser explotadas por atacantes. Este proceso puede automatizarse mediante sistemas de gestión centralizados.

La seguridad en redes WISP no es un lujo, sino una necesidad operativa que garantiza la protección de los recursos, la confidencialidad de los usuarios y la continuidad del negocio. Frente a un panorama cada vez más hostil y sofisticado, es imprescindible que los proveedores implementen un enfoque proactivo, integrando estándares robustos de cifrado, segmentación de red, monitoreo activo y mecanismos de actualización continua. La adopción de buenas prácticas y

tecnologías modernas permite fortalecer las defensas de la red y ofrecer un servicio confiable, estable y seguro que satisfaga tanto las exigencias técnicas como la confianza de los usuarios finales. La siguiente Figura 5 muestra el resumen de este apartado sobre la seguridad de las redes WISP.

Figura 5. Seguridad de las redes WISP y mecanismos de protección



2.2.2. Emulación y simulación de redes híbridas WISP

En este apartado se lleva a cabo un análisis técnico de redes híbridas y WISP utilizando herramientas de emulación y simulación que permiten recrear entornos reales de operación. Se inicia con la integración de GNS3 y Workstation para la emulación conjunta de redes de datos y servidores, lo que facilita el estudio del comportamiento de redes complejas. Luego se evalúa el rendimiento de estas redes emuladas, considerando factores como la eficiencia, estabilidad y respuesta ante distintos escenarios. Además, se realiza la simulación de redes WISP en el software Atoll, introduciendo condiciones variables para comprender cómo factores externos afectan la cobertura y calidad del servicio. Finalmente, se caracteriza el tráfico en redes VoIP dentro de

entornos simulados, permitiendo identificar patrones de consumo, comportamiento del ancho de banda y posibles cuellos de botella en aplicaciones de voz sobre IP.

Integración de GNS3 con VMware Workstation para la emulación de redes híbridas (red + servidores)

En el ámbito de la simulación y diseño de redes, la capacidad de emular entornos híbridos que combinen dispositivos de red (como routers, switches y firewalls) con máquinas virtuales que representen servidores y clientes es esencial para realizar pruebas realistas. Esta integración es especialmente útil en entornos académicos y profesionales, como en el desarrollo de proyectos de redes WISP (Wireless Internet Service Provider), donde no solo se requiere validar el enrutamiento o la topología de red, sino también los servicios que se ejecutan sobre ella, como DNS, DHCP, web, VPN, firewall, entre otros. En este contexto, la integración de GNS3 (Graphical Network Simulator-3) con VMware Workstation se presenta como una solución poderosa para la emulación de redes híbridas [26].

GNS3: Simulación avanzada de redes

GNS3 es un simulador de redes de código abierto ampliamente utilizado por ingenieros de redes, estudiantes de telecomunicaciones y profesionales de TI. Permite crear topologías complejas utilizando imágenes reales de IOS (Cisco), MikroTik CHR, VyOS, etc., y combinar estos elementos con dispositivos virtualizados. Su entorno gráfico facilita el diseño, configuración, monitoreo y depuración de redes, siendo ideal para realizar laboratorios prácticos y escenarios realistas [26].

VMware Workstation: Virtualización de sistemas operativos

VMware Workstation es una plataforma de virtualización que permite ejecutar múltiples sistemas operativos como máquinas virtuales (VMs) en un solo equipo físico. Estas VMs pueden emular servidores Linux, Windows u otros sistemas operativos, y pueden configurarse con servicios de red esenciales como servidores web (Apache/Nginx), bases de datos (MySQL/PostgreSQL), servidores de correo, entre otros. La flexibilidad de VMware Workstation permite asignar adaptadores de red personalizados, lo cual es fundamental para su integración con GNS3 en entornos de simulación de redes WISP [26].

Beneficios de la integración GNS3 + VMware Workstation

La integración entre GNS3 y VMware Workstation permite emular un entorno de red híbrido donde los dispositivos de red simulados interactúan directamente con servidores virtuales reales, replicando de forma precisa el comportamiento de una red de producción. Algunos de los beneficios clave son [26]:

- Simulación completa del plano de control y de datos.
- Pruebas de conectividad entre redes virtuales y servidores reales.
- Validación de configuraciones de servicios como DNS, DHCP, FTP, VPN y web.
- Evaluación de políticas de firewall, segmentación VLAN y ruteo dinámico.
- Preparación para certificaciones como Cisco CCNA, CCNP o MikroTik MTCNA.
- Implementación de escenarios tipo laboratorio para capacitación o investigación.

Proceso de integración

A continuación, se describe el proceso general para integrar VMware Workstation con GNS3 [26]:

1. Instalación y configuración básica

- Instalar GNS3 y su componente GNS3 VM (recomendado para mejor rendimiento).
- Instalar VMware Workstation y crear las máquinas virtuales necesarias (por ejemplo, una VM con Ubuntu Server para simular un servidor).
- Instalar GNS3 VMware Workstation Guest Additions para mejorar la compatibilidad entre GNS3 y VMware Workstation.

2. Crear una máquina virtual en VMware Workstation

- Configurar una nueva máquina virtual con los recursos adecuados (CPU, RAM, disco).

- Instalar un sistema operativo adecuado (por ejemplo, Ubuntu Server, CentOS o Windows Server).
- Instalar y configurar los servicios deseados (como Apache, Samba, DNS, DHCP, etc.).

3. Vinculación de VMware Workstation con GNS3

- En GNS3, dirigirse a "Preferencias" → "VMware Workstation VMs".
- Añadir la máquina virtual previamente creada.
- Asignar el número de interfaces de red que se desean conectar a la topología.
- Establecer la conexión de red en modo adaptador genérico (Host-Only o Bridged, según el caso).

4. Conexión en topología

- Insertar la máquina virtual desde el panel de dispositivos de GNS3.
- Conectarla con otros dispositivos simulados (por ejemplo, un router Cisco o un switch MikroTik).
- Configurar las direcciones IP y realizar pruebas de conectividad.

5. Ejecución y prueba del entorno

- Ejecutar toda la topología.
- Verificar la conectividad mediante comandos como ping, traceroute o utilizando servicios como SSH, HTTP o FTP.
- Capturar tráfico con Wireshark directamente desde GNS3 para análisis detallado.

Aplicación en entornos WISP

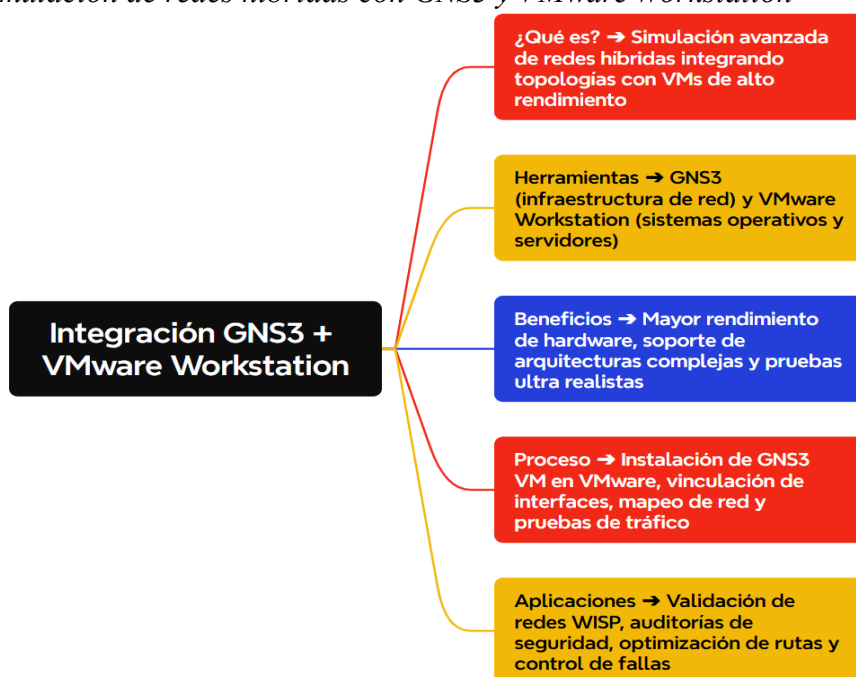
En el contexto de redes WISP, esta integración permite simular:

- Red troncal con routers que realizan NAT, enrutamiento OSPF o BGP.

- Enlaces inalámbricos punto a punto o punto a multipunto usando routers virtualizados o CHR (Cloud Hosted Router).
- Servidores de autenticación (RADIUS), gestión de clientes, portales cautivos, monitoreo y administración remota.
- Escenarios de seguridad, probando configuraciones de firewalls, detección de intrusos y túneles VPN.
- Implementación de servidores de contenido local para optimizar el ancho de banda.

La integración de GNS3 con VMware Workstation representa una herramienta poderosa para la emulación de redes híbridas que combinan infraestructura de red y servidores. Esta acción conjunta permite a los estudiantes, técnicos y administradores de red recrear escenarios realistas para pruebas, aprendizaje, validación y despliegue de soluciones antes de su implementación en un entorno de producción. En proyectos como el diseño de redes WISP, esta metodología no solo permite optimizar recursos y evitar errores costosos, sino también proveer una plataforma de experimentación altamente flexible, económica y eficiente. La Figura 6 resume el tema de la integración de GNS3 con máquinas virtuales [26].

Figura 6. *Emulación de redes híbridas con GNS3 y VMware Workstation*



Evaluación de rendimiento en redes emuladas con GNS3

La evaluación del rendimiento en redes emuladas se ha convertido en una actividad fundamental para los ingenieros de telecomunicaciones, especialmente en el contexto del diseño, simulación y prueba de infraestructuras de redes inalámbricas como las WISP (Wireless Internet Service Provider). GNS3 (Graphical Network Simulator-3) es una de las plataformas más utilizadas para este propósito, debido a su capacidad de emular redes complejas utilizando imágenes reales de routers, switches y firewalls, así como su integración con máquinas virtuales y servicios de red [37].

Importancia de la evaluación de rendimiento

Emular redes en un entorno controlado permite no solo probar configuraciones antes de implementarlas en el campo, sino también estudiar el impacto que ciertas decisiones de diseño pueden tener en parámetros fundamentales como el ancho de banda, la latencia, el jitter y el consumo de recursos. Esto es especialmente útil en redes WISP, donde la infraestructura puede estar compuesta por enlaces punto a punto, enlaces multipunto, routers de borde y servidores de servicios de red, todo lo cual puede ser modelado eficientemente en GNS3 [37].

Estudio comparativo: GNS3 vs SEED

La siguiente Tabla 3 resume los resultados del estudio comparativo entre GNS3 y SEED, considerando métricas clave como latencia, jitter, ancho de banda, consumo energético, escalabilidad y flexibilidad. Se observa que GNS3 ofrece mayor personalización y escalabilidad, mientras que SEED destaca por su eficiencia y estabilidad en entornos educativos controlados [38].

Tabla 3. *Comparación de características entre GNS3 y SEED*

Parámetros comparativos	GNS3	SEED (Secure and Efficient Emulated Data-plane)
Latencia promedio	Aproximadamente 20 ms en escenarios básicos; puede aumentar con configuraciones pesadas.	Generalmente más baja y estable, debido a una optimización enfocada en prácticas educativas.
Jitter	Mínimo bajo condiciones controladas, pero aumenta con múltiples VMs o imágenes pesadas.	Muy bajo y estable, incluso con múltiples nodos, el emulador está diseñado para priorizar la estabilidad.
Ancho de banda simulado	Interfaces GigabitEthernet simuladas, limitadas por CPU/RAM y el tipo de hipervisor usado.	Eficiente para el tráfico académico, pero limitado en escenarios avanzados o exigentes.
Consumo energético	Alto, debido a la emulación completa del sistema operativo de red y múltiples máquinas virtuales.	Bajo: uso eficiente de recursos por arquitectura ligera.
Escalabilidad	Alta: permite integración con Docker, VirtualBox, VMware y conexión con hardware físico.	Media: se limita más a entornos académicos controlados.
Flexibilidad	Muy alta: ideal para entornos personalizados (WISP, portales cautivos, pruebas de seguridad).	Enfocada en prácticas guiadas. Menor capacidad de personalización.

Aplicación en el diseño de redes WISP

En el contexto de redes WISP, la capacidad de evaluar el rendimiento en un entorno emulado es vital. A través de GNS3 se puede [27]:

- Medir el retardo de transmisión en la red troncal ante diferentes configuraciones de enrutamiento (OSPF, BGP).
- Verificar el comportamiento de servicios de red como DHCP, DNS, NAT y VPN en servidores virtuales integrados.
- Analizar cómo se ve afectado el tráfico bajo condiciones de congestión, fallos de enlace o ataques simulados.
- Comprobar el impacto de cambios de firmware o reglas de firewall antes de aplicarlos en la infraestructura real.

Limitaciones y recomendaciones

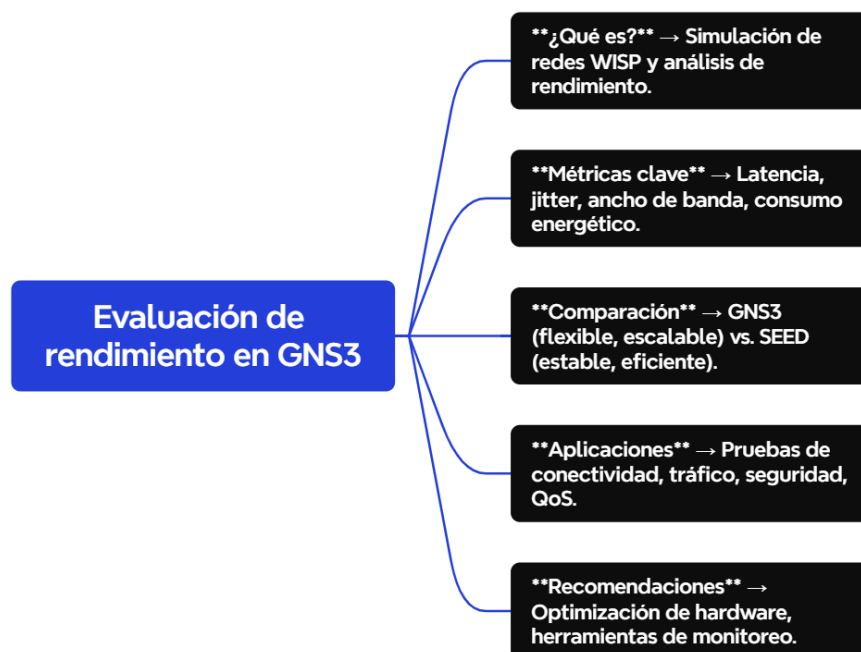
Si bien GNS3 es una herramienta poderosa, su rendimiento está directamente relacionado con el hardware del equipo anfitrión. En simulaciones grandes, es recomendable [27]:

- Usar la GNS3 VM con asignación de múltiples núcleos de CPU y RAM suficiente.
- Evitar el uso de demasiadas máquinas virtuales simultáneamente.
- Configurar correctamente los enlaces para evitar bucles de red o sobrecarga de CPU.
- Hacer uso de herramientas de monitoreo (como Wireshark o iPerf) para analizar tráfico en tiempo real.

Además, para una evaluación más precisa, se recomienda complementar las simulaciones con entornos híbridos donde se incluyan dispositivos físicos (como routers MikroTik, Ubiquiti o switches administrables) que puedan comunicarse con el entorno virtual mediante interfaces bridged o adaptadores host-only [27].

La evaluación de rendimiento en redes emuladas con GNS3 permite a los diseñadores y administradores de redes WISP validar sus configuraciones y tomar decisiones fundamentadas antes de realizar implementaciones reales. Aunque presenta algunas limitaciones en cuanto al consumo de recursos y precisión absoluta de métricas como la latencia o el jitter, GNS3 proporciona un entorno extremadamente flexible y potente para simular redes reales con alta fidelidad. Su integración con herramientas complementarias y la posibilidad de incluir servicios en máquinas virtuales lo convierten en una plataforma indispensable para la formación, la investigación y la validación de arquitecturas de red inalámbricas modernas. En la Figura 7 se resume este apartado [27].

Figura 7. *Evaluación de rendimiento en GNS3*



Simulación de redes WISP en Atoll bajo condiciones variables

La simulación de redes WISP (Wireless Internet Service Provider) es una etapa crítica dentro del proceso de planificación e implementación de infraestructuras inalámbricas. En este contexto, Atoll se consolida como una de las herramientas profesionales más robustas y precisas para el análisis, modelado y simulación de redes inalámbricas bajo una gran variedad de condiciones operativas. Desarrollado por la empresa Forsk, Atoll es ampliamente utilizado en el sector de telecomunicaciones, no solo por operadores móviles, sino también por proveedores de internet inalámbrico (WISPs) que buscan optimizar la cobertura y eficiencia de sus redes [39].

Atoll permite a los diseñadores realizar simulaciones altamente realistas que integran parámetros geográficos, técnicos y ambientales, lo cual es crucial para redes WISP que operan en entornos con topografías y niveles de interferencia muy variables [39].

Modelos de propagación en Atoll

Uno de los pilares fundamentales de la simulación en Atoll es la implementación de modelos de propagación avanzados, los cuales permiten predecir cómo se comportarán las ondas de radio en diferentes escenarios físicos. Entre los modelos más utilizados se encuentran:

- Okumura-Hata: Ideal para entornos urbanos y suburbanos, este modelo empírico permite calcular la pérdida de propagación considerando la frecuencia, la altura de las antenas transmisoras y receptoras, y la distancia entre ellas [32].
- COST-231 Hata: Es una extensión del modelo Hata, optimizada para frecuencias de hasta 2 GHz, lo cual la hace más adecuada para aplicaciones WISP en bandas como 2.4 GHz o 5 GHz [33].
- ITU-R P.1812 y otros modelos de línea de vista (LOS y NLOS): Utilizados en escenarios más complejos, con obstáculos naturales o construcciones urbanas densas, que afectan directamente la propagación de la señal [34].

Estos modelos pueden configurarse con parámetros específicos del entorno, como tipo de vegetación, densidad de edificaciones, humedad y relieve geográfico, lo cual brinda una representación más precisa de la realidad.

Condiciones de enlace y comportamiento dinámico

Una de las funcionalidades más relevantes de Atoll es la capacidad de simular condiciones variables en los enlaces de red. Las redes WISP no operan en condiciones estáticas; por el contrario, se ven constantemente afectadas por [39]:

- Interferencias provenientes de otras redes inalámbricas vecinas o fuentes electromagnéticas.
- Carga de tráfico variable, dependiendo del número de usuarios conectados, el tipo de servicio (streaming, navegación, VoIP) y la hora del día.
- Variaciones ambientales, como lluvia, humedad o cambios estacionales, que pueden influir en la atenuación de la señal, especialmente en bandas de frecuencia altas.

Atoll permite configurar todos estos factores, generando escenarios que simulan desde condiciones ideales hasta situaciones de alto estrés en la red. Esto posibilita prever el rendimiento real que se obtendría tras la implementación del diseño propuesto [39].

Además, mediante el análisis del margen de enlace (link budget), es posible calcular la relación señal/ruido (SNR), la probabilidad de pérdida de paquetes y la estabilidad de la conexión en cada punto de cobertura.

Análisis de cobertura efectiva

Otra función esencial de Atoll en la simulación de redes WISP es el análisis de cobertura efectiva. Gracias a la integración de mapas digitales detallados (topográficos, satelitales, modelos de elevación – DEM), Atoll puede [39]:

- Determinar con alta precisión las áreas donde la señal es lo suficientemente fuerte para garantizar una conexión estable.
- Identificar zonas de sombra o “dead zones” donde la cobertura no es viable debido a obstáculos o a la lejanía del nodo emisor.
- Evaluar la superposición de coberturas entre nodos, para analizar redundancias, interferencias o posibilidad de handover entre puntos de acceso.

Este análisis es visual y cuantitativo, ya que genera mapas de calor de cobertura, informes estadísticos de disponibilidad de servicio por zona y representaciones gráficas del rendimiento estimado en función del RSSI (Received Signal Strength Indicator) y el SINR (Signal-to-Interference-plus-Noise-Ratio) [39].

Despliegue de redes WISP aplicadas al diseño

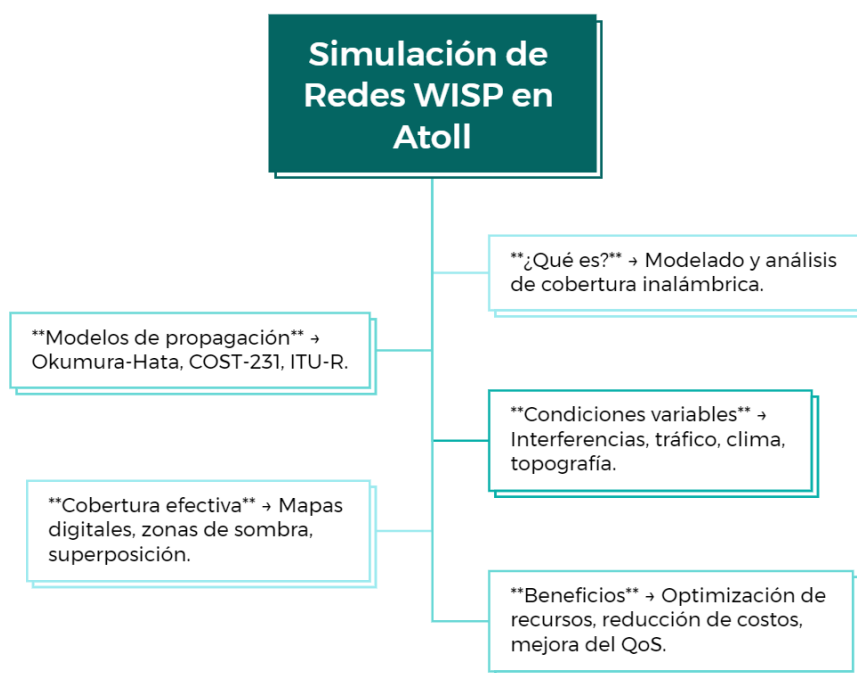
Simular redes WISP bajo condiciones variables no solo permite optimizar el diseño inicial, sino que también facilita la toma de decisiones estratégicas en fases posteriores del proyecto. Entre los principales beneficios destacan [1]:

- Optimización de recursos, al ubicar torres o nodos solo donde son necesarios.

- Reducción de costos, al minimizar pruebas físicas e inversiones innecesarias.
- Mejora de la calidad del servicio (QoS), al prever puntos críticos y solucionarlos desde la fase de diseño.
- Planificación de escalabilidad, al simular cómo se comportará la red ante el crecimiento del número de usuarios.

La simulación de redes WISP en Atoll bajo condiciones variables representa una herramienta de altísimo valor técnico y estratégico. Permite a los diseñadores prever el comportamiento de la red en situaciones reales y complejas, mejorando la eficiencia de cobertura, la calidad del servicio y la resiliencia ante condiciones adversas. La capacidad de Atoll para integrar múltiples parámetros físicos y operativos lo convierte en un aliado indispensable en la planificación profesional de redes inalámbricas modernas, especialmente en entornos rurales o suburbanos donde los desafíos topográficos y de conectividad son mayores. La siguiente Figura 8 resume los aspectos fundamentales de la simulación de redes WISP en Atoll [39].

Figura 8. *Simulación de cobertura WISP en Atoll*



2.2.3. Fortalecer la formación en redes inalámbricas mediante simulación

Este apartado busca mejorar los procesos de enseñanza-aprendizaje en el campo de las redes inalámbricas, aprovechando la tecnología como aliada pedagógica. Se inicia con el análisis del valor de la simulación como recurso didáctico, destacando su capacidad para representar escenarios reales sin necesidad de infraestructura física. Se aborda el uso combinado de las herramientas Atoll y GNS3 como una estrategia práctica para formar y evaluar competencias en redes WISP, facilitando la integración teoría-práctica. Además, se exploran metodologías activas que promueven el aprendizaje significativo, incentivando la participación del estudiante mediante retos, simulaciones y resolución de problemas. Finalmente, se plantea la estandarización de prácticas de simulación con el objetivo de estructurar y unificar criterios en el diseño y análisis de redes, asegurando la calidad y consistencia en la formación técnica.

Simulación como recurso didáctico en la formación de redes inalámbricas

La simulación ha cobrado un papel protagónico en la formación académica en áreas de telecomunicaciones, y particularmente en el estudio de redes inalámbricas como las WISP (Wireless Internet Service Provider), gracias a su capacidad para replicar escenarios reales de transmisión, configuración y administración de redes sin necesidad de hardware físico. La simulación se posiciona como una herramienta pedagógica de alto valor, especialmente en entornos educativos con limitaciones presupuestarias o de infraestructura [40].

Importancia en la formación técnica y universitaria

En la educación técnica y superior, el uso de simuladores ha evolucionado desde simples representaciones de redes estáticas hacia entornos altamente interactivos que permiten emular dinámicas reales de una red inalámbrica. Herramientas como GNS3 (Graphical Network Simulator-3) y Atoll (software profesional de planificación de radiofrecuencia) se han integrado progresivamente en los programas académicos, permitiendo a los estudiantes no solo entender la teoría, sino experimentar activamente con topologías, protocolos, interferencias, tipos de tráfico y coberturas de red [40].

Desde 2022, diversos estudios e iniciativas de innovación educativa han promovido activamente la incorporación de estos simuladores en la enseñanza de redes inalámbricas. Estas

investigaciones demuestran que el aprendizaje mediante simulación mejora significativamente la comprensión de fenómenos complejos como [40]:

- La propagación de señales y las pérdidas por trayectoria.
- El comportamiento del espectro radioeléctrico en distintos entornos (urbanos, rurales, interiores).
- Los efectos de la interferencia entre canales y la congestión de nodos de red.
- La configuración de enlaces punto a punto o punto a multipunto en redes WISP.
- El impacto de distintas configuraciones de antenas, frecuencias y potencias de transmisión.

Aprendizaje activo y descubrimiento guiado

El uso de la simulación permite aplicar metodologías de enseñanza activas, donde el estudiante deja de ser un receptor pasivo de información para convertirse en protagonista de su proceso formativo. Bajo este enfoque, el aprendizaje por descubrimiento toma fuerza: los estudiantes exploran, experimentan y comprueban hipótesis dentro de entornos controlados y seguros, sin temor a dañar equipos o cometer errores costosos [40].

Este tipo de aprendizaje fomenta competencias clave para el ámbito profesional, como:

- La solución de problemas técnicos complejos mediante el análisis de causas y consecuencias.
- La toma de decisiones informada, basada en datos cuantificables y observaciones empíricas.
- El desarrollo de pensamiento crítico, al contrastar distintos enfoques de diseño y configuración de redes.
- El trabajo colaborativo, ya que muchos simuladores permiten trabajo en grupo, incluso en entornos virtuales.

Integración con enfoques constructivistas

Desde una perspectiva pedagógica, la simulación se alinea perfectamente con los enfoques constructivistas del aprendizaje, que consideran que el conocimiento se construye a través de la experiencia, la reflexión y la interacción con el entorno. Al brindar entornos interactivos que simulan el comportamiento real de las redes inalámbricas, las herramientas de simulación permiten al estudiante [40]:

- Identificar patrones de comportamiento en las redes inalámbricas.
- Analizar el rendimiento de diferentes configuraciones sin necesidad de implementarlas físicamente.
- Experimentar con fallos, cambios de topología y condiciones adversas para evaluar la resiliencia de la red.

Ventajas frente a métodos tradicionales

En el ámbito educativo, especialmente en la formación técnica relacionada con redes inalámbricas, el uso de simuladores se ha convertido en una herramienta cada vez más habitual. Su implementación ofrece múltiples beneficios tanto para docentes como para estudiantes, pero también conlleva ciertos desafíos. A continuación, en la siguiente Tabla 4, se presenta un análisis equilibrado de sus principales ventajas y desventajas [40].

Tabla 4. *Ventajas y desventajas del uso de simuladores en redes inalámbricas*

Ventajas	Desventajas
Ahorro en costos: permite reducir significativamente el gasto en laboratorios, evitando la compra y el mantenimiento de equipos costosos.	Distanciamiento de lo real: los simuladores no siempre logran reflejar fielmente interferencias, clima o fallas físicas de los dispositivos.
Accesibilidad para todos: los estudiantes pueden acceder desde sus computadoras personales, sin depender de un laboratorio físico.	Curva de aprendizaje técnica: herramientas como Atoll o GNS3 pueden ser complejas y demandan tiempo para su dominio efectivo.
Repetición ilimitada: los ejercicios pueden realizarse varias veces, facilitando el refuerzo de conceptos sin restricciones de tiempo o recursos.	Limitaciones de hardware: para ejecutar simulaciones avanzadas, se requiere una computadora con buena capacidad de procesamiento.
Ambiente seguro para fallos: se pueden cometer errores sin consecuencias costosas, lo cual favorece el aprendizaje sin presión.	Falsa sensación de control: puede generar expectativas poco realistas sobre el manejo de redes en entornos reales, donde abundan imprevistos.
Versatilidad en el aprendizaje: permite experimentar con distintos escenarios y tecnologías de red sin riesgos ni limitaciones físicas.	Falta de práctica física: el uso exclusivo de simuladores podría dejar de lado habilidades como el cableado, el manejo de equipos o instrumentos.

Aplicación en redes WISP

En el contexto específico de redes WISP, la simulación permite modelar con precisión escenarios reales de cobertura, interferencia, densidad de usuarios y calidad de servicio. Así, los estudiantes pueden desarrollar habilidades prácticas para [4]:

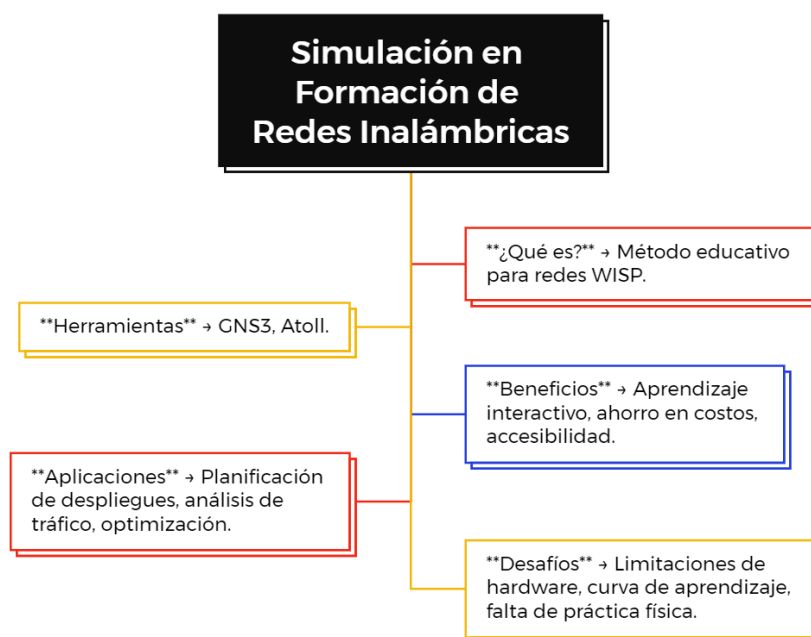
- Planificar despliegues inalámbricos con base en mapas de cobertura.
- Analizar el rendimiento bajo distintas condiciones de tráfico y carga de red.
- Configurar enlaces inalámbricos respetando parámetros técnicos como el margen de enlace, la ganancia de antena y la separación de canales.

La simulación como recurso didáctico no solo complementa, sino que en muchos casos supera en efectividad a los métodos tradicionales de enseñanza en el campo de las redes inalámbricas. Su capacidad para representar fenómenos complejos de manera interactiva, reproducible y sin riesgos reales la convierte en un componente fundamental de los planes de

estudio en carreras técnicas y universitarias. Particularmente en el ámbito de las redes WISP, la simulación no solo mejora la comprensión conceptual, sino que prepara a los estudiantes para enfrentar desafíos reales del entorno profesional con mayor seguridad y competencia técnica [4].

La Figura 9 ilustra el marco operativo descrito, detallando los beneficios, aplicaciones y desafíos esenciales de la simulación en formación de redes inalámbricas.

Figura 9. *Simulación educativa en redes WISP*



Uso de Atoll y GNS3 como herramientas integradas en la formación y evaluación de redes WISP

El avance en la educación técnica en telecomunicaciones ha impulsado la integración de herramientas especializadas que permitan una formación más cercana a la realidad del campo profesional. En este contexto, Atoll y GNS3 se han consolidado como plataformas fundamentales para la simulación, análisis y evaluación de redes inalámbricas, particularmente en el diseño y despliegue de redes WISP (Wireless Internet Service Provider). Su uso combinado permite una aproximación integral que abarca tanto la dimensión física de la propagación inalámbrica como la capa lógica y de configuración de red [11].

GNS3 (Graphical Network Simulator-3) es ampliamente reconocido por su capacidad para emular arquitecturas de red complejas, permitiendo la configuración de routers, switches, firewalls y otros dispositivos en un entorno virtual. Esta herramienta es especialmente útil en la formación de redes WISP, ya que permite a los estudiantes diseñar la estructura lógica de la red, configurar rutas, políticas de calidad de servicio (QoS), VLAN, NAT y mecanismos de seguridad. Su compatibilidad con imágenes reales de dispositivos (como MikroTik, Cisco, Juniper, etc.) ofrece un entorno de aprendizaje realista y técnicamente riguroso [15].

Por otro lado, Atoll se centra en la planificación y simulación radioeléctrica, ofreciendo funciones avanzadas para el diseño de cobertura, el análisis de interferencias, el estudio del perfil del terreno y la estimación del rendimiento de enlaces punto a punto o punto a multipunto. Esta herramienta permite incorporar modelos de propagación como Okumura-Hata, COST-231, ITU-R, entre otros, los cuales son fundamentales para entender cómo las condiciones del entorno — como edificaciones, vegetación, altura de antenas y condiciones atmosféricas— influyen directamente en la calidad de los enlaces inalámbricos. En el contexto de redes WISP, Atoll se convierte en un aliado esencial para decidir la ubicación óptima de torres, calcular márgenes de enlace y determinar las zonas de cobertura efectiva [17].

La integración pedagógica de GNS3 y Atoll desde el año 2022 ha sido promovida por diversos proyectos educativos que buscan formar a los estudiantes de telecomunicaciones no solo en la teoría, sino también en la práctica basada en simulaciones realistas. Esta combinación metodológica permite al estudiante realizar un recorrido completo por las etapas de diseño de una red WISP: desde el análisis del entorno físico hasta la configuración lógica de los dispositivos de red [11].

El uso combinado de estas herramientas también habilita la simulación de escenarios críticos, como la saturación de canales en zonas densamente pobladas, la presencia de interferencia co-canal y la degradación del servicio durante condiciones climáticas adversas [4].

La interferencia co-canal ocurre cuando múltiples transmisores utilizan el mismo canal de frecuencia dentro de una misma área de cobertura o en zonas adyacentes, lo que genera colisiones y una degradación significativa en la calidad de la señal. Esta situación es común en redes

inalámbricas mal planificadas y puede manifestarse en forma de pérdida de paquetes, baja velocidad de transmisión o desconexiones intermitentes. Por ello, es esencial considerar este tipo de interferencia al diseñar redes WISP, especialmente en bandas no licenciadas como la de 2.4 GHz, donde existe una alta probabilidad de congestión del espectro debido al uso masivo de dispositivos [4].

En este sentido, la simulación se enfocará en el diseño y análisis de una red WISP que opera en la banda de 5 GHz, utilizando Atoll para evaluar la cobertura y las condiciones de propagación en el entorno físico, y GNS3 para configurar la lógica de red con dispositivos MikroTik. Esta banda, si bien presenta un menor alcance y una penetración más limitada en interiores en comparación con la banda de 2.4 GHz, resulta ventajosa para enlaces exteriores con línea de vista, al ofrecer menor congestión espectral y un mayor número de canales disponibles, lo que favorece tasas de transferencia más altas. No obstante, al ser una banda ampliamente adoptada por otros sistemas inalámbricos, también resulta susceptible a interferencias, lo que refuerza la importancia de un diseño preciso y bien planificado. La simulación buscará demostrar cómo una correcta gestión de frecuencias, la ubicación estratégica de las torres y una configuración eficiente de los dispositivos pueden mitigar los efectos negativos de la interferencia co-canal y mejorar el rendimiento general de la red [4].

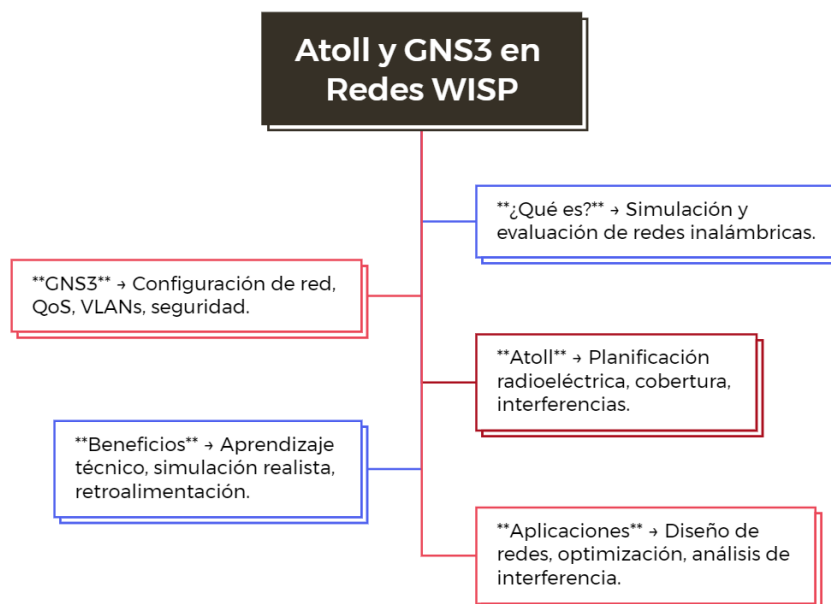
En estos contextos, los estudiantes pueden modificar variables, aplicar soluciones técnicas y observar los efectos en tiempo casi real, lo cual fortalece su capacidad de análisis y su criterio técnico para la toma de decisiones [4].

Desde la perspectiva evaluativa, esta metodología proporciona retroalimentación inmediata sobre el rendimiento de la red diseñada, tanto desde el punto de vista de la calidad de la señal (medida en parámetros como SNR o RSSI) como del comportamiento del tráfico (latencia, jitter, throughput, etc.). Esta retroalimentación permite identificar errores de diseño o configuración y mejorar el rendimiento general del sistema antes de una implementación física [35].

En conclusión, el uso integrado de Atoll y GNS3 en la formación y evaluación de redes WISP representa un enfoque educativo innovador, completo y adaptado a las exigencias del sector

de las telecomunicaciones. No solo permite a los estudiantes desarrollar competencias técnicas robustas en el diseño, configuración y análisis de redes inalámbricas, sino que también fomenta el pensamiento crítico, la resolución de problemas y la capacidad de simulación avanzada en contextos reales. Esta combinación se proyecta como una práctica pedagógica altamente efectiva que reduce la brecha entre la teoría académica y la realidad profesional del mundo de las telecomunicaciones. En la Figura 10 se resume lo esencial de GNS3 y Atoll para la implementación de una red WISP [11].

Figura 10. Integración de Atoll y GNS3 para la evaluación de redes WISP



Metodologías activas para la enseñanza de redes inalámbricas con simuladores

En el contexto de la formación en redes inalámbricas, especialmente aquellas orientadas al diseño e implementación de redes WISP (Wireless Internet Service Provider), las metodologías activas de enseñanza han emergido como una estrategia pedagógica eficaz que transforma al estudiante de un receptor pasivo de información a un protagonista activo en el proceso de aprendizaje. Estas metodologías, entre las que destacan el Aprendizaje Basado en Proyectos (ABP) y el Aprendizaje Basado en Problemas (ABP), han sido ampliamente adoptadas en entornos de educación técnica y universitaria desde el año 2022, especialmente en carreras de telecomunicaciones, redes y tecnologías de la información [4].

Aplicación de metodologías activas en redes inalámbricas

El Aprendizaje Basado en Proyectos (Project-Based Learning, PBL) consiste en que los estudiantes desarrollen un proyecto completo que simule un escenario real, desde la planificación hasta la implementación. En el ámbito de las redes inalámbricas, esto puede implicar la creación de una red WISP ficticia utilizando simuladores como GNS3 y Atoll, con condiciones realistas de cobertura, topografía, interferencia y configuración de nodos. Esta metodología permite aplicar conocimientos teóricos en situaciones prácticas, lo que fortalece el entendimiento de conceptos complejos como la propagación de ondas, el dimensionamiento de enlaces, la gestión de tráfico y la calidad de servicio [4].

Por otro lado, el Aprendizaje Basado en Problemas (Problem-Based Learning, PBL) plantea a los estudiantes desafíos técnicos específicos que deben ser resueltos mediante el uso de herramientas tecnológicas y trabajo colaborativo. Por ejemplo, se pueden presentar casos como la optimización de una red WISP existente que sufre pérdidas de paquetes por saturación, o la necesidad de ampliar la cobertura sin comprometer la calidad del servicio. En este contexto, el uso de simuladores como Atoll para evaluar cobertura e interferencia, junto con GNS3 para analizar configuraciones lógicas y flujos de tráfico, resulta esencial [4].

Integración con simuladores: GNS3 y Atoll como recursos didácticos

La combinación de metodologías activas con herramientas de simulación permite una experiencia educativa más completa. GNS3, al permitir la emulación de equipos reales (como routers MikroTik, Cisco o firewalls), facilita que los estudiantes configuren y prueben protocolos, esquemas de direccionamiento, NAT, VLAN, VPN y otras tecnologías clave para redes WISP. Atoll, por su parte, aporta una dimensión de análisis físico que incluye la simulación de enlaces de radiofrecuencia, el análisis de cobertura en terreno, el modelado de interferencias y la visualización de KPIs como SNR o BER [4].

Esta integración es adecuada para generar un entorno donde los estudiantes pueden experimentar de manera segura con configuraciones complejas, evaluar resultados cuantitativos, identificar errores y proponer soluciones técnicas, todo dentro de un marco guiado por los principios del constructivismo educativo.

Beneficios pedagógicos y desarrollo de competencias

La aplicación de estas metodologías ha demostrado múltiples beneficios pedagógicos. Desde el punto de vista del aprendizaje, se ha comprobado que los estudiantes retienen mejor el conocimiento, comprenden más profundamente los conceptos técnicos y desarrollan una mayor autonomía en el proceso educativo. A nivel de competencias, se fortalecen habilidades transversales altamente valoradas en el campo profesional, como [1]:

- Pensamiento crítico y analítico, al evaluar resultados de simulaciones.
- Toma de decisiones basada en datos, al seleccionar configuraciones óptimas o rutas de red.
- Trabajo colaborativo, esencial en la resolución conjunta de proyectos.
- Capacidad de documentación técnica, necesaria para presentar informes de implementación y evaluación de redes.
- Adaptabilidad tecnológica, al familiarizarse con herramientas de simulación de última generación.

Evaluación auténtica del aprendizaje

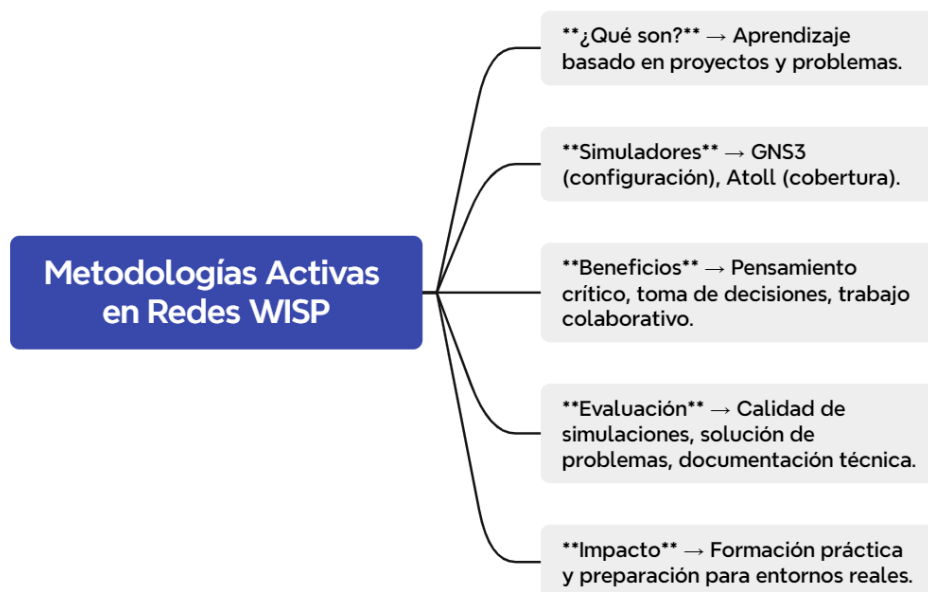
Otro aspecto relevante es que la combinación de simulación y metodologías activas permite una evaluación auténtica, es decir, una valoración del aprendizaje basada en tareas que se asemejan a las que el estudiante deberá enfrentar en su práctica profesional. En lugar de limitarse a pruebas escritas, el rendimiento del estudiante se puede valorar mediante la calidad de sus configuraciones, la documentación técnica del proyecto, la solución de problemas simulados y la argumentación de sus decisiones de diseño [1].

Las metodologías activas, al integrarse con simuladores como GNS3 y Atoll, transforman la enseñanza de redes inalámbricas en una experiencia inmersiva, práctica y significativa. Este enfoque no solo mejora la comprensión teórica, sino que prepara a los futuros profesionales para enfrentar los retos del mundo real con una base sólida en diseño, análisis y optimización de redes

WISP. La implementación de estas metodologías representa un avance pedagógico que debería ser consolidado y expandido en los currículos de formación técnica en telecomunicaciones.

La Figura 11 ofrece una perspectiva gráfica unificada del apartado, esquematizando el rol de los simuladores, los beneficios de aprendizaje y los criterios de evaluación propuestos.

Figura 11. *Metodologías activas para la enseñanza en redes inalámbricas*



Estandarización de prácticas de simulación en el diseño y análisis de redes WISP

La estandarización de prácticas de simulación representa un paso crucial en el diseño, evaluación y análisis de redes inalámbricas WISP (Wireless Internet Service Provider). Esta estandarización tiene como objetivo garantizar la coherencia, confiabilidad y comparabilidad de los resultados obtenidos mediante herramientas de simulación como GNS3, Atoll, Packet Tracer, entre otras. En el contexto de la formación técnica y la investigación universitaria, establecer directrices claras y reproducibles no solo eleva la calidad académica, sino que también promueve una mejor preparación de los estudiantes para enfrentar situaciones reales en la industria [1].

Desde el año 2022, diversos grupos de investigación, especialmente en facultades de ingeniería en telecomunicaciones, han desarrollado propuestas metodológicas orientadas a definir marcos de referencia estandarizados para la simulación de redes WISP. Estas iniciativas han

buscado igualar los criterios técnicos empleados durante los estudios, de modo que los resultados obtenidos sean válidos para comparaciones entre diferentes proyectos, contextos geográficos o configuraciones de red [4].

Parámetros técnicos estandarizados

Entre los elementos fundamentales que se han identificado como necesarios de estandarizar se encuentran [4]:

- Frecuencias de operación: Las simulaciones deben contemplar principalmente las bandas de 2.4 GHz y 5 GHz, por ser las más utilizadas en redes WISP debido a su equilibrio entre cobertura, penetración y capacidad de datos. En algunos casos, también se estudian bandas superiores como los 60 GHz en enlaces cortos de alta velocidad.
- Niveles de ruido: Se establecen valores típicos de ruido de fondo ambiental y ruido térmico en entornos urbanos, suburbanos y rurales, con el fin de simular condiciones realistas de interferencia.
- Distancia entre estaciones: Se determinan rangos estándar de separación entre estaciones base y clientes, que varían dependiendo del entorno (urbano con obstáculos, zonas abiertas, topografía montañosa).
- Sensibilidad de los receptores: Se definen umbrales de sensibilidad mínimos aceptables (en dBm) para diferentes tipos de equipos WISP, como CPE y APs, con base en especificaciones reales de mercado.
- Características del terreno: La clasificación del entorno (urbano, rural, mixto) es indispensable, ya que afecta directamente la propagación de la señal. Los modelos deben incluir mapas digitales de elevación y consideraciones sobre obstáculos como edificios, vegetación o colinas.

Técnicas recomendadas para evaluación

Un aspecto clave de la estandarización es la selección y definición de métricas de rendimiento que permitan una evaluación integral del comportamiento de la red. Entre las métricas recomendadas destacan [4]:

- Throughput (rendimiento efectivo): Medición de la cantidad de datos útiles transmitidos con éxito por segundo, tanto en sentido ascendente como descendente.
- Latencia: Tiempo que tarda un paquete en ir del emisor al receptor. Es fundamental para evaluar la capacidad de respuesta de la red.
- Jitter: Variación en el retardo de entrega de paquetes, crucial en aplicaciones sensibles al tiempo como VoIP y videollamadas.
- PER (Packet Error Rate): Tasa de errores por paquetes recibidos, que permite evaluar la calidad general del canal.

Estas métricas deben medirse bajo distintas condiciones de carga, interferencia y escenarios topográficos, asegurando una cobertura amplia y precisa de los posibles comportamientos de la red simulada.

Documentación estandarizada de escenarios

Un componente clave de la estandarización consiste en la documentación estructurada de los escenarios simulados; esto implica crear formatos y plantillas para describir [1]:

- El objetivo del experimento.
- Las herramientas utilizadas y su configuración.
- Los parámetros técnicos del modelo (frecuencias, distancias, niveles de ruido, etc.).
- Los resultados obtenidos con gráficas y tablas.
- Las observaciones sobre el comportamiento de la red.
- Las recomendaciones o conclusiones derivadas del análisis.

La documentación clara y replicable permite reutilizar los escenarios simulados en futuros trabajos de investigación, proyectos académicos o estudios profesionales, además de facilitar la evaluación por parte de tutores, asesores o equipos técnicos.

Impacto educativo y profesional

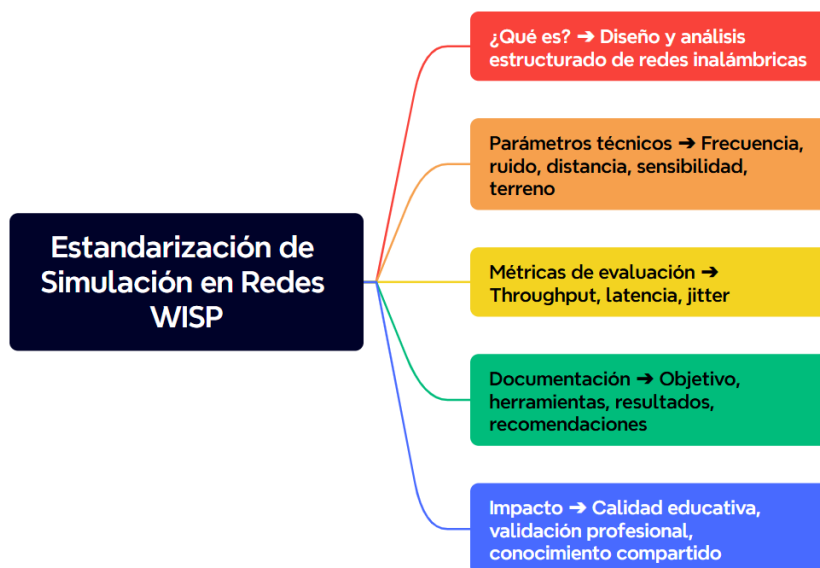
La estandarización de prácticas de simulación también representa un avance en el ámbito educativo, ya que permite a los estudiantes adquirir una metodología sólida para el diseño de redes. Al trabajar con guías claras y métricas bien definidas, se refuerzan competencias como el análisis técnico, la interpretación de datos, la planificación de redes reales y la comunicación efectiva de resultados [1].

Asimismo, en el ámbito profesional, la estandarización sienta las bases para desarrollar procesos de validación técnica en proyectos de implementación de redes WISP, asegurando que los diseños sean reproducibles, escalables y sostenibles en el tiempo [1].

La estandarización de prácticas de simulación en redes WISP constituye un paso esencial hacia una enseñanza más estructurada, una investigación más rigurosa y una práctica profesional más eficiente. A través de la definición de parámetros técnicos comunes, métricas de evaluación claras y protocolos de documentación estandarizados, se promueve la calidad y consistencia en el análisis de redes inalámbricas. Esto permite no solo mejorar los resultados académicos y profesionales, sino también construir una base de conocimiento colectivo que puede ser compartida, reutilizada y mejorada continuamente en el campo de las telecomunicaciones [1].

Para una comprensión visual rápida, la Figura 12 condensa los ejes esenciales tratados en este ítem respecto a la estandarización de simulación en redes WISP.

Figura 12. *Estandarización de simulación en redes WISP*



2.3. Simuladores de tráfico en redes

El desarrollo de redes inalámbricas de tipo WISP (Wireless Internet Service Provider) requiere de un enfoque técnico riguroso, incluso en su fase de diseño simulado. Para lograrlo, es esencial contar con plataformas de simulación que permitan emular no solo el tráfico de red, sino también la arquitectura, los protocolos de enrutamiento, las interfaces y los equipos reales involucrados. En esta sección se presenta un análisis comparativo de las herramientas más utilizadas para la generación de tráfico y la emulación de redes en entornos académicos y profesionales, con el fin de fundamentar la elección de las tecnologías aplicadas a este proyecto [1].

2.3.1. Tecnologías de simulación para generación de tráfico en redes

Fundamentos de la simulación de tráfico en redes virtuales

Simular tráfico en redes virtuales permite recrear escenarios técnicos que, de realizarse físicamente, implicarían altos costos logísticos, tiempo de montaje y equipos de red especializados. En el contexto académico y de investigación, estas simulaciones no solo permiten verificar el funcionamiento de una topología o protocolo, sino también experimentar con configuraciones reales, observar el comportamiento de tráfico ante congestiones, pérdidas, latencia o cambios de

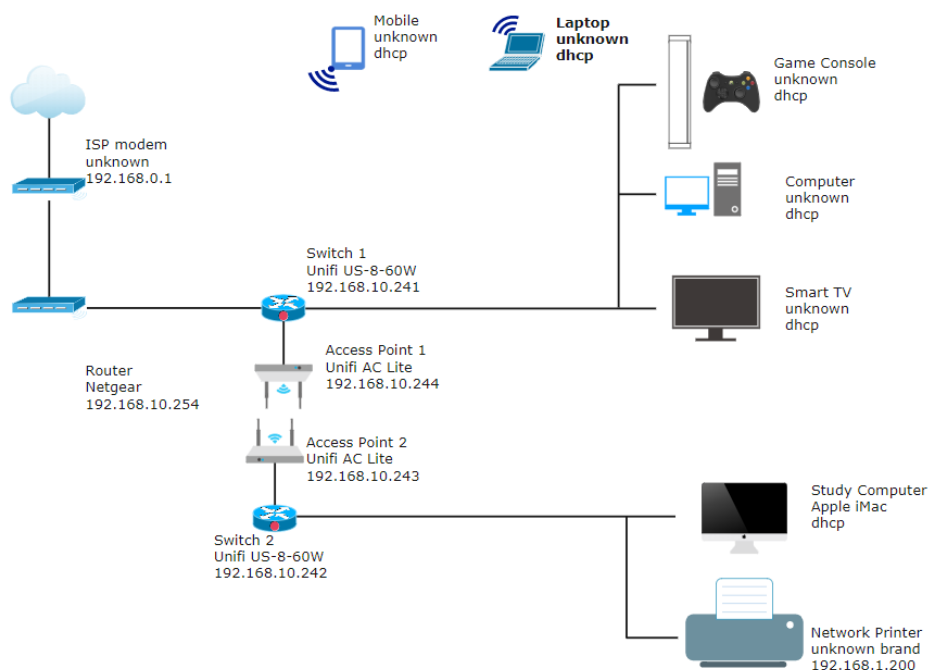
ruta, y evaluar métricas clave como el throughput, la calidad de servicio y la eficiencia en la gestión de recursos [1].

Existen dos enfoques principales:

- **Simulación visual con interfaz gráfica (GUI):** usada en entornos educativos por su facilidad de uso; permite arrastrar nodos, configurar dispositivos y visualizar tráfico. (ejemplo, Packet Tracer, GNS3, EVE-NG).
- **Simulación basada en eventos o algoritmos:** orientada a investigación avanzada, con simuladores como NS-3 u OMNeT++, que modelan eventos matemáticamente, pero sin interfaz gráfica intuitiva.

Dado que este proyecto busca tanto la formación de competencias profesionales como la posibilidad de integración con equipos reales, se prioriza el uso de simuladores visuales con soporte de imágenes reales. A continuación, en la Figura 13 se muestra el diseño de una red en un entorno de simulación.

Figura 13. *Diseño de una red en un entorno de simulación*



Características técnicas de GNS3

GNS3 (Graphical Network Simulator-3) es una plataforma de simulación y emulación de redes ampliamente adoptada en entornos académicos, técnicos y profesionales. Su principal fortaleza radica en que emula sistemas operativos reales de equipos de red, mediante tecnologías como QEMU, lo que permite ejecutar imágenes originales de fabricantes como Cisco, MikroTik, Juniper y VyOS, entre otros [27].

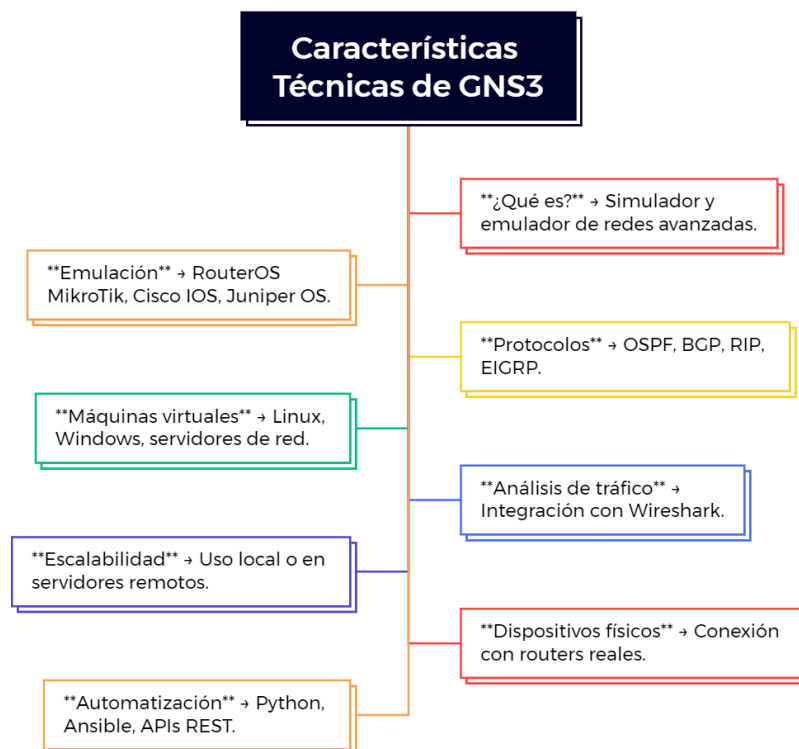
Entre sus características técnicas destacadas se encuentran [27]:

- **Emulación completa de RouterOS de MikroTik:** GNS3 permite ejecutar imágenes CHR (Cloud Hosted Router) de MikroTik, lo que posibilita la práctica directa con configuraciones reales de este fabricante ampliamente utilizado en redes WISP. Esto permite simular funcionalidades como túneles GRE, VPN, colas, reglas de firewall, routing avanzado y más [27].
- **Soporte para enrutamiento dinámico:** se pueden configurar y probar protocolos de enrutamiento como OSPF, BGP, RIP y EIGRP (con IOS reales), lo que permite estudiar la convergencia, el balanceo de carga, la redistribución entre protocolos, entre otros escenarios críticos [27].
- **Capacidad para correr máquinas virtuales:** GNS3 permite integrar máquinas virtuales completas, tanto de sistemas operativos Linux y Windows. Esto permite, por ejemplo, simular servidores DHCP, DNS, bases de datos, controladores de dominio o simplemente estaciones de trabajo desde donde ejecutar pruebas como ping, traceroute, escaneos de red o aplicaciones cliente-servidor [27].
- **Integración con Wireshark para análisis de paquetes:** cada enlace entre dispositivos puede ser monitorizado a través de capturas en tiempo real utilizando Wireshark. Esta integración permite analizar protocolos como ARP, TCP, UDP, ICMP, BGP, OSPF, entre otros, lo que es esencial para comprender el comportamiento real del tráfico de red y detectar posibles fallos o cuellos de botella [27].

- **Interfaz gráfica intuitiva y personalizable:** su entorno visual permite organizar los nodos de red en diferentes capas, agrupar equipos, añadir etiquetas, iconos personalizados, zonas de colores y hacer zoom a distintas secciones del diseño, lo que mejora la comprensión de topologías complejas [27].
- **Funcionamiento local o en servidores remotos:** GNS3 puede ejecutarse de manera local en un equipo de escritorio, o también puede desplegarse en servidores remotos para aprovechar mayores recursos computacionales. Esta opción permite simular redes a gran escala, incluso en laboratorios compartidos, o integrarse con nubes privadas o entornos de virtualización empresarial [27].
- **Compatibilidad con dispositivos físicos:** Una funcionalidad avanzada de GNS3 es la posibilidad de integrar equipos físicos a la simulación mediante interfaces de red del sistema anfitrión (host). Esto permite, por ejemplo, conectar un router físico MikroTik o Cisco directamente al entorno virtual, facilitando laboratorios híbridos donde coexisten dispositivos virtuales y reales [27].
- **Extensa biblioteca de plantillas e imágenes preconfiguradas:** La comunidad de GNS3 ha contribuido con una gran cantidad de plantillas, laboratorios prediseñados, configuraciones básicas y avanzadas, lo cual reduce significativamente el tiempo de implementación de prácticas comunes y facilita el aprendizaje autodidacta [27].
- **Automatización y scripting:** Para usuarios avanzados, GNS3 ofrece integración con herramientas de automatización como Ansible, Python (usando APIs REST) y otros entornos de orquestación, permitiendo realizar pruebas automatizadas, configuraciones masivas o integraciones con sistemas de gestión de red. Gracias a estas capacidades, GNS3 no se limita a ser un entorno de laboratorio, sino que se convierte en una herramienta casi idéntica a un entorno de red real [27].

La Figura 14 resume de manera esquemática los elementos técnicos esenciales analizados en este ítem sobre GNS3, facilitando la comprensión visual de su potencial en la emulación de redes avanzadas, soporte de protocolos, análisis de tráfico y escalabilidad del entorno virtualizado.

Figura 14. Características de GNS3 para la simulación de redes



Comparativa técnica: GNS3 vs. Cisco Packet Tracer vs. EVE-NG

A continuación, en la Tabla 5 se detalla una comparación técnica entre los tres simuladores más conocidos y utilizados en el ámbito académico y profesional [22]:

Tabla 5. *Comparativa técnica de GNS3 vs otros simuladores*

Característica	GNS3	Cisco Packet Tracer	EVE-NG
Tipo de tecnología	Emulación real	Simulación (no ejecuta imágenes reales)	Emulación (completa, versión gratuita o Pro)
Compatibilidad con RouterOS MikroTik	Sí, usando imagen CHR	No	Sí (pero con configuración más avanzada)
Imágenes reales soportadas	Cisco IOS, MikroTik CHR, JunOS, VyOS, etc.	Solo IOS genérico de Cisco	Cisco, MikroTik, Juniper, Palo Alto, etc.
Consumo de recursos	Medio a alto (depende de las imágenes usadas)	Bajo (por ser más básico)	Alto (requiere hardware potente y buena RAM)
Curva de aprendizaje	Media, con buena documentación	Baja, ideal para principiantes	Alta (especialmente en versión Community gratuita)
Entorno gráfico	Muy completo, editable, interactivo	Interfaz limitada a topologías Cisco	Menos intuitivo (basado en navegador web)
Colaboración en la red	Red Limitada (versión standalone)	No permite colaboración	Sí, múltiples usuarios (versión Pro o web)
Costo	Totalmente gratuito y open-source	Gratuito pero restringido a productos Cisco	Gratuito (Community), pago en versión Pro

Análisis de compatibilidad con equipos reales y protocolos

Una de las características más valoradas de GNS3 es su nivel de fidelidad con equipos reales, ya que utiliza las mismas imágenes de software que los routers y switches comerciales. Esto permite que las configuraciones que se aplican en el entorno simulado sean prácticamente idénticas a las que se aplicarían en la vida real [27].

Compatibilidad destacada:

- Emulación directa de RouterOS MikroTik.
- Soporte completo de protocolos de enrutamiento como OSPF, BGP, PPPoE, VLAN, DHCP, NAT, VPN.
- Integración con switches y routers físicos conectados por red LAN.

- Captura de paquetes con herramientas reales como Wireshark.
- Importación de máquinas virtuales (por ejemplo, un servidor Linux para pruebas de ping, traceroute, SNMP o NetFlow).

Estas características hacen de GNS3 una plataforma ideal para la enseñanza técnica en telecomunicaciones, ya que el estudiante interactúa con un entorno prácticamente indistinguible de un sistema en producción [27].

Comparativa de analizadores de tráfico

En cualquier entorno de simulación avanzada de redes, la capacidad de analizar el tráfico capturado entre dispositivos es crucial para validar configuraciones, entender el comportamiento del protocolo y detectar errores de diseño o congestión. En este contexto, Wireshark destaca como una herramienta ampliamente utilizada, aunque existen otras opciones como NetFlow (integrado en routers y switches Cisco) y Ntop (orientado a monitoreo en tiempo real desde interfaces web) [41].

A continuación, en la Tabla 6 se presenta una comparativa técnica de estas tres herramientas de análisis [41]:

Tabla 6. *Análisis comparativo de capturadores y analizadores de tráfico de red*

Característica	Wireshark	NetFlow (Cisco)	Ntop / NtopNG
Tipo de análisis	Análisis profundo de paquetes (sniffing)	Estadístico por flujo	Análisis por interfaz / tiempo real
Interfaz de usuario	Gráfica (GUI), amigable y detallada	Requiere consola o integración externa	Interfaz web con gráficos dinámicos
Niveles de protocolo soportados	Capa 2 a Capa 7 (Ethernet, TCP, HTTP, etc.)	Capa 3 y 4 principalmente	Capa 3 a 7, pero menos detallado
Captura de tráfico en tiempo real	Sí, con filtros personalizados	No captura paquetes, solo resumen de flujo	Sí, pero no tan detallado como Wireshark
Exportación y análisis forense	Exportación en .pcap, decodificación completa	Exportación limitada a estadísticas	Exportación en CSV, JSON
Costo / licencia	Gratuito, código abierto (GPL)	Depende del fabricante	Versión gratuita limitada, versión pro

Tipo de análisis

Uno de los principales factores que diferencian las herramientas de análisis de red es el tipo de enfoque que aplican para estudiar el tráfico. Mientras algunas se especializan en la inspección directa de cada paquete transmitido, otras agrupan la información en flujos o estadísticas generales. Esta distinción es esencial, ya que influye directamente en la profundidad del análisis y en su utilidad dependiendo del objetivo técnico. A continuación, en la Tabla 7 se presenta una comparativa del tipo de análisis que ofrecen Wireshark, NetFlow y NtopNG [42]:

Tabla 7. *Tipos de análisis de tráfico en herramientas de monitoreo*

Tipo de análisis	Wireshark	NetFlow (Cisco)	Ntop / NtopNG
Análisis por paquete (sniffing)	Captura individual de cada paquete, con encabezados, payload y checksum.	No captura paquetes, solo los resume como flujo.	Parcial, solo encabezados y tipo de tráfico.
Análisis por flujo	No nativo, pero posible con plugins externos o scripts.	Nativo, agrupa paquetes según sesión de origen y destino.	Nativo, muestra comportamiento agregado por host y servicio.
Análisis por protocolo (Capa 2–7)	Completo: Ethernet, IP, TCP, UDP, HTTP, DNS, SSL, etc.	Limitado a Capa 3–4 (IP, UDP, TCP).	Capa 3–7, pero sin detalles por paquete.
Detección de errores de red	CRCs, colisiones, retransmisiones, SYN fallidos, NAT mal configurado.	Solo se detecta pérdida de paquetes por volumen.	Detección básica por anomalías de flujo.
Detección de comportamiento malicioso	ARP Spoofing, DNS hijacking, escaneos, DoS detectables por firmas.	Detección estadística por volumen (si se configura correctamente).	Puede mostrar patrones anómalos, pero no tan específico como Wireshark.
Análisis forense (offline)	Exportación PCAP para posterior revisión detallada.	Estadísticas exportables, sin paquetes.	Exportación en CSV/JSON, útil para auditoría general.
Aplicabilidad en simulación educativa	Altamente efectiva para entender protocolos y errores comunes.	No se integra con simuladores, análisis limitado.	Aceptable como panel de resumen, no técnico a nivel de bit.

Interfaz de usuario

La forma en la que el usuario interactúa con la herramienta también determina su accesibilidad y facilidad de uso. Algunas soluciones están orientadas a técnicos con experiencia y consola, mientras que otras ofrecen entornos gráficos más amigables e intuitivos. A continuación, en la Tabla 8 se comparan las interfaces que ofrecen Wireshark, NetFlow y NtopNG [43]:

Tabla 8. *Comparativa de interfaz de usuario en herramientas de análisis de tráfico*

Característica	Wireshark	NetFlow (Cisco)	Ntop/NtopNG
Tipo de interfaz	Gráfica (GUI) de escritorio con múltiples paneles interactivos.	No posee GUI nativa, depende de herramientas externas (CLI/SNMP).	Interfaz web dinámica, accesible desde navegador.
Curva de aprendizaje	Media: requiere conocimientos básicos de redes para sacarle provecho.	Alta: requiere conocimientos avanzados de redes Cisco.	Baja-media: fácil para visualizar tráfico general.
Nivel de personalización	Alto: filtros personalizados, vistas por protocolo o flujo.	Bajo: configuración predefinida por el router.	Medio: gráficas configurables, pero menos detalle por paquete.
Visualización del tráfico	Detallada por paquete, protocolos y capas.	Gráficas generales por volumen, sin paquetes individuales.	Gráficas por host, tipo de tráfico, puertos y consumo.
Interacción en tiempo real	Sí, actualiza automáticamente durante la captura.	No (datos exportados cada cierto tiempo).	Sí, con refresco continuo vía web.
Exportación de datos desde interfaz	Sí: PCAP, XML, JSON, TXT.	Limitada, requiere herramientas como NetFlow Analyzer.	Sí: CSV, JSON desde la interfaz web.
Compatibilidad con simuladores (GNS3)	Alta: integración directa y fácil en enlaces de GNS3.	Nula: no diseñado para simulación, depende de routers físicos.	Media: posible integración, pero no común en entornos académicos.

Niveles de protocolo

Otro criterio técnico fundamental es la profundidad de protocolos que cada herramienta puede interpretar. En un entorno simulado, donde se busca evaluar desde el comportamiento de tramas Ethernet hasta la gestión de servicios de capa de aplicación como HTTP o DNS, es

importante contar con una solución que brinde una lectura amplia del stack de red. A continuación, en la Tabla 9 se especifica el nivel de protocolo que pueden analizar Wireshark, NetFlow y NtopNG [43]:

Tabla 9. *Comparativa de niveles de protocolo soportados por herramientas de análisis*

Característica	Wireshark	NetFlow (Cisco)	Ntop / NtopNG
Capa 2 (Enlace)	Soporta análisis de tramas Ethernet, ARP, VLAN, PPP.	No soporta, no captura paquetes.	Parcial, identificación de interfaces y estadísticas básicas.
Capa 3 (Red)	IP, ICMP, IPv6, enrutamiento, NAT.	Soporta IP, identifica flujos por IP origen/destino.	Visualiza tráfico IP, subredes y rutas.
Capa 4 (Transporte)	TCP, UDP, puertos, sesiones, control de congestión.	Extrae estadísticas de flujos TCP y UDP.	Identifica conexiones activas y puertos utilizados.
Capa 5-7 (Aplicación)	DNS, HTTP, FTP, HTTPS, SIP, Telnet, SMB, protocolos industriales, etc.	No analiza contenido de aplicación.	Parcial: identifica tipos de tráfico, pero sin inspección profunda (no DPI).
Análisis profundo (DPI)	Sí, inspección completa de encabezados y datos en cada capa.	No, basado en encabezados y estadísticas.	Parcial, depende de plugins y configuración.
Reconocimiento automático	Identifica protocolos automáticamente incluso en puertos no estándar.	Limitado a flujos IP.	Reconocimiento parcial, depende de la base de firmas.

Captura de tráfico en tiempo real

La capacidad de capturar tráfico en tiempo real es clave cuando se necesita observar directamente cómo fluye la información entre dispositivos, especialmente en pruebas de configuración dinámica o detección de errores en vivo. A continuación, en la Tabla 10 se compara esta funcionalidad entre las tres herramientas Wireshark, NetFlow y NtopNG [44]:

Tabla 10. *Comparativa de captura de tráfico en tiempo real*

Característica	Wireshark	NetFlow (Cisco)	Ntop / NtopNG
Captura directa de paquetes	Captura cada paquete en tiempo real, en interfaces locales o remotas.	No captura paquetes, solo resume información de flujos IP.	Captura parcial; muestra estadísticas en tiempo real por interfaz.
Filtrado en tiempo real	Sí, con filtros personalizados BPF (Berkeley Packet Filter).	No aplica.	Sí, con filtros limitados por protocolo o interfaz.
Visualización en vivo	Vista de cada paquete, encabezado, payload y árbol de protocolos.	No aplica.	Estadísticas gráficas (ancho de banda, top talkers, protocolos más usados).
Análisis simultáneo mientras captura	Sí, permite pausar, marcar, clasificar y seguir paquetes durante captura.	Solo exporta al final del flujo.	Sí, aunque el análisis profundo depende del rendimiento del sistema.
Soporte de múltiples interfaces	Sí, incluso en interfaces virtuales dentro de simuladores como GNS3.	Sí, pero solo para dispositivos habilitados con NetFlow.	Sí, puede monitorizar varias interfaces físicas y virtuales simultáneamente.

Exportación y análisis forense

Además del análisis en vivo, es esencial que una herramienta permita almacenar las capturas para su revisión posterior. Esta funcionalidad resulta útil en escenarios forenses, donde se necesita volver sobre los datos para realizar auditorías, entrenar a estudiantes o documentar el comportamiento de una red. La siguiente Tabla 11 muestra las capacidades de exportación y análisis fuera de línea de las tres herramientas: Wireshark, NetFlow y NtopNG [45].

Tabla 11. *Comparativa de exportación y análisis forense*

Característica	Wireshark	NetFlow (Cisco)	Ntop / NtopNG
Exportación de datos	Exporta en formatos .pcap, .csv, .txt y .json, entre otros.	Exporta solo estadísticas agregadas, en formatos limitados como .csv.	Exporta en .csv, .json y bases de datos SQLite, InfluxDB, Prometheus.
Reanálisis de tráfico capturado	Permite reabrir sesiones para decodificar protocolos, aplicar filtros nuevos, reconstruir sesiones TCP.	No permite reanálisis a nivel de paquetes; solo consulta de datos históricos.	Permite análisis de sesiones históricas por interfaz, flujo y host.
Análisis forense	Ideal para análisis forense detallado: detección de malware, intrusiones, sniffing DNS, ataques ARP.	Muy limitado para análisis forense profundo.	Análisis forense superficial; útil para tendencias, no para inspección paquete a paquete.
Compatibilidad con otras herramientas	Integra con TShark, tcpdump, Zeek, Security Onion, Elastic Stack.	Compatible con SIEM, herramientas de monitoreo de red empresarial.	Compatible con Grafana, Elasticsearch, Kibana, Loki, etc.

Costo y licencia

Finalmente, un aspecto no menor a considerar es la viabilidad de uso en entornos académicos y de simulación, donde el acceso a herramientas comerciales puede ser limitado. En este punto, el tipo de licencia y el costo asociado determinan si una solución es accesible para estudiantes y docentes. En la siguiente Tabla 12 se comparan las condiciones de uso de cada una de estas herramientas: Wireshark, NetFlow y NtopNG [46].

Tabla 12. *Comparativa de costo y licenciamiento*

Característica	Wireshark	NetFlow (Cisco)	Ntop / NtopNG
Licencia	GPL (General Public License) – Software libre.	Propietaria – Incluida en equipos Cisco.	GPLv3 (versión gratuita) / Licencia comercial (versión Pro).
Costo base	Gratuito y de código abierto.	Sin costo adicional si se tiene hardware Cisco compatible.	Versión gratuita con funciones limitadas / Versión Pro: de pago.
Acceso a todas las funciones	Todas las funciones están disponibles sin restricciones.	Algunas funciones avanzadas requieren hardware específico.	La versión Pro desbloquea análisis extendido, alertas y plugins.
Soporte oficial	Comunidad activa, documentación extensa, foros.	Soporte disponible a través de Cisco con contrato vigente.	Soporte técnico disponible solo en versión Pro.
Actualizaciones	Comunidad activa, documentación extensa, foros.	Dependen del modelo y contrato de soporte.	Gratuitas en versión libre; frecuentes en versión Pro.

Justificación técnica: Selección de Wireshark como analizador de tráfico

La elección de Wireshark como herramienta principal de análisis de tráfico en este proyecto no es casual, sino el resultado de un análisis comparativo profundo basado en características técnicas, capacidad de procesamiento, adaptabilidad a entornos simulados y viabilidad educativa [47].

A diferencia de herramientas como NetFlow, que se enfocan en estadísticas agregadas a nivel de flujo, Wireshark permite una inspección extremadamente detallada de cada paquete que circula por la red. Esta capacidad de “sniffing” o captura profunda de paquetes es esencial para comprender el comportamiento real de protocolos como TCP, UDP, ICMP, OSPF o BGP, identificar errores de configuración (por ejemplo, NAT o VLAN mal implementadas) e incluso simular escenarios de ataque como ARP spoofing, algo imposible de visualizar con NetFlow [48].

Asimismo, en comparación con NtopNG, que se enfoca más en gráficos de uso general desde una interfaz web, Wireshark ofrece una precisión de nivel forense. Esto permite capturar sesiones reales, aplicar filtros avanzados, decodificar paquetes en diferentes capas del modelo OSI

(desde Ethernet hasta HTTP o DNS) y exportar los resultados en formatos estándar como .pcap, los cuales pueden ser utilizados en auditorías o reanálisis posterior [49].

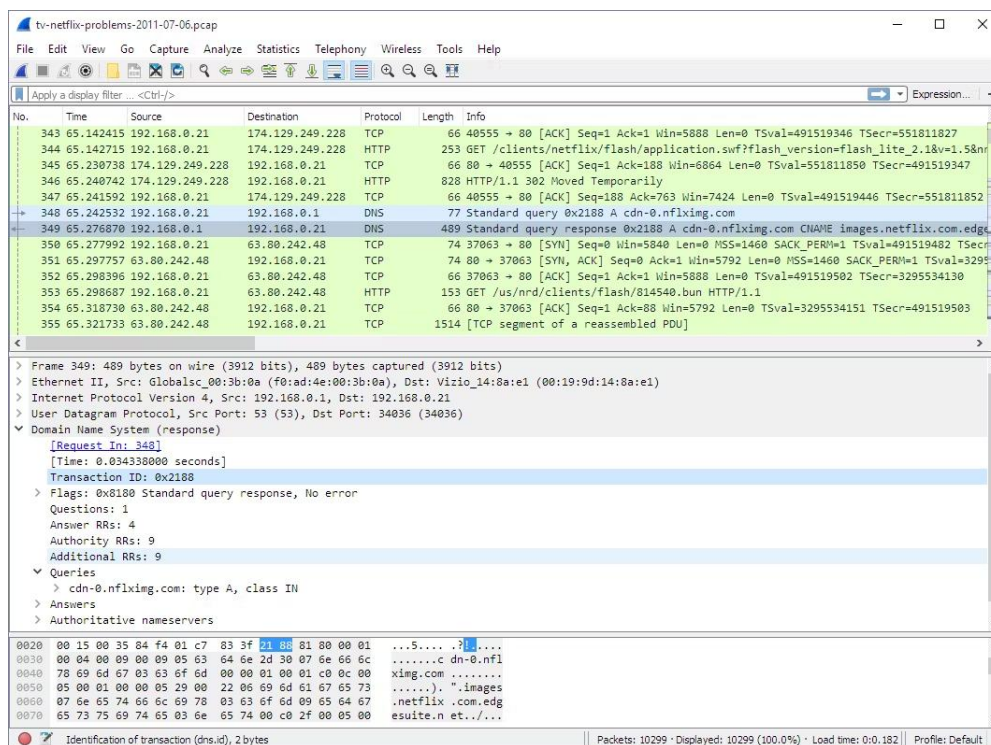
Desde el punto de vista técnico, Wireshark destaca por:

- Su integración nativa con GNS3, permitiendo iniciar capturas directamente en enlaces virtuales.
- Su soporte para múltiples protocolos de capa 2 a capa 7, lo que lo hace ideal tanto para análisis de red como de aplicaciones.
- Su funcionalidad en tiempo real, facilitando el estudio de congestiones, latencia o pérdidas de paquetes durante la simulación.
- Ser gratuito, de código abierto y multiplataforma, lo cual facilita su implementación en ambientes académicos con recursos limitados.

Además, las tablas comparativas presentadas en esta sección han evidenciado que Wireshark supera a sus alternativas en casi todos los criterios relevantes para un entorno de simulación educativa, desde la profundidad de análisis hasta la usabilidad. A esto se suma su baja barrera de entrada para estudiantes, gracias a su interfaz intuitiva, extensa documentación y comunidad activa de soporte.

En conclusión, Wireshark es la opción más viable, efectiva y alineada con los objetivos técnicos y pedagógicos de este trabajo, permitiendo no solo simular redes, sino comprenderlas a profundidad con un enfoque práctico y realista. La Figura 15 muestra la ventana de trabajo de Wireshark realizando una captura de paquetes.

Figura 15. Captura de paquetes en Wireshark



Justificación técnica: selección de GNS3 como simulador principal

Después del análisis técnico realizado, la elección de GNS3 como simulador principal se justifica por varias razones clave [27]:

1. **Alta fidelidad en la emulación:** A diferencia de Cisco Packet Tracer, que simula de manera básica y solo equipos Cisco con funcionalidades limitadas, GNS3 permite emular imágenes reales, especialmente MikroTik, lo cual es fundamental en este proyecto [27].
2. **Software gratuito y de código abierto:** A diferencia de EVE-NG, cuya versión completa requiere licencias de pago y recursos de hardware elevados, GNS3 es completamente gratuito y funcional incluso en equipos de gama media [27].
3. **Compatibilidad educativa y profesional:** GNS3 permite que los estudiantes aprendan configuraciones reales que luego podrán aplicar directamente en el campo laboral. Esto cierra la brecha entre la teoría y la práctica.

- 4. Amplia comunidad de soporte y documentación:** Su comunidad activa proporciona acceso a tutoriales, plantillas, foros y proyectos compartidos, lo cual facilita el aprendizaje y la resolución de problemas.

A modo de síntesis, la Figura 16 esquematiza los fundamentos de la virtualización, vinculando sus beneficios teóricos con la aplicación práctica mediante software especializado.

Figura 16. *Justificación de GNS3 para la simulación de redes*



En conclusión, GNS3 representa el equilibrio perfecto entre realismo técnico, accesibilidad, facilidad de uso y aplicabilidad académica, por lo que se adopta como herramienta central para las simulaciones de este proyecto.

2.3.2. Estudio técnico de factibilidad en sistemas de propagación

Esta sección analiza los aspectos esenciales relacionados con la simulación y el modelado de propagación en redes inalámbricas, con énfasis en entornos WISP. Dado que las redes WISP dependen de enlaces de radiofrecuencia altamente sensibles a la distancia, la topografía, las interferencias y las condiciones atmosféricas, resulta imprescindible realizar un estudio técnico de factibilidad que permita anticipar el comportamiento de la señal antes de su implementación física.

El objetivo de esta evaluación es determinar si los enlaces planificados podrán operar con niveles adecuados de potencia recibida, relación señal/ruido (SNR), probabilidad de interferencia

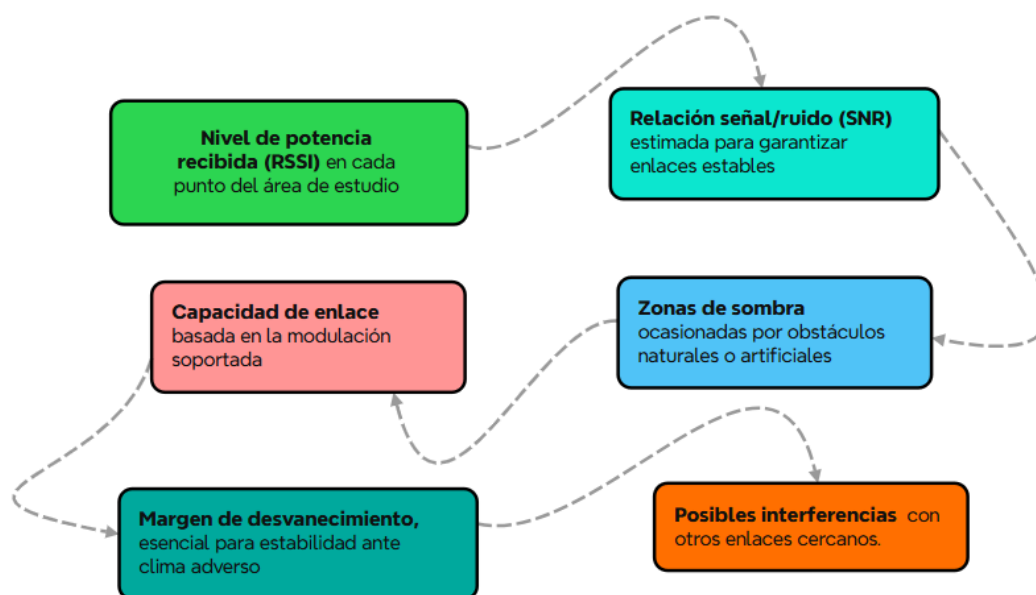
y cobertura. Para ello se utilizan herramientas especializadas como Atoll, que permite simular escenarios reales y analizar parámetros críticos que afectan el desempeño inalámbrico [17].

Fundamentos de simulación de cobertura y propagación

La simulación de cobertura y propagación constituye uno de los procesos fundamentales en el diseño de redes inalámbricas. Este proceso permite modelar matemáticamente cómo se comportan las ondas electromagnéticas en un entorno geográfico determinado, tomando en cuenta factores como la frecuencia de operación, altura de las antenas, relieve del terreno, presencia de edificaciones, vegetación y condiciones ambientales [17].

En redes WISP, la precisión del modelo de propagación es crucial, ya que determina la viabilidad de los enlaces punto a punto y punto a multipunto. A través de la simulación se puede conocer:

Figura 17. Factores que se pueden determinar en una simulación



Las simulaciones permiten evaluar diferentes escenarios sin incurrir en costos de instalación o pruebas en campo, lo cual resulta especialmente valioso en un contexto educativo, donde se busca comprender los principios de propagación y validar diseños antes de pasar a una fase experimental o física [17].

Características técnicas de Atoll

Atoll es una herramienta profesional utilizada mundialmente para la planificación, optimización y simulación de redes inalámbricas. Su arquitectura combina modelos matemáticos de propagación con información geográfica digital, lo cual permite obtener resultados altamente precisos para el análisis de cobertura en redes WISP [17].

Entre sus características destacan:

Tabla 13. *Características del simulador Atoll*

Modelado avanzado de propagación	• Compatibilidad con modelos empíricos, semiempíricos y determinísticos • Simulación en bandas desde 400 MHz hasta más de 6 GHz • Análisis de pérdidas por trayectoria, difracción, reflexión y dispersión
Integración con mapas y datos geográficos.	• Importación de modelos digitales de terreno (DEM) • Inclusión de capas cartográficas como edificaciones, alturas, vías y vegetación • Procesamiento de obstáculos naturales y urbanos en el cálculo del enlace
Herramientas de planificación de redes punto a punto y multipunto.	• Cálculo de línea de vista (LOS) y primera zona de Fresnel • Diseño de celdas, estaciones base, enlaces backhaul y redes distribuidas • Reportes automáticos de enlaces, niveles de RF y SNR.
Simulación de interferencia e intermodulación.	• Análisis de canales, superposición y solapamiento espectral • Estimación de interferencia cocanal y adyacente
Salidas gráficas y reportes.	• Mapas temáticos: cobertura, interferencia, potencia, SNR • Reportes exportables en PDF, CSV, DXF y formatos GIS

Comparativa de modelos de propagación: COST231, Okumura-Hata, Longley-Rice e ITU-R P.526

Atoll permite seleccionar diferentes modelos de propagación, cada uno adecuado para un tipo de entorno o frecuencia. En la siguiente Tabla 14 se muestra una comparativa que resume los modelos más utilizados en redes WISP [50]:

Tabla 14. *Modelos de propagación en el simulador Atoll*

Modelo de propagación	Entorno	Frecuencia	Ventajas	Desventajas
COST231	Adecuado para entornos urbanos y suburbanos.	Diseñado para frecuencias entre 1500 y 2000 MHz.	Buen rendimiento en ciudades.	No es ideal para zonas rurales.
Okumura-Hata	Utilizado principalmente en áreas rurales o semiurbanas.	Su rango de frecuencia va desde 150 hasta 1500 MHz.	Tiene simplicidad matemática y fácil implementación.	Menor precisión en entornos urbanos.
Longley-Rice	Permite analizar trayectorias no lineales en terrenos irregulares.	Funciona en bandas desde 20 MHz hasta 20 GHz.	Alta precisión topográfica.	Requiere muchos datos de entorno.
ITU-R P.526	Modelado de propagación por difracción en enlaces punto a punto (LOS/NLOS).	Aplicable a enlaces de microondas y bandas superiores.	Alta precisión en enlaces con obstáculos y perfiles de terreno.	Requiere información detallada del perfil topográfico, complejo de implementar.

Comparativa de herramientas: Atoll vs. Radio Mobile vs. iBwave

En el proceso de planificación y simulación de redes inalámbricas, la elección de la herramienta adecuada resulta determinante para garantizar precisión en los cálculos, confiabilidad en la estimación de la cobertura y utilidad práctica de los resultados obtenidos. Existen múltiples plataformas orientadas al análisis de propagación y diseño de enlaces, pero no todas poseen las mismas capacidades ni están orientadas al mismo tipo de redes.

Entre las soluciones más utilizadas se encuentran Atoll, Radio Mobile e iBwave, cada una con enfoques distintos: Atoll se especializa en planificación profesional outdoor con integración GIS avanzada; Radio Mobile, en enlaces punto a punto rurales mediante modelos empíricos; e iBwave, en diseño indoor orientado a redes WiFi y sistemas DAS. En la siguiente Tabla 15 se observa una comparativa que permite evaluar sus diferentes características y determinar cuál resulta más adecuada para el diseño y simulación de redes WISP.

Tabla 15. *Comparativa técnica entre Atoll, Radio Mobile e iBwave*

Característica	Atoll	Radio Mobile	iBwave
Tipo de análisis	Simulación avanzada, redes PTP y PTMP	Cálculo básico mediante el modelo Longley-Rice para enlaces PTP	Modelado indoor de alta precisión (WiFi, DAS)
Interfaz de usuario	GUI profesional con integración de GIS 3D	Interfaz sencilla y menos intuitiva	Interfaz gráfica detallada orientada a edificios
Modelos de propagación soportados	COST231, Okumura-Hata, Longley-Rice, modelos determinísticos	Longley-Rice (principal), modelos empíricos básicos	Modelos empíricos especializados para ambientes interiores
Capacidad de análisis GIS	Muy alta: mapas 3D, DEM, capas urbanísticas	Limitada a mapas básicos y altimetría	Limitada al diseño de planos internos
Aplicación ideal	Redes WISP, LTE, enlaces outdoor, planificación profesional	Enlaces experimentales rurales, proyectos educativos básicos	Redes indoor corporativas y DAS
Precisión general	Muy alta	Media	Alta (únicamente indoor)
Herramientas adicionales	Análisis de interferencia y optimización SNR, zona de Fresnel	Cálculos simplificados de cobertura PTP	Simulación de plantas arquitectónicas con detalles estructurales
Licenciamiento	Comercial	Gratuito	Comercial (alto costo)

Del análisis realizado se observa que Atoll ofrece el conjunto más completo de funcionalidades para el diseño de redes WISP, integrando modelos avanzados de propagación, análisis GIS profesional y soporte para enlaces punto a punto y punto a multipunto.

Por ello, para los fines de esta investigación académica, Atoll se establece como la herramienta más apropiada para garantizar simulaciones realistas y técnicamente confiables.

Justificación técnica: selección de Atoll para simulación de cobertura

Atoll destaca frente a otras herramientas de simulación por ofrecer un entorno de planificación radioeléctrica diseñado para modelar redes inalámbricas de forma precisa mediante el uso de modelos avanzados de propagación, integración cartográfica y análisis detallado de

variables radioeléctricas. Estas características lo convierten en una herramienta adecuada para evaluar enlaces inalámbricos en escenarios reales, considerando factores como la topografía del terreno, la presencia de obstáculos, la potencia transmitida, las pérdidas por trayectoria y la calidad de la señal recibida [17].

Desde el punto de vista técnico, una de las principales ventajas de Atoll es la posibilidad de trabajar con modelos de propagación reconocidos, tales como COST231, Okumura-Hata, Longley-Rice e ITU-R P.526, los cuales permiten adaptar la simulación a diferentes tipos de entornos rurales, suburbanos o urbanos. Esta flexibilidad resulta especialmente útil en redes WISP, donde las condiciones geográficas influyen directamente en la estabilidad y disponibilidad del servicio [17].

Asimismo, Atoll ofrece herramientas especializadas para el análisis de línea de vista (LOS), zonas de Fresnel, relación señal/ruido (SNR) y niveles de interferencia, parámetros esenciales para determinar la factibilidad técnica de los enlaces inalámbricos. Gracias a estas funcionalidades, es posible prever el comportamiento del enlace antes de la implementación física, reduciendo riesgos técnicos y optimizando el diseño de la red [17].

Otra ventaja relevante es su capacidad de integración con sistemas de información geográfica (GIS), lo que permite utilizar mapas digitales, modelos de elevación y datos cartográficos detallados para representar de manera más realista el entorno donde operará la red [17].

Por lo expuesto, se justifica técnicamente la selección de Atoll como herramienta principal para la simulación de cobertura dentro de esta investigación, al ofrecer mayor precisión en el modelado de propagación, mejores capacidades de análisis técnico y una representación más realista del comportamiento de la red WISP, contribuyendo así al cumplimiento de los objetivos planteados en el proyecto.

2.4. Redes WISP

Las redes WISP (Wireless Internet Service Provider) constituyen una alternativa eficiente para proporcionar conectividad inalámbrica en zonas donde la infraestructura cableada no resulta

viable técnica o económicamente. Estas redes utilizan tecnologías de radiofrecuencia para distribuir servicios de internet mediante distintas arquitecturas de enlace, adaptándose a las condiciones geográficas, la densidad de usuarios y los requerimientos de cobertura [4].

La selección de la arquitectura adecuada dentro de una red WISP influye directamente en factores como la capacidad de transmisión, la escalabilidad, la estabilidad del servicio y los costos de implementación. Por esta razón, es necesario analizar comparativamente las principales técnicas de implementación utilizadas en redes inalámbricas, entre las que destacan los enlaces punto a punto (PTP), punto a multipunto (PTMP) y las redes malladas o topologías híbridas [51].

Cada una de estas técnicas presenta características particulares en términos de cobertura, rendimiento y complejidad operativa, por lo que su elección dependerá del escenario de despliegue y de los objetivos técnicos del proveedor.

2.4.1. Técnicas de implementación de redes WISP

Las técnicas de implementación en redes WISP definen la manera en que se establece la comunicación entre la estación base y los usuarios finales. Estas arquitecturas determinan la distribución del tráfico, la cobertura alcanzada y la eficiencia en la utilización de los recursos inalámbricos [51].

Entre las técnicas más utilizadas se encuentran los enlaces punto a punto, que permiten conectar dos nodos específicos mediante un enlace dedicado; los enlaces punto a multipunto, utilizados para distribuir señal desde un nodo central hacia múltiples clientes; y las redes malladas e híbridas, que combinan múltiples rutas de interconexión para mejorar la redundancia y la cobertura.

Enlaces punto a punto (PTP)

Los enlaces punto a punto (Point to Point, PTP) constituyen una de las arquitecturas más utilizadas en redes WISP para interconectar dos ubicaciones específicas mediante un enlace inalámbrico dedicado. Este tipo de enlace establece una comunicación directa entre dos nodos, generalmente entre una estación principal y un nodo remoto, permitiendo transportar tráfico de datos con alta capacidad y estabilidad [51].

En este modelo, se emplean antenas direccionales orientadas entre sí, garantizando la concentración de la señal en una única trayectoria de transmisión. Esta configuración mejora la potencia efectiva radiada, reduce la interferencia y permite alcanzar distancias considerables manteniendo niveles aceptables de rendimiento.

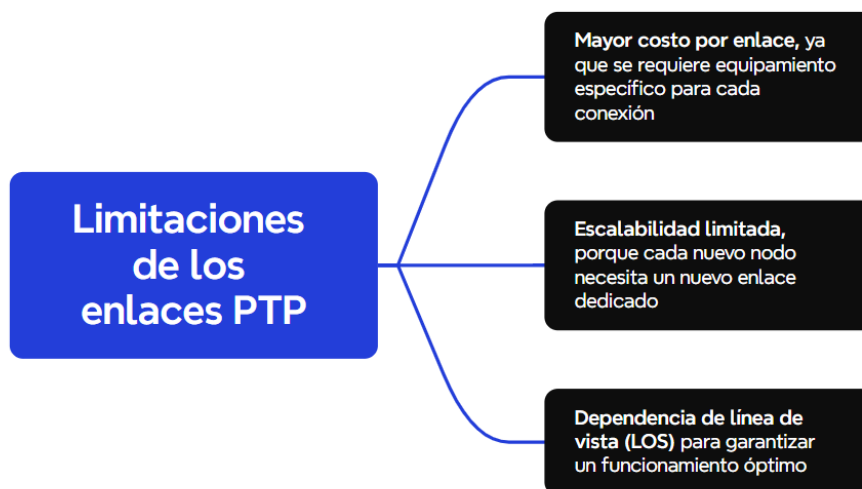
Las principales ventajas de los enlaces PTP se muestran en la siguiente Figura 18:

Figura 18. *Ventajas de los enlaces PTP*



Sin embargo, también presentan ciertas limitaciones, como se muestra en la siguiente Figura 19:

Figura 19. *Limitaciones de los enlaces PTP*



Los enlaces PTP son especialmente útiles como enlaces troncales o backhaul dentro de una red WISP, permitiendo transportar conectividad desde el nodo principal hacia torres secundarias o zonas de distribución.

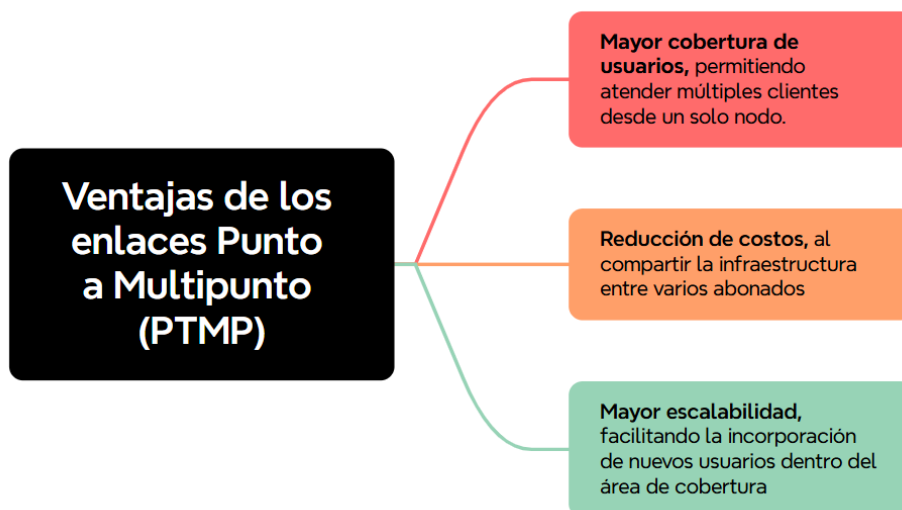
Enlaces punto a multipunto (PTMP)

Los enlaces punto a multipunto (Point to Multipoint, PTMP) son ampliamente utilizados en redes WISP para distribuir conectividad desde una estación base central hacia múltiples usuarios finales. En esta arquitectura, un nodo transmisor principal emite una señal a varios receptores dentro de su área de cobertura, permitiendo compartir recursos inalámbricos entre varios clientes [51].

Esta técnica resulta adecuada para la distribución de internet en sectores residenciales, rurales o suburbanos, donde múltiples usuarios pueden conectarse a una misma estación base mediante antenas sectoriales o equipos de acceso inalámbrico [51].

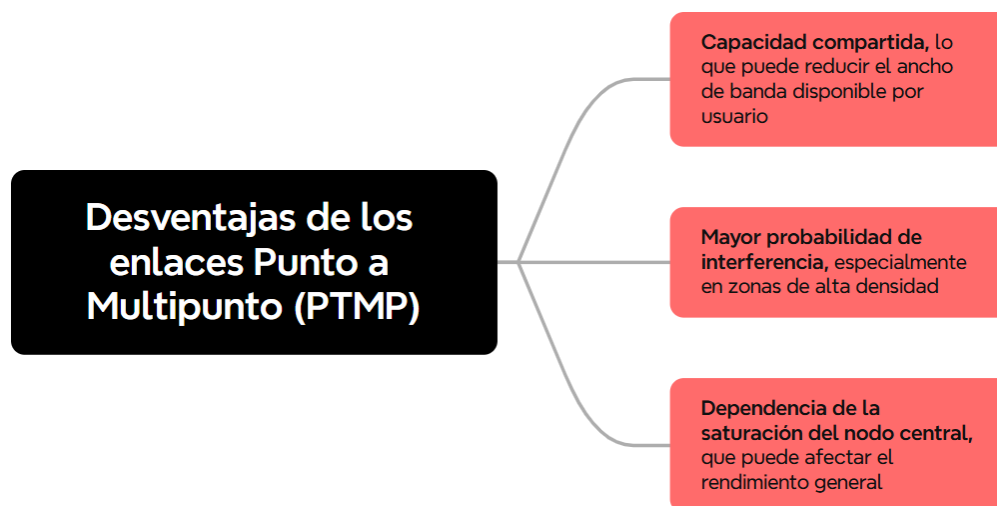
Las ventajas principales de esta arquitectura se muestran en la siguiente Figura 20:

Figura 20. *Ventajas de los enlaces punto a multipunto (PTMP)*



No obstante, presenta ciertas desventajas, como se muestra en la siguiente Figura 21:

Figura 21. *Desventajas de los enlaces punto a multipunto (PTMP)*



Los enlaces PTMP representan la base operativa de la mayoría de las redes WISP comerciales, ya que permiten una distribución eficiente de la conectividad a múltiples clientes utilizando infraestructura centralizada [51].

Redes malladas y topologías híbridas

Las redes malladas (Mesh) y las topologías híbridas representan arquitecturas más avanzadas dentro de las redes WISP, orientadas a mejorar la redundancia, la disponibilidad del servicio y la flexibilidad de expansión.

En una red mallada, cada nodo puede conectarse con varios nodos vecinos, permitiendo múltiples rutas de comunicación para el tráfico de datos. Esto significa que, si un enlace falla, la red puede redirigir automáticamente la información por otra ruta disponible, aumentando la resiliencia del sistema.

Entre sus ventajas se destacan las que se muestran en la siguiente Figura 22:

Figura 22. *Ventajas de las redes malladas*



Sin embargo, presentan desafíos importantes, como se muestra en la siguiente Figura 23:

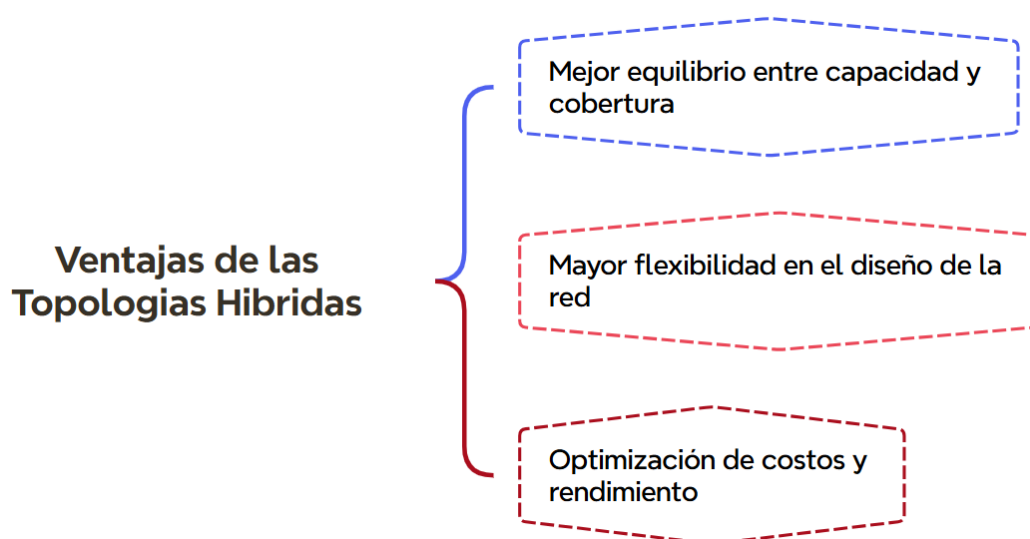
Figura 23. *Desventajas de las redes malladas*



Por otro lado, las topologías híbridas combinan enlaces PTP y PTMP con elementos mallados, permitiendo aprovechar las ventajas de cada arquitectura. Por ejemplo, un proveedor WISP puede utilizar enlaces PTP para conectar torres principales y enlaces PTMP para distribuir señal a usuarios finales.

Las principales ventajas de esta combinación se presentan en la siguiente Figura 24:

Figura 24. *Ventajas de las topologías híbridas*



Debido a estas ventajas, las topologías híbridas son frecuentemente utilizadas en redes WISP modernas, especialmente en despliegues donde se requiere escalabilidad y alta disponibilidad.

2.4.2. Tipos de redes WISP y su arquitectura

Las redes WISP (Wireless Internet Service Provider) pueden diseñarse e implementarse de diferentes maneras según las condiciones geográficas, la densidad poblacional, la demanda de usuarios y los recursos técnicos disponibles. Su arquitectura varía en función del entorno donde serán desplegadas, dando lugar principalmente a redes rurales y urbanas, cada una con características técnicas y operativas específicas [4].

La arquitectura de una red WISP generalmente está compuesta por un nodo principal de distribución, enlaces de transporte o backhaul y estaciones de acceso para usuarios finales. Dependiendo del escenario, estos componentes pueden variar en cantidad, capacidad y topología, con el objetivo de garantizar cobertura eficiente, estabilidad del servicio y aprovechamiento adecuado del espectro radioeléctrico [17].

El análisis de los distintos tipos de redes WISP y su comparación con otras tecnologías de acceso, como FTTH, LTE y redes satelitales, permiten identificar sus ventajas competitivas y sus limitaciones, justificando su aplicación en escenarios donde las soluciones cableadas no resultan viables.

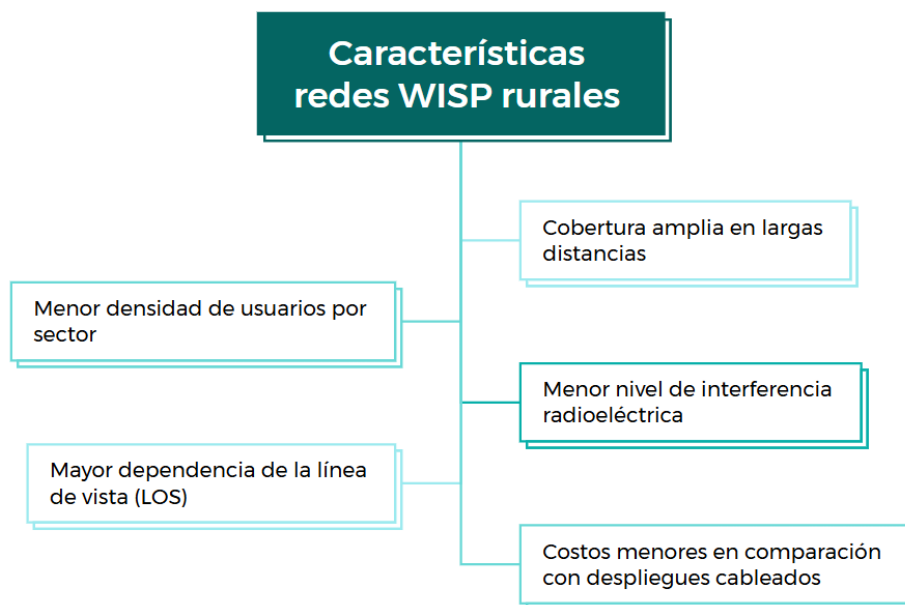
Redes WISP rurales vs urbanas

Las redes WISP presentan diferencias significativas cuando se implementan en zonas rurales o en zonas urbanas, debido a factores como la densidad de usuarios, la distancia entre nodos, la topografía y el nivel de interferencia radioeléctrica.

En las redes WISP rurales, el principal objetivo es cubrir grandes distancias con baja densidad de usuarios, conectando comunidades alejadas donde no existe infraestructura de fibra óptica o redes cableadas. En este entorno se utilizan frecuentemente enlaces punto a punto (PTP) para transportar la conectividad entre torres y enlaces punto a multipunto (PTMP) para distribuir el servicio a los usuarios finales [17].

Las principales características de las redes WISP rurales se muestran en la siguiente Figura 25:

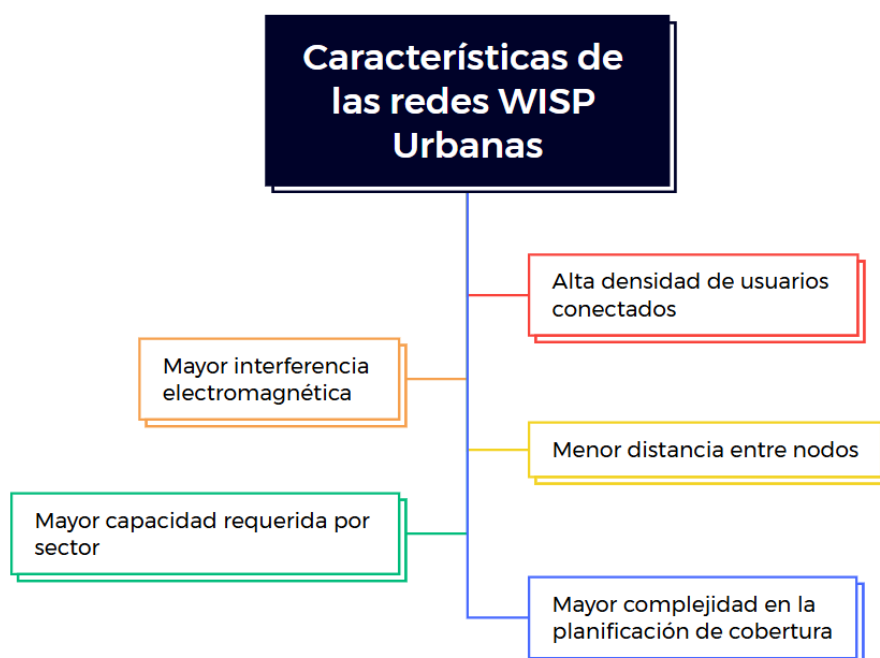
Figura 25. Características de redes WISP en zonas rurales



Estas redes resultan altamente viables en áreas donde el acceso por medios tradicionales no es económicamente rentable.

Por otro lado, las redes WISP urbanas están diseñadas para atender una mayor concentración de usuarios dentro de áreas geográficas más reducidas. En estos entornos existe mayor presencia de edificaciones, obstáculos y saturación del espectro, lo que obliga a emplear diseños más densos y una planificación radioeléctrica más precisa [1].

Las principales características de las redes WISP urbanas se muestran en la siguiente Figura 26:

Figura 26. Características de redes WISP en zonas urbanas

En zonas urbanas se requieren estrategias avanzadas de sectorización, control de interferencias y reutilización de frecuencias para garantizar niveles adecuados de calidad de servicio.

A continuación, se presenta en la Tabla 16 una comparación entre ambos escenarios:

Tabla 16. Comparativa entre redes WISP rurales y urbanas

Característica	WISP Rural	WISP Urbano
Cobertura	Amplia	Reducida por sector
Densidad de usuarios	Baja	Alta
Interferencia	Baja	Alta
Distancia entre nodos	Mayor	Menor
Complejidad de diseño	Media	Alta
Costo por usuario	Moderado	Variable

Esta comparación evidencia que las redes WISP rurales son ideales para ampliar cobertura en zonas alejadas, mientras que las urbanas requieren mayor optimización técnica para garantizar capacidad y estabilidad.

Comparativa con redes FTTH, LTE y satelitales

Las redes WISP representan una alternativa tecnológica importante frente a otras soluciones de acceso como FTTH (Fiber To The Home), LTE y redes satelitales, especialmente en zonas donde el despliegue de infraestructura convencional presenta limitaciones técnicas o económicas.

Cada tecnología posee ventajas específicas en términos de velocidad, cobertura, latencia, costos de implementación y facilidad de despliegue; por ello, es necesario realizar una comparación que permita identificar en qué escenarios las redes WISP resultan más convenientes [4].

Las redes FTTH ofrecen altas velocidades y baja latencia gracias al uso de fibra óptica hasta el usuario final; sin embargo, requieren una inversión elevada en infraestructura física, canalización y mantenimiento, lo que dificulta su implementación en zonas rurales o de baja densidad poblacional [4].

Las redes LTE proporcionan cobertura inalámbrica móvil y buena capacidad de transmisión, pero dependen de licencias de espectro, infraestructura celular especializada y mayores costos operativos [4].

Las redes satelitales permiten cobertura en zonas remotas donde no existen otras alternativas, pero presentan alta latencia y costos elevados tanto en equipos como en servicio.

Frente a estas tecnologías, las redes WISP destacan por ofrecer un equilibrio entre costo, cobertura y facilidad de implementación, especialmente en zonas rurales o de difícil acceso.

A continuación, se presenta en la Tabla 17 una comparación técnica:

Tabla 17. *Comparativa entre redes WISP, FTTH, LTE y satelitales*

Tecnología	Velocidad	Latencia	Costo de implementación	Cobertura	Escenario ideal
WISP	Media - Alta	Baja - Media	Medio	Alta	Zonas rurales y suburbanas
FTTH	Muy Alta	Muy Baja	Alto	Media	Zonas urbanas
LTE	Alta	Media	Alto	Alta	Cobertura móvil
Satelital	Media	Alta	Alto	Muy Alta	Zonas remotas

De esta comparación se concluye que las redes WISP constituyen una solución técnicamente viable y económicamente accesible para brindar conectividad en áreas donde tecnologías como FTTH o LTE no pueden desplegarse fácilmente. Su flexibilidad, rapidez de implementación y menor costo de infraestructura las convierten en una alternativa adecuada para proyectos orientados a ampliar cobertura y reducir la brecha digital.

2.4.3. Calidad de servicio en redes WISP

La calidad de servicio (QoS, Quality of Service) en redes WISP es un conjunto de mecanismos y parámetros técnicos destinados a garantizar un nivel adecuado de rendimiento en la transmisión de datos, asegurando estabilidad, eficiencia y una experiencia satisfactoria para el usuario final. En este tipo de redes, donde la comunicación se realiza mediante enlaces inalámbricos, la QoS adquiere una relevancia fundamental debido a la influencia de factores como interferencias electromagnéticas, obstáculos físicos, saturación del canal y variaciones en la intensidad de señal [51].

A diferencia de las redes cableadas, las redes WISP están expuestas a condiciones ambientales y radioeléctricas que pueden afectar significativamente el desempeño del servicio, generando retrasos, pérdidas de paquetes o degradación en aplicaciones sensibles como voz sobre IP, videoconferencias y servicios en tiempo real. Por esta razón, la evaluación de parámetros como la relación señal/ruido (SNR), la latencia y el jitter resulta indispensable para medir la eficiencia de la red y determinar su nivel de calidad [7].

Además, la implementación de buenas prácticas de diseño y planificación permite optimizar estos parámetros, mejorar la disponibilidad del servicio y garantizar el cumplimiento de los requerimientos operativos en escenarios reales de implementación de redes WISP.

Parámetros técnicos: SNR, latencia, jitter

La evaluación del rendimiento en redes WISP se fundamenta en la medición de parámetros técnicos que permiten analizar la calidad de los enlaces inalámbricos y determinar si la red cumple con los niveles esperados de desempeño. Entre los indicadores más importantes se encuentran la relación señal/ruido (SNR), la latencia y el jitter, ya que estos reflejan la estabilidad y confiabilidad de la transmisión.

1. Relación señal/ruido (SNR)

La relación señal/ruido (Signal-to-Noise Ratio, SNR) representa la diferencia entre la potencia de la señal recibida y el nivel de ruido presente en el canal de comunicación; se expresa en decibelios (dB) y constituye un indicador esencial de la calidad del enlace inalámbrico [8].

Un valor alto de SNR indica que la señal recibida es significativamente mayor que el ruido, lo cual mejora la estabilidad del enlace y reduce la probabilidad de errores en la transmisión; por el contrario, un valor bajo de SNR incrementa la posibilidad de pérdidas de paquetes, retransmisiones y reducción en la capacidad efectiva del enlace [8].

En redes WISP, mantener un nivel adecuado de SNR es fundamental para garantizar un rendimiento estable, especialmente en enlaces de larga distancia o en entornos con alta interferencia.

2. Latencia

La latencia es el tiempo que tarda un paquete de datos en viajar desde el origen hasta el destino dentro de la red; generalmente se mide en milisegundos (ms) y constituye un indicador clave en aplicaciones sensibles al retardo [4].

En redes WISP, la latencia puede verse afectada por diversos factores como la distancia entre nodos, la congestión del enlace, el procesamiento de los dispositivos y las retransmisiones causadas por errores de transmisión [5].

Valores bajos de latencia garantizan mejor desempeño en servicios interactivos como videollamadas, voz sobre IP y plataformas en tiempo real, mientras que una latencia elevada puede generar retardos perceptibles y degradación en la experiencia del usuario.

3. Jitter

El jitter es la variación en el tiempo de llegada de los paquetes dentro de la red; aunque dos paquetes se transmitan consecutivamente, pueden llegar en tiempos distintos debido a fluctuaciones en el canal o congestión.

Este parámetro es particularmente importante en aplicaciones en tiempo real, ya que una variación excesiva provoca interrupciones, pérdida de sincronización y degradación de calidad en servicios de voz o video [34].

En redes WISP, un nivel reducido de jitter es señal de estabilidad en la transmisión, mientras que valores elevados indican inestabilidad o saturación en la red.

A continuación, se presenta en la Tabla 18 un resumen comparativo de estos parámetros:

Tabla 18. *Parámetros técnicos de calidad de servicio en redes WISP*

Parámetro	Función principal	Unidad	Impacto en la red
SNR	Mide la calidad de la señal frente al ruido	dB	A mayor SNR, mejor calidad del enlace
Latencia	Mide el retardo en la transmisión	ms	A menor latencia, mejor respuesta
Jitter	Mide la variación en la llegada de paquetes	ms	A menor jitter, mayor estabilidad

Estos indicadores serán fundamentales en la fase experimental del proyecto, ya que permitirán evaluar el comportamiento de la red simulada y validar la eficiencia de los parámetros configurados.

Mejores prácticas y consideraciones de diseño

La calidad de servicio en una red WISP no depende únicamente del equipamiento utilizado, sino también de la correcta aplicación de criterios técnicos durante la planificación, configuración y operación de la red; la implementación de buenas prácticas de diseño permite optimizar los recursos disponibles, reducir interferencias y garantizar niveles adecuados de rendimiento [2].

Una de las prácticas fundamentales consiste en realizar una adecuada planificación de cobertura, considerando la topografía del terreno, la altura de las antenas y la línea de vista entre

los nodos. La presencia de obstáculos o una mala alineación puede afectar la señal recibida y reducir significativamente la calidad del enlace.

Asimismo, la correcta selección de frecuencias y canales permite minimizar interferencias y mejorar la eficiencia espectral. En zonas con alta densidad de enlaces, la reutilización adecuada de frecuencias es esencial para evitar la degradación del servicio [2].

Otra consideración importante es el uso de equipos con capacidad suficiente, capaces de soportar la cantidad de usuarios y el tráfico esperado sin generar congestión. La saturación de la capacidad disponible incrementa la latencia, el jitter y la pérdida de paquetes [2].

También resulta recomendable implementar mecanismos de priorización de tráfico (QoS) para garantizar que aplicaciones críticas como voz y video tengan prioridad sobre otros tipos de tráfico menos sensibles al retardo.

Entre las mejores prácticas más relevantes destacan:

- Mantener niveles adecuados de SNR, garantizando enlaces estables.
- Optimizar la alineación y altura de antenas, reduciendo pérdidas por obstrucción.
- Controlar la saturación del canal, distribuyendo adecuadamente los usuarios.
- Aplicar políticas de QoS, priorizando tráfico crítico.
- Monitorear continuamente parámetros de red para detectar degradaciones.
- Reducir interferencias mediante planificación de frecuencias.

La aplicación de estas prácticas mejora el rendimiento general de la red WISP, incrementa la disponibilidad del servicio y reduce fallas operativas. En el contexto del presente proyecto, estas consideraciones serán tomadas en cuenta durante la simulación en GNS3 y Atoll, permitiendo evaluar escenarios optimizados y validar parámetros de diseño orientados a maximizar la calidad de servicio.

2.4.4. Características técnicas en redes WISP

Con el propósito de sintetizar las características técnicas de las principales arquitecturas utilizadas en redes WISP, se presenta a continuación una comparación entre los enlaces punto a punto (PTP), punto a multipunto (PTMP) y las redes malladas o híbridas, considerando criterios como capacidad, cobertura, escalabilidad, complejidad y aplicaciones recomendadas.

Esta comparación permite identificar las ventajas y limitaciones de cada técnica de implementación, facilitando la selección de la arquitectura más adecuada según los requerimientos de cobertura, número de usuarios y nivel de complejidad de la red [1].

A continuación, se presenta en la Tabla 19 un resumen comparativo de características técnicas en arquitecturas de redes WISP.

Tabla 19. *Comparativa de características técnicas en arquitecturas de redes WISP*

Característica	PTP	PTMP	Mallada / Híbrida
Tipo de conexión	Enlace dedicado entre dos nodos	Un nodo central hacia varios usuarios	Múltiples rutas entre nodos
Cobertura	Media a larga distancia	Cobertura sectorizada	Variable y expandible
Capacidad por enlace	Alta	Compartida entre usuarios	Variable según topología
Escalabilidad	Baja	Alta	Alta
Complejidad de implementación	Baja	Media	Alta
Tolerancia a fallos	Baja	Media	Alta
Costo de implementación	Medio	Bajo a medio	Alto
Uso recomendado	Backhaul y enlaces troncales	Distribución a clientes finales	Redes avanzadas con redundancia
Dependencia de línea de vista	Alta	Media	Variable
Facilidad de administración	Alta	Media	Baja

Del análisis comparativo se observa que los enlaces PTP ofrecen alta capacidad y estabilidad para conexiones dedicadas, siendo apropiados para enlaces troncales entre nodos principales. Por su parte, la arquitectura PTMP permite una distribución eficiente del servicio hacia

múltiples usuarios, optimizando costos y escalabilidad, lo que la convierte en la opción más utilizada en redes WISP comerciales.

En contraste, las redes malladas o híbridas proporcionan mayor redundancia y flexibilidad operativa, aunque requieren una configuración más compleja y mayores recursos de administración. Estas arquitecturas son recomendables en escenarios donde la disponibilidad y la expansión de la red constituyen prioridades estratégicas [7].

En consecuencia, la elección de la arquitectura dependerá del entorno de implementación, del número de usuarios y de los objetivos técnicos del proveedor, siendo común la combinación de enlaces PTP y PTMP para lograr un equilibrio entre capacidad, cobertura y eficiencia operativa.

2.4.5. Justificación de las redes WISP en entornos académicos

La implementación y el análisis de redes WISP en entornos académicos representan una estrategia técnica y pedagógica de gran valor para la formación de estudiantes en el área de telecomunicaciones. Estas redes permiten reproducir escenarios reales de conectividad inalámbrica, facilitando la comprensión práctica de conceptos relacionados con planificación de cobertura, diseño de enlaces, evaluación de rendimiento y gestión de calidad de servicio [1].

Desde una perspectiva técnica, las redes WISP integran múltiples elementos esenciales en la formación profesional, tales como:

- Diseño de topologías inalámbricas
- Configuración de enlaces punto a punto y punto a multipunto
- Análisis de cobertura y propagación
- Monitoreo de parámetros técnicos como SNR, BER, latencia y jitter
- Evaluación de calidad de servicio (QoS)
- Optimización de recursos inalámbricos

Estos elementos convierten a las redes WISP en un modelo adecuado para prácticas de simulación orientadas al aprendizaje aplicado, permitiendo a los estudiantes desarrollar competencias técnicas mediante escenarios similares a los utilizados en despliegues reales.

Además, la simulación de redes WISP mediante herramientas especializadas como GNS3 y Atoll permite crear entornos controlados donde es posible analizar el comportamiento de la red sin necesidad de disponer de infraestructura física costosa. Esto representa una ventaja significativa en instituciones académicas, ya que reduce costos de implementación y amplía las oportunidades de experimentación técnica [1].

La utilización de estas tecnologías en laboratorios académicos facilita la comprensión integral de procesos como la planificación radioeléctrica, la administración de tráfico, la evaluación de cobertura y la identificación de fallos en enlaces inalámbricos, fortaleciendo la capacidad analítica y práctica del estudiante.

Desde el punto de vista pedagógico, la aplicación de redes WISP en entornos simulados contribuye a:

- Vincular teoría y práctica en el aprendizaje
- Fortalecer habilidades técnicas en diseño y análisis de redes
- Mejorar la capacidad de resolución de problemas
- Preparar al estudiante para escenarios reales del ámbito laboral
- Promover el uso de herramientas profesionales de simulación

En el contexto del presente proyecto, la aplicación de redes WISP en un entorno académico permite desarrollar un laboratorio virtual orientado a la validación de parámetros técnicos, proporcionando una plataforma práctica para el análisis de rendimiento y la optimización de configuraciones inalámbricas [1].

Por lo tanto, se justifica técnicamente el uso de redes WISP en entornos académicos debido a que estas constituyen una herramienta integral para fortalecer la formación profesional en telecomunicaciones, permitiendo simular escenarios reales, evaluar parámetros críticos de

desempeño y desarrollar competencias aplicables al diseño e implementación de soluciones inalámbricas en el ámbito laboral.

2.5. Equipos de red simulados

La selección de los equipos de red utilizados en una simulación es un aspecto fundamental para garantizar que los escenarios desarrollados representen de manera adecuada las condiciones operativas de una implementación real. En entornos de simulación WISP, la elección de routers y switches virtualizados debe considerar factores como capacidad de enrutamiento, soporte de protocolos, escalabilidad, facilidad de integración y compatibilidad con herramientas de laboratorio como GNS3.

En el presente proyecto se emplearon dispositivos virtuales MikroTik CHR y MikroTik CRS328, seleccionados por su flexibilidad, capacidad de configuración avanzada y compatibilidad con escenarios de redes inalámbricas. Estos equipos permiten simular funciones esenciales de una red WISP, como enrutamiento, segmentación mediante VLAN, distribución de tráfico y administración centralizada [52].

La comparación técnica de estos equipos frente a otras alternativas disponibles en GNS3 permite justificar la elección de la plataforma utilizada en la simulación.

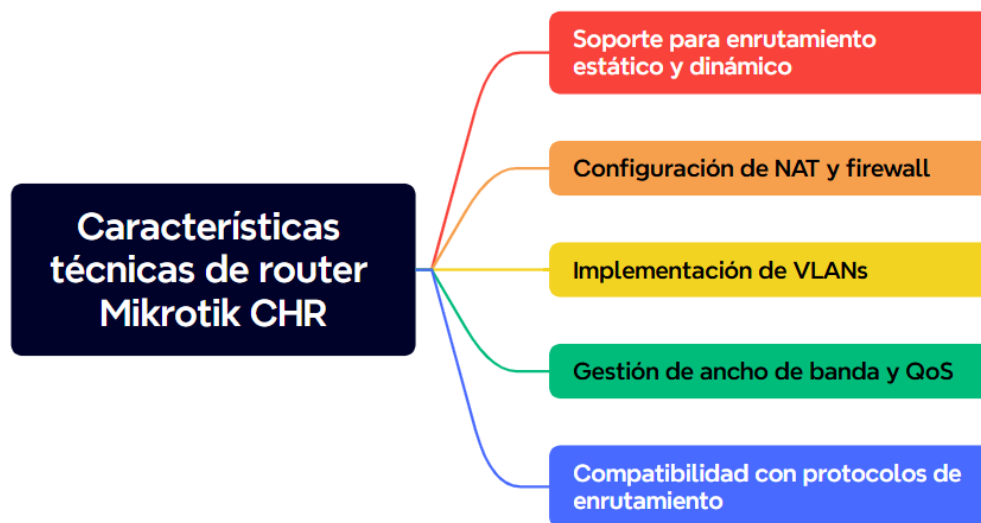
2.5.1. Equipos MikroTik

Para el desarrollo de la simulación se utilizaron principalmente los dispositivos virtuales MikroTik CHR (Cloud Hosted Router) y MikroTik CRS328-24P-4S+, ambos integrados en la plataforma GNS3 como appliances compatibles para virtualización de redes [53].

El MikroTik CHR es una versión virtualizada del sistema operativo RouterOS, diseñada para ejecutarse en entornos virtuales. Este dispositivo ofrece las mismas funcionalidades que un router físico MikroTik, permitiendo configurar enrutamiento dinámico, NAT, firewall, administración de VLAN, control de tráfico y monitoreo de interfaces [52].

En la Figura 27 se observan sus principales características técnicas destacadas:

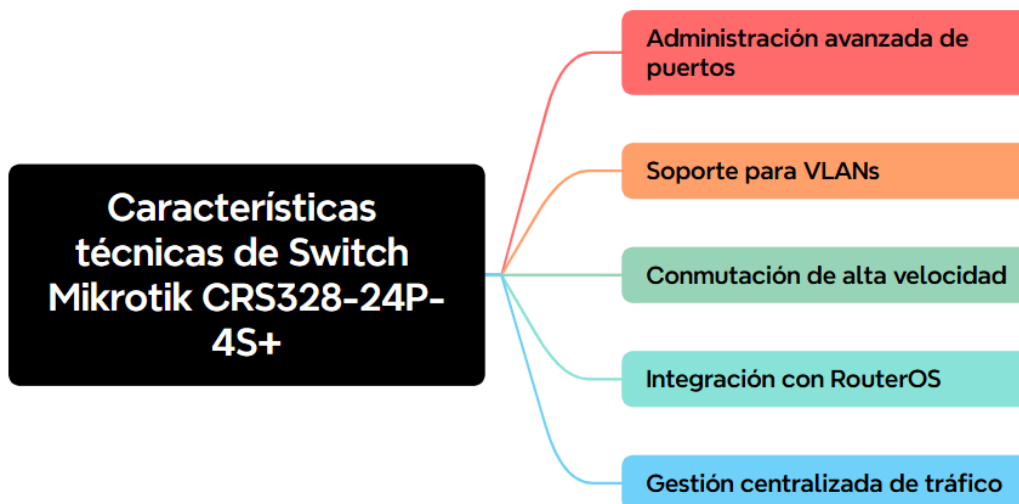
Figura 27. Características técnicas destacadas del router MikroTik



Por otra parte, el MikroTik CRS328-24P-4S+ es un switch administrable que permite realizar funciones avanzadas de conmutación y segmentación de red. En la simulación, este equipo cumple el papel de concentrador principal para la distribución de tráfico entre las diferentes VLAN definidas en la topología [52].

En la siguiente Figura 28 se pueden observar sus principales características:

Figura 28. Características técnicas destacadas del switch MikroTik CRS328-24P-4S+



La combinación de ambos equipos permitió simular una infraestructura funcional compuesta por un núcleo de distribución, segmentación lógica de red y conectividad entre nodos, reproduciendo un entorno cercano al funcionamiento real de una red WISP.

2.5.2. MikroTik vs otros equipos WISP

Dentro de la plataforma GNS3 existen múltiples appliances disponibles para la simulación de routers y switches, incluyendo soluciones de fabricantes como Cisco, Juniper, Huawei, OpenWrt y MikroTik. Cada una de estas opciones presenta características técnicas específicas orientadas a diferentes escenarios de red [52].

Con el fin de identificar la plataforma más adecuada para la simulación de la red WISP propuesta, se presenta en la Tabla 20 una comparación entre MikroTik, Cisco IOSv y OpenWrt, considerando criterios técnicos relevantes para el entorno del proyecto.

Tabla 20. *Comparativa técnica entre MikroTik y otros equipos virtuales en GNS3*

Característica	MikroTik	Cisco IOSv	OpenWrt
Sistema operativo	RouterOS	Cisco IOS	Linux OpenWrt
Facilidad de configuración	Alta	Media	Media
Soporte de VLAN	Sí	Sí	Sí
Firewall y NAT	Avanzado	Avanzado	Avanzado
QoS / Control de ancho de banda	Sí	Sí	Limitado
Curva de aprendizaje	Media	Alta	Media
Compatibilidad con entornos WISP	Alta	Media	Alta
Consumo de recursos en GNS3	Moderado	Alto	Bajo
Licenciamiento en laboratorio	Flexible	Restringido	Libre
Orientación práctica en WISP	Alta	Media	Media

Del análisis comparativo se observa que MikroTik CHR presenta ventajas importantes frente a otras alternativas, principalmente por su equilibrio entre facilidad de configuración, capacidades avanzadas de administración y compatibilidad con escenarios WISP [52].

Aunque Cisco IOSv ofrece funcionalidades empresariales robustas, requiere mayor consumo de recursos y presenta una curva de aprendizaje más elevada. Por su parte, OpenWrt es flexible y de bajo consumo, pero no proporciona el mismo nivel de herramientas integradas orientadas a la administración profesional de redes WISP [52].

Por ello, MikroTik se posiciona como una opción más adecuada para la simulación desarrollada en esta investigación.

2.5.3. Justificación técnica de la selección de equipos simulados

La selección de MikroTik CHR y MikroTik CRS328 como equipos principales para la simulación se fundamenta en criterios técnicos, operativos y académicos que los convierten en herramientas apropiadas para representar una red WISP funcional dentro de un entorno virtual.

Desde el punto de vista técnico, MikroTik CHR ofrece funcionalidades avanzadas de enrutamiento, segmentación de tráfico, administración de políticas y control de calidad de servicio, características indispensables para reproducir escenarios de distribución inalámbrica. Estas capacidades permiten implementar configuraciones similares a las utilizadas en redes WISP reales, lo que facilita la simulación de enlaces, VLAN, rutas y políticas de administración [52].

Además, el uso del switch MikroTik CRS328 permite representar la capa de distribución de la red, integrando funciones de conmutación y segmentación lógica que mejoran la organización del tráfico dentro de la topología simulada.

Otro aspecto relevante es la compatibilidad con GNS3, ya que ambos dispositivos se integran adecuadamente en el entorno de simulación, mantienen estabilidad operativa y permiten la interacción con otros elementos virtuales como estaciones de trabajo, servidores y nodos de usuario [52].

Desde el enfoque académico, la elección de equipos MikroTik proporciona una plataforma adecuada para el aprendizaje práctico, ya que su interfaz y sus herramientas permiten a los estudiantes desarrollar competencias en:

- Configuración de redes segmentadas
- Administración de rutas
- Control de tráfico
- Implementación de políticas de seguridad
- Simulación de entornos WISP reales

Asimismo, MikroTik es ampliamente utilizado en implementaciones reales de redes inalámbricas de mediana escala, lo cual incrementa la relevancia práctica del laboratorio propuesto y fortalece la preparación técnica de los estudiantes para entornos profesionales [52].

Por estas razones, se justifica técnicamente la selección de MikroTik CHR y MikroTik CRS328 como los equipos simulados principales del proyecto. Ambos proporcionan la funcionalidad necesaria para representar de manera precisa la arquitectura WISP propuesta y facilitan la evaluación de parámetros técnicos dentro del entorno de simulación.

Capítulo 3: Diseño y desarrollo de la red WISP

3.1. Introducción del capítulo

El diseño e implementación de una red WISP (Wireless Internet Service Provider) requiere una planificación minuciosa y un análisis previo que permita anticipar el comportamiento de la red en diferentes escenarios técnicos y geográficos. Antes de ejecutar cualquier despliegue físico, es indispensable estudiar cómo interactúan los componentes, cómo se distribuye el tráfico y cómo se comportan los enlaces inalámbricos frente a variaciones topológicas o de propagación. Este proceso reduce fallas, optimiza recursos y garantiza una calidad de servicio estable para los usuarios finales, especialmente en entornos donde la conectividad inalámbrica constituye la principal alternativa tecnológica [4].

En este capítulo se desarrolla el diseño completo del prototipo de red WISP propuesto, integrando tanto la estructura lógica y física del sistema. Para ello, se emplean herramientas de simulación y análisis que permiten modelar el funcionamiento real de la red, evaluar la factibilidad de los enlaces y validar los parámetros de configuración antes de su implementación práctica. Esta etapa resulta fundamental en proyectos académicos y de formación técnica, ya que brinda un entorno controlado donde el estudiante puede comprender, experimentar y corregir aspectos esenciales del diseño sin incurrir en los costos y riesgos de un despliegue real [4].

El desarrollo inicia con la definición de la metodología empleada y los criterios de selección de equipos, considerando dispositivos de fabricantes utilizados ampliamente en entornos

WISP, tales como MikroTik, Ubiquiti y Cisco. Estos equipos pueden ser representados o emulados dentro de GNS3 mediante imágenes de RouterOS, IOS o dispositivos equivalentes, lo que permite modelar de forma cercana el funcionamiento de una red inalámbrica profesional.

Asimismo, se presentan las simulaciones realizadas en GNS3 y Atoll. GNS3 permite emular el comportamiento de routers y equipos de red con características reales, facilitando la validación de la arquitectura, el análisis del tráfico, las políticas de enrutamiento y la administración del sistema. Por su parte, Atoll ofrece un análisis profesional de propagación para los enlaces inalámbricos, permitiendo evaluar distancias, pérdidas por trayectoria, línea de vista, márgenes de enlace y cobertura en escenarios punto a punto o punto multipunto. El uso combinado de estas herramientas proporciona una visión integral del diseño, integrando la lógica de red con la viabilidad de los enlaces inalámbricos [1].

3.2. Metodología de desarrollo del prototipo

El desarrollo del prototipo de red WISP se basa íntegramente en entornos de simulación, razón por la cual la metodología adoptada se orienta a reproducir de la manera más fiel posible las condiciones técnicas presentes en un despliegue real. Este enfoque permite evaluar el comportamiento de la red sin necesidad de contar con infraestructura física, facilitando la experimentación, el análisis y la corrección de parámetros de diseño antes de aplicar las configuraciones en un entorno práctico [51].

La metodología utilizada sigue un proceso secuencial y estructurado, que integra fases de análisis, modelado, simulación y validación. En primer lugar, se realiza la identificación de los requerimientos técnicos del proyecto, considerando aspectos como la topología propuesta, el tipo de enlaces inalámbricos necesarios, la capacidad de transporte, las necesidades de seguridad y la gestión del tráfico. Con base en estos requerimientos, se seleccionan las herramientas de simulación que permiten reproducir dichos elementos con mayor precisión [51].

En este estudio se emplean dos plataformas principales: GNS3, encargada de la emulación de los equipos de red, el enrutamiento, la administración y el análisis del tráfico; y Atoll, utilizado para la simulación de propagación en enlaces inalámbricos. La combinación de ambas tecnologías permite abordar tanto el diseño lógico de la red como la viabilidad radioeléctrica de los enlaces de

transporte. Para ello, se importan imágenes compatibles con GNS3 que representan equipos de fabricantes utilizados en entornos WISP, y se configuran enlaces inalámbricos en Atoll empleando modelos de terreno y parámetros de propagación adecuados [27].

Una vez definidos los elementos técnicos, se construye la topología en GNS3 y se procede a configurar los dispositivos simulados, estableciendo rutas, políticas de seguridad, esquemas de direccionamiento y mecanismos de administración. Paralelamente, en Atoll se modelan los enlaces punto a punto y punto multipunto para evaluar la cobertura, la visibilidad entre nodos, la pérdida por trayectoria y los márgenes de enlace. Los resultados obtenidos en ambas plataformas se integran para verificar la coherencia del diseño y asegurar que los parámetros establecidos permitan un funcionamiento estable de la red [17].

Finalmente, la metodología incluye un proceso de validación mediante pruebas dentro de los entornos de simulación. Estas pruebas comprenden la verificación de conectividad, el análisis de rendimiento, la evaluación del comportamiento del tráfico y la revisión de las políticas de seguridad implementadas. La finalidad de esta etapa es detectar inconsistencias, ajustar configuraciones y asegurar que el prototipo responda adecuadamente a las condiciones definidas en el diseño.

3.2.1. Herramientas utilizadas en el desarrollo

Para el desarrollo del prototipo de red WISP se emplearon diversas herramientas de simulación, análisis geográfico y modelado radioeléctrico, seleccionadas de acuerdo con las necesidades técnicas del proyecto. Estas herramientas permitieron reproducir el comportamiento de una red inalámbrica real, modelar el entorno geográfico, analizar la propagación de la señal y configurar dispositivos de red dentro de un entorno completamente simulado. A continuación, se describen las principales plataformas y recursos utilizados durante el desarrollo del presente trabajo de investigación.

GNS3

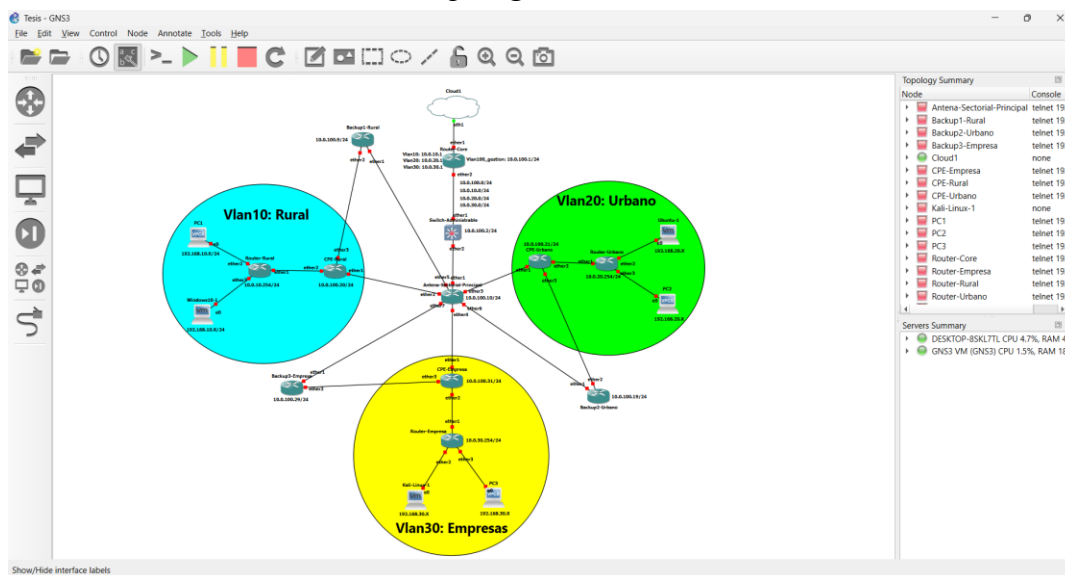
GNS3 (Graphical Network Simulator-3) es una plataforma de simulación y emulación de redes utilizada para reproducir entornos de telecomunicaciones de manera virtual. Esta herramienta permite integrar imágenes de sistemas operativos de red reales, facilitando la

configuración de routers, switches, firewalls y otros dispositivos utilizados en escenarios empresariales y proveedores de servicios de internet [27].

En el presente trabajo, GNS3 fue empleado como plataforma principal para la construcción de la topología lógica de la red WISP propuesta. Mediante esta herramienta se implementaron los dispositivos simulados, incluyendo routers basados en MikroTik RouterOS y equipos equivalentes a la infraestructura utilizada en entornos WISP reales. Asimismo, permitió configurar el direccionamiento IP, el enrutamiento, las políticas de seguridad, el control de tráfico y la verificación de conectividad entre los diferentes segmentos de la red [27].

El uso de GNS3 permitió recrear un entorno cercano a una implementación real, facilitando la experimentación y validación de configuraciones sin necesidad de disponer de infraestructura física, lo cual representa una ventaja significativa en entornos académicos y de investigación [27].

Figura 29. Entorno de simulación de la topología WISP en GNS3



En la Figura 29 se presenta el entorno de trabajo utilizado en GNS3, donde se implementó la topología lógica de la red WISP propuesta.

Atoll

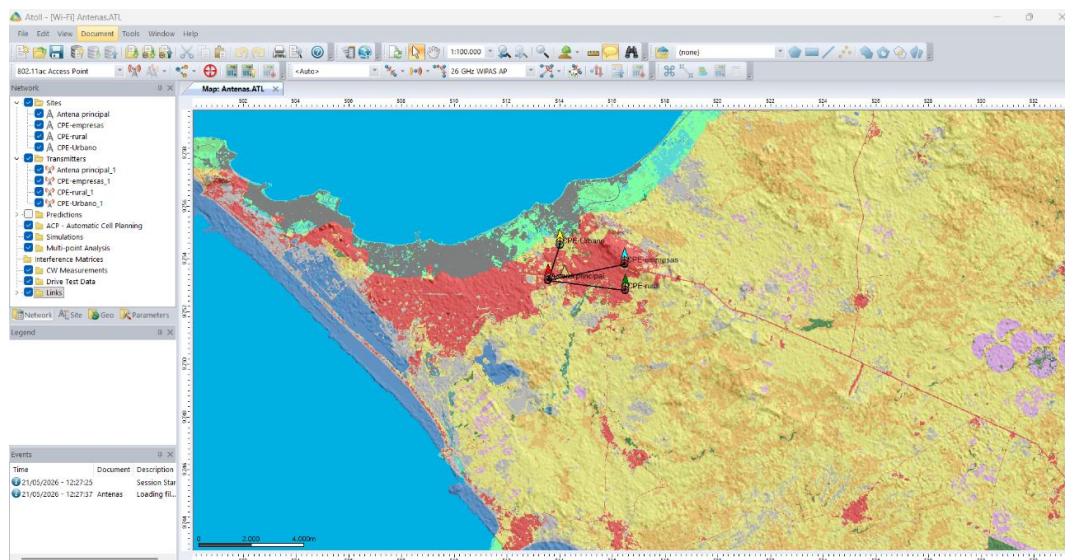
Atoll es una herramienta profesional de planificación y análisis radioeléctrico ampliamente utilizada en el diseño de redes inalámbricas y telecomunicaciones. Su principal función consiste

en modelar escenarios de propagación, analizar coberturas y evaluar la factibilidad técnica de enlaces inalámbricos mediante información geográfica y parámetros de transmisión [17].

Dentro del desarrollo de esta investigación, Atoll fue utilizado para el diseño y simulación de los enlaces inalámbricos de la red WISP, permitiendo modelar tanto enlaces punto a punto (PTP) como punto a multipunto (PTMP). Mediante esta plataforma se evaluaron aspectos relevantes como la línea de vista, pérdidas por trayectoria, cobertura, márgenes de enlace y viabilidad de transmisión entre nodos [17].

El uso de Atoll permitió complementar el diseño lógico realizado en GNS3, proporcionando una representación más cercana al comportamiento físico de la propagación de señal en escenarios reales [17].

Figura 30. Entorno de modelado radioeléctrico en Atoll



La Figura 30 muestra el entorno de simulación desarrollado en Atoll, utilizado para el modelado de los enlaces inalámbricos de la red WISP.

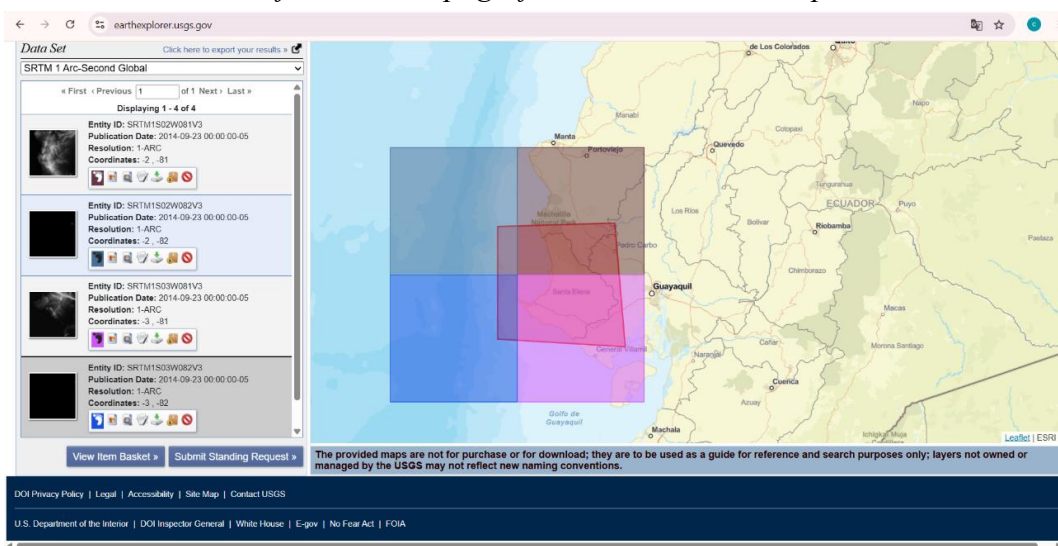
EarthExplorer

EarthExplorer es una plataforma de acceso a información geoespacial desarrollada por el Servicio Geológico de los Estados Unidos (USGS), la cual permite descargar imágenes satelitales, modelos digitales del terreno y datos topográficos de distintas regiones geográficas [54].

En esta investigación, EarthExplorer fue utilizado para obtener modelos digitales de elevación (DEM) del área de estudio, información necesaria para representar las variaciones topográficas del terreno dentro del software Atoll. Los datos descargados permitieron analizar factores como alturas del relieve, obstáculos naturales y condiciones geográficas que pueden influir en el comportamiento de los enlaces inalámbricos [54].

La incorporación de esta herramienta permitió incrementar el nivel de realismo de la simulación radioeléctrica, aproximando el análisis a condiciones similares a un despliegue físico [54].

Figura 31. *Obtención de información topográfica mediante EarthExplorer*



La Figura 31 presenta la plataforma EarthExplorer empleada para la descarga de información geográfica correspondiente al área de estudio.

ESA WorldCover

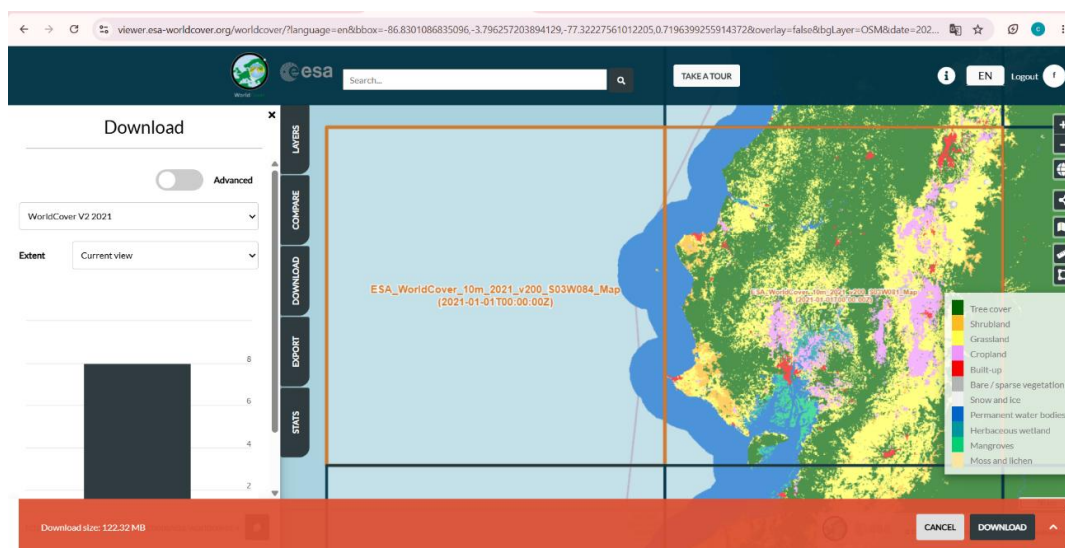
ESA WorldCover es un conjunto de datos geospaciales desarrollado por la Agencia Espacial Europea (ESA), diseñado para representar la cobertura terrestre mediante clasificación de elementos como vegetación, áreas urbanas, cuerpos de agua, cultivos y bosques [55].

En el presente trabajo, ESA WorldCover fue utilizado como fuente de información para la asignación de clutter o cobertura del terreno dentro del software Atoll. Esta información permitió

representar elementos que pueden influir en la propagación de la señal, tales como edificaciones, árboles, vegetación densa y superficies urbanas [55].

La utilización de esta herramienta permitió mejorar la precisión del análisis radioeléctrico, proporcionando un entorno de simulación más cercano a las condiciones reales de propagación presentes en una red WISP [55].

Figura 32. *Información de cobertura terrestre obtenida mediante ESA WorldCover*



La Figura 32 muestra la clasificación de cobertura terrestre correspondiente al área de estudio utilizada durante el desarrollo de la simulación radioeléctrica.

Global Mapper

Global Mapper es un software de procesamiento y visualización de información geográfica utilizado para manipular modelos digitales del terreno, imágenes en formato ráster y diferentes formatos cartográficos. Esta herramienta facilita la integración, conversión y edición de datos geoespaciales empleados en estudios de telecomunicaciones y análisis de cobertura [56].

Durante el desarrollo del proyecto, Global Mapper fue empleado para procesar la información topográfica obtenida desde EarthExplorer, así como los datos de cobertura terrestre provenientes de ESA WorldCover, permitiendo convertir los archivos a formatos compatibles con el software Atoll. Este procedimiento resultó necesario debido a las limitaciones de compatibilidad

existentes entre los formatos originales de los datos geográficos y los requeridos por la plataforma de simulación radioeléctrica [57].

Adicionalmente, esta herramienta permitió verificar la correcta representación del relieve, visualizar características del terreno y realizar ajustes preliminares sobre la información geográfica antes de incorporarla al proceso de simulación y análisis de propagación inalámbrica [56].

Figura 33. *Procesamiento de datos de cobertura terrestre de ESA WorldCover en Global Mapper*

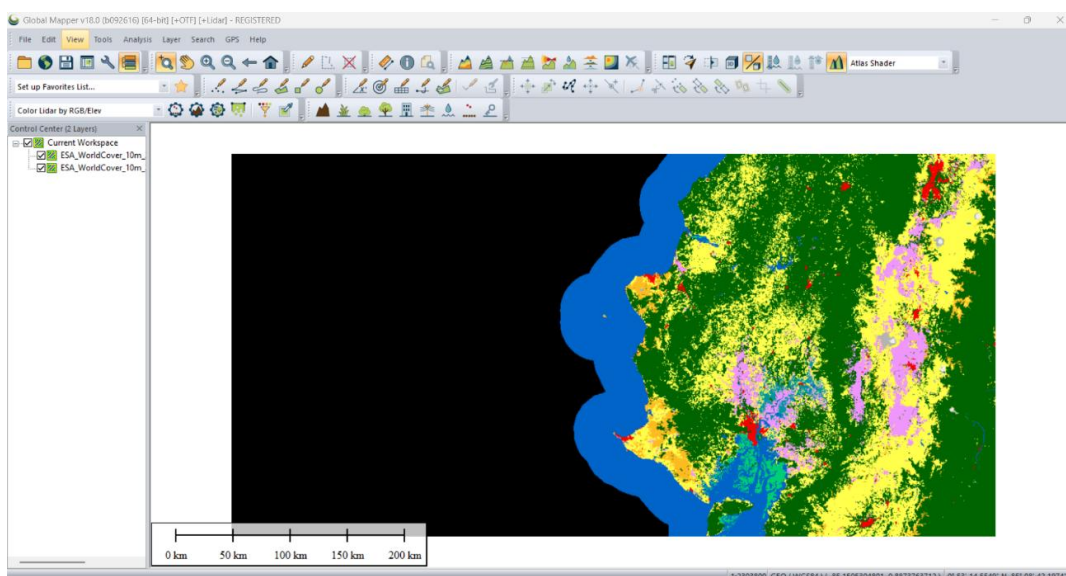
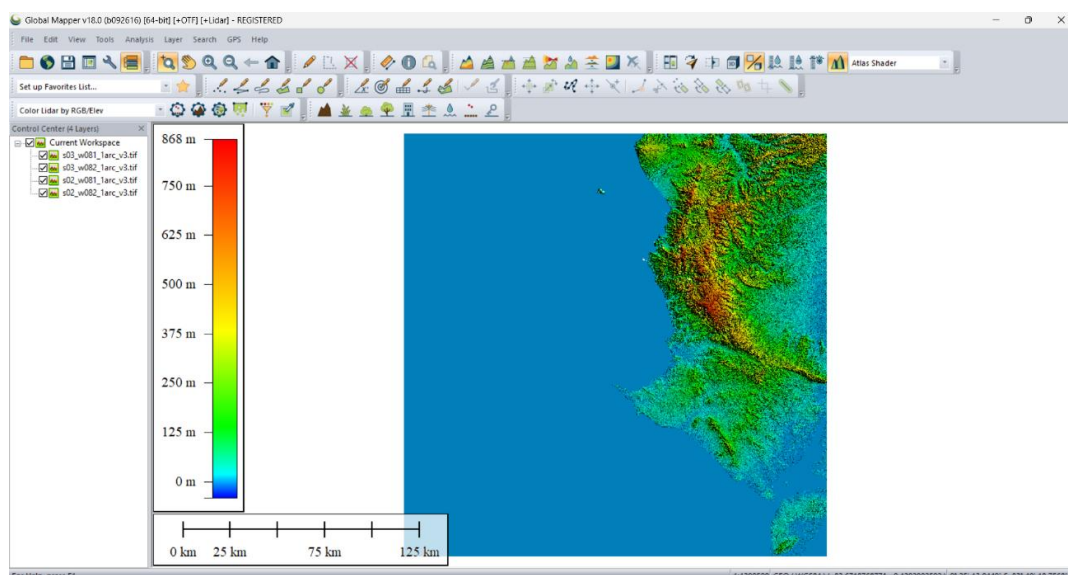


Figura 34. *Modelo digital del terreno obtenido de EarthExplorer en Global Mapper*



Las Figuras 33 y 34 muestran el procesamiento de la información geográfica realizado en Global Mapper previo a su incorporación en Atoll. En la Figura 33 se observa el tratamiento de los datos provenientes de ESA WorldCover, utilizados posteriormente para la asignación de alturas asociadas a la cobertura del terreno (clutter), permitiendo representar elementos superficiales que influyen en la propagación de la señal y obtener un análisis de cobertura más cercano a condiciones reales. Por otra parte, la Figura 34 presenta el procesamiento del modelo digital del terreno obtenido desde EarthExplorer, empleado para representar las variaciones de elevación del área de estudio, información fundamental para el análisis topográfico y la evaluación de propagación inalámbrica.

3.2.2. Flujo de trabajo del diseño de la red

El desarrollo del prototipo de red WISP siguió un flujo de trabajo estructurado, orientado a garantizar la coherencia entre el diseño lógico de la red y el análisis radioeléctrico de los enlaces inalámbricos. Para ello, se estableció una secuencia metodológica que permitió integrar herramientas de simulación, procesamiento geográfico y configuración de dispositivos dentro de un entorno controlado [4].

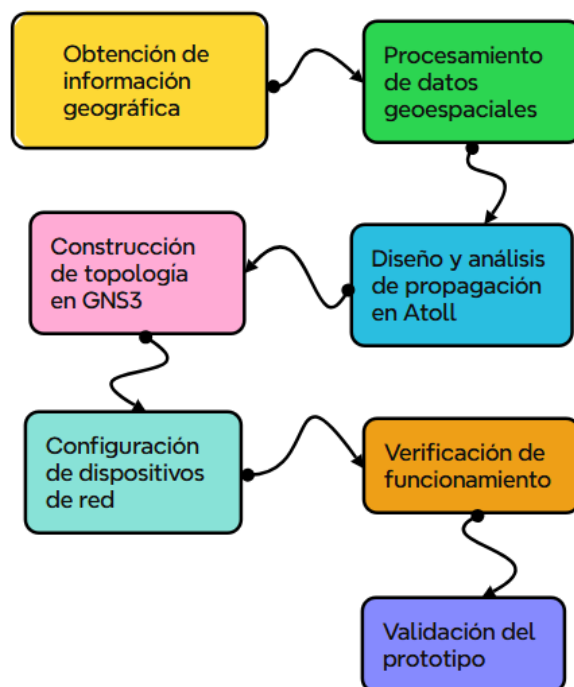
El proceso inició con la obtención de información geográfica del área de estudio mediante plataformas especializadas, permitiendo recopilar datos topográficos y de cobertura terrestre necesarios para el modelado del entorno. Posteriormente, esta información fue procesada mediante herramientas de tratamiento geoespacial con el propósito de convertir los datos a formatos compatibles y verificar su correcta representación [58].

Una vez preparados los datos geográficos, se realizó el modelado de propagación en Atoll, donde se analizaron los enlaces inalámbricos propuestos considerando variables relacionadas con cobertura, propagación y viabilidad técnica de transmisión. De forma complementaria, se desarrolló la topología lógica de la red en GNS3, permitiendo integrar los dispositivos simulados, establecer configuraciones de direccionamiento, políticas de seguridad y mecanismos de comunicación entre nodos.

Finalmente, se efectuaron pruebas de funcionamiento dentro de los entornos de simulación, con el objetivo de verificar la conectividad, analizar el comportamiento de la red y validar el

desempeño general del prototipo desarrollado. En la Figura 35 se presenta el flujo de trabajo seguido durante el diseño y desarrollo del prototipo de red WISP, evidenciando la secuencia de actividades realizadas desde la obtención de información geográfica hasta la validación del sistema simulado.

Figura 35. *Flujo de trabajo del diseño del prototipo de red WISP*



3.3. Diseño de la red WISP propuesta

El diseño de la red WISP propuesta se fundamenta en la construcción de una topología orientada a representar el funcionamiento de un proveedor inalámbrico de internet dentro de un entorno de simulación. La arquitectura planteada fue estructurada para reproducirse mediante herramientas especializadas, integrando tanto el comportamiento lógico de la red en GNS3 como el análisis de propagación inalámbrica desarrollado en Atoll.

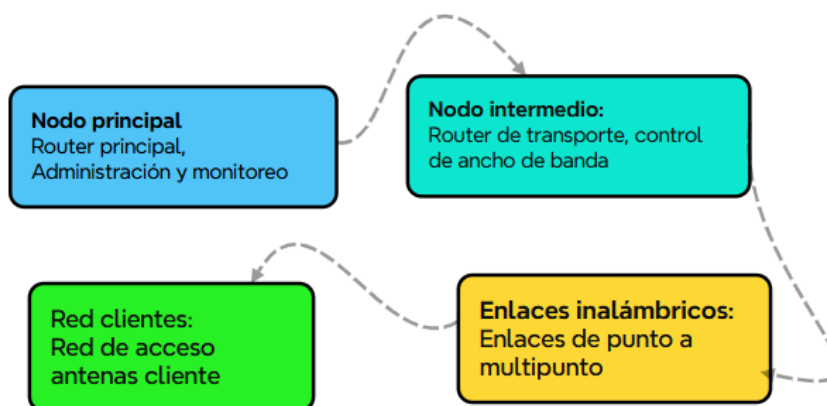
La propuesta considera una arquitectura jerárquica compuesta por un nodo principal de distribución, un nodo intermedio de transporte y una red de clientes finales conectados mediante enlaces inalámbricos. Para representar el backbone de la red se establecen enlaces punto a punto (PTP), mientras que la distribución del servicio hacia los usuarios se realiza mediante un esquema

punto a multipunto (PTMP), simulando un escenario característico de operación en entornos WISP [58].

El diseño integra elementos fundamentales de administración y funcionamiento de red, incluyendo direccionamiento IPv4, segmentación lógica, políticas de enrutamiento y mecanismos básicos de seguridad, permitiendo representar de forma cercana las condiciones técnicas presentes en un despliegue real [59].

La topología propuesta permite validar aspectos esenciales como la distribución del servicio, la gestión de tráfico entre segmentos, el rendimiento de los enlaces, la escalabilidad y la factibilidad técnica del despliegue. Adicionalmente, facilita el proceso educativo al ofrecer una representación visual y funcional completa del comportamiento de una red WISP desde el backbone hasta el cliente final.

Figura 36. *Diseño esquemático de la red WISP*



3.3.1. Descripción de los componentes de red

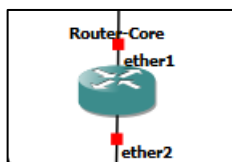
La red WISP propuesta integra diversos componentes de red orientados a representar de forma cercana la operación de un proveedor inalámbrico de internet dentro de un entorno de simulación. Debido a las limitaciones existentes para la representación nativa de enlaces inalámbricos en GNS3, algunos dispositivos fueron emulados mediante equipos equivalentes basados en MikroTik Cloud Hosted Router (CHR), mientras que el modelado radioeléctrico de los enlaces inalámbricos se realizó en Atoll empleando características técnicas de dispositivos utilizados en implementaciones WISP reales.

Router principal

El router principal de la red fue implementado mediante un MikroTik Cloud Hosted Router (CHR) dentro del entorno GNS3, actuando como nodo central encargado de la administración, segmentación y distribución del tráfico de red. Este dispositivo permitió establecer configuraciones relacionadas con direccionamiento IPv4, enrutamiento, administración de VLAN y control general de comunicación entre los distintos segmentos de la red [60].

En la Figura 37 se evidencia el router principal implementado dentro de la topología simulada, encargado de gestionar la comunicación entre los diferentes nodos de la red WISP.

Figura 37. Router principal implementado mediante MikroTik CHR en GNS3



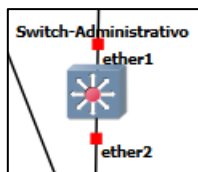
Switch administrable

Para la interconexión de los dispositivos de red se utilizó un switch administrable equivalente a un MikroTik Cloud Router Switch (CRS), encargado de facilitar la segmentación lógica de la red mediante VLAN y la comunicación entre los diferentes componentes de la topología [59].

Este dispositivo permitió organizar el tráfico correspondiente a los distintos tipos de usuarios simulados dentro de la red WISP, diferenciando segmentos rurales, urbanos y empresariales [59].

En la Figura 38 se presenta el switch administrable implementado dentro de la topología de red, utilizado para la distribución del tráfico y la administración lógica de segmentos.

Figura 38. *Switch administrable implementado en la red WISP simulada*



Antena sectorial principal

La distribución inalámbrica principal de la red fue representada mediante una antena sectorial encargada de operar bajo un esquema punto a multipunto (PTMP), simulando el comportamiento de una estación base utilizada en entornos WISP para la distribución del servicio hacia múltiples usuarios.

Debido a las limitaciones de GNS3 para simular enlaces inalámbricos, la representación lógica de este componente fue realizada mediante un MikroTik CHR configurado en modo bridge, permitiendo mantener la conectividad entre nodos dentro del entorno virtual. Sin embargo, para el análisis de propagación realizado en Atoll se emplearon parámetros técnicos equivalentes a una antena sectorial Ubiquiti LiteAP LAP-120, permitiendo representar condiciones más cercanas a una implementación real [58].

En la Figura 39 se evidencia la representación lógica de la antena sectorial dentro de GNS3, mientras que la Figura 40 presenta el modelo de referencia utilizado para el análisis radioeléctrico en Atoll.

Figura 39. *Representación lógica de la antena sectorial en GNS3*

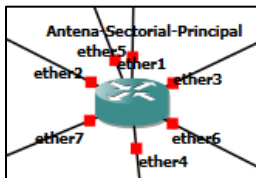


Figura 40. *Antena sectorial Ubiquiti LiteAP LAP-120 utilizada como referencia en Atoll*



Asimismo, en la Tabla 21 se presentan las principales características técnicas empleadas para el modelado de la antena sectorial dentro del análisis de cobertura inalámbrica [61].

Tabla 21. Características técnicas de la antena sectorial utilizada como referencia en Atoll

Parámetro	Característica
Modelo	Ubiquiti LiteAP LAP-120
Tipo	Antena sectorial airMAX AC
Frecuencia	5 GHz
Ganancia	16 dBi
Ángulo de cobertura	120°
Tecnología	MIMO 2x2
Polarización	Dual Linear
Puerto	1 × Ethernet Gigabit
Uso	Punto de acceso sectorial PTMP en WISP

Antenas CPE de clientes

Los clientes finales fueron representados mediante antenas tipo Customer Premises Equipment (CPE), encargadas de recibir la señal inalámbrica distribuida desde la antena sectorial principal.

En GNS3, debido a la imposibilidad de modelar propagación inalámbrica, estos equipos fueron representados mediante MikroTik CHR configurados en modo bridge, permitiendo simular la continuidad lógica del enlace entre el nodo de acceso y los clientes finales. Por otra parte, en Atoll se utilizaron características técnicas equivalentes a equipos Ubiquiti NanoStation Loco 5AC, ampliamente empleados en redes WISP para enlaces de acceso inalámbrico [58].

En la Figura 41 se evidencia la representación lógica de los clientes inalámbricos en GNS3, mientras que la Figura 42 presenta el dispositivo utilizado como referencia para el modelado radioeléctrico.

Figura 41. Representación lógica de los clientes inalámbricos en GNS3

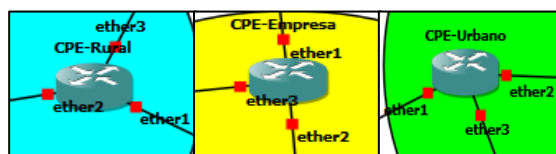


Figura 42. Antena Ubiquiti NanoStation Loco5AC utilizada como referencia en Atoll

Las características técnicas consideradas para el análisis de cobertura se presentan en la Tabla 22 [62].

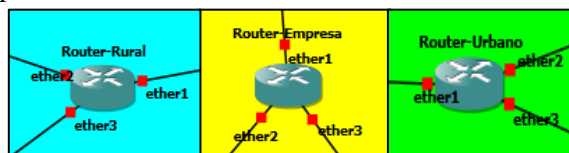
Tabla 22. Características técnicas de la antena CPE utilizada como referencia en Atoll

Parámetro	Característica
Modelo	NanoStation Loco 5AC
Radio	airMAX AC
Frecuencia	5 GHz
Throughput	Hasta 450+ Mbps
Antena integrada	13 dBi
Tecnología	MIMO 2x2
Puerto	1 × Ethernet Gigabit
Alcance	Hasta 10+ km
Uso	Cliente CPE en redes WISP

Routers de cliente

Para la administración de la red local de los usuarios finales se implementaron routers cliente mediante MikroTik CHR dentro del entorno GNS3. Estos dispositivos fueron utilizados para representar el comportamiento de routers domésticos encargados de gestionar la conectividad interna de cada usuario, permitiendo la comunicación con los diferentes dispositivos finales presentes en cada segmento [60].

En la Figura 43 se presentan los routers cliente implementados dentro de la topología, utilizados para simular el acceso final al servicio.

Figura 43. Routers cliente implementados en GNS3

3.3.2. Plan de direccionamiento IPv4

El plan de direccionamiento IPv4 de la red WISP propuesta fue diseñado bajo un esquema de segmentación lógica basado en redes privadas organizadas mediante VLAN, con el propósito de separar el tráfico de los distintos perfiles de usuario simulados —rural, urbano y empresarial—, facilitar la administración centralizada de los dispositivos de infraestructura y optimizar el control del flujo de datos dentro del entorno de simulación [60].

Un elemento diferenciador del diseño implementado es la incorporación de una VLAN exclusivamente dedicada a la administración de la infraestructura, denominada VLAN 100 de Gestión. Esta VLAN opera de forma completamente aislada del tráfico de usuarios finales y constituye el canal mediante el cual el personal técnico del ISP puede acceder remotamente a cada dispositivo de red para realizar tareas de configuración, monitoreo, diagnóstico de fallos y aseguramiento del nivel de servicio (SLA). La existencia de este segmento administrativo independiente representa una buena práctica de ingeniería de redes, ya que elimina la exposición del plano de control ante el tráfico no confiable de los abonados y reduce significativamente la superficie de ataque ante posibles amenazas internas.

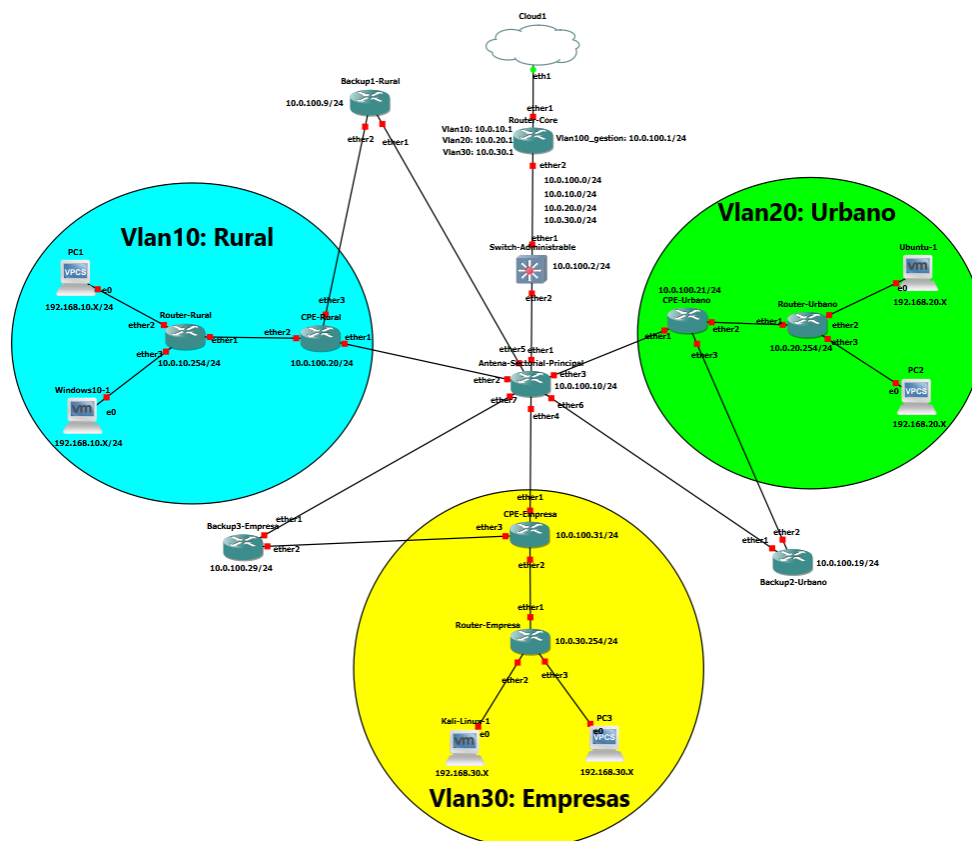
Dentro de la VLAN 100 se asignaron direcciones IP estáticas y únicas a cada nodo de infraestructura de la red, incluyendo el switch administrable, la antena sectorial principal, los equipos en la premisa del cliente (CPE) de cada sector, los backup zonales y el router central. Este direccionamiento estático garantiza la identificación precisa de cada dispositivo dentro del plano de gestión, permitiendo mantener visibilidad permanente sobre el estado operativo de toda la infraestructura desde un punto centralizado de administración.

La arquitectura de direccionamiento adoptada establece además una subred de distribución independiente para cada segmento de usuario, administrada desde el router central (Router_Core), el cual actúa como puerta de enlace predeterminada (default gateway) para todos los dispositivos pertenecientes a cada VLAN. Este enfoque permite que el tráfico inter-VLAN sea gestionado de forma centralizada, garantizando el aislamiento lógico entre segmentos y reduciendo la posibilidad de interferencias o desbordamientos de tráfico entre dominios de difusión [60].

De manera complementaria, cada cliente final dispone de una red de área local (LAN) independiente destinada a la conectividad de sus dispositivos internos. Para ello, se implementaron servidores DHCP en los routers de cliente de cada segmento, encargados de la asignación dinámica de parámetros de red —dirección IP, máscara de subred, puerta de enlace y servidores DNS— a los equipos finales conectados localmente. Esta implementación permite automatizar la conectividad de los dispositivos de usuario, representando de forma más fidedigna el comportamiento operativo de una infraestructura WISP real.

La Figura 44 presenta la topología lógica completa de la red simulada en GNS3, en la cual se identifican visualmente los cuatro segmentos definidos: la VLAN 100 de gestión, representada mediante las direcciones del plano de administración presentes en cada nodo, y los tres segmentos de usuario diferenciados cromáticamente —sector rural (VLAN 10), sector urbano (VLAN 20) y sector empresarial (VLAN 30)—. Esta representación constituye la referencia visual para interpretar el esquema de direccionamiento IPv4 detallado en las tablas subsiguientes.

Figura 44. Topología lógica de la red WISP simulada en GNS3



En la Tabla 23 se presenta el esquema general de direccionamiento IPv4 implementado, incluyendo la VLAN de gestión administrativa y los tres segmentos de usuario definidos.

Tabla 23. *Esquema general de direccionamiento IPv4*

Segmento	VLAN	Red de distribución	Gateway	Red LAN cliente	Gateway LAN	Rango DHCP
Gestión/Administración	100	10.0.100.0/24	10.0.10.0.1	—	—	—
Rural	10	10.0.10.0/24	10.0.10.1	192.168.10.0/24	192.168.1.0.1	192.168.10.10 – 192.168.10.100
Urbano	20	10.0.20.0/24	10.0.20.1	192.168.20.0/24	192.168.2.0.1	192.168.20.10 – 192.168.20.100
Empresas	30	10.0.30.0/24	10.0.30.1	192.168.30.0/24	192.168.3.0.1	192.168.30.100 – 192.168.30.200

A fin de complementar la representación gráfica anterior, la Tabla 24 resume los enlaces troncales que parten del Router_Core hacia cada segmento de red, indicando la VLAN asociada y las direcciones IP de ambos extremos.

Tabla 24. *Resumen de enlaces troncales entre el Router_Core y cada segmento de red*

Segmento	VLAN	Dispositivo	IP	Se conecta con	IP
Gestión/Administración	100	Router_Core	10.0.100.1/24	Switch_Administrable	10.0.100.2/24
Rural	10	Router_Core	10.0.10.1/24	Router-Rural	10.0.10.254/24
Urbano	20	Router_Core	10.0.20.1/24	Router-Urbano	10.0.20.254/24
Empresas	30	Router_Core	10.0.30.1/24	Router-Empresas	10.0.30.254/24

Asimismo, se definieron direcciones IP estáticas para cada dispositivo de infraestructura dentro de la VLAN 100 de gestión, así como para los elementos terminales de cada segmento de

usuario. Las Tablas 25, 27, 29 y 31 presentan el esquema de direccionamiento implementado para la red de administración y los sectores rural, urbano y empresarial, respectivamente.

La Tabla 25 detalla el direccionamiento IPv4 asignado a los dispositivos que conforman el segmento de gestión y administración de la red (VLAN 100). A diferencia de las VLAN de usuario, este segmento no transporta tráfico de datos de abonados, sino que constituye el canal exclusivo mediante el cual el personal técnico del ISP accede remotamente a cada nodo de infraestructura para realizar tareas de configuración, monitoreo y mantenimiento. Todos los dispositivos de la red, independientemente del sector al que pertenezcan, cuentan con una interfaz lógica activa dentro de esta VLAN, lo que garantiza visibilidad administrativa centralizada sobre la totalidad de la infraestructura desde un único punto de gestión. Los dispositivos listados en esta tabla son identificables en la Figura 45 mediante sus respectivas etiquetas de dirección IP superpuestas sobre cada nodo.

Tabla 25. *Direccionamiento IPv4 de la VLAN 100 — segmento de gestión y administración*

Dispositivo	Dirección IP	Gateway
Router_Core (Gateway central)	10.0.100.1/24	—
Switch administrable	10.0.100.2/24	10.0.100.1
Backup rural (Backup1 - Rural)	10.0.100.9/24	10.0.100.1
Antena sectorial principal	10.0.100.10/24	10.0.100.1
Backup urbano (Backup2 - Urbano)	10.0.100.19/24	10.0.100.1
CPE rural	10.0.100.20/24	10.0.100.1
CPE urbano	10.0.100.21/24	10.0.100.1
Backup empresarial (Backup3 - Empresas)	10.0.100.29/24	10.0.100.1
CPE empresas	10.0.100.31/24	10.0.100.1

La Tabla 26 detalla la totalidad de las conexiones de la topología, incluyendo los equipos intermedios (switch administrable, antena sectorial y CPE), los routers cliente y los dispositivos finales de cada segmento, con la VLAN asociada y las direcciones IP de ambos extremos.

Tabla 26. *Detalle de conexiones entre dispositivos de la topología lógica*

Segmento	VLAN	Dispositivo	IP	Se conecta con	IP
Gestión	100	Router_Core	10.0.100.1/ 24	Switch_Administrable	10.0.100.2/ 24
Gestión	100	Switch_Administrable	10.0.100.2/ 24	Antena_Sectorial_Principal	10.0.100.10/ 24
Gestión	100	Antena_Sectorial_Principal	10.0.100.10/ 24	CPE-Rural	10.0.100.20/ 24
Gestión	100	Antena_Sectorial_Principal	10.0.100.10/ 24	CPE-Urbano	10.0.100.21/ 24
Gestión	100	Antena_Sectorial_Principal	10.0.100.10/ 24	CPE-Empresas	10.0.100.31/ 24
Gestión	100	Antena_Sectorial_Principal	10.0.100.10/ 24	Backup1-Rural	10.0.100.9/ 24
Gestión	100	Antena_Sectorial_Principal	10.0.100.10/ 24	Backup2-Urbano	10.0.100.19/ 24
Gestión	100	Antena_Sectorial_Principal	10.0.100.10/ 24	Backup3-Empresas	10.0.100.29/ 24
Rural	10	Backup1-Rural	10.0.100.9/ 24	CPE-Rural	10.0.100.20/ 24
Rural	10	CPE-Rural	10.0.100.20/ 24	Router-Rural	10.0.10.254/ 24
Rural	10	Router-Rural	10.0.10.254/ 24	PC1 / Windows10-1	192.168.10. X
Urbano	20	Backup2-Urbano	10.0.100.19/ 24	CPE-Urbano	10.0.100.21/ 24
Urbano	20	CPE-Urbano	10.0.100.21/ 24	Router-Urbano	10.0.20.254/ 24
Urbano	20	Router-Urbano	10.0.20.254/ 24	Ubuntu-1 / PC2	192.168.20. X
Empresas	30	Backup3-Empresas	10.0.100.29/ 24	CPE-Empresas	10.0.100.31/ 24
Empresas	30	CPE-Empresas	10.0.100.31/ 24	Router-Empresas	10.0.30.254/ 24
Empresas	30	Router-Empresas	10.0.30.254/ 24	Kali-Linux-1 / PC3	192.168.30. X

La Tabla 27 presenta el esquema de direccionamiento IPv4 correspondiente al segmento rural, asociado a la VLAN 10. En este sector, el Router_Core actúa como puerta de enlace principal de la red de distribución, mientras que el router del cliente rural opera como dispositivo de frontera entre la red del ISP y la red de área local interna del abonado. La dirección IP asignada al router

cliente (10.0.10.254/24) fue seleccionada deliberadamente en el extremo superior del rango de subred, siguiendo una convención de direccionamiento que facilita la identificación visual de los equipos de borde dentro del esquema de administración. La red LAN interna del cliente (192.168.10.0/24) se encuentra completamente separada de la red de distribución del ISP mediante NAT, garantizando el aislamiento del tráfico privado del abonado.

En la Figura 44, este segmento corresponde a la zona celeste de la topología.

Tabla 27. *Direccionamiento IPv4 del segmento rural (VLAN 10)*

Dispositivo	Dirección IP	Gateway
Router principal (Router_Core)	10.0.10.1/24	—
Router cliente rural	10.0.10.254/24	10.0.10.1
Gateway LAN cliente	192.168.10.1/24	—

A fin de complementar el direccionamiento del segmento rural, la Tabla 28 describe las conexiones entre los dispositivos correspondientes a la VLAN 10, indicando las direcciones IP de cada extremo del enlace.

Tabla 28. *Conexiones de dispositivos — segmento rural (VLAN 10)*

Segmento	VLAN	Dispositivo	IP	Se conecta con	IP
Rural	10	Antena_Sectorial_Principal	10.0.100.10/24	CPE-Rural	10.0.100.20/24
Rural	10	Antena_Sectorial_Principal	10.0.100.10/24	Backup1-Rural	10.0.100.9/24
Rural	10	Backup1-Rural	10.0.100.9/24	CPE-Rural	10.0.100.20/24
Rural	10	CPE-Rural	10.0.100.20/24	Router-Rural	10.0.10.254/24
Rural	10	Router-Rural	10.0.10.254/24	PC1 / Windows10-1	192.168.10.X

La Tabla 29 expone el direccionamiento IPv4 implementado en el segmento urbano, correspondiente a la VLAN 20. Al igual que en el sector rural, el Router_Core centraliza el enrutamiento del tráfico de distribución, mientras que el router del cliente urbano (10.0.20.254/24) establece la demarcación lógica entre la infraestructura del proveedor y la red doméstica del

abonado. Este segmento fue configurado con un rango de red LAN interno diferenciado (192.168.20.0/24), evitando solapamientos de direccionamiento con los demás sectores y permitiendo identificar con claridad el origen del tráfico en caso de requerir análisis o diagnóstico.

de la red.

En la Figura 44, este segmento corresponde a la zona verde de la topología.

Tabla 29. *Direccionamiento IPv4 del segmento urbano (VLAN 20)*

Dispositivo	Dirección IP	Gateway
Router principal (Router_Core)	10.0.20.1/24	—
Router cliente urbano	10.0.20.254/24	10.0.20.1
Gateway LAN cliente	192.168.20.1/24	—

A fin de complementar el direccionamiento del segmento urbano, la Tabla 30 describe las conexiones entre los dispositivos correspondientes a la VLAN 20, indicando las direcciones IP de cada extremo del enlace.

Tabla 30. *Conexiones de dispositivos — segmento urbano (VLAN 20)*

Segmento	VLAN	Dispositivo	IP	Se conecta con	IP
Urbano	20	Antena_Sectorial_Principal	10.0.100.10/24	CPE-Urbano	10.0.100.21/24
Urbano	20	Antena_Sectorial_Principal	10.0.100.10/24	Backup2-Urbano	10.0.100.19/24
Urbano	20	Backup2-Urbano	10.0.100.19/24	CPE-Urbano	10.0.100.21/24
Urbano	20	CPE-Urbano	10.0.100.21/24	Router-Urbano	10.0.20.254/24
Urbano	20	Router-Urbano	10.0.20.254/24	Ubuntu-1 / PC2	192.168.20.X

Finalmente, la Tabla 31 describe el esquema de direccionamiento IPv4 del segmento empresarial, asociado a la VLAN 30. A diferencia de los sectores residenciales, este segmento fue concebido para brindar un servicio de conectividad dedicada y de alta prioridad, por lo que el router de empresas (10.0.30.254/24) fue configurado bajo un esquema de enrutamiento estático puro, sin aplicar traducción de direcciones dinámica masiva (NAT/Masquerade). Esta decisión de

diseño garantiza que los flujos de datos bidireccionales hacia los servidores internos de la organización —tales como servicios VPN, plataformas web o sistemas ERP— transiten de forma directa y transparente a través del backbone del WISP, sin penalizaciones de procesamiento asociadas al NAT. La red LAN interna corporativa (192.168.30.0/24) dispone de un rango de asignación DHCP reservado exclusivamente para estaciones de trabajo administrativas, preservando las primeras direcciones del segmento para asignaciones estáticas de servidores críticos.

En la Figura 44, este segmento corresponde a la zona amarilla de la topología.

Tabla 31. *Direccionamiento IPv4 del segmento empresarial (VLAN 30)*

Dispositivo	Dirección IP	Gateway
Router principal (Router_Core)	10.0.30.1/24	—
Router empresas	10.0.30.254/24	10.0.30.1
Gateway LAN cliente	192.168.30.1/24	—

A fin de complementar el direccionamiento del segmento empresarial, la Tabla 32 describe las conexiones entre los dispositivos correspondientes a la VLAN 30, indicando las direcciones IP de cada extremo del enlace.

Tabla 32. *Conexiones de dispositivos — segmento empresarial (VLAN 30)*

Segmento	VLAN	Dispositivo	IP	Se conecta con	IP
Empresas	30	Antena_Sectorial_Principa 1	10.0.100.10/2 4	CPE- Empresas	10.0.100.31/2 4
Empresas	30	Antena_Sectorial_Principa 1	10.0.100.10/2 4	Backup3- Empresas	10.0.100.29/2 4
Empresas	30	Backup3-Empresas	10.0.100.29/2 4	CPE- Empresas	10.0.100.31/2 4
Empresas	30	CPE-Empresas	10.0.100.31/2 4	Router- Empresas	10.0.30.254/2 4
Empresas	30	Router-Empresas	10.0.30.254/2 4	Kali- Linux-1 / PC3	192.168.30.X

3.3.3. Diseño lógico de comunicación

El diseño lógico de comunicación de la red WISP propuesta define la manera en que los datos fluyen entre los distintos segmentos de la red, estableciendo los mecanismos de segmentación, enrutamiento, traducción de direcciones, administración y redundancia que gobiernan el comportamiento del sistema. Este apartado describe la arquitectura lógica implementada, detallando las decisiones de diseño adoptadas para garantizar el aislamiento entre segmentos, la disponibilidad del servicio y la administración centralizada de la infraestructura [4].

Arquitectura de segmentación mediante VLAN

La segmentación lógica de la red fue implementada mediante el protocolo IEEE 802.1Q, el cual permite dividir un mismo medio físico de transporte en múltiples dominios de difusión independientes a través del etiquetado de tramas. Esta técnica constituye el pilar fundamental del diseño lógico, ya que posibilita la coexistencia de múltiples tipos de tráfico sobre una única infraestructura física sin que exista interferencia entre ellos [4].

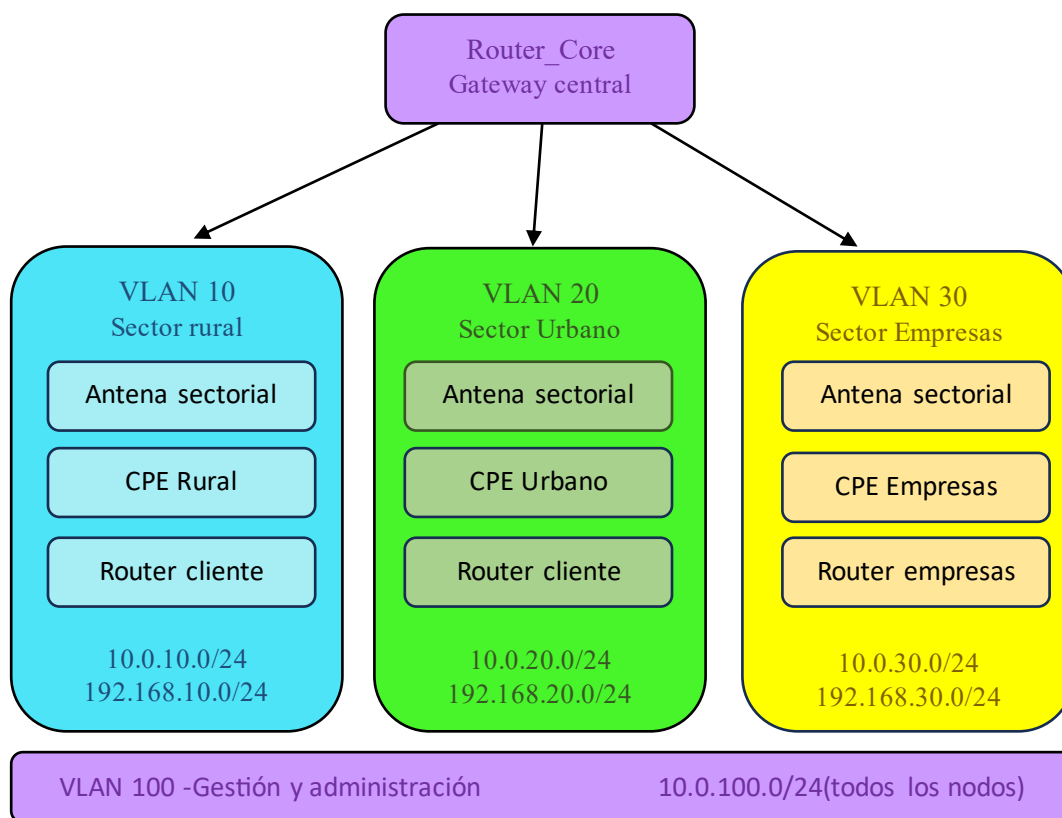
La arquitectura implementada contempla cuatro VLAN diferenciadas, cada una asociada a un perfil de usuario o función administrativa específica. Las VLAN 10, 20 y 30 transportan el tráfico de datos de los usuarios pertenecientes a los sectores rural, urbano y empresarial respectivamente, mientras que la VLAN 100 opera exclusivamente como canal de gestión y administración de la infraestructura, completamente aislada del tráfico de abonados. En la Tabla 33 se presenta el resumen de las VLAN implementadas y su función dentro de la arquitectura de red.

Tabla 33. *VLAN implementadas en la red WISP propuesta*

VLAN	Nombre	Función	Tipo de tráfico
10	VLAN Rural	Servicio de datos sector rural	Tráfico de usuarios residenciales rurales
20	VLAN Urbano	Servicio de datos sector urbano	Tráfico de usuarios residenciales urbanos
30	VLAN Empresas	Servicio de datos sector empresarial	Tráfico corporativo dedicado
100	VLAN Gestión	Administración de infraestructura	Tráfico de control y monitoreo del ISP

El etiquetado de tramas se aplica en los enlaces troncales (trunk) que interconectan los dispositivos de infraestructura —switch administrable, antena sectorial, repetidores zonales y CPE—, garantizando que cada trama sea identificada con su VLAN de origen durante todo su recorrido por el backbone de la red. En los puertos de acceso orientados hacia los equipos de cliente, las etiquetas se remueven antes de la entrega, de modo que los routers residenciales y empresariales reciben un flujo de datos nativo sin necesidad de procesar tramas estructuradas 802.1Q [63].

Figura 45. *Arquitectura de segmentación VLAN de la red WISP*



En la Figura 45 se presenta la arquitectura de segmentación lógica implementada, donde se observan las cuatro VLAN definidas. Las VLAN 10, 20 y 30 agrupan los dispositivos de cada sector de usuario con sus respectivas subredes de distribución y LAN interna, mientras que la VLAN 100 atraviesa horizontalmente toda la infraestructura como canal exclusivo de gestión y administración centralizada.

Flujo de tráfico por segmento de red

El flujo de tráfico dentro de la red WISP sigue una trayectoria jerárquica desde el dispositivo final del usuario hasta el nodo central de distribución, y desde este hacia la red pública de internet. Si bien los tres sectores comparten la misma infraestructura física de transporte, cada uno opera de forma lógicamente aislada gracias a la segmentación VLAN implementada. A continuación, se describe el recorrido del tráfico para cada segmento.

- **Sector Rural (VLAN 10)**

El tráfico generado por los dispositivos finales del usuario rural es recibido por el Router_Cliente_Rural, que actúa como puerta de enlace de la red local interna (192.168.10.0/24). Este router aplica una regla de enmascaramiento NAT sobre su interfaz WAN, traduciendo las direcciones privadas de la LAN doméstica hacia la dirección IP estática asignada en la VLAN 10 (10.0.10.254/24). El paquete resultante es entregado al CPE_Rural, que lo transporta de forma etiquetada (Tagged VLAN 10) a través del enlace inalámbrico hacia la Antena_Sectorial_Principal. Desde allí, el tráfico continúa etiquetado por el Switch_Administrable hasta alcanzar el Router_Core, que realiza el enrutamiento hacia internet a través de su interfaz WAN.

- **Sector Urbano (VLAN 20)**

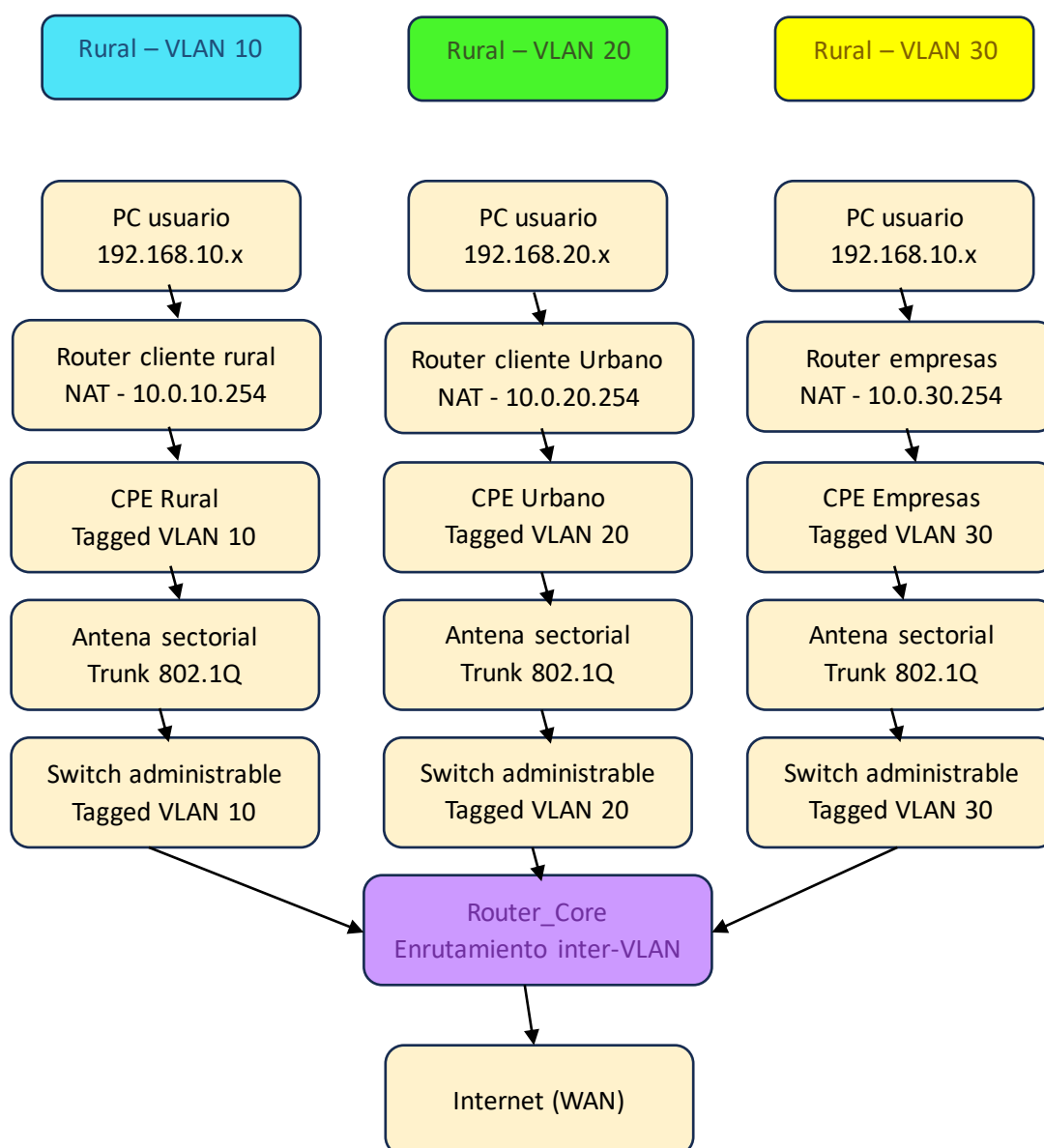
El flujo de tráfico del sector urbano sigue una trayectoria equivalente a la del sector rural. El Router_Cliente_Urbano gestiona la red local interna (192.168.20.0/24) y aplica NAT sobre su interfaz WAN antes de entregar el tráfico al CPE_Urbano, el cual lo transporta etiquetado como VLAN 20 hacia la Antena_Sectorial_Principal. El tráfico continúa por el backbone hasta el Router_Core, que lo enruta hacia internet.

- **Sector Empresarial (VLAN 30)**

El sector empresarial presenta una diferencia fundamental respecto a los sectores residenciales: el Router_Empresas no aplica traducción de direcciones NAT sobre su interfaz WAN. En su lugar, opera bajo un esquema de enrutamiento estático puro, lo que permite que los flujos de datos bidireccionales —incluyendo servicios VPN, plataformas web y sistemas ERP—

transiten de forma directa y transparente a través del backbone del WISP sin penalizaciones de procesamiento. El tráfico corporativo se etiqueta como VLAN 30 desde el CPE_Empresas y se transporta hasta el Router_Core, que lo enruta directamente hacia internet o hacia otros segmentos de la red según corresponda.

Figura 46. *Flujo de tráfico por segmento de red*



En la Figura 46 se ilustra el recorrido del tráfico desde el dispositivo final del usuario hasta internet en cada sector. Se observa que los sectores rural y urbano aplican NAT en el router cliente antes de ingresar al backbone del ISP, mientras que el sector empresarial transmite de forma directa sin modificación de cabeceras IP.

Enrutamiento inter-VLAN

El enrutamiento entre los distintos segmentos de red fue centralizado en el Router_Core mediante la técnica conocida como Router on a Stick, en la cual un único dispositivo de Capa 3 gestiona el tráfico entre múltiples VLAN a través de subinterfaces lógicas configuradas sobre un enlace troncal físico. Esta arquitectura elimina la necesidad de dispositivos de enrutamiento independientes por segmento, simplificando la gestión y reduciendo la complejidad de la infraestructura [60].

Cada VLAN dispone de una subinterfaz lógica en el Router_Core con su respectiva dirección IP gateway, permitiendo que los paquetes destinados a otros segmentos sean procesados y reenviados de forma centralizada. La ruta por defecto hacia internet se obtiene dinámicamente a través del cliente DHCP configurado en la interfaz WAN (ether1) y se redistribuye hacia los segmentos internos mediante la tabla de enrutamiento del router central. En la Tabla 34 se presentan las subinterfaces y rutas configuradas en el Router_Core.

Tabla 34. *Subinterfaces y rutas del Router_Core*

Subinterfaz	VLAN	Dirección IP	Función
VLAN 10_Rural	10	10.0.10.1/24	Gateway sector rural
VLAN 20_Urbano	20	10.0.20.1/24	Gateway sector urbano
VLAN 30_Empresas	30	10.0.30.1/24	Gateway sector empresarial
VLAN 100_Gestión	100	10.0.100.1/24	Gateway administración
ether1 (WAN)	—	Dinámica (DHCP)	Salida a internet

Traducción de direcciones de red (NAT)

Con el propósito de permitir que los dispositivos de los usuarios finales, cuyas direcciones IP pertenecen a rangos privados no enrutables en internet, puedan acceder a la red pública de forma transparente, se implementó el mecanismo de traducción de direcciones de red mediante Source NAT/Masquerade en los routers de cliente de los sectores rural y urbano.

La acción masquerade intercepta los paquetes salientes de la red LAN interna y reemplaza dinámicamente la dirección IP de origen por la dirección IP estática asignada a la interfaz WAN del router cliente, ocultando la topología interna del abonado ante el backbone del ISP. Este mecanismo opera de forma transparente para los dispositivos finales, que no requieren ninguna configuración especial para acceder a internet [60].

El sector empresarial constituye una excepción deliberada a este esquema, dado que los servicios corporativos requieren comunicación bidireccional directa sin modificación de cabeceras IP para el correcto funcionamiento de protocolos como VPN o servicios alojados en servidores locales. El Router_Empresas fue configurado sin NAT y opera bajo enrutamiento estático puro. Esta decisión evita fallas de enrutamiento asimétrico y garantiza la transparencia de los flujos de datos entre la red corporativa y el backbone del WISP.

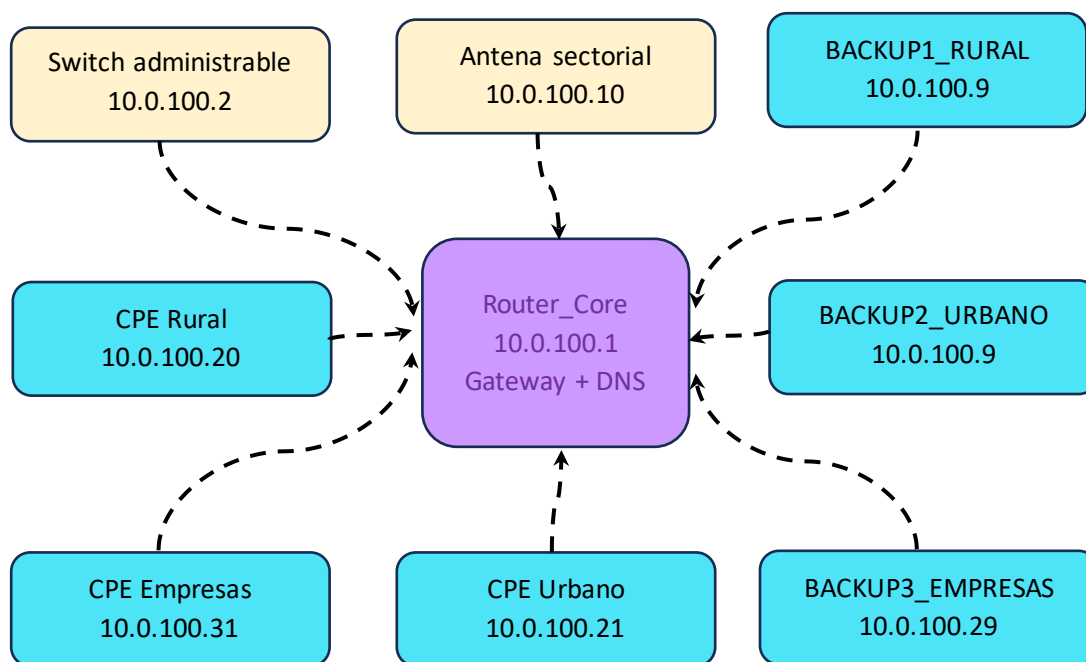
Plano de gestión y administración (VLAN 100)

La administración remota de todos los dispositivos de infraestructura de la red se realiza a través de la VLAN 100, denominada segmento de gestión. Este canal administrativo opera de forma completamente independiente del tráfico de usuarios finales, circulando de forma etiquetada sobre los mismos enlaces físicos de transporte sin interferir con los datos de los abonados [59].

Todos los nodos de infraestructura, independientemente del sector de usuario al que pertenezcan, cuentan con una interfaz lógica activa dentro de la VLAN 100, a la cual se le asignó una dirección IP estática única. Esta configuración permite al personal técnico del ISP acceder remotamente a cualquier dispositivo de la red desde un único punto de administración centralizado, facilitando tareas de configuración, monitoreo de parámetros operativos, diagnóstico de fallos y aseguramiento del nivel de servicio (SLA) [59].

El Router_Core actúa simultáneamente como gateway de la VLAN 100 (10.0.100.1/24) y como servidor caché DNS para toda la infraestructura, resolviendo las peticiones de nombres de dominio generadas tanto por los dispositivos de gestión como por los usuarios finales de cada segmento. Esta centralización del servicio DNS optimiza los tiempos de resolución y simplifica la configuración de los nodos de infraestructura, que delegan todas sus consultas DNS hacia el nodo central.

Figura 47. Topología lógica del plano de gestión y administración (VLAN 100)



La Figura 47 representa la centralización de la administración de red mediante la VLAN 100. Se observa al Router_Core actuando como nodo convergente para todos los dispositivos de infraestructura (switches, antenas sectoriales, backup y CPE), cada uno identificado con su dirección IP estática dentro del segmento de gestión 10.0.100.0/24. Esta arquitectura permite que el Router_Core gestione el tráfico administrativo y provea servicios de resolución DNS de manera unificada, garantizando la independencia respecto al tráfico de datos de los abonados.

Redundancia de enlace mediante RSTP

Con el objetivo de garantizar la continuidad del servicio ante posibles fallos en los enlaces inalámbricos —ocasionados por condiciones climáticas adversas, obstrucciones transitorias o pérdidas de línea de vista (LOS)— se implementó una topología de anillo redundante en la última milla de cada sector, gobernada por el protocolo Rapid Spanning Tree (RSTP, IEEE 802.1w) [64].

El protocolo RSTP opera en la Capa 2 del modelo OSI y permite la existencia de múltiples caminos físicos entre nodos sin generar bucles de conmutación. Para ello, establece una jerarquía de caminos mediante la asignación de prioridades a los puertos del bridge, definiendo un enlace

principal activo y un enlace de respaldo en estado de bloqueo. Ante la detección de un fallo en el enlace principal, RSTP activa automáticamente el camino de respaldo en un tiempo de convergencia notablemente inferior al del protocolo STP convencional, minimizando el impacto sobre la continuidad del servicio [64].

En la arquitectura implementada, cada CPE de cliente queda interconectado mediante dos caminos concurrentes en Capa 2: el canal directo desde la Antena_Sectorial_Principal (ether1, prioridad 0x80) y el canal de contingencia que pasa a través del backup zonal correspondiente (ether3, prioridad 0x90). El camino directo opera como enlace preferencial durante el funcionamiento normal de la red, mientras que el enlace a través del backup permanece en espera, listo para asumir el transporte del tráfico ante cualquier interrupción del camino principal. La Tabla 35 resume la jerarquía de caminos configurada para cada sector.

Tabla 35. *Jerarquía de caminos RSTP por sector*

Sector	Enlace principal	Prioridad	Enlace de respaldo	Prioridad	Repetidor zonal
Rural	ether1 (directo desde antena)	0x80 (128)	ether3 (vía backup)	0x90 (144)	BACKUP_ZONAL_1
Urbano	ether1 (directo desde antena)	0x80 (128)	ether3 (vía backup)	0x90 (144)	BACKUP_ZONAL_2
Empresarial	ether1 (directo desde antena)	0x80 (128)	ether3 (vía backup)	0x90 (144)	BACKUP_ZONAL_3

3.4. Desarrollo de la simulación en GNS3

3.4.1. Instalación e integración de GNS3 con VMware Workstation

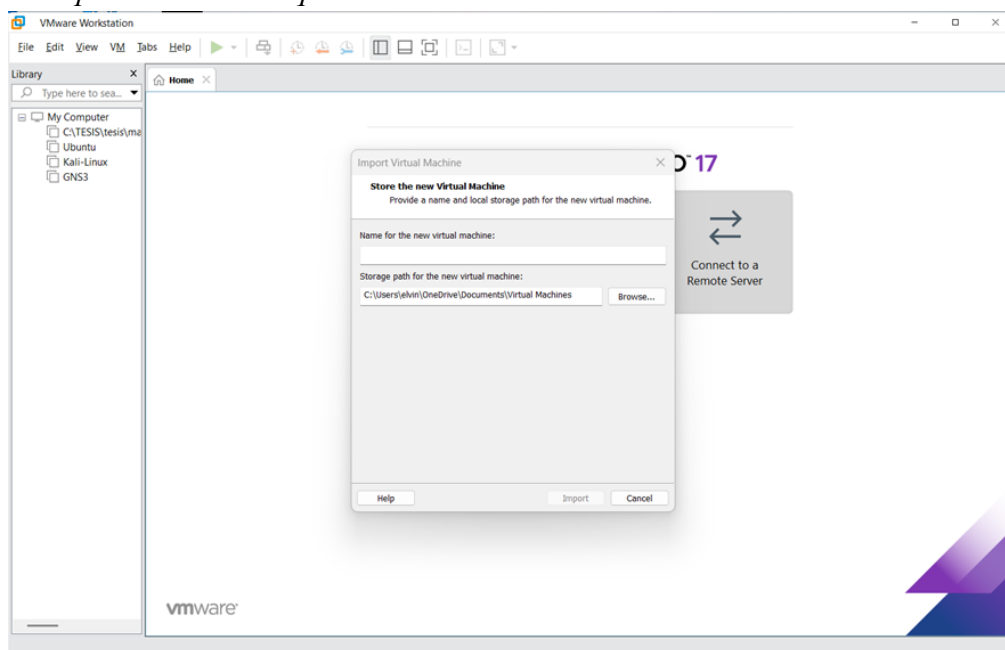
Como primer paso para la implementación del entorno de simulación, se procedió a descargar los archivos correspondientes al software GNS3, VMware Workstation y la máquina virtual GNS3 VM, compatible con VMware, desde sus respectivas páginas oficiales [65].

Una vez completado el proceso de descarga e instalación de las herramientas necesarias, se realizó la integración de la máquina virtual GNS3 VM dentro del software VMware Workstation. Este procedimiento resulta necesario para permitir el funcionamiento adecuado del entorno virtual utilizado durante la simulación de la red [65].

Para ello, inicialmente se accedió a VMware Workstation y desde el menú principal se seleccionó la opción File > Open, permitiendo localizar y abrir el archivo correspondiente a la máquina virtual GNS3 VM previamente almacenada en el equipo [65].

Al seleccionar el archivo, el sistema carga la configuración inicial de la máquina virtual y presenta la ventana de importación correspondiente, tal como se muestra en la Figura 48.

Figura 48. *Apertura de la máquina virtual GNS3 VM en VMware Workstation*



Una vez abierta la ventana de importación, se procedió a asignar un nombre de identificación a la máquina virtual; en este caso, se utilizó el nombre GNS3. Asimismo, se mantuvo la ruta de almacenamiento predeterminada propuesta por el software, con el propósito de conservar la configuración recomendada. Posteriormente, se seleccionó la opción Import, iniciando el proceso de incorporación de la máquina virtual al entorno VMware Workstation [65].

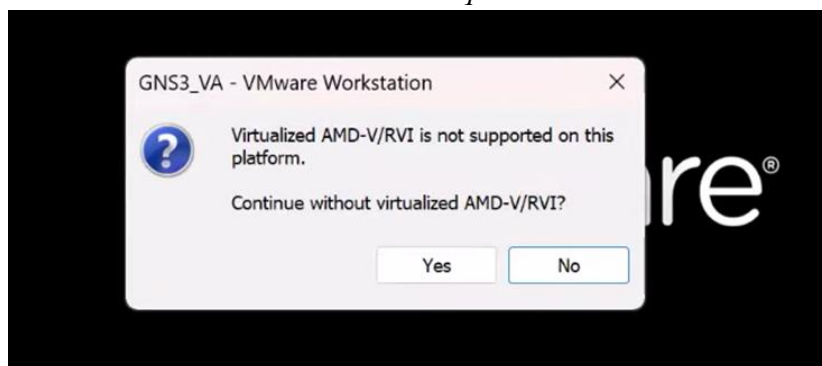
Finalizado el proceso de importación, la máquina virtual fue agregada automáticamente al entorno VMware conservando los recursos de hardware asignados por defecto. Posteriormente, se procedió a ejecutar la máquina virtual mediante la opción Power on this virtual machine, permitiendo iniciar el entorno necesario para la simulación de red [65].

En la mayoría de los casos, durante el arranque de la máquina virtual, puede presentarse un error relacionado con la virtualización del procesador, impidiendo el correcto funcionamiento de GNS3 VM. Este inconveniente suele mostrarse mediante el siguiente mensaje del sistema [65]:

“Virtualized AMD-V/RVI is not supported on this platform. Continue without virtualized AMD-V/RVI?”

La presencia de este error puede impedir el inicio adecuado de la máquina virtual, debido a conflictos con configuraciones de virtualización o mecanismos de seguridad habilitados en el sistema operativo, tal como se evidencia en la Figura 49 [65].

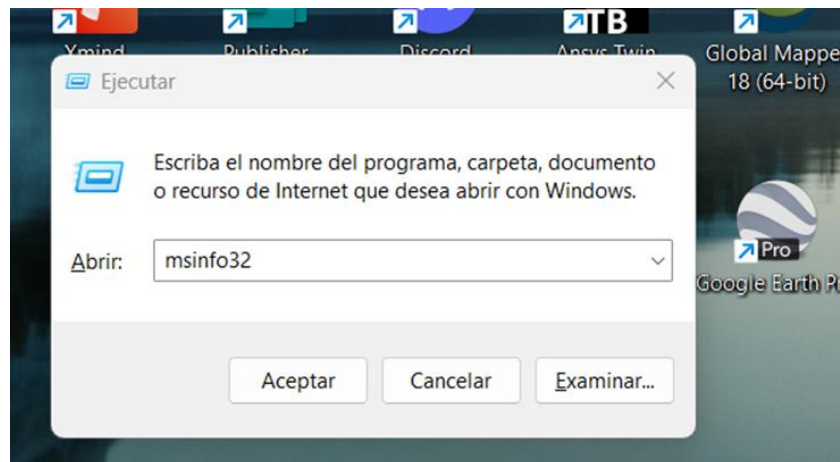
Figura 49. *Error de virtualización durante el arranque de GNS3 VM*



En caso de presentarse el error de virtualización mencionado anteriormente, fue necesario verificar la configuración del sistema operativo relacionada con la seguridad basada en virtualización. Para ello, inicialmente se minimizó VMware Workstation y, mediante la combinación de teclas Windows + R, se abrió la ventana de ejecución de comandos del sistema [66].

Posteriormente, se ingresó el comando **msinfo32** y se seleccionó la opción Aceptar, permitiendo acceder a la ventana de información del sistema operativo, tal como se muestra en la Figura 50 [66].

Figura 50. Ejecución del comando *msinfo32* desde Windows



Una vez abierta la ventana de información del sistema, se procedió a verificar el estado de la opción Seguridad basada en virtualización (Virtualization-Based Security), parámetro que puede generar conflictos con el funcionamiento de VMware Workstation e impedir la correcta ejecución de la máquina virtual GNS3 VM [66].

En el presente caso, dicha funcionalidad se encontraba en estado de ejecución, tal como se evidencia en la Figura 51, por lo que fue necesario deshabilitarla para permitir el correcto arranque de la máquina virtual dentro del entorno VMware [66].

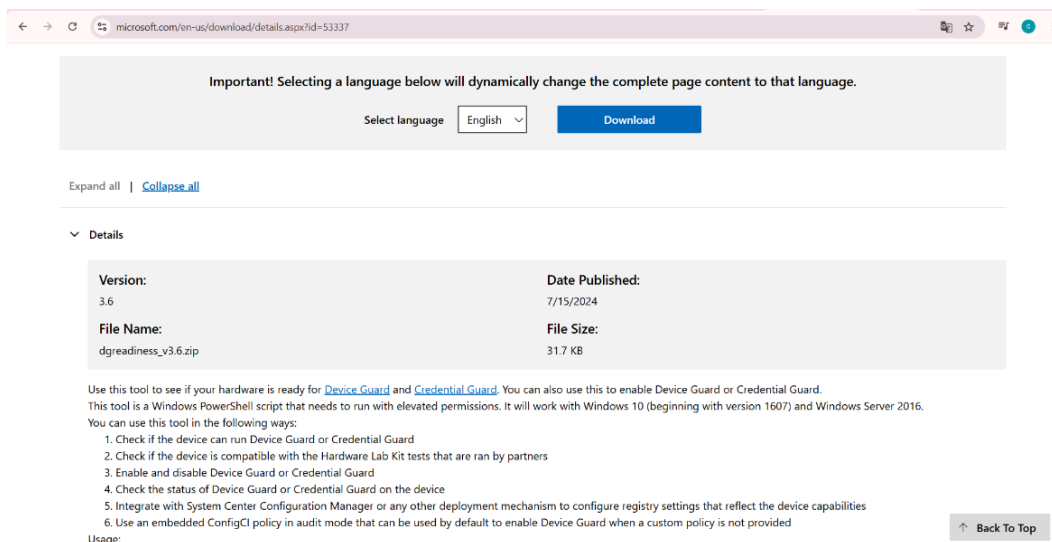
Figura 51. Verificación del estado de seguridad basada en virtualización

tema	Elemento	Valor
Ver	Estado de arranque seguro	Activada
Hardware	Configuración de PCR7	Se necesita elevación de privilegios para ver
Software	Directorio de Windows	C:\WINDOWS
	Directorio del sistema	C:\WINDOWS\system32
	Dispositivo de arranque	\Device\HarddiskVolume1
	Configuración regional	España
	Capa de abstracción de hard...	Versión = "10.0.26100.1"
	Nombre de usuario	DESKTOP-8SKL7TL\elvin
	Zona horaria	Hora est. Pacífico, Sudamérica
	Memoria física instalada (RAM)	16,0 GB
	Memoria física total	15,6 GB
	Memoria física disponible	9,67 GB
	Memoria virtual total	17,6 GB
	Memoria virtual disponible	11,0 GB
	Espacio de archivo de paginac...	2,00 GB
	Archivo de paginación	C:\pagefile.sys
	Protección de DMA de kernel	Activada
	Seguridad basada en virtualiz...	Ejecutándose
	Propiedades de seguridad nec...	
	Propiedades de seguridad dis...	Compatibilidad con la virtualización base, Arranque seguro, Protección de ...
	Servicios configurados para la...	
	Servicios en ejecución para la ...	Hipervisor exige la integridad de código
	Directiva de Control de aplica...	Impuesta
	Directiva de modo de usuario ...	Desactivada
	Compatibilidad automática co...	Se necesita elevación de privilegios para ver
	Se detectó un hipervisor. No s...	

Para solucionar el conflicto relacionado con la seguridad basada en virtualización, fue necesario deshabilitar esta funcionalidad mediante la herramienta de preparación de **Device Guard and Credential Guard**, proporcionada por Microsoft [66].

Como primer paso, se accedió al portal oficial de Microsoft para descargar el archivo comprimido **dgreadiness_v3.6.zip**, utilizado para habilitar o deshabilitar configuraciones relacionadas con la virtualización del sistema operativo. Posteriormente, se procedió a realizar la descarga del archivo correspondiente, tal como se muestra en la Figura 52 [66].

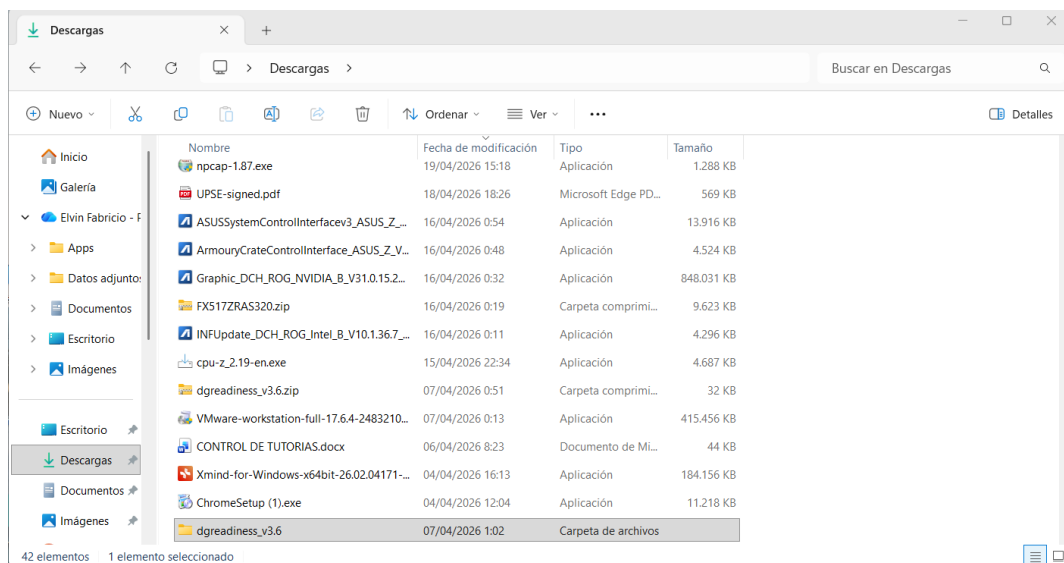
Figura 52. Descarga del archivo *dgreadiness_v3.6.zip* desde el portal oficial de Microsoft



Nota: enlace para descargar el archivo utilizado: <https://www.microsoft.com/en-us/download/details.aspx?id=53337>

Una vez completada la descarga, el archivo se almacenó automáticamente en la carpeta Descargas (Downloads) del sistema operativo. Por consiguiente, se realizó el proceso de descompresión del archivo en la misma ubicación, obteniendo una carpeta que contiene los scripts necesarios para la administración de la seguridad basada en virtualización, como se evidencia en la Figura 53 [66].

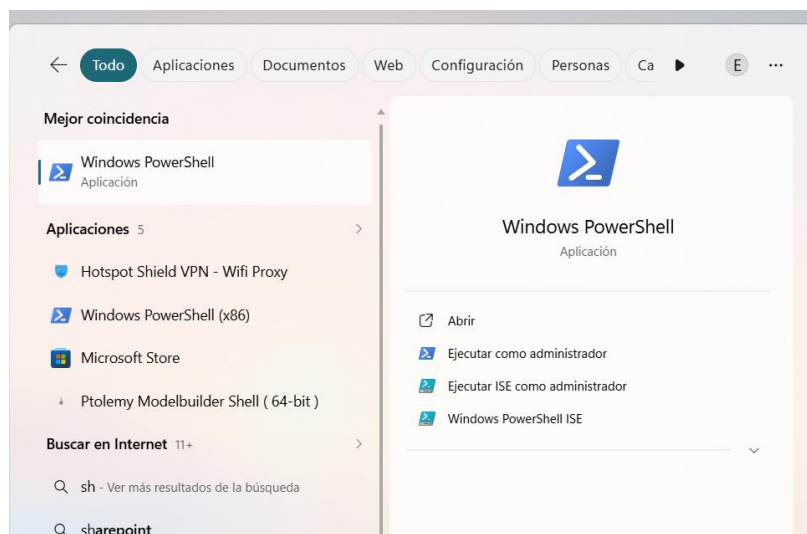
Figura 53. Extracción del archivo *dgreaddiness_v3.6.zip*



Una vez realizada la descarga y extracción del archivo, se procedió a ejecutar una serie de configuraciones en el sistema operativo con el propósito de deshabilitar los servicios de virtualización que generan conflicto con VMware Workstation y la ejecución de GNS3 VM [66].

Como primer paso, se abrió la herramienta Windows PowerShell con privilegios de administrador. Para ello, se buscó la aplicación en el sistema operativo y se seleccionó la opción Ejecutar como administrador, tal como se muestra en la Figura 54 [66].

Figura 54. Ejecución de Windows PowerShell como administrador

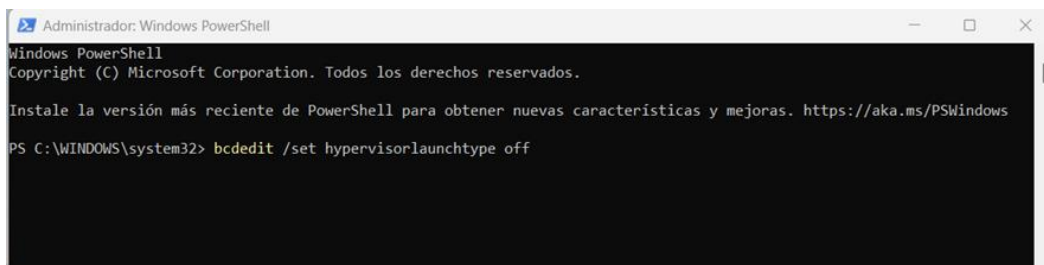


Una vez abierto PowerShell, se procedió a deshabilitar el servicio Hyper-V Hypervisor, responsable de generar incompatibilidad con VMware Workstation. Para ello, se ejecutó el siguiente comando [66]:

```
bcdedit /set hypervisorlaunchtype off
```

Este comando permite impedir el inicio automático del hipervisor de Windows durante el arranque del sistema operativo, reduciendo conflictos relacionados con la virtualización de hardware. La ejecución correcta del comando se presenta en la Figura 55 [66].

Figura 55. *Desactivación del hipervisor mediante PowerShell*



Posteriormente, fue necesario acceder a la carpeta donde se encontraba almacenado el archivo descargado **dgreadiness_v3.6.zip**, previamente extraído dentro de la carpeta Downloads (Descargas) del sistema operativo [66].

Para ello, desde PowerShell se realizó la navegación entre directorios utilizando comandos de acceso a carpetas. Es importante mencionar que el nombre de usuario puede variar dependiendo del equipo utilizado; en el presente caso se empleó el usuario elvin, razón por la cual la ruta utilizada corresponde a dicho nombre [66].

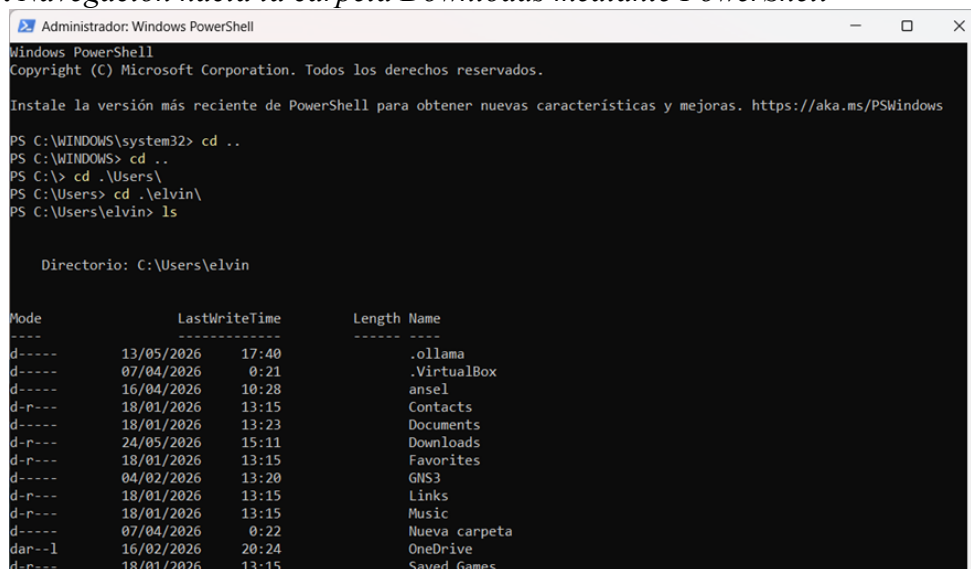
Los comandos ejecutados para acceder a la carpeta del usuario y localizar el directorio Downloads se muestran a continuación [66]:

```
cd..  
cd..  
cd.\Users\
```

```
cd.\elvin\
ls
```

Estos comandos permitieron desplazarse hasta la carpeta del usuario y visualizar las carpetas disponibles dentro del sistema, facilitando la localización del directorio Downloads, tal como se evidencia en la Figura 56 [66].

Figura 56. *Navegación hacia la carpeta Downloads mediante PowerShell*

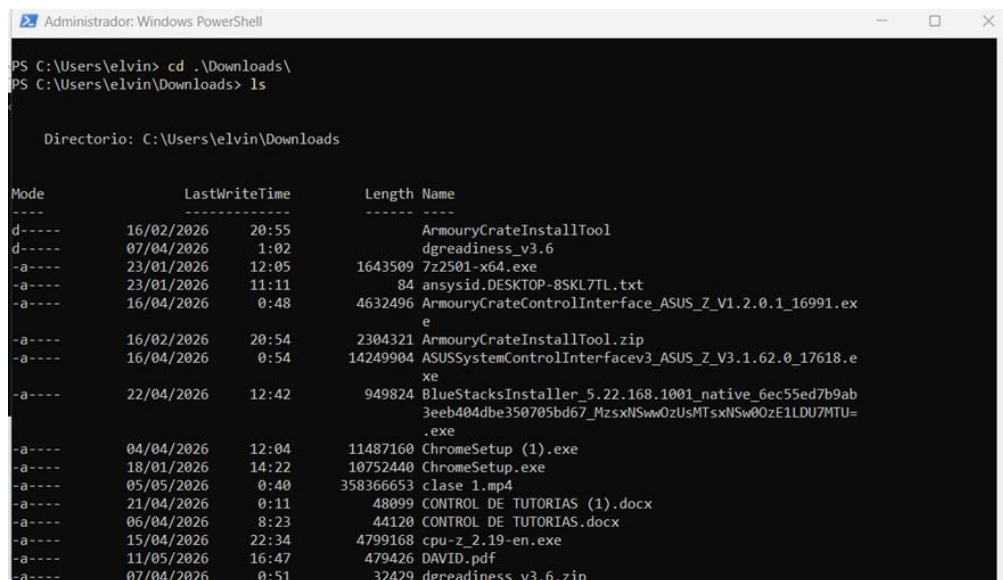


Posteriormente, se procedió a ingresar a la carpeta Downloads (Descargas) mediante comandos de navegación en PowerShell, permitiendo localizar el directorio correspondiente al archivo previamente descargado. Para ello, se ejecutaron los siguientes comandos [66]:

```
cd .\Downloads\
ls
```

La ejecución de estos comandos permitió acceder a la carpeta de descargas y visualizar los archivos contenidos en ella, incluyendo el directorio `dgreediness_v3.6`, tal como se muestra en la Figura 57 [66].

Figura 57. Acceso a la carpeta Downloads desde PowerShell



```

Administrador: Windows PowerShell

PS C:\Users\elvin> cd .\Downloads\
PS C:\Users\elvin\Downloads> ls

Directorio: C:\Users\elvin\Downloads

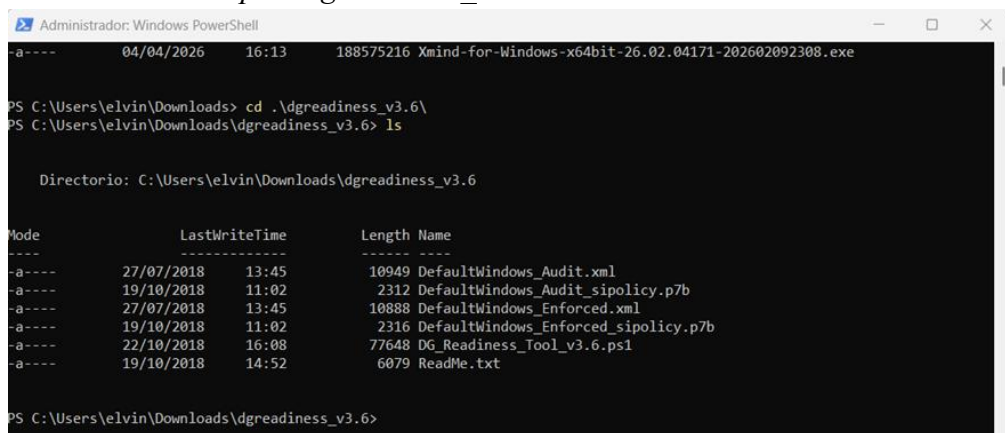
Mode                LastWriteTime         Length Name
----                -
d-----         16/02/2026    20:55             ArmouryCrateInstallTool
d-----         07/04/2026     1:02             dgreaddiness_v3.6
-a-----        23/01/2026    12:05    1643509 7z2501-x64.exe
-a-----        23/01/2026    11:11         84 ansysid.DESKTOP-8SKL7TL.txt
-a-----        16/04/2026     0:48    4632496 ArmouryCrateControlInterface_ASUS_Z_V1.2.0.1_16991.exe
-a-----        16/02/2026    20:54    2304321 ArmouryCrateInstallTool.zip
-a-----        16/04/2026     0:54    14249904 ASUSSystemControlInterfacev3_ASUS_Z_V3.1.62.0_17618.exe
-a-----        22/04/2026    12:42    949824 BlueStacksInstaller_5.22.168.1001_native_6ec55ed7b9ab3eeb404dbe350705bd67_MzSxNSwW0zUsMTsXNSw0zE1LDU7MTU=.exe
-a-----         04/04/2026    12:04    11487160 ChromeSetup (1).exe
-a-----        18/01/2026    14:22    10752440 ChromeSetup.exe
-a-----        05/05/2026     0:40    358366653 clase 1.mp4
-a-----        21/04/2026     0:11     48099 CONTROL DE TUTORIAS (1).docx
-a-----        06/04/2026     8:23     44120 CONTROL DE TUTORIAS.docx
-a-----        15/04/2026    22:34    4799168 cpu-z_2.19-en.exe
-a-----        11/05/2026    16:47    479426 DAVID.pdf
-a-----        07/04/2026     0:51     32429 dgreaddiness_v3.6.zip
  
```

Una vez identificado el directorio correspondiente, se procedió a ingresar a la carpeta `dgreaddiness_v3.6` mediante el siguiente comando [66]:

```
cd .\dgreaddiness_v3.6\

ls
```

Este procedimiento permitió verificar el contenido de la carpeta y localizar el script `DG_Readiness_Tool_v3.6.ps1`, encargado de administrar las configuraciones relacionadas con la seguridad basada en virtualización del sistema operativo. En la Figura 58 se muestra el acceso a dicha carpeta [66].

Figura 58. Acceso a la carpeta *dgreadiness_v3.6*


```

Administrador: Windows PowerShell
-a---- 04/04/2026 16:13 188575216 Xmind-for-Windows-x64bit-26.02.04171-202602092308.exe

PS C:\Users\elvin\Downloads> cd .\dgreadiness_v3.6\
PS C:\Users\elvin\Downloads\dgreadiness_v3.6> ls

Directorio: C:\Users\elvin\Downloads\dgreadiness_v3.6

Mode                LastWriteTime         Length Name
-----
-a----          27/07/2018   13:45           10949 DefaultWindows_Audit.xml
-a----          19/10/2018   11:02            2312 DefaultWindows_Audit_sipolicy.p7b
-a----          27/07/2018   13:45           10888 DefaultWindows_Enforced.xml
-a----          19/10/2018   11:02            2316 DefaultWindows_Enforced_sipolicy.p7b
-a----          22/10/2018   16:08           77648 DG_Readiness_Tool_v3.6.ps1
-a----          19/10/2018   14:52            6079 ReadMe.txt

PS C:\Users\elvin\Downloads\dgreadiness_v3.6>

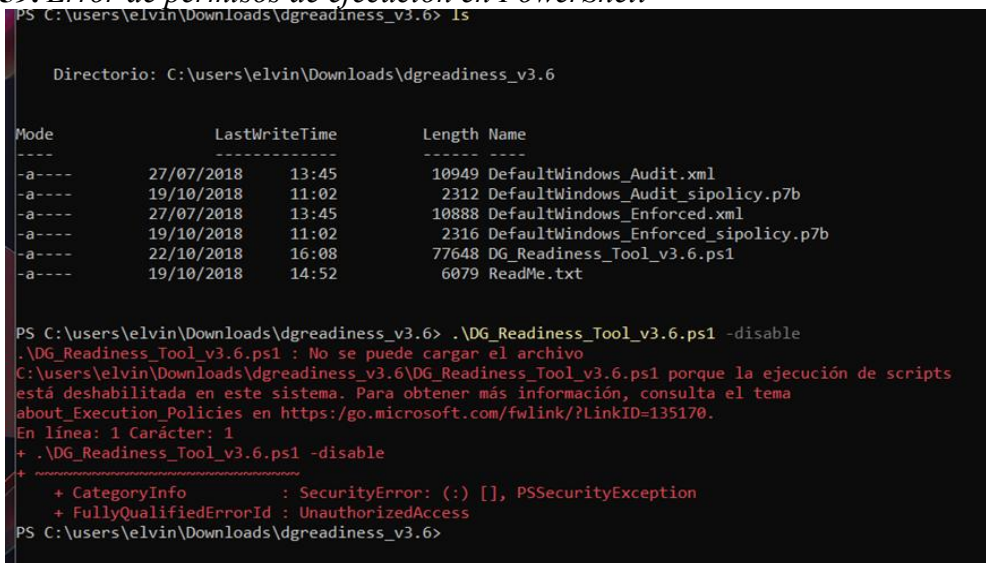
```

Posteriormente, se ejecutó el script con el parámetro `-disable`, permitiendo deshabilitar las funcionalidades de seguridad relacionadas con Device Guard y Credential Guard, responsables de generar conflictos con VMware Workstation [66].

Para ello, se ingresó el siguiente comando:

```
.\DG_Readiness_Tool_v3.6.ps1 -disable
```

Sin embargo, en algunos casos el sistema puede impedir la ejecución del script debido a restricciones de seguridad de PowerShell, generando un error de permisos similar al mostrado en la Figura 59 [66].

Figura 59. Error de permisos de ejecución en PowerShell


```

PS C:\users\elvin\Downloads\dgreadiness_v3.6> ls

Directorio: C:\users\elvin\Downloads\dgreadiness_v3.6

Mode                LastWriteTime         Length Name
-----
-a----          27/07/2018   13:45           10949 DefaultWindows_Audit.xml
-a----          19/10/2018   11:02            2312 DefaultWindows_Audit_sipolicy.p7b
-a----          27/07/2018   13:45           10888 DefaultWindows_Enforced.xml
-a----          19/10/2018   11:02            2316 DefaultWindows_Enforced_sipolicy.p7b
-a----          22/10/2018   16:08           77648 DG_Readiness_Tool_v3.6.ps1
-a----          19/10/2018   14:52            6079 ReadMe.txt

PS C:\users\elvin\Downloads\dgreadiness_v3.6> .\DG_Readiness_Tool_v3.6.ps1 -disable
.\DG_Readiness_Tool_v3.6.ps1 : No se puede cargar el archivo
C:\users\elvin\Downloads\dgreadiness_v3.6\DG_Readiness_Tool_v3.6.ps1 porque la ejecución de scripts
está deshabilitada en este sistema. Para obtener más información, consulta el tema
about_Execution_Policies en https://go.microsoft.com/fwlink/?LinkID=135170.
En línea: 1 Carácter: 1
+ ~.\DG_Readiness_Tool_v3.6.ps1 -disable
+ ~~~~~
+ CategoryInfo          : SecurityError: (:) [], PSSecurityException
+ FullyQualifiedErrorId : UnauthorizedAccess

PS C:\users\elvin\Downloads\dgreadiness_v3.6>

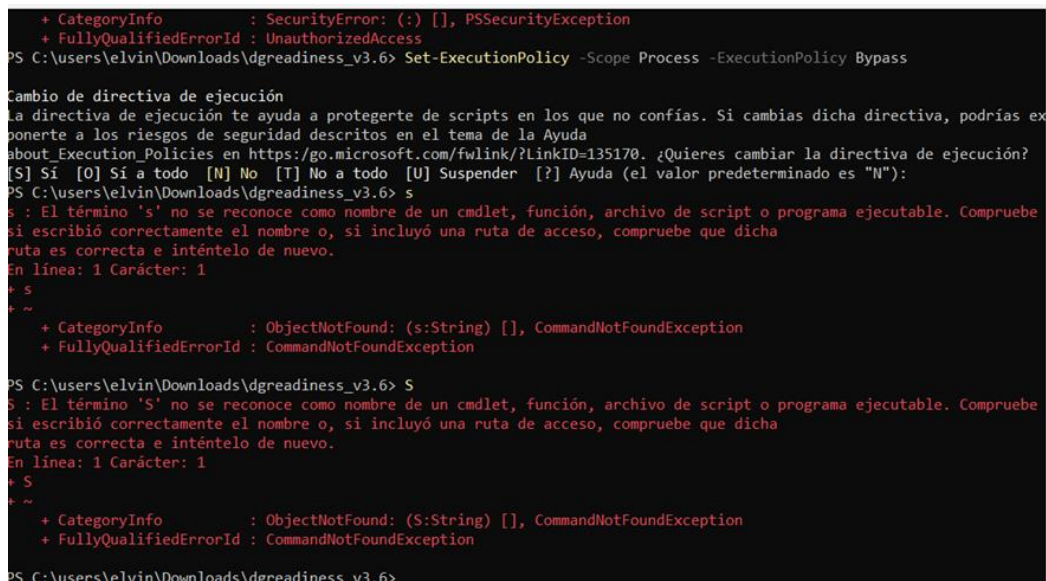
```

Para solucionar este inconveniente, fue necesario modificar temporalmente la política de ejecución de PowerShell, permitiendo la ejecución del script dentro de la sesión activa. Para ello, se ejecutó el siguiente comando [66]:

```
Set-ExecutionPolicy -Scope Process -ExecutionPolicy Bypass
```

Una vez ejecutado el comando, el sistema solicitó confirmación del procedimiento, debiendo ingresar la opción S (Sí) y posteriormente presionar la tecla Enter, tal como se evidencia en la Figura 60 [66].

Figura 60. *Modificación temporal de la política de ejecución en PowerShell*



```
+ CategoryInfo          : SecurityError: (:) [], PSSecurityException
+ FullyQualifiedErrorId : UnauthorizedAccess

PS C:\users\elvin\Downloads\dgreediness_v3.6> Set-ExecutionPolicy -Scope Process -ExecutionPolicy Bypass

Cambio de directiva de ejecución
La directiva de ejecución te ayuda a protegerte de scripts en los que no confías. Si cambias dicha directiva, podrías exponerte a los riesgos de seguridad descritos en el tema de la Ayuda
about_Execution_Policies en https://go.microsoft.com/fwlink/?LinkID=135170. ¿Quieres cambiar la directiva de ejecución?
[S] Sí [O] No [T] No a todo [U] Suspender [?] Ayuda (el valor predeterminado es "N"):
PS C:\users\elvin\Downloads\dgreediness_v3.6> S
S : El término 'S' no se reconoce como nombre de un cmdlet, función, archivo de script o programa ejecutable. Compruebe si escribió correctamente el nombre o, si incluyó una ruta de acceso, compruebe que dicha ruta es correcta e inténtelo de nuevo.
En línea: 1 Carácter: 1
+ S
+ ~
+ CategoryInfo          : ObjectNotFound: (S:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

PS C:\users\elvin\Downloads\dgreediness_v3.6> S
S : El término 'S' no se reconoce como nombre de un cmdlet, función, archivo de script o programa ejecutable. Compruebe si escribió correctamente el nombre o, si incluyó una ruta de acceso, compruebe que dicha ruta es correcta e inténtelo de nuevo.
En línea: 1 Carácter: 1
+ S
+ ~
+ CategoryInfo          : ObjectNotFound: (S:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

PS C:\users\elvin\Downloads\dgreediness_v3.6>
```

Finalmente, se volvió a ejecutar el script de desactivación mediante el siguiente comando [66]:

```
.\DG_Readiness_Tool_v3.6.ps1 -disable
```

Si el procedimiento se ejecuta correctamente, el sistema mostrará un mensaje indicando que la desactivación fue realizada con éxito, tal como se presenta en la Figura 61 [66].

Figura 61. Ejecución exitosa del script *DG_Readiness_Tool_v3.6.ps1*

```

especificados.
ERROR: El sistema no ha podido encontrar la clave o el valor del Registro
especificados.
ERROR: El sistema no ha podido encontrar la clave o el valor del Registro
especificados.
ERROR: El sistema no ha podido encontrar la clave o el valor del Registro
especificados.
ERROR: El sistema no ha podido encontrar la clave o el valor del Registro
especificados.
del : No se encuentra la ruta de acceso 'C:\WINDOWS\System32\CodeIntegrity\SIPolicy.p7b' porque no existe.
En línea: 1 Carácter: 1
+ del "$env:windir\System32\CodeIntegrity\SIPolicy.p7b"
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (C:\WINDOWS\Syst...ty\SIPolicy.p7b:String) [Remove-Item], ItemNotFoundEx
ception
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.RemoveItemCommand

Disabling Hyper-V and IOMMU
Disabling Hyper-V failed please check the log file
Copy-Item : No se encuentra la ruta de acceso 'C:\WINDOWS\System32\SecConfig.efi' porque no existe.
En C:\Users\elvin\Downloads\dgreadiness_v3.6\DG_Readiness_Tool_v3.6.ps1: 1246 Carácter: 22
+ ... CmdOutput = Copy-Item "$env:windir\System32\SecConfig.efi" $FreeDrive ...
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (C:\WINDOWS\System32\SecConfig.efi:String) [Copy-Item], ItemNotFoundExce
ption
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.CopyItemCommand

Please reboot the machine, for settings to be applied.
PS C:\Users\elvin\Downloads\dgreadiness_v3.6>

```

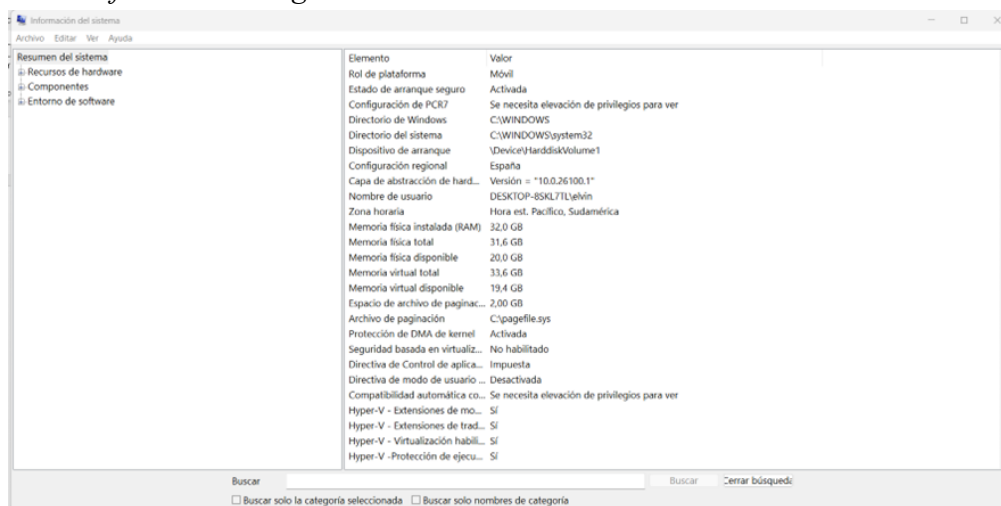
Para completar el proceso de deshabilitación de la seguridad basada en virtualización, fue necesario reiniciar el sistema operativo con el propósito de aplicar los cambios realizados previamente mediante PowerShell [66].

Durante el reinicio del equipo, el sistema presentó una pantalla de configuración relacionada con la aplicación de cambios de seguridad. En esta etapa fue necesario confirmar el procedimiento seleccionando la opción correspondiente mediante la tecla F3, la cual permitió continuar con el proceso de desactivación hasta completar la carga normal del sistema operativo Windows [66].

Una vez reiniciado el equipo, se procedió nuevamente a verificar el estado de la seguridad basada en virtualización. Para ello, mediante la combinación de teclas Windows + R, se abrió la ventana de ejecución del sistema y se ingresó nuevamente el comando `msinfo32`, seleccionando posteriormente la opción Aceptar [66].

Al acceder a la ventana de información del sistema, se verificó que el parámetro Seguridad basada en virtualización se encontraba deshabilitado, confirmando la correcta aplicación del procedimiento realizado, tal como se muestra en la Figura 62 [66].

Figura 62. Verificación de seguridad basada en virtualización deshabilitada



Finalmente, al ejecutar nuevamente la máquina virtual GNS3 VM dentro de VMware Workstation, el error relacionado con la virtualización del procesador dejó de presentarse, permitiendo el correcto arranque del entorno virtual y garantizando la continuidad del proceso de simulación de la red WISP [66].

3.4.2. Integración de GNS3 con la máquina virtual GNS3 VM

Una vez verificado el correcto funcionamiento de la máquina virtual en VMware Workstation, se procedió a realizar el enlace entre GNS3 y GNS3 VM, permitiendo optimizar el rendimiento del entorno de simulación y garantizar la correcta ejecución de los dispositivos virtuales empleados en el desarrollo de la red WISP [65].

Para ello, inicialmente se accedió al software GNS3 y desde el menú principal se seleccionó la ruta Edit > Preferences > GNS3 VM, permitiendo ingresar al panel de configuración de la máquina virtual [65].

Dentro del apartado de configuración de GNS3 VM, se establecieron los parámetros necesarios para enlazar correctamente la máquina virtual con el entorno de simulación. En primer lugar, se habilitó la opción Enable the GNS3 VM, permitiendo activar el uso de la máquina virtual dentro del software [65].

Posteriormente, en el apartado Virtualization Engine, se seleccionó la opción VMware Workstation/Player (Recommended), debido a su compatibilidad y estabilidad con el entorno de virtualización utilizado [65].

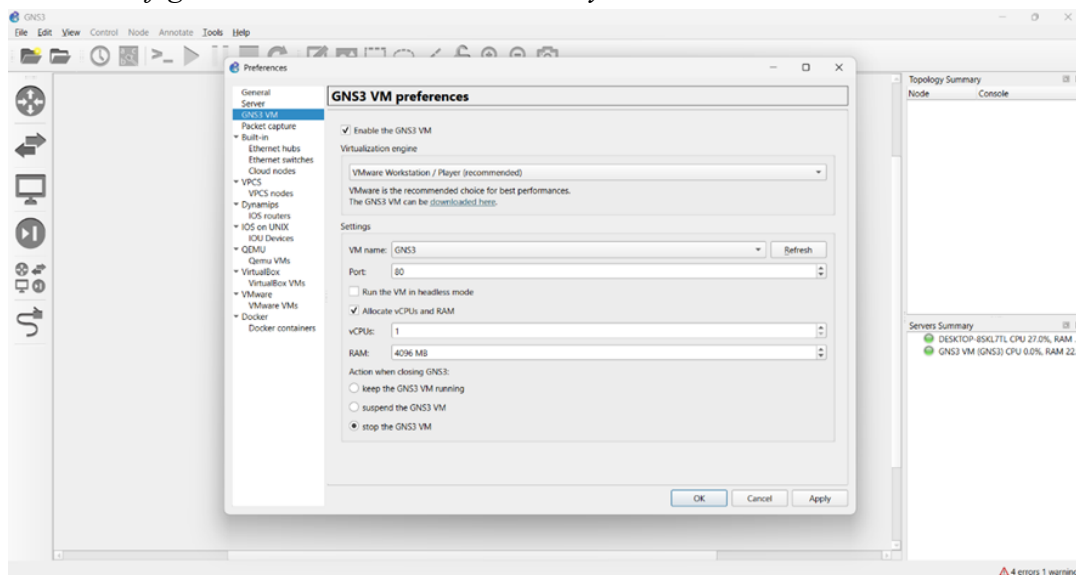
Asimismo, en el parámetro VM Name, se seleccionó la máquina virtual previamente importada, la cual fue identificada con el nombre GNS3; el puerto de comunicación fue conservado con la configuración predeterminada (80), mientras que los recursos asignados a la máquina virtual fueron establecidos de la siguiente manera [65]:

- vCPUs: 1
- RAM: 4096 MB

Adicionalmente, en el parámetro Action when closing GNS3, se seleccionó la opción Stop the GNS3 VM, permitiendo detener automáticamente la máquina virtual al cerrar el software GNS3. Aunque esta configuración es opcional, facilita la administración del entorno de simulación [65].

Finalmente, se seleccionaron las opciones Apply y OK, completando el proceso de integración entre GNS3 y VMware Workstation, tal como se muestra en la Figura 63 [65].

Figura 63. Configuración del enlace entre GNS3 y GNS3 VM



Una vez realizado este procedimiento, el entorno de simulación quedó correctamente enlazado, permitiendo ejecutar dispositivos virtuales mediante la máquina GNS3 VM sin inconvenientes de rendimiento o compatibilidad.

3.4.3. Instalación de dispositivos MikroTik en GNS3

Por defecto, GNS3 no incorpora dispositivos específicos preconfigurados para escenarios WISP, razón por la cual fue necesario instalar manualmente los equipos virtuales empleados durante el desarrollo del prototipo [52].

Para ello, se accedió al panel lateral izquierdo del software, específicamente al apartado Routers, y posteriormente se seleccionó la opción New Template, ubicada en la parte superior del panel [52].

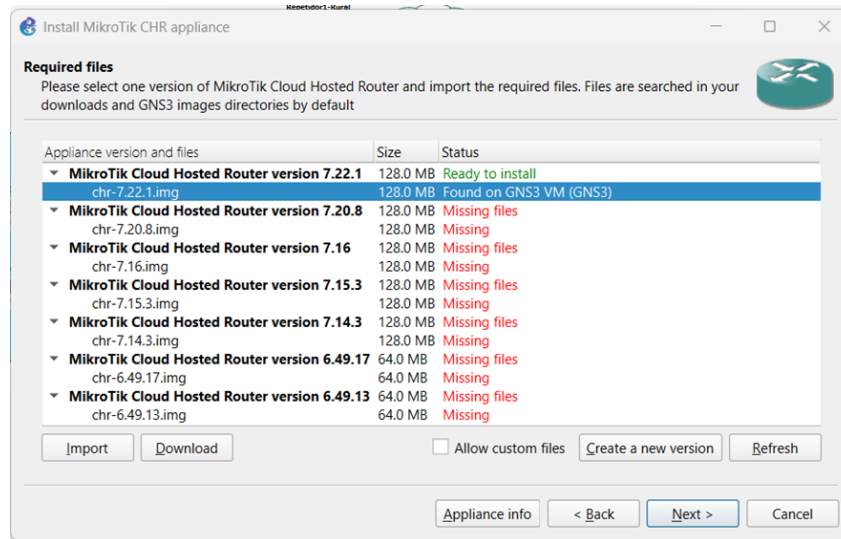
Una vez abierta la ventana de creación de plantillas, se seleccionó la opción Install an appliance from the GNS3 server (recommended) y posteriormente se presionó Next, permitiendo acceder al catálogo de dispositivos disponibles dentro del servidor de GNS3 [52].

Dentro del catálogo de dispositivos, se seleccionó la categoría Routers, donde se buscó el equipo MikroTik CHR (Cloud Hosted Router), utilizado posteriormente para representar los routers del entorno WISP [52].

Una vez seleccionado el dispositivo, se presionó la opción Install y posteriormente Next hasta llegar al apartado de selección de versiones disponibles. En este punto, se seleccionó la versión más reciente disponible y se procedió con la descarga del archivo correspondiente [52].

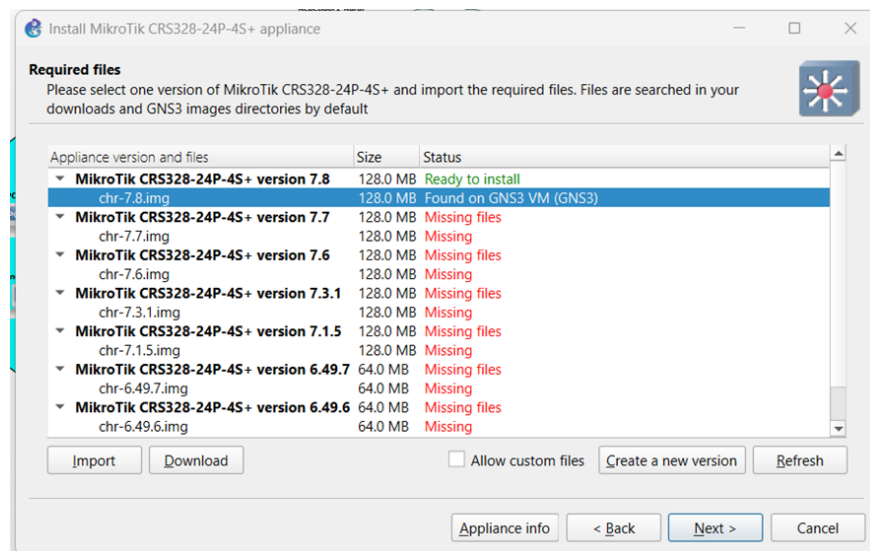
Posteriormente, el archivo descargado fue descomprimido e importado dentro del entorno GNS3. Una vez completado el proceso, la versión instalada apareció correctamente identificada en color verde, indicando que el dispositivo se encontraba listo para su utilización dentro del software, tal como se observa en la Figura 64 [52].

Figura 64. *Instalación del router MikroTik CHR en GNS3*



De forma similar, se realizó la instalación del switch MikroTik CRS, siguiendo el mismo procedimiento utilizado para el router MikroTik CHR. Una vez completada la instalación, el dispositivo quedó disponible dentro del panel de equipos de GNS3, permitiendo su utilización dentro de la topología de red propuesta [52].

Figura 65. *Instalación del switch MikroTik CRS en GNS3*



3.4.4. Selección de dispositivos para el prototipo WISP

Una vez instalados los dispositivos virtuales, se procedió a definir los equipos que formarían parte de la topología de red implementada dentro de GNS3.

Para el desarrollo del prototipo, se utilizó el router MikroTik CHR como dispositivo principal (core router), así como para los routers de clientes correspondientes a los sectores rural, urbano y empresarial [60].

Debido a que GNS3 no permite simular enlaces inalámbricos reales de forma nativa, se optó por utilizar routers MikroTik CHR configurados en modo bridge, con el propósito de representar funcionalmente las antenas sectoriales principales, los equipos CPE de clientes y los equipos de backup implementados dentro de cada segmento de red.

Por otra parte, el dispositivo MikroTik CRS fue empleado para representar el switch administrable principal, encargado de la segmentación lógica y distribución de tráfico dentro de la red WISP simulada [59].

La equivalencia funcional de los equipos utilizados dentro del entorno de simulación se presenta en la Tabla 36 [59].

Tabla 36. *Equivalencia de dispositivos implementados en GNS3*

Equipo real	Dispositivo simulado en GNS3	Función
Router principal	MikroTik CHR	Core principal
Antena sectorial	MikroTik CHR (Bridge)	Distribución PTMP
Antena CPE	MikroTik CHR (Bridge)	Recepción cliente
Backup	MikroTik CHR (Bridge)	Extensión de señal
Router cliente	MikroTik CHR	Red LAN cliente
Switch administrable	MikroTik CRS	Segmentación y distribución

Posteriormente, se dio inicio al proceso de configuración de los dispositivos que conforman la red WISP simulada.

3.4.5. Configuración del Router_Core (Gateway Central)

El presente apartado describe el procedimiento de configuración del nodo central de la infraestructura de red, denominado Router_Core, encargado de desempeñar funciones

fundamentales dentro de la arquitectura WISP propuesta. Entre sus principales responsabilidades se encuentran el enrutamiento inter-VLAN, la resolución de nombres de dominio (DNS), la traducción de direcciones de red (NAT) y la asignación de puertas de enlace (gateways) para los segmentos rural, urbano, empresarial y de gestión [53].

El Router_Core constituye el dispositivo principal de comunicación dentro de la topología de red, permitiendo la interconexión entre los diferentes segmentos implementados y proporcionando acceso a internet para los dispositivos de la infraestructura [53].

Configuración de identidad del sistema y conectividad WAN

Como etapa inicial de configuración, se estableció la identidad lógica del dispositivo dentro de la topología, permitiendo su identificación durante los procesos de administración y monitoreo de red. Posteriormente, se configuró un cliente DHCP sobre la interfaz orientada al proveedor de servicios (ISP), con el propósito de obtener automáticamente direccionamiento IP, servidores DNS y la ruta por defecto hacia internet [53].

Para definir la identidad del router principal se empleó el siguiente comando:

```
# Definir la identidad del router central

/system identity set name="Router_Core"
```

Posteriormente, se habilitó el cliente DHCP sobre la interfaz ether1, utilizada como interfaz WAN del sistema:

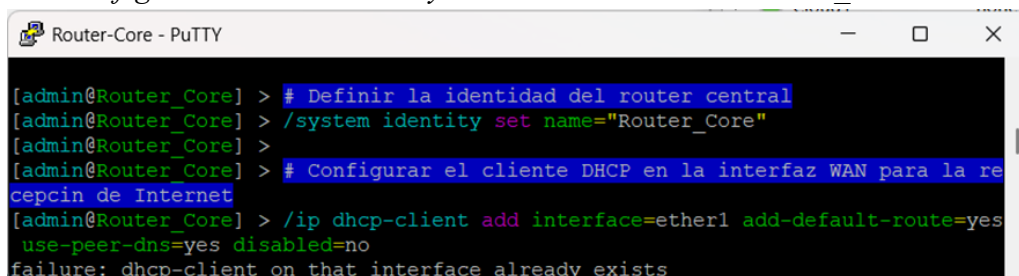
```
# Configurar el cliente DHCP en la interfaz WAN para la recepción de
internet

/ip dhcp-client add interface=ether1 add-default-route=yes use-peer-
dns=yes disabled=no
```

La configuración anterior permite que el Router_Core reciba automáticamente los parámetros de red proporcionados por el proveedor de internet, garantizando la conectividad externa del prototipo implementado [53].

En la Figura 66 se evidencia la configuración aplicada al Router_Core, donde se observa la asignación de identidad del dispositivo y la habilitación del cliente DHCP sobre la interfaz WAN para la obtención automática de conectividad hacia internet.

Figura 66. Configuración de identidad y conectividad WAN del Router_Core



```
[admin@Router_Core] > # Definir la identidad del router central
[admin@Router_Core] > /system identity set name="Router_Core"
[admin@Router_Core] >
[admin@Router_Core] > # Configurar el cliente DHCP en la interfaz WAN para la re
cepción de Internet
[admin@Router_Core] > /ip dhcp-client add interface=ether1 add-default-route=yes
use-peer-dns=yes disabled=no
failure: dhcp-client on that interface already exists
```

Segmentación de red mediante VLAN (Capa 2)

Con el propósito de aislar los dominios de difusión (broadcast domains) y organizar el tráfico correspondiente a los diferentes sectores de cobertura de la red WISP, se implementó un esquema de segmentación lógica mediante VLAN (Virtual Local Area Network), utilizando el protocolo IEEE 802.1Q sobre una interfaz troncal física [53].

La implementación de VLAN permitió separar el tráfico de los sectores rural, urbano, empresarial y de gestión, optimizando la administración de red, reduciendo el tráfico innecesario entre segmentos y fortaleciendo el control lógico de la infraestructura [53].

- **Preparación de la interfaz troncal**

Como primera etapa, se realizó el renombramiento de la interfaz física encargada del transporte troncal, con el objetivo de mantener coherencia en la nomenclatura empleada dentro del diseño de red y facilitar la administración de los dispositivos [53].

Para ello, se utilizó el siguiente comando:

```
/interface set ether2 name=ether2-WISP-Troncal
```

Posteriormente, se procedió a la creación de las interfaces virtuales VLAN sobre la interfaz troncal configurada.

- **Creación de interfaces VLAN**

Se declararon los identificadores VLAN (VLAN IDs) correspondientes a cada uno de los segmentos de red implementados en el prototipo WISP.

VLAN 10 – Sector Rural

```
# Creación de la VLAN para el Sector Rural

/interface vlan add name=VLAN10_Rural vlan-id=10 interface=ether2-WISP-
Troncal
```

VLAN 20 – Sector Urbano

```
# Creación de la VLAN para el Sector Urbano

/interface vlan add name=VLAN20_Urbano vlan-id=20 interface=ether2-WISP-
Troncal
```

VLAN 30 – Sector Empresas

```
# Creación de la VLAN para el Sector Empresas

/interface vlan add name=VLAN30_Empresas vlan-id=30 interface=ether2-
WISP-Troncal
```

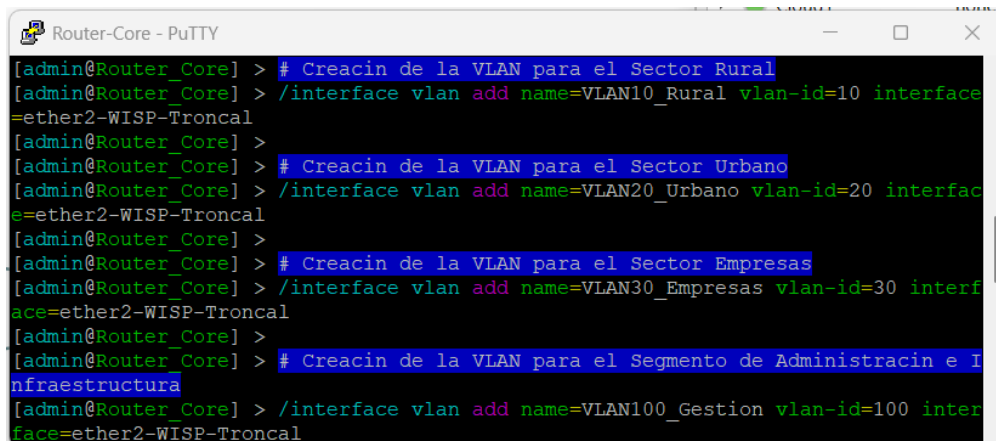
VLAN 100 – Gestión e Infraestructura

```
# Creación de la VLAN para el Segmento de Administración e Infraestructura

/interface vlan add name=VLAN100_Gestion vlan-id=100 interface=ether2-
WISP-Troncal
```

La configuración anterior permitió establecer una separación lógica del tráfico entre los distintos sectores implementados en la red, posibilitando una mejor administración de recursos, segmentación de servicios y control de comunicaciones dentro del entorno simulado [53].

En la Figura 67 se evidencia la configuración de segmentación lógica aplicada en el Router_Core, donde se observa la creación de las interfaces VLAN correspondientes a los sectores rural, urbano, empresarial y de gestión sobre la interfaz troncal principal.

Figura 67. Configuración de VLAN en el Router_Core


```

[admin@Router_Core] > # Creacin de la VLAN para el Sector Rural
[admin@Router_Core] > /interface vlan add name=VLAN10_Rural vlan-id=10 interface=ether2-WISP-Troncal
[admin@Router_Core] >
[admin@Router_Core] > # Creacin de la VLAN para el Sector Urbano
[admin@Router_Core] > /interface vlan add name=VLAN20_Urbano vlan-id=20 interface=ether2-WISP-Troncal
[admin@Router_Core] >
[admin@Router_Core] > # Creacin de la VLAN para el Sector Empresas
[admin@Router_Core] > /interface vlan add name=VLAN30_Empresas vlan-id=30 interface=ether2-WISP-Troncal
[admin@Router_Core] >
[admin@Router_Core] > # Creacin de la VLAN para el Segmento de Administracin e Infraestructura
[admin@Router_Core] > /interface vlan add name=VLAN100_Gestion vlan-id=100 interface=ether2-WISP-Troncal

```

Direccionamiento IP y configuraci3n de gateways (Capa 3)

Una vez establecidas las interfaces l3gicas VLAN, se procedi3 a la asignaci3n del direccionamiento IPv4 correspondiente a cada segmento de red implementado dentro del prototipo WISP. Estas direcciones cumplen la funci3n de puertas de enlace predeterminadas (default gateways), permitiendo la comunicaci3n entre los distintos dispositivos pertenecientes a cada VLAN y facilitando el enrutamiento hacia otros segmentos de la red [53].

La asignaci3n de direccionamiento se realiz3 considerando una estructura jer3rquica organizada por sectores, permitiendo diferenciar el tr3fico correspondiente a las zonas rural, urbana, empresarial y de gesti3n, optimizando la administraci3n de red y facilitando el control del tr3fico interno [53].

Asignaci3n de direccionamiento IPv4 por segmento

VLAN 10 – Sector Rural

Se asign3 la direcci3n 10.0.10.1/24, utilizada como puerta de enlace predeterminada para los dispositivos pertenecientes al sector rural.

```

# Asignaci3n de IP Gateway para el Sector Rural (VLAN 10)

/ip address add address=10.0.10.1/24 interface=VLAN10_Rural

```

VLAN 20 – Sector Urbano

Para el segmento urbano se configuró la dirección 10.0.20.1/24, encargada de actuar como gateway de la red correspondiente.

```
# Asignación de IP Gateway para el Sector Urbano (VLAN 20)

/ip address add address=10.0.20.1/24 interface=VLAN20_Urbano
```

VLAN 30 – Sector Empresas

En el caso del segmento empresarial, se asignó la dirección 10.0.30.1/24 como puerta de enlace principal.

```
# Asignación de IP Gateway para el Sector Empresas (VLAN 30)

/ip address add address=10.0.30.1/24 interface=VLAN30_Empresas
```

VLAN 100 – Gestión e Infraestructura

Finalmente, para el segmento de administración y gestión de red se configuró la dirección 10.0.100.1/24, destinada al control de infraestructura y monitoreo del sistema.

```
# Asignación de IP Gateway para el Segmento de Administración (VLAN 100)

/ip address add address=10.0.100.1/24 interface=VLAN100_Gestion
```

La configuración del direccionamiento IP permitió establecer la estructura de comunicación de Capa 3 dentro del prototipo, garantizando que los dispositivos pertenecientes a cada segmento puedan comunicarse correctamente mediante sus respectivas puertas de enlace [53].

En la Figura 68 se evidencia la configuración del direccionamiento IPv4 implementado en el Router_Core, donde se observan las direcciones IP asignadas a cada interfaz VLAN utilizadas como gateways para los diferentes segmentos de red.

Figura 68. Configuración de direccionamiento IPv4 en el Router_Core

```

Router-Core - PuTTY
[admin@Router_Core] > # Asignacin de IP Gateway para el Sector Rural (VLAN 10)
[admin@Router_Core] > /ip address add address=10.0.10.1/24 interface=VLAN10_Rural
[admin@Router_Core] >
[admin@Router_Core] > # Asignacin de IP Gateway para el Sector Urbano (VLAN 20)
[admin@Router_Core] > /ip address add address=10.0.20.1/24 interface=VLAN20_Urbano
[admin@Router_Core] >
[admin@Router_Core] > # Asignacin de IP Gateway para el Sector Empresas (VLAN 30)
[admin@Router_Core] > /ip address add address=10.0.30.1/24 interface=VLAN30_Empresas
[admin@Router_Core] >
[admin@Router_Core] > # Asignacin de IP Gateway para el Segmento de Administraci
[admin@Router_Core] > n (VLAN 100)
[admin@Router_Core] > /ip address add address=10.0.100.1/24 interface=VLAN100_Gestion

```

Servicios de red y mecanismos de transmisión (NAT / DNS)

Con el propósito de garantizar el acceso a internet y la correcta resolución de nombres dentro de la red WISP, se implementaron mecanismos de servicios de red relacionados con DNS (Domain Name System) y NAT (Network Address Translation). Estas configuraciones permiten que los dispositivos internos puedan resolver dominios de internet y transmitir tráfico hacia redes externas utilizando direccionamiento privado [53].

- **Configuración del servicio DNS**

Como primera etapa, se configuraron servidores DNS públicos, permitiendo al Router_Core procesar solicitudes de resolución de nombres provenientes de los diferentes segmentos de red. Asimismo, se habilitaron las solicitudes remotas, permitiendo que el router actúe como intermediario de resolución DNS para los clientes conectados [53].

La configuración realizada se presenta a continuación:

```
/ip dns set servers=8.8.8.8,8.8.4.4 allow-remote-requests=yes
```

La configuración anterior permite utilizar los servidores DNS públicos de Google, optimizando el acceso a servicios externos y reduciendo problemas asociados a la resolución de nombres de dominio [53].

- **Configuración de NAT (Masquerade)**

Posteriormente, se implementó una regla de traducción de direcciones de red (Source NAT), utilizando el mecanismo de masquerade, con el objetivo de permitir que las direcciones privadas internas pertenecientes a las VLAN implementadas sean traducidas dinámicamente hacia la dirección IP asignada en la interfaz WAN (ether1) [53].

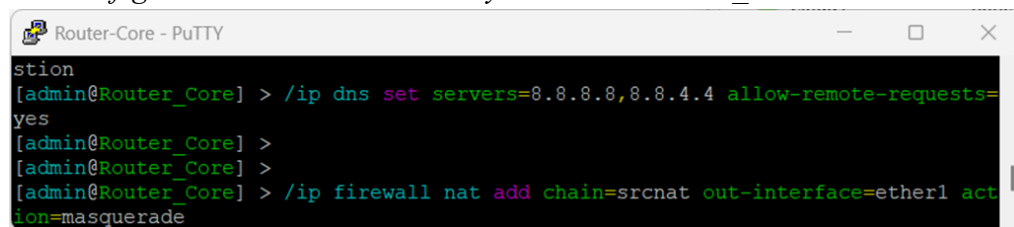
La configuración aplicada fue la siguiente:

```
/ip firewall nat add chain=srcnat out-interface=ether1 action=masquerade
```

Esta configuración permite que los dispositivos pertenecientes a las redes privadas 10.0.X.X puedan establecer comunicación con redes externas, posibilitando el acceso a internet mediante una única dirección IP obtenida dinámicamente desde el proveedor de servicios [53].

En la Figura 69 se evidencia la configuración de los servicios DNS y NAT implementados en el Router_Core, donde se observa la habilitación de la resolución de nombres y el mecanismo de traducción de direcciones necesario para el acceso hacia redes externas.

Figura 69. Configuración de servicios DNS y NAT en el Router_Core



```
Router-Core - PuTTY
stion
[admin@Router_Core] > /ip dns set servers=8.8.8.8,8.8.4.4 allow-remote-requests=
yes
[admin@Router_Core] >
[admin@Router_Core] >
[admin@Router_Core] > /ip firewall nat add chain=srcnat out-interface=ether1 act
ion=masquerade
```

3.4.6. Configuración del Switch_Administrable

El presente apartado describe el procedimiento de configuración del Switch_Administrable, encargado de la distribución del tráfico dentro de la infraestructura WISP propuesta. Este dispositivo cumple la función de transportar el tráfico segmentado mediante VLAN entre el Router_Core y los diferentes segmentos de red implementados, permitiendo mantener la separación lógica de los servicios y facilitando la administración centralizada del sistema [53].

Para el desarrollo del prototipo se utilizó un dispositivo MikroTik CRS, configurado bajo el estándar IEEE 802.1Q, permitiendo el transporte de múltiples VLAN a través de enlaces troncales [53].

Configuración de identidad y estructura base de conmutación

Como primera etapa de configuración, se estableció la identidad lógica del switch dentro de la topología de red, permitiendo una identificación clara durante las tareas de administración y monitoreo [53].

Para ello, se configuró el nombre del dispositivo mediante el siguiente comando:

```
# Definir la identidad unívoca del switch administrador

/system identity set name="Switch_Administrable"
```

Posteriormente, se creó un Bridge principal destinado al transporte lógico del tráfico segmentado. Durante esta fase inicial, el filtrado de VLAN se mantuvo deshabilitado (vlan-filtering=no) con el propósito de facilitar la incorporación de interfaces físicas antes de implementar las políticas definitivas de segmentación [53].

La configuración aplicada fue la siguiente:

```
# Crear la entidad Bridge principal de transporte lógico

/interface bridge add name=Bridge_Tesis vlan-filtering=no
```

Una vez creado el Bridge principal, se asociaron las interfaces físicas encargadas de la interconexión entre el Router_Core y los dispositivos de distribución de la red.

```
# Asociar las interfaces físicas ether1 (Uplink) y ether2 (Downlink) al
Bridge

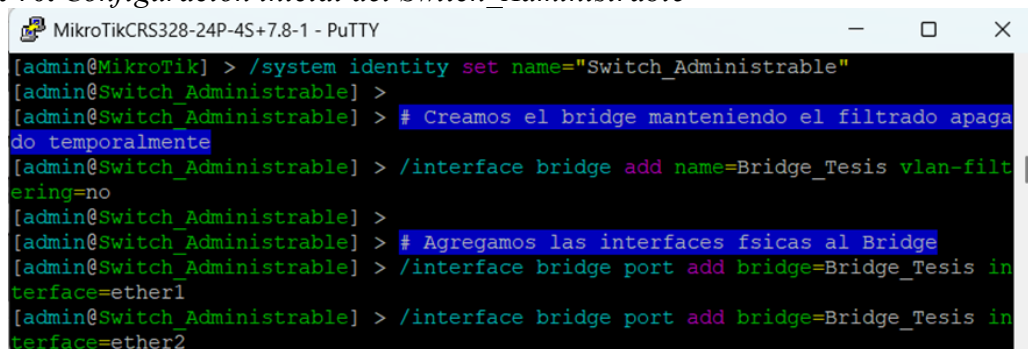
/interface bridge port add bridge=Bridge_Tesis interface=ether1

/interface bridge port add bridge=Bridge_Tesis interface=ether2
```

La configuración anterior permitió establecer la estructura base de conmutación necesaria para el transporte del tráfico VLAN dentro del entorno de simulación implementado [53].

En la Figura 70 se evidencia la configuración inicial aplicada al Switch_Administrable, donde se observa la asignación de identidad del dispositivo, la creación del Bridge principal y la asociación de las interfaces físicas utilizadas para el transporte troncal de la red.

Figura 70. Configuración inicial del Switch_Administrable



```

MikroTikCRS328-24P-4S+7.8-1 - PuTTY
[admin@MikroTik] > /system identity set name="Switch_Administrable"
[admin@Switch_Administrable] >
[admin@Switch_Administrable] > # Creamos el bridge manteniendo el filtrado apaga
do temporalmente
[admin@Switch_Administrable] > /interface bridge add name=Bridge_Tesis vlan-filt
ering=no
[admin@Switch_Administrable] >
[admin@Switch_Administrable] > # Agregamos las interfaces fsicas al Bridge
[admin@Switch_Administrable] > /interface bridge port add bridge=Bridge_Tesis in
terface=ether1
[admin@Switch_Administrable] > /interface bridge port add bridge=Bridge_Tesis in
terface=ether2

```

Configuración de la interfaz de gestión, direccionamiento IP y servicio DNS

Con el propósito de separar el tráfico de administración de la infraestructura respecto al tráfico generado por los usuarios finales, se implementó una interfaz lógica de gestión sobre la VLAN 100, destinada exclusivamente a la administración de dispositivos de red [53].

En primer lugar, se creó una interfaz virtual asociada al Bridge principal, permitiendo establecer un segmento independiente para la administración del switch dentro de la red WISP [53].

La configuración aplicada fue la siguiente:

```

# Crear la interfaz virtual de gestión sobre el dominio de aislamiento
VLAN 100

/interface      vlan      add      name=VLAN100_Gestion_SW      vlan-id=100
interface=Bridge_Tesis

```

Posteriormente, se asignó una dirección IPv4 estática correspondiente al segmento de gestión, permitiendo la administración remota del dispositivo dentro de la red implementada [53].

```
# Asignar la dirección IP fija de infraestructura correspondiente al
Switch
```

```
/ip address add address=10.0.100.2/24 interface=VLAN100_Gestion_SW
```

Una vez configurado el direccionamiento IP, se estableció la ruta predeterminada hacia el Router_Core, permitiendo la comunicación entre el switch y el resto de la infraestructura de red [53].

```
# Declarar la ruta estática por defecto apuntando al Gateway Central
(Router_Core)
```

```
/ip route add gateway=10.0.100.1
```

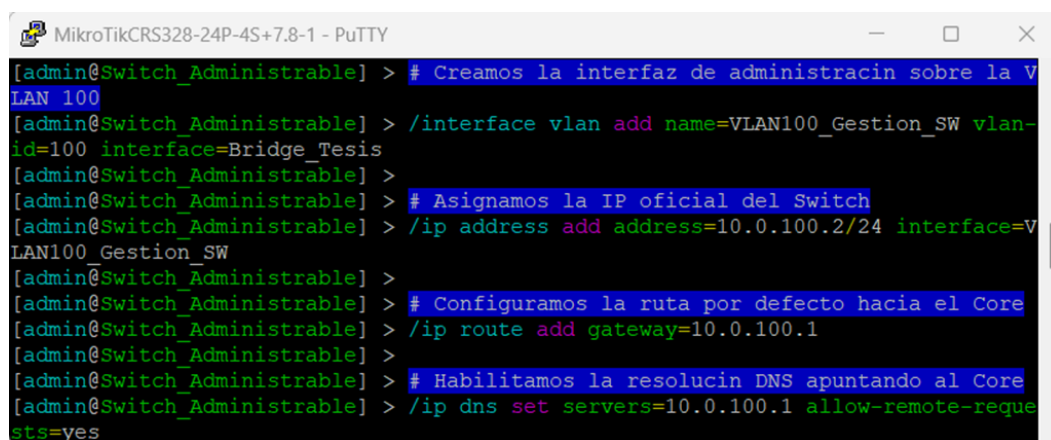
Finalmente, se configuró el servicio de resolución de nombres (DNS), delegando las solicitudes hacia el servidor configurado en el nodo central de la red, facilitando así procesos de conectividad, diagnóstico y administración.

```
# Parametrizar el servidor DNS local delegando las peticiones al nodo
central
```

```
/ip dns set servers=10.0.100.1 allow-remote-requests=yes
```

En la Figura 71 se evidencia la configuración aplicada al segmento de gestión del Switch_Administrable, incluyendo la creación de la interfaz VLAN 100, la asignación del direccionamiento IPv4, la configuración de la puerta de enlace predeterminada y el servicio DNS utilizado para la administración del dispositivo.

Figura 71. Configuración de la interfaz de gestión del Switch_Administrable



```
MikroTikCRS328-24P-4S+7.8-1 - PuTTY
[admin@Switch_Administrable] > # Creamos la interfaz de administracin sobre la V
LAN 100
[admin@Switch_Administrable] > /interface vlan add name=VLAN100_Gestion_SW vlan-
id=100 interface=Bridge_Tesis
[admin@Switch_Administrable] >
[admin@Switch_Administrable] > # Asignamos la IP oficial del Switch
[admin@Switch_Administrable] > /ip address add address=10.0.100.2/24 interface=V
LAN100_Gestion_SW
[admin@Switch_Administrable] >
[admin@Switch_Administrable] > # Configuramos la ruta por defecto hacia el Core
[admin@Switch_Administrable] > /ip route add gateway=10.0.100.1
[admin@Switch_Administrable] >
[admin@Switch_Administrable] > # Habilitamos la resolucin DNS apuntando al Core
[admin@Switch_Administrable] > /ip dns set servers=10.0.100.1 allow-remote-reque
sts=yes
```

Configuración de enlaces troncales mediante VLAN (Trunking)

Con el objetivo de permitir el transporte simultáneo de múltiples segmentos de red sobre las interfaces físicas del switch, se implementó la configuración de enlaces troncales (Trunk) mediante el protocolo IEEE 802.1Q. Este mecanismo permitió transportar las diferentes VLAN definidas en el proyecto a través de un único medio físico, manteniendo la segmentación lógica del tráfico correspondiente a cada sector [53].

Para ello, se declararon explícitamente las VLAN correspondientes al sector rural (VLAN 10), sector urbano (VLAN 20), sector empresarial (VLAN 30) y segmento de gestión e infraestructura (VLAN 100) como tráfico etiquetado (Tagged) sobre las interfaces físicas de interconexión utilizadas entre el Router_Core y el Switch_Administrable [53].

La configuración aplicada fue la siguiente:

Registro de la VLAN 10 correspondiente al sector rural:

```
# Registrar el transporte de la VLAN 10 (Sector Rural) en los enlaces
troncales

/interface      bridge      vlan      add      bridge=Bridge_Tesis
tagged=Bridge_Tesis,ether1,ether2 vlan-ids=10
```

Registro de la VLAN 20 correspondiente al sector urbano:

```
# Registrar el transporte de la VLAN 20 (Sector Urbano) en los enlaces
troncales

/interface      bridge      vlan      add      bridge=Bridge_Tesis
tagged=Bridge_Tesis,ether1,ether2 vlan-ids=20
```

Registro de la VLAN 30 correspondiente al sector empresarial:

```
# Registrar el transporte de la VLAN 30 (Sector Empresarial) en los
enlaces troncales

/interface      bridge      vlan      add      bridge=Bridge_Tesis
tagged=Bridge_Tesis,ether1,ether2 vlan-ids=30
```

Registro de la VLAN 100 correspondiente al segmento de gestión e infraestructura:

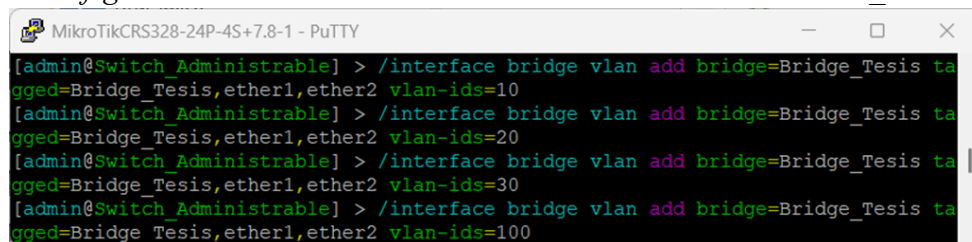
```
# Registrar el transporte de la VLAN 100 (Sector Gestión) en los enlaces
troncales
```

```
/interface bridge vlan add bridge=Bridge_Tesis
tagged=Bridge_Tesis,ether1,ether2 vlan-ids=100
```

La configuración anterior permitió establecer un esquema de transporte troncal entre dispositivos, garantizando la correcta circulación del tráfico segmentado sin perder el aislamiento lógico entre redes.

En la Figura 72 se evidencia la configuración de las VLAN transportadas a través del enlace troncal implementado en el Switch_Administrable, donde se observa la asignación de tráfico etiquetado para los diferentes segmentos de red definidos en el prototipo WISP.

Figura 72. Configuración de enlaces troncales mediante VLAN en el Switch_Administrable



```
MikroTikCRS328-24P-4S+7.8-1 - PuTTY
[admin@Switch_Administrable] > /interface bridge vlan add bridge=Bridge_Tesis ta
gged=Bridge_Tesis,ether1,ether2 vlan-ids=10
[admin@Switch_Administrable] > /interface bridge vlan add bridge=Bridge_Tesis ta
gged=Bridge_Tesis,ether1,ether2 vlan-ids=20
[admin@Switch_Administrable] > /interface bridge vlan add bridge=Bridge_Tesis ta
gged=Bridge_Tesis,ether1,ether2 vlan-ids=30
[admin@Switch_Administrable] > /interface bridge vlan add bridge=Bridge_Tesis ta
gged=Bridge_Tesis,ether1,ether2 vlan-ids=100
```

Configuración de seguridad y activación del filtrado de VLAN

Como etapa final de la configuración del Switch_Administrable, se habilitó el mecanismo de filtrado de VLAN sobre el Bridge principal, permitiendo aplicar de forma efectiva la segmentación lógica previamente establecida [53].

La activación del filtrado garantiza que únicamente el tráfico perteneciente a las VLAN configuradas pueda circular a través de las interfaces definidas, contribuyendo al ordenamiento del tráfico y al aislamiento entre segmentos de red [53].

Para ello, se habilitó el filtrado de VLAN en el Bridge principal mediante el siguiente comando:

```
# Activar el filtrado de VLAN definitivo a nivel de hardware/software

/interface bridge set Bridge_Tesis vlan-filtering=yes
```

Posteriormente, se configuraron las interfaces físicas utilizadas como enlaces troncales (ether1 y ether2) para permitir únicamente tráfico etiquetado bajo el estándar IEEE 802.1Q, evitando el paso de tramas no identificadas dentro de la infraestructura de red [53].

La configuración aplicada fue la siguiente:

```
# Forzar restricción perimetral: admitir únicamente tramas etiquetadas en
ether1 y ether2

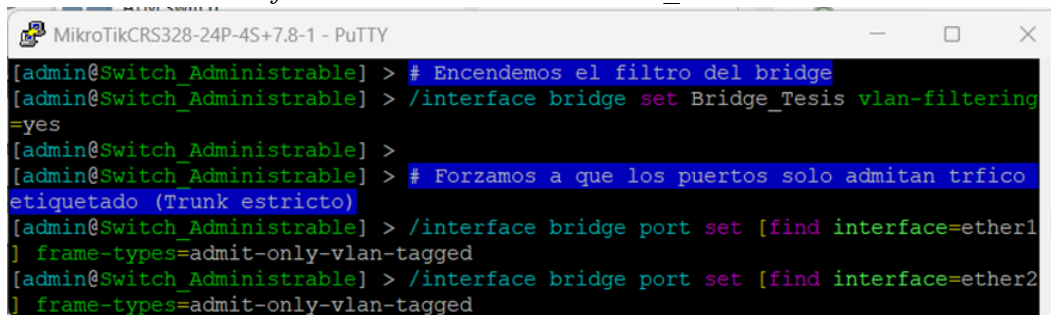
/interface bridge port set [find interface=ether1] frame-types=admit-
only-vlan-tagged

/interface bridge port set [find interface=ether2] frame-types=admit-
only-vlan-tagged
```

Esta configuración permitió reforzar el funcionamiento de la segmentación implementada, asegurando que las VLAN definidas fueran transportadas correctamente a través de los enlaces troncales del sistema [53].

En la Figura 73 se evidencia la configuración final aplicada al Switch_Administrable, donde se observa la activación del filtrado de VLAN y la restricción de tráfico etiquetado en las interfaces utilizadas para el transporte troncal de la red.

Figura 73. Activación del filtrado de VLAN en el Switch_Administrable



```
MikroTikCRS328-24P-4S+7.8-1 - PuTTY
[admin@Switch_Administrable] > # Encendemos el filtro del bridge
[admin@Switch_Administrable] > /interface bridge set Bridge_Tesis vlan-filtering
=yes
[admin@Switch_Administrable] >
[admin@Switch_Administrable] > # Forzamos a que los puertos solo admitan trfco
etiquetado (Trunk estricto)
[admin@Switch_Administrable] > /interface bridge port set [find interface=ether1
] frame-types=admit-only-vlan-tagged
[admin@Switch_Administrable] > /interface bridge port set [find interface=ether2
] frame-types=admit-only-vlan-tagged
```

3.4.7. Configuración de Antena_Sectorial_Principal (Sector Rural)

El presente apartado describe el procedimiento de configuración de la Antena_Sectorial_Principal, encargada de distribuir el servicio inalámbrico hacia el sector rural dentro de la topología WISP propuesta. Debido a las limitaciones de simulación inalámbrica

presentes en GNS3, este dispositivo fue representado mediante un router MikroTik CHR configurado en modo Bridge, permitiendo simular el comportamiento de una antena sectorial de distribución [53].

Dentro de la arquitectura diseñada, este equipo cumple la función de transportar el tráfico correspondiente a la VLAN 10 (Sector Rural), permitiendo la interconexión entre el nodo de distribución y los dispositivos cliente del segmento rural [53].

Configuración de identidad y estructura Bridge

Como primera etapa de configuración, se definió la identidad lógica del dispositivo dentro de la topología, facilitando su identificación durante las tareas de administración y monitoreo de red [53].

Para ello, se asignó el nombre correspondiente mediante el siguiente comando:

```
# Definir la identidad institucional de la estación base sectorial
/system identity set name="Antena_Sectorial_Principal"
```

Posteriormente, se creó una interfaz de tipo Bridge, utilizada para transportar el tráfico entre las interfaces físicas del dispositivo. Durante esta fase inicial, el filtrado de VLAN se mantuvo deshabilitado (vlan-filtering=no) con el propósito de facilitar la incorporación de interfaces antes de aplicar la segmentación definitiva [53].

La configuración implementada fue la siguiente:

```
# Inicializar el Bridge de transporte general
/interface bridge add name=Bridge_Sectorial vlan-filtering=no
```

Una vez creado el Bridge principal, se procedió a asociar las interfaces físicas encargadas del transporte de datos dentro del enlace.

La interfaz ether1 fue configurada como puerto de entrada (uplink) desde el Switch_Administrable, mientras que la interfaz ether2 fue destinada al enlace de salida (downlink) hacia el segmento rural [53].

```
# Asociar el puerto físico Ethernet de entrada (uplink desde el Switch de
Distribución)
```

```
/interface bridge port add bridge=Bridge_Sectorial interface=ether1
```

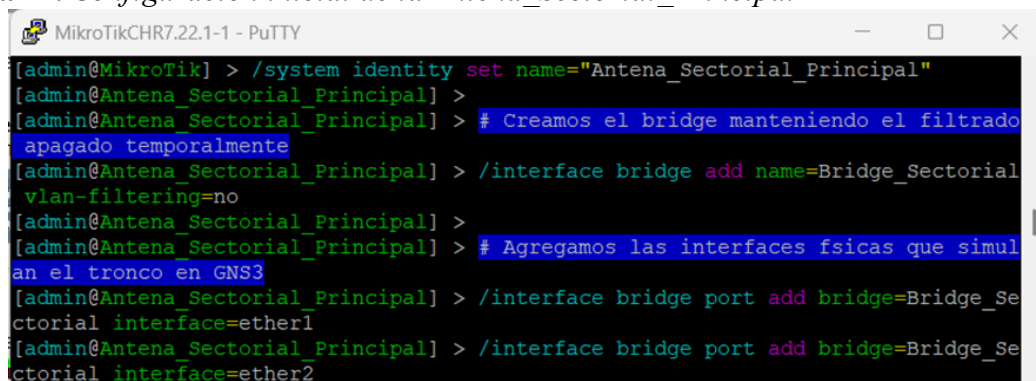
```
# Asociar el puerto físico de bajada (Downlink asignado al enlace de
última milla)
```

```
/interface bridge port add bridge=Bridge_Sectorial interface=ether2
```

Esta configuración permitió establecer una estructura de transporte transparente entre dispositivos, facilitando el paso del tráfico correspondiente al sector rural dentro del entorno de simulación implementado [53].

En la Figura 74 se evidencia la configuración inicial aplicada a la Antena_Sectorial_Principal, donde se observa la asignación de identidad del dispositivo, la creación del Bridge de transporte y la asociación de interfaces físicas utilizadas para la interconexión del segmento rural.

Figura 74. Configuración inicial de la Antena_Sectorial_Principal



```
MikroTikCHR7.22.1-1 - PuTTY
[admin@MikroTik] > /system identity set name="Antena_Sectorial_Principal"
[admin@Antena_Sectorial_Principal] >
[admin@Antena_Sectorial_Principal] > # Creamos el bridge manteniendo el filtrado
apagado temporalmente
[admin@Antena_Sectorial_Principal] > /interface bridge add name=Bridge_Sectorial
vlan-filtering=no
[admin@Antena_Sectorial_Principal] >
[admin@Antena_Sectorial_Principal] > # Agregamos las interfaces físicas que simul
an el tronco en GNS3
[admin@Antena_Sectorial_Principal] > /interface bridge port add bridge=Bridge_Se
ctorial interface=ether1
[admin@Antena_Sectorial_Principal] > /interface bridge port add bridge=Bridge_Se
ctorial interface=ether2
```

Configuración de la interfaz de gestión, direccionamiento IP y servicio DNS

Con el propósito de mantener separado el tráfico de administración respecto al tráfico de usuarios finales, se implementó una interfaz lógica de gestión sobre la VLAN 100, destinada exclusivamente a la administración de la infraestructura de red.

Para ello, se creó una subinterfaz virtual asociada al Bridge_Sectorial, permitiendo integrar el dispositivo dentro del segmento de gestión previamente definido en la topología de red [53].

La configuración aplicada fue la siguiente:

```
# Crear la interfaz virtual de gestión aislada sobre el dominio de la
VLAN 100
```

```
/interface      vlan      add      name=VLAN100_Gestion_Antena      vlan-id=100
interface=Bridge_Sectorial
```

Posteriormente, se asignó una dirección IPv4 estática correspondiente al segmento de gestión, permitiendo la identificación y administración remota de la Antena_Sectorial_Principal dentro de la red implementada.

```
# Asignar la dirección IP fija de infraestructura asignada a la estación
base
```

```
/ip address add address=10.0.100.10/24 interface=VLAN100_Gestion_Antena
```

Una vez configurado el direccionamiento IP, se estableció la puerta de enlace predeterminada hacia el Router_Core, permitiendo la comunicación del dispositivo con el resto de la infraestructura de red.

```
# Declarar la ruta estática por defecto apuntando al Gateway Central
(Router_Core)
```

```
/ip route add gateway=10.0.100.1
```

Finalmente, se configuró el servicio de resolución de nombres (DNS), delegando las solicitudes hacia el servidor definido en el nodo central de la red para facilitar procesos de administración y conectividad [53].

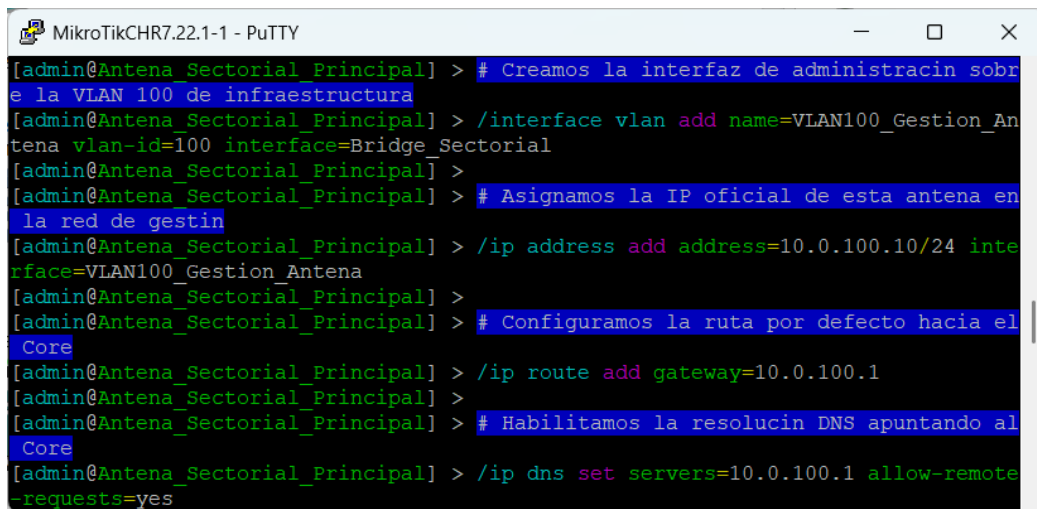
```
# Habilitar la resolución DNS delegando las peticiones al servidor caché
del núcleo
```

```
/ip dns set servers=10.0.100.1 allow-remote-requests=yes
```

Esta configuración permitió integrar la antena sectorial al segmento de administración, facilitando el monitoreo y acceso remoto del dispositivo dentro del entorno de simulación implementado [53].

En la Figura 75 se evidencia la configuración aplicada a la interfaz de gestión de la Antena_Sectorial_Principal, donde se observa la creación de la VLAN de administración, la asignación del direccionamiento IPv4, la configuración de la puerta de enlace y el servicio DNS correspondiente al segmento de gestión.

Figura 75. Configuración de la interfaz de gestión de la Antena_Sectorial_Principal



```

MikroTikCHR7.22.1-1 - PuTTY
[admin@Antena_Sectorial_Principal] > # Creamos la interfaz de administracin sobre
e la VLAN 100 de infraestructura
[admin@Antena_Sectorial_Principal] > /interface vlan add name=VLAN100_Gestion_An
tena vlan-id=100 interface=Bridge_Sectorial
[admin@Antena_Sectorial_Principal] >
[admin@Antena_Sectorial_Principal] > # Asignamos la IP oficial de esta antena en
la red de gestin
[admin@Antena_Sectorial_Principal] > /ip address add address=10.0.100.10/24 inte
rface=VLAN100_Gestion_Antena
[admin@Antena_Sectorial_Principal] >
[admin@Antena_Sectorial_Principal] > # Configuramos la ruta por defecto hacia el
Core
[admin@Antena_Sectorial_Principal] > /ip route add gateway=10.0.100.1
[admin@Antena_Sectorial_Principal] >
[admin@Antena_Sectorial_Principal] > # Habilitamos la resolucin DNS apuntando al
Core
[admin@Antena_Sectorial_Principal] > /ip dns set servers=10.0.100.1 allow-remote
-requests=yes
  
```

Configuración de canales troncales y activación del filtrado VLAN

Con el propósito de garantizar la correcta segmentación del tráfico dentro de la red WISP, se realizó la configuración de los canales troncales encargados del transporte de las VLAN utilizadas en el sector rural. Esta configuración permitió mantener separado el tráfico de usuarios finales del tráfico de administración, evitando interferencias entre ambos segmentos de red [53].

Para ello, se registraron de forma explícita las VLAN autorizadas dentro del Bridge_Sectorial, definiendo el transporte de la VLAN 10, correspondiente al tráfico de datos del sector rural, y la VLAN 100, destinada exclusivamente al tráfico de administración y monitoreo de infraestructura [53].

La configuración aplicada fue la siguiente:

```

# Registrar de forma estática las VLAN autorizadas en los enlaces de
transporte
  
```

```

/interface      bridge      vlan      add      bridge=Bridge_Sectorial
tagged=Bridge_Sectorial,ether1,ether2 vlan-ids=10

```

```

/interface      bridge      vlan      add      bridge=Bridge_Sectorial
tagged=Bridge_Sectorial,ether1,ether2 vlan-ids=100

```

Posteriormente, se habilitó el mecanismo de filtrado VLAN sobre el Bridge principal, permitiendo al dispositivo operar bajo el estándar IEEE 802.1Q y garantizando que únicamente el tráfico autorizado pueda circular por el enlace configurado [53].

```

# Activar el filtrado de VLAN definitivo a nivel de hardware/software

/interface bridge set Bridge_Sectorial vlan-filtering=yes

```

Finalmente, se estableció una política de restricción sobre las interfaces físicas del enlace, permitiendo exclusivamente el ingreso de tramas etiquetadas (Tagged) y evitando el tránsito de paquetes sin identificación VLAN o tráfico no autorizado.

```

# Forzar restricción perimetral: admitir únicamente tramas etiquetadas en
ambos extremos

/interface bridge port set [find interface=ether1] frame-types=admit-
only-vlan-tagged

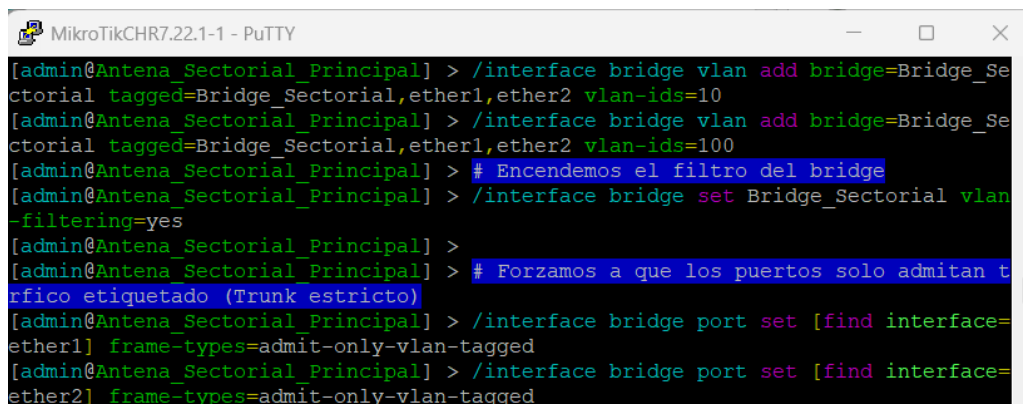
/interface bridge port set [find interface=ether2] frame-types=admit-
only-vlan-tagged

```

Esta configuración permitió asegurar el transporte adecuado de las VLAN definidas dentro de la infraestructura inalámbrica, garantizando la segmentación lógica del tráfico y fortaleciendo el control sobre los enlaces de comunicación implementados en el entorno de simulación [53].

En la Figura 76 se evidencia la configuración realizada sobre la Antena_Sectorial_Principal, donde se observa el registro de las VLAN autorizadas, la habilitación del filtrado VLAN y la restricción de tramas etiquetadas en los puertos físicos del enlace.

Figura 76. Configuración de canales troncales y filtrado VLAN de la Antena_Sectorial_Principal



```

MikroTikCHR7.22.1-1 - PuTTY
[admin@Antena_Sectorial_Principal] > /interface bridge vlan add bridge=Bridge_Sectorial tagged=Bridge_Sectorial,ether1,ether2 vlan-ids=10
[admin@Antena_Sectorial_Principal] > /interface bridge vlan add bridge=Bridge_Sectorial tagged=Bridge_Sectorial,ether1,ether2 vlan-ids=100
[admin@Antena_Sectorial_Principal] > # Encendemos el filtro del bridge
[admin@Antena_Sectorial_Principal] > /interface bridge set Bridge_Sectorial vlan-filtering=yes
[admin@Antena_Sectorial_Principal] >
[admin@Antena_Sectorial_Principal] > # Forzamos a que los puertos solo admitan tráfico etiquetado (Trunk estricto)
[admin@Antena_Sectorial_Principal] > /interface bridge port set [find interface=ether1] frame-types=admit-only-vlan-tagged
[admin@Antena_Sectorial_Principal] > /interface bridge port set [find interface=ether2] frame-types=admit-only-vlan-tagged

```

3.4.8. Configuración del CPE_Rural (Sector Rural – VLAN 10)

La configuración del CPE_Rural se realizó con el propósito de representar el equipo terminal encargado de recibir la señal proveniente de la Antena_Sectorial_Principal y entregarla al router doméstico del usuario final dentro del entorno de simulación. En el diseño propuesto, este dispositivo opera como un puente lógico de Capa 2 (Bridge), permitiendo el transporte y distribución del tráfico correspondiente al sector rural [53].

Identificación del sistema y arquitectura del Bridge local

Como primer paso, se definió la identidad del dispositivo dentro de la topología de red con el fin de facilitar su identificación y administración. Posteriormente, se creó una interfaz lógica tipo Bridge, utilizada para integrar las interfaces físicas involucradas en el transporte de tráfico entre el nodo principal y el usuario final [53].

La configuración aplicada fue la siguiente:

```

# Establecer la identidad del terminal del abonado rural

/system identity set name="CPE_Rural"

# Inicializar el Bridge de distribución local (Filtrado inicialmente desactivado)

/interface bridge add name=Bridge_CPE vlan-filtering=no

```

Una vez creada la estructura lógica del Bridge, se procedió a asociar las interfaces físicas del dispositivo. La interfaz ether1 fue configurada como enlace ascendente (uplink) para la recepción del tráfico proveniente de la antena sectorial principal, mientras que la interfaz ether2 fue destinada al enlace local hacia el router del cliente, asignándole el identificador PVID 10, correspondiente al segmento rural implementado mediante VLAN [53].

```
# Asociar la interfaz de enlace ascendente (Uplink de RF hacia la estación base)
```

```
/interface bridge port add bridge=Bridge_CPE interface=ether1
```

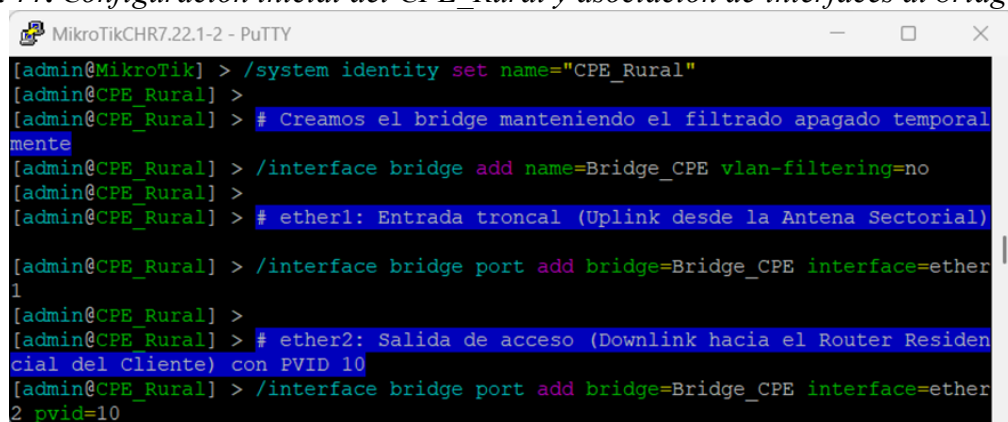
```
# Asociar la interfaz de abonado (Downlink local) configurando el PVID de acceso rural
```

```
/interface bridge port add bridge=Bridge_CPE interface=ether2 pvid=10
```

Esta configuración permitió que el CPE_Rural recibiera el tráfico etiquetado correspondiente a la VLAN 10 desde la infraestructura principal y lo entregara hacia la red local del usuario mediante un puerto de acceso, facilitando la conectividad entre el segmento de distribución inalámbrica y el router doméstico del cliente [53].

En la Figura 77 se evidencia la configuración realizada sobre el dispositivo CPE_Rural, donde se observa la creación del Bridge local, la asignación de interfaces físicas y la configuración del identificador PVID 10 correspondiente al sector rural.

Figura 77. Configuración inicial del CPE_Rural y asociación de interfaces al bridge



```
MikroTikCHR7.22.1-2 - PuTTY
[admin@MikroTik] > /system identity set name="CPE_Rural"
[admin@CPE_Rural] >
[admin@CPE_Rural] > # Creamos el bridge manteniendo el filtrado apagado temporalmente
[admin@CPE_Rural] > /interface bridge add name=Bridge_CPE vlan-filtering=no
[admin@CPE_Rural] >
[admin@CPE_Rural] > # ether1: Entrada troncal (Uplink desde la Antena Sectorial)
[admin@CPE_Rural] > /interface bridge port add bridge=Bridge_CPE interface=ether1
[admin@CPE_Rural] >
[admin@CPE_Rural] > # ether2: Salida de acceso (Downlink hacia el Router Residencial del Cliente) con PVID 10
[admin@CPE_Rural] > /interface bridge port add bridge=Bridge_CPE interface=ether2 pvid=10
```

Configuración de la interfaz de gestión, direccionamiento IP y servicio DNS

Con el propósito de permitir la administración y monitoreo del CPE_Rural dentro de la infraestructura de red, se implementó una interfaz lógica de gestión sobre la VLAN 100, destinada exclusivamente al tráfico de administración. Esta configuración permite integrar el dispositivo al segmento de gestión del WISP, facilitando tareas de supervisión, diagnóstico y acceso remoto desde el nodo principal de la red [53].

Para ello, se creó una subinterfaz virtual asociada al Bridge_CPE, permitiendo incorporar el dispositivo al dominio lógico de administración previamente establecido dentro de la topología implementada [53].

La configuración aplicada fue la siguiente:

```
# Instanciar la interfaz virtual de gestión sobre el puente de
distribución

/interface      vlan      add      name=VLAN100_Gestion_CPE      vlan-id=100
interface=Bridge_CPE
```

Posteriormente, se asignó una dirección IPv4 estática correspondiente al segmento de gestión, permitiendo identificar de forma única al CPE_Rural dentro de la red administrativa implementada [53].

```
# Asignar la dirección IP estática unívoca del terminal dentro del rango
administrativo

/ip address add address=10.0.100.20/24 interface=VLAN100_Gestion_CPE
```

Una vez configurado el direccionamiento IP, se estableció la puerta de enlace predeterminada hacia el Router_Core, permitiendo la comunicación del dispositivo con el resto de la infraestructura de red [53].

```
# Declarar el salto de enrutamiento por defecto apuntando al Gateway
Central (Router_Core)

/ip route add gateway=10.0.100.1
```

Finalmente, se configuró el servicio de resolución de nombres (DNS), delegando las solicitudes al servidor definido dentro del nodo central de la red para facilitar procesos de administración y conectividad [53].

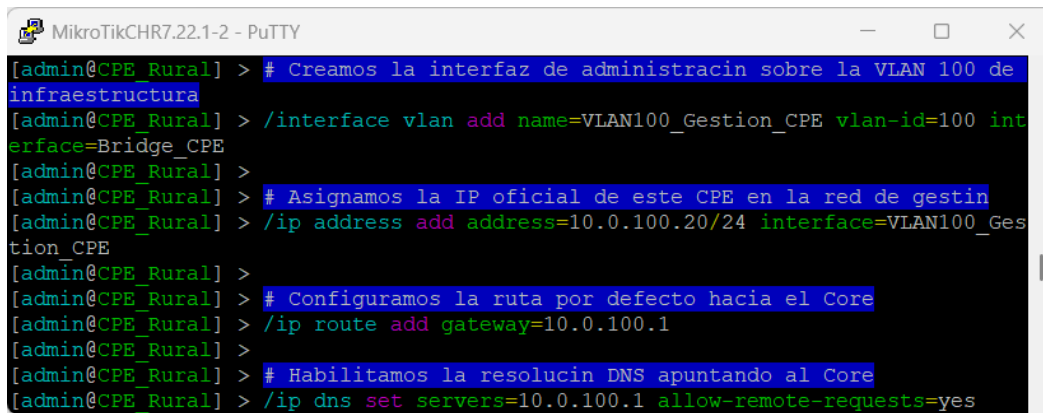
```
# Enlazar la resolución de nombres hacia la entidad caché del núcleo del
WISP
```

```
/ip dns set servers=10.0.100.1 allow-remote-requests=yes
```

Esta configuración permitió integrar el CPE_Rural al segmento de gestión de la red, facilitando su administración y monitoreo dentro del entorno de simulación implementado [53].

En la Figura 78 se evidencia la configuración aplicada al CPE_Rural, donde se observa la creación de la interfaz de gestión, la asignación del direccionamiento IPv4, la configuración de la puerta de enlace y el servicio DNS correspondiente al segmento administrativo.

Figura 78. Configuración de la interfaz de gestión del CPE_Rural



```
MikroTikCHR7.22.1-2 - PuTTY
[admin@CPE_Rural] > # Creamos la interfaz de administracin sobre la VLAN 100 de
infraestructura
[admin@CPE_Rural] > /interface vlan add name=VLAN100_Gestion_CPE vlan-id=100 int
erface=Bridge_CPE
[admin@CPE_Rural] >
[admin@CPE_Rural] > # Asignamos la IP oficial de este CPE en la red de gestin
[admin@CPE_Rural] > /ip address add address=10.0.100.20/24 interface=VLAN100_Ges
tion_CPE
[admin@CPE_Rural] >
[admin@CPE_Rural] > # Configuramos la ruta por defecto hacia el Core
[admin@CPE_Rural] > /ip route add gateway=10.0.100.1
[admin@CPE_Rural] >
[admin@CPE_Rural] > # Habilitamos la resolucin DNS apuntando al Core
[admin@CPE_Rural] > /ip dns set servers=10.0.100.1 allow-remote-requests=yes
```

Configuración de VLAN y filtrado de tráfico en el CPE_Rural

Con el propósito de garantizar la correcta distribución del tráfico dentro del CPE_Rural, se realizó la configuración de las VLAN encargadas del transporte de información entre la infraestructura principal y el usuario final. Esta configuración permitió separar el tráfico de datos del cliente respecto al tráfico de administración, manteniendo el aislamiento lógico dentro de la red implementada [53].

Para ello, se definió el comportamiento de la VLAN 10, correspondiente al tráfico de datos del sector rural, estableciendo su transporte de forma etiquetada (Tagged) desde el enlace principal y permitiendo su entrega sin etiquetas (Untagged) hacia el router doméstico del cliente mediante

el puerto local de acceso. De forma complementaria, se configuró la VLAN 100, destinada exclusivamente al tráfico de gestión y monitoreo de infraestructura [53].

La configuración aplicada fue la siguiente:

```
# Configurar la matriz para la VLAN 10: Tagged en transporte, Untagged en
el puerto del usuario
```

```
/interface bridge vlan add bridge=Bridge_CPE tagged=Bridge_CPE,ether1
untagged=ether2 vlan-ids=10
```

```
# Configurar la matriz para la VLAN 100 de control de infraestructura
```

```
/interface bridge vlan add bridge=Bridge_CPE tagged=Bridge_CPE,ether1
vlan-ids=100
```

Posteriormente, se habilitó el mecanismo de filtrado VLAN sobre el Bridge_CPE, permitiendo al dispositivo gestionar el tráfico bajo el estándar IEEE 802.1Q y garantizando el tratamiento adecuado de las tramas de red [53].

```
# Habilitar el motor de inspección estructural de tramas en el puente
```

```
/interface bridge set Bridge_CPE vlan-filtering=yes
```

Finalmente, se establecieron restricciones sobre los tipos de tramas admitidas en las interfaces físicas, configurando el puerto ether1 para aceptar únicamente tráfico etiquetado proveniente de la infraestructura principal, mientras que el puerto ether2 fue configurado para admitir exclusivamente tráfico no etiquetado destinado a la red local del usuario [53].

```
# Endurecimiento perimetral: restringir el tipo de tramas permitidas según
el rol del puerto
```

```
/interface bridge port set [find interface=ether1] frame-types=admit-
only-vlan-tagged
```

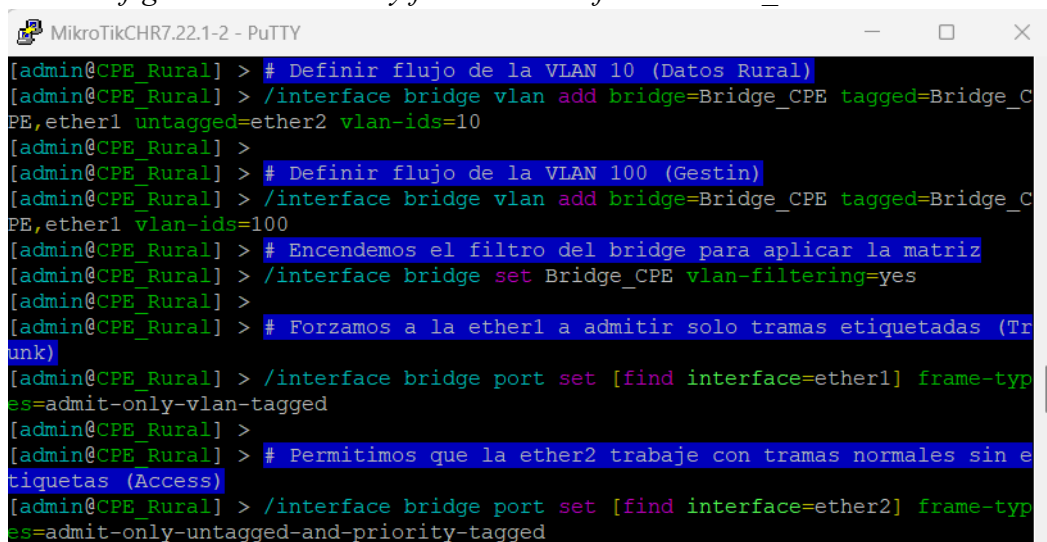
```
/interface bridge port set [find interface=ether2] frame-types=admit-
only-untagged-and-priority-tagged
```

Esta configuración permitió que el CPE_Rural realizara correctamente la transición entre el tráfico etiquetado proveniente de la red troncal y el tráfico local del usuario final, asegurando la

segmentación lógica de la red y el aislamiento del tráfico de administración dentro del entorno de simulación implementado [53].

En la Figura 79 se evidencia la configuración aplicada al CPE_Rural, donde se observa la parametrización de las VLAN utilizadas, la habilitación del filtrado de tráfico y las restricciones aplicadas sobre las interfaces físicas del dispositivo.

Figura 79. Configuración de VLAN y filtrado de tráfico del CPE_Rural



```

MikroTikCHR7.22.1-2 - PuTTY
[admin@CPE_Rural] > # Definir flujo de la VLAN 10 (Datos Rural)
[admin@CPE_Rural] > /interface bridge vlan add bridge=Bridge_CPE tagged=Bridge_CPE,ether1 untagged=ether2 vlan-ids=10
[admin@CPE_Rural] >
[admin@CPE_Rural] > # Definir flujo de la VLAN 100 (Gestin)
[admin@CPE_Rural] > /interface bridge vlan add bridge=Bridge_CPE tagged=Bridge_CPE,ether1 vlan-ids=100
[admin@CPE_Rural] > # Encendemos el filtro del bridge para aplicar la matriz
[admin@CPE_Rural] > /interface bridge set Bridge_CPE vlan-filtering=yes
[admin@CPE_Rural] >
[admin@CPE_Rural] > # Forzamos a la ether1 a admitir solo tramas etiquetadas (Trunk)
[admin@CPE_Rural] > /interface bridge port set [find interface=ether1] frame-types=admit-only-vlan-tagged
[admin@CPE_Rural] >
[admin@CPE_Rural] > # Permitimos que la ether2 trabaje con tramas normales sin etiquetas (Access)
[admin@CPE_Rural] > /interface bridge port set [find interface=ether2] frame-types=admit-only-untagged-and-priority-tagged

```

3.4.9. Configuración del Router_Cliente_Rural

La configuración del Router_Cliente_Rural se realizó con el propósito de representar el dispositivo encargado de administrar la conectividad local del usuario final dentro del sector rural. En el diseño de red implementado, este equipo opera en la Capa 3 del modelo OSI, permitiendo la interconexión entre la red de distribución WISP y la red privada del cliente, además de gestionar el acceso a servicios externos mediante mecanismos de enrutamiento y traducción de direcciones [53].

Configuración de identidad del sistema y enlace WAN

Como primer paso, se estableció la identidad del dispositivo dentro de la topología de red, permitiendo su identificación y administración dentro del entorno de simulación [53].

La configuración aplicada fue la siguiente:


```
# Definir la identidad del enrutador residencial del cliente

/system identity set name="Router_Cliente_Rural"
```

Posteriormente, se configuró el direccionamiento IP estático en la interfaz WAN (ether1), correspondiente al segmento de red rural implementado mediante la VLAN 10, permitiendo establecer la comunicación entre el router residencial y la infraestructura principal de la red WISP [53].

La configuración aplicada fue la siguiente:

```
# Configurar el direccionamiento IP estático en la interfaz WAN (VLAN 10)

/ip address add address=10.0.10.254/24 interface=ether1 comment="Enlace
de internet - VLAN 10"
```

Una vez configurado el direccionamiento IP, se estableció la puerta de enlace predeterminada apuntando al Router_Core, permitiendo el encaminamiento del tráfico hacia el resto de la infraestructura de red y el acceso a internet [53].

La configuración aplicada fue la siguiente:

```
# Declarar la ruta estática por defecto apuntando al Gateway Central de
la red rural

/ip route add gateway=10.0.10.1
```

Finalmente, se configuró el servicio de resolución de nombres (DNS), utilizando servidores públicos para facilitar el acceso a servicios externos y garantizar el funcionamiento de procesos de navegación y conectividad [53].

La configuración aplicada fue la siguiente:

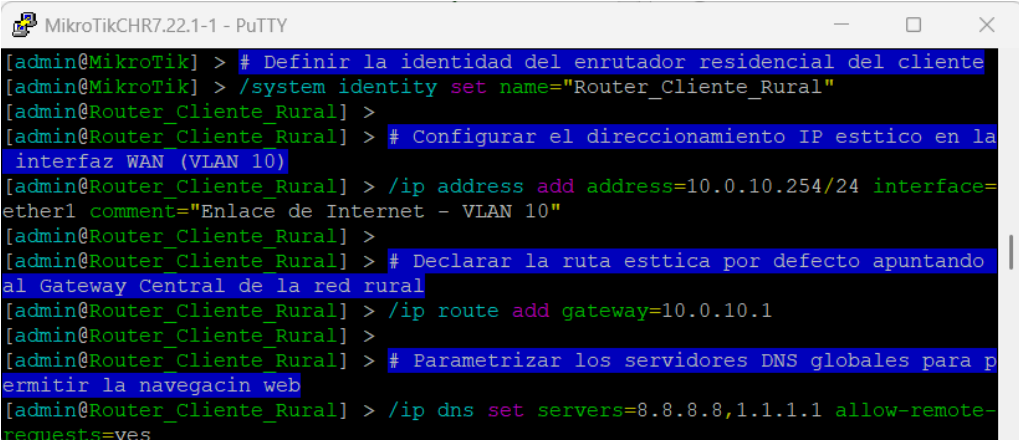
```
# Parametrizar los servidores DNS globales para permitir la navegación
web

/ip dns set servers=8.8.8.8,1.1.1.1 allow-remote-requests=yes
```

Esta configuración permitió establecer la conectividad inicial del Router_Cliente_Rural con la infraestructura principal del WISP, garantizando el direccionamiento adecuado del tráfico hacia la red de distribución y habilitando los servicios básicos de comunicación dentro del entorno de simulación implementado [53].

En la Figura 80 se evidencia la configuración realizada sobre el Router_Cliente_Rural, donde se observa la asignación de identidad del sistema, el direccionamiento IP de la interfaz WAN, la configuración de la puerta de enlace predeterminada y los parámetros del servicio DNS [53].

Figura 80. Configuración del enlace WAN del Router_Cliente_Rural



```

MikroTikCHR7.22.1-1 - PuTTY
[admin@MikroTik] > # Definir la identidad del enrutador residencial del cliente
[admin@MikroTik] > /system identity set name="Router_Cliente_Rural"
[admin@Router_Cliente_Rural] >
[admin@Router_Cliente_Rural] > # Configurar el direccionamiento IP esttico en la
interfaz WAN (VLAN 10)
[admin@Router_Cliente_Rural] > /ip address add address=10.0.10.254/24 interface=
ether1 comment="Enlace de Internet - VLAN 10"
[admin@Router_Cliente_Rural] >
[admin@Router_Cliente_Rural] > # Declarar la ruta esttica por defecto apuntando
al Gateway Central de la red rural
[admin@Router_Cliente_Rural] > /ip route add gateway=10.0.10.1
[admin@Router_Cliente_Rural] >
[admin@Router_Cliente_Rural] > # Parametrizar los servidores DNS globales para p
ermidir la navegacin web
[admin@Router_Cliente_Rural] > /ip dns set servers=8.8.8.8,1.1.1.1 allow-remote-
requests=yes
  
```

Configuración del segmento LAN local y servicios de infraestructura doméstica

Con el propósito de habilitar la conectividad interna del usuario final dentro del sector rural, se implementó una red de área local (LAN) mediante la creación de un Bridge de conmutación, permitiendo integrar múltiples interfaces físicas dentro de un mismo dominio de red [53].

Para ello, se creó la interfaz lógica denominada Bridge_Hogar, la cual actúa como elemento de interconexión entre los dispositivos internos del cliente. Posteriormente, se asociaron las interfaces ether2 y ether3, destinadas a la conexión de equipos finales dentro de la red doméstica [53].

La configuración aplicada fue la siguiente:

```
# Inicializar el Bridge de conmutación local interna

/interface bridge add name=Bridge_Hogar

# Agregar las interfaces Ethernet físicas al dominio del Bridge doméstico

/interface bridge port add bridge=Bridge_Hogar interface=ether2

/interface bridge port add bridge=Bridge_Hogar interface=ether3
```

Una vez configurada la infraestructura de conmutación local, se asignó el direccionamiento IPv4 correspondiente al gateway residencial, permitiendo establecer el punto de acceso principal para los dispositivos internos del cliente [53].

La configuración aplicada fue la siguiente:

```
# Asignar la dirección IP del Gateway local sobre el Bridge residencial

/ip address add address=192.168.10.1/24 interface=Bridge_Hogar
```

Posteriormente, se configuró un pool de direcciones IP, destinado a la asignación automática de direcciones dentro de la red doméstica, definiendo un rango de direccionamiento disponible para los dispositivos conectados [53].

La configuración aplicada fue la siguiente:

```
# Configurar el pool de direcciones IP disponibles para los dispositivos
del hogar

/ip pool add name=pool_rural ranges=192.168.10.10-192.168.10.100
```

Finalmente, se habilitó el servidor DHCP, permitiendo automatizar la asignación de parámetros de red a los dispositivos finales conectados al entorno doméstico, incluyendo dirección IP, gateway predeterminado y servidores DNS [53].

La configuración aplicada fue la siguiente:

```
# Instanciar y activar el servidor DHCP en la red LAN doméstica

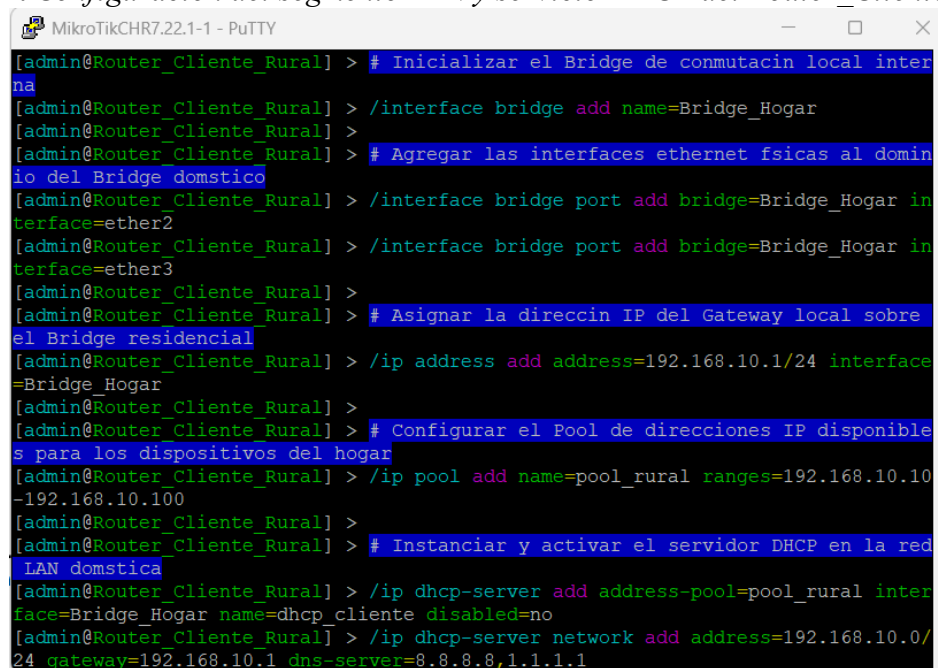
/ip dhcp-server add address-pool=pool_rural interface=Bridge_Hogar
name=dhcp_cliente disabled=no
```

```
/ip dhcp-server network add address=192.168.10.0/24 gateway=192.168.10.1
dns-server=8.8.8.8,1.1.1.1
```

Esta configuración permitió habilitar una red local funcional dentro del entorno residencial del abonado, facilitando la conexión automática de dispositivos finales mediante DHCP y permitiendo el acceso a la infraestructura principal de la red WISP implementada [53].

En la Figura 81 se evidencia la configuración aplicada al segmento LAN local del Router_Cliente_Rural, donde se observa la creación del Bridge_Hogar, la asignación del direccionamiento IPv4, la configuración del pool de direcciones y la habilitación del servicio DHCP para los dispositivos internos de la red doméstica [53].

Figura 81. Configuración del segmento LAN y servicio DHCP del Router_Cliente_Rural



```
MikroTikCHR7.22.1-1 - PuTTY
[admin@Router_Cliente_Rural] > # Inicializar el Bridge de conmutación local interna
[admin@Router_Cliente_Rural] > /interface bridge add name=Bridge_Hogar
[admin@Router_Cliente_Rural] > # Agregar las interfaces ethernet físicas al dominio del Bridge doméstico
[admin@Router_Cliente_Rural] > /interface bridge port add bridge=Bridge_Hogar interface=ether2
[admin@Router_Cliente_Rural] > /interface bridge port add bridge=Bridge_Hogar interface=ether3
[admin@Router_Cliente_Rural] > # Asignar la dirección IP del Gateway local sobre el Bridge residencial
[admin@Router_Cliente_Rural] > /ip address add address=192.168.10.1/24 interface=Bridge_Hogar
[admin@Router_Cliente_Rural] > # Configurar el Pool de direcciones IP disponibles para los dispositivos del hogar
[admin@Router_Cliente_Rural] > /ip pool add name=pool_rural ranges=192.168.10.10-192.168.10.100
[admin@Router_Cliente_Rural] > # Instanciar y activar el servidor DHCP en la red LAN doméstica
[admin@Router_Cliente_Rural] > /ip dhcp-server add address-pool=pool_rural interface=Bridge_Hogar name=dhcp_cliente disabled=no
[admin@Router_Cliente_Rural] > /ip dhcp-server network add address=192.168.10.0/24 gateway=192.168.10.1 dns-server=8.8.8.8,1.1.1.1
```

Implementación del protocolo de enmascaramiento de tráfico (Source NAT)

Con el propósito de permitir que los dispositivos pertenecientes a la red local del cliente puedan acceder a redes externas mediante una única dirección IP de salida, se implementó un mecanismo de traducción de direcciones de red (NAT) sobre el Router_Cliente_Rural [53].

Debido a que el segmento LAN interno configurado (192.168.10.0/24) pertenece a un rango de direccionamiento privado no enrutable dentro de la infraestructura externa de la red WISP, fue necesario establecer una regla de Source NAT (srcnat), permitiendo encapsular el tráfico originado desde los dispositivos del hogar hacia la interfaz WAN del router [53].

La configuración aplicada fue la siguiente:

```
# Configurar la regla de Source NAT para el enmascaramiento de la LAN
hacia internet
```

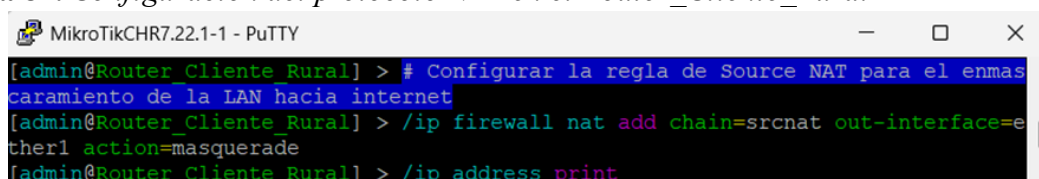
```
/ip firewall nat add chain=srcnat out-interface=ether1 action=masquerade
```

La implementación de la acción masquerade permitió realizar el enmascaramiento dinámico de las direcciones IP privadas pertenecientes a la red local del cliente, sustituyéndolas temporalmente por la dirección IP configurada en la interfaz de salida (ether1). Este procedimiento permitió establecer comunicación con el resto de la infraestructura de red y garantizar el acceso a servicios externos sin exponer directamente el direccionamiento interno del abonado [53].

Asimismo, esta configuración contribuyó al aislamiento de la red doméstica, permitiendo una mejor organización del tráfico y un nivel básico de seguridad al ocultar la estructura interna de la LAN frente a segmentos externos [53].

En la Figura 82 se evidencia la configuración de la regla Source NAT (Masquerade) implementada sobre el Router_Cliente_Rural, donde se observa la creación de la política de traducción de direcciones aplicada a la interfaz de salida hacia la red WISP.

Figura 82. Configuración del protocolo NAT en el Router_Cliente_Rural



```
MikroTikCHR7.22.1-1 - PuTTY
[admin@Router_Cliente_Rural] > # Configurar la regla de Source NAT para el enmas
caramiento de la LAN hacia internet
[admin@Router_Cliente_Rural] > /ip firewall nat add chain=srcnat out-interface=e
ther1 action=masquerade
[admin@Router_Cliente_Rural] > /ip address print
```

3.4.10. Configuración de dispositivos finales (PC1 y Windows-10)

Con el propósito de verificar la correcta entrega del servicio hacia los usuarios finales, se implementaron dispositivos terminales dentro del entorno de simulación, permitiendo validar la

conectividad de extremo a extremo desde la infraestructura WISP hasta la red local del cliente [53].

Para las pruebas funcionales del sector rural se utilizaron dos tipos de dispositivos finales: una PC virtual básica (VPCS) integrada en GNS3 y una máquina virtual de usuario, ambas conectadas a la red local del Router_Cliente_Rural. Esta configuración permitió simular distintos escenarios de consumo de red y validar el funcionamiento del servicio bajo diferentes entornos de usuario [53].

Obtención automática de direccionamiento IP mediante DHCP

Como primer paso, se verificó la asignación dinámica de parámetros de red mediante el protocolo DHCP (Dynamic Host Configuration Protocol). Para ello, el dispositivo final solicitó automáticamente una dirección IP, una puerta de enlace y parámetros de conectividad desde el router local del cliente [53].

La configuración aplicada en la terminal VPCS fue la siguiente:

```
PC1> ip dhcp
```

Como resultado esperado, el sistema debía asignar automáticamente un direccionamiento perteneciente al segmento local rural (192.168.10.0/24), junto con su respectiva puerta de enlace [53].

Resultado esperado:

```
DORA IP 192.168.10.100/24 GW 192.168.10.1.
```

Esta validación permitió comprobar el correcto funcionamiento del servidor DHCP configurado previamente en el Router_Cliente_Rural, asegurando la entrega automática de parámetros de red a los dispositivos del usuario [53].

Almacenamiento persistente de configuración

Finalmente, con el propósito de evitar la pérdida de configuración al reiniciar el laboratorio de simulación, se procedió al almacenamiento permanente de los parámetros aplicados dentro del entorno VPCS [53].

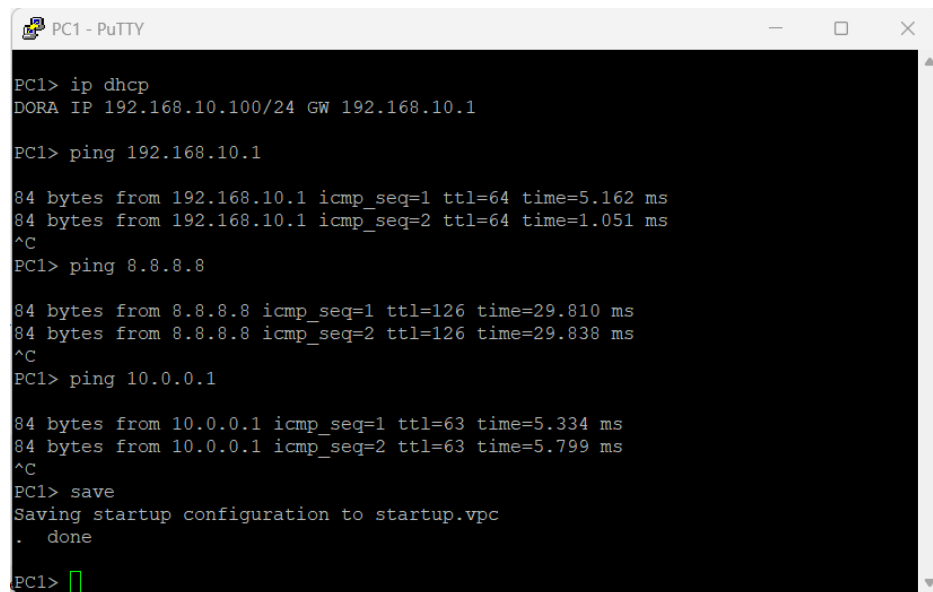
La instrucción utilizada fue la siguiente:

```
PC1> save
```

Esta acción permitió conservar la configuración de red del dispositivo final para futuras pruebas dentro del entorno de simulación [53].

En la Figura 83 se evidencia la configuración y validación realizadas sobre los dispositivos finales del sector rural, donde se observa la obtención dinámica del direccionamiento IP, las pruebas de conectividad local y externa, así como el almacenamiento persistente de la configuración implementada.

Figura 83. Configuración y validación de conectividad en dispositivos finales del sector rural



```
PC1 - PuTTY
PC1> ip dhcp
DORA IP 192.168.10.100/24 GW 192.168.10.1

PC1> ping 192.168.10.1

84 bytes from 192.168.10.1 icmp_seq=1 ttl=64 time=5.162 ms
84 bytes from 192.168.10.1 icmp_seq=2 ttl=64 time=1.051 ms
^C
PC1> ping 8.8.8.8

84 bytes from 8.8.8.8 icmp_seq=1 ttl=126 time=29.810 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=126 time=29.838 ms
^C
PC1> ping 10.0.0.1

84 bytes from 10.0.0.1 icmp_seq=1 ttl=63 time=5.334 ms
84 bytes from 10.0.0.1 icmp_seq=2 ttl=63 time=5.799 ms
^C
PC1> save
Saving startup configuration to startup.vpc
. done
PC1> 
```

Configuración de dispositivo final Windows 10 (Usuario residencial)

Con el propósito de simular un entorno de usuario final con mayores capacidades de interacción y validación de servicios de red, se implementó una máquina virtual con sistema operativo Windows 10, permitiendo realizar pruebas de navegación web, conectividad y acceso a servicios dentro del entorno WISP desarrollado [53].

La utilización de este sistema operativo permitió representar de manera más cercana el comportamiento de un usuario residencial real, facilitando la validación del acceso a internet y la

correcta asignación de parámetros de red mediante el servicio DHCP configurado previamente en el Router_Cliente_Rural [53].

1. Configuración del adaptador de red dedicado en VMware Workstation

Para integrar la máquina virtual de Windows 10 dentro del entorno de simulación sin interferir con las interfaces utilizadas por GNS3, se optó por crear un segmento de red virtual independiente mediante VMware Workstation, utilizando un adaptador dedicado para el enlace con el laboratorio [65].

Para ello, se accedió al apartado Edit → Virtual Network Editor dentro de VMware Workstation, permitiendo la creación y parametrización de una nueva red virtual [65].

Paso 1: Creación de la red virtual VMnet10

Dentro del Virtual Network Editor, se creó un adaptador virtual denominado VMnet10, configurado bajo un esquema de red privada para garantizar el aislamiento del tráfico generado por la máquina virtual respecto al sistema anfitrión [65].

La configuración aplicada fue la siguiente:

Tipo de red: Host-only, permitiendo la comunicación interna entre dispositivos virtuales dentro de una red privada [65].

Servidor DHCP de VMware: Deshabilitado, permitiendo que la asignación de direccionamiento IP sea realizada exclusivamente por el router MikroTik implementado en GNS3 [65].

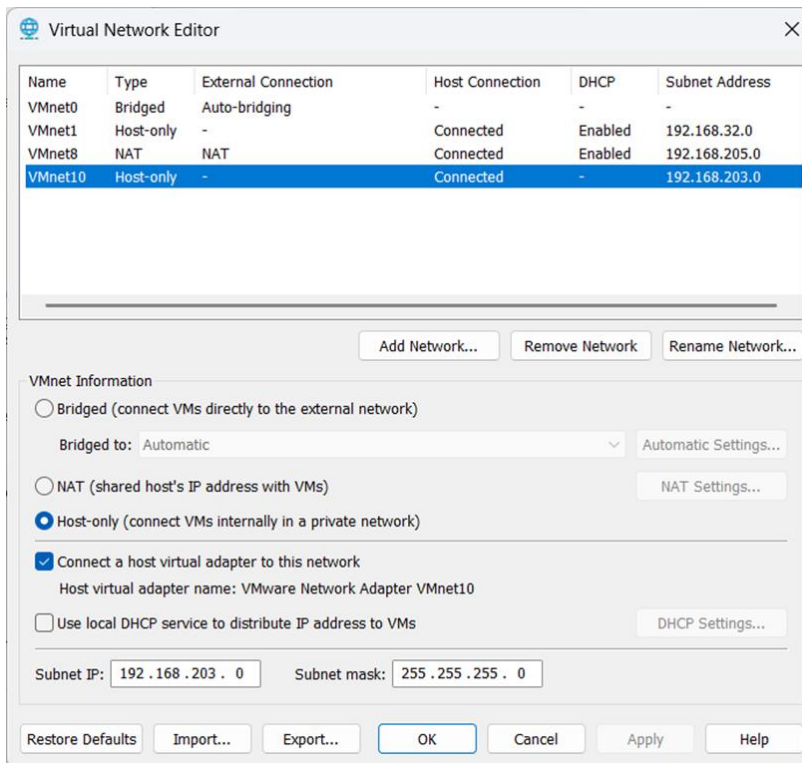
Adaptador virtual del host: Habilitado (Connect a host virtual adapter to this network), utilizando la interfaz VMware Network Adapter VMnet10 [65].

Subred utilizada: 192.168.203.0/24, destinada únicamente a la identificación del tráfico virtual dentro del sistema anfitrión [65].

Una vez aplicados los parámetros de configuración, se procedió a seleccionar las opciones Apply y OK, finalizando la creación del adaptador virtual requerido para la integración de la máquina virtual con el entorno de simulación [65].

En la Figura 84 se evidencia la configuración realizada dentro del Virtual Network Editor de VMware Workstation, donde se observa la creación del adaptador VMnet10, así como los parámetros de aislamiento y segmentación implementados para la conexión de la máquina virtual Windows 10 al laboratorio WISP.

Figura 84. Configuración del adaptador virtual VMnet10 en VMware Workstation



2. Asignación de hardware y configuración de red

Una vez creado el segmento de red VMnet10, se configuraron los recursos de hardware de la máquina virtual Windows 10, así como su adaptador de red para permitir la comunicación con el entorno de simulación implementado en GNS3 [65].

La configuración aplicada fue la siguiente:

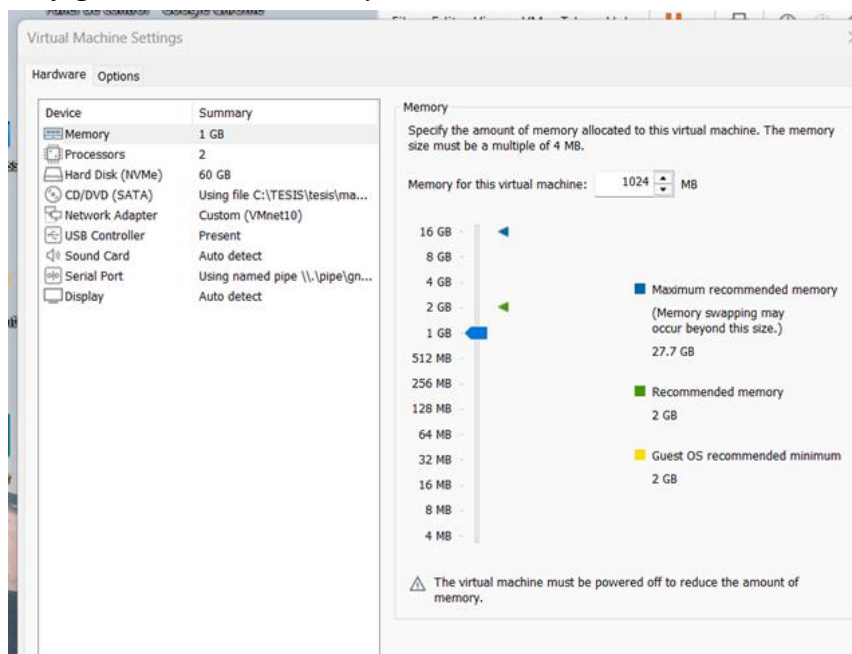
- Memoria RAM: 1024 MB (1 GB), permitiendo un funcionamiento estable con un consumo eficiente de recursos.

- Adaptador de red: Configurado en modo Custom (VMnet10), enlazando directamente la máquina virtual al segmento de red previamente creado.

Esta configuración permitió integrar la máquina virtual al entorno de simulación y facilitar la obtención de direccionamiento IP desde el Router_Cliente_Rural [65].

En la Figura 85 se evidencia la configuración de hardware y del adaptador de red aplicada a la máquina virtual Windows 10 dentro de VMware Workstation.

Figura 85. Configuración de hardware y red de Windows 10



3. Integración de la máquina virtual Windows 10 en GNS3

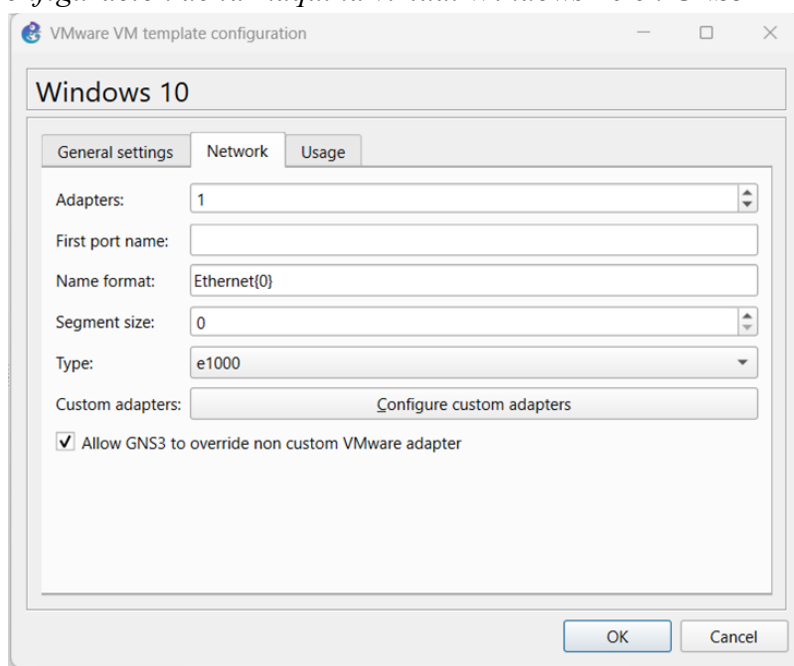
Una vez configurada la máquina virtual Windows 10 en VMware Workstation, se procedió a realizar su integración dentro del entorno de simulación de GNS3 [65].

Para ello, en GNS3 se accedió al apartado Edit → Preferences → VMware VMs, donde se seleccionó la máquina virtual correspondiente al cliente final (Windows 10) y posteriormente se ingresó a la opción Edit [65].

Dentro de la configuración de red de la máquina virtual, se habilitó la opción Allow GNS3 to override non-custom adapter, permitiendo que GNS3 gestione correctamente la interfaz de red y establezca la comunicación con la topología implementada [65].

En la Figura 86 se evidencia el proceso de selección y configuración de la máquina virtual Windows 10 dentro del apartado VMware VMs de GNS3, previo a su incorporación a la topología de red implementada [65].

Figura 86. Configuración de la máquina virtual Windows 10 en GNS3



Una vez aplicada esta configuración, la máquina virtual fue incorporada desde el panel de dispositivos de GNS3 a la topología de red, conectándola como cliente final del sector rural. Al establecer la conexión, el sistema obtuvo automáticamente una dirección IP mediante el servicio DHCP, quedando integrado correctamente dentro de la infraestructura de red simulada [65].

3.4.11. Configuración de los sectores Urbano y Empresas

Con el propósito de evitar la repetición de procedimientos equivalentes, los sectores Urbano (VLAN 20) y Empresas (VLAN 30) se documentan de forma consolidada en el presente apartado. Ambos sectores replican íntegramente el flujo de configuración descrito en detalle para el sector rural en los apartados 3.4.7 a 3.4.10, a saber: incorporación de la interfaz física

correspondiente al Bridge_Sectorial, mapeo estático de la matriz de conmutación bajo el estándar IEEE 802.1Q, configuración de la interfaz lógica de gestión sobre la VLAN 100, definición del enlace WAN en el router del abonado, creación del segmento LAN con servicio DHCP y aplicación de la regla de traducción de direcciones Source NAT para la salida hacia internet.

En la siguiente Tabla 37 se presentan los parámetros de configuración que diferencian a cada uno de los tres sectores implementados, tomando como referencia el procedimiento detallado del sector rural.

Tabla 37. *Parámetros comparativos de configuración de los sectores Rural, Urbano y Empresas*

Parámetro	Sector Rural	Sector Urbano	Sector Empresas
VLAN de usuario	10	20	30
Interfaz en Bridge_Sectoria 1	ether2	ether3	ether4
Identidad del CPE	CPE_Rural	CPE_Urbano	CPE_Empresas
Bridge del CPE	Bridge_CPE	Bridge_Urbano	Bridge_Corporativo
Puerto de acceso (pvid)	ether2 (pvid=10)	ether2 (pvid=20)	ether2 (pvid=30)
IP de gestión del CPE (VLAN 100)	10.0.100.20/24	10.0.100.21/24	10.0.100.31/24
Router del abonado	Router_Cliente_Rural	Router_Cliente_Urbano	Router_Empresas
IP WAN del router (ether1)	10.0.10.254/24	10.0.20.254/24	10.0.30.254/24
Puerta de enlace hacia el Core	10.0.10.1	10.0.20.1	10.0.30.1
Bridge LAN del abonado	Bridge_Hogar	Bridge_Hogar	Bridge_Corporativo_LAN
Gateway de la red LAN	192.168.10.1/24	192.168.20.1/24	192.168.30.1/24
Pool DHCP	pool_rural (192.168.10.10 – .100)	pool_urbano (192.168.20.10 – .100)	pool_empresa (192.168.30.100 – .200)
Servidor DHCP	dhcp_cliente	dhcp_cliente_urbano	dhcp_empresa
Servidores DNS del abonado	8.8.8.8 / 1.1.1.1	8.8.8.8 / 1.1.1.1	8.8.8.8 / 1.1.1.1
Salida a internet	srcnat masquerade (ether1)	srcnat masquerade (ether1)	srcnat masquerade (ether1)
Dispositivo final VPCS	PC1	PC2	PC3
Máquina virtual de validación	Windows 10	Ubuntu Desktop	Kali Linux
Adaptador VMware / subred	VMnet10– 192.168.203.0/24	VMnet11– 192.168.25.0/24	VMnet12– 192.168.50.0/24

Las diferencias sustantivas entre los tres sectores se limitan a tres aspectos. En primer lugar, el sector empresarial emplea un rango de asignación DHCP distinto (192.168.30.100 –

192.168.30.200), reservando las primeras direcciones del segmento para servidores y equipos que requieren direccionamiento estático. En segundo lugar, sobre la interfaz ether4 de la Antena_Sectorial_Principal se aplicó de forma explícita el parámetro frame-types=admit-only-vlan-tagged, como política de seguridad perimetral del enlace corporativo. En tercer lugar, cada dispositivo final fue validado con un sistema operativo distinto —Windows 10 en el sector rural, Ubuntu Desktop en el urbano y Kali Linux en el empresarial—, con el fin de comprobar la interoperabilidad de la red frente a diferentes implementaciones de cliente DHCP.

El procedimiento completo paso a paso de los tres sectores, incluyendo las capturas de pantalla de cada comando ejecutado y los archivos de configuración exportados, se encuentra disponible en el repositorio referenciado en el Anexo A, con el fin de permitir la replicación íntegra del prototipo.

Backups (enlaces de respaldo)

El presente apartado describe el procedimiento de configuración de los nodos Backup implementados dentro de la infraestructura WISP propuesta. Estos nodos fueron incorporados con el propósito de garantizar la continuidad del servicio ante posibles fallos, interrupciones o degradaciones en los enlaces principales de la última milla, especialmente en sectores donde las condiciones geográficas, las obstrucciones físicas o las pérdidas de línea de vista (LOS) representan un riesgo para la disponibilidad de la red.

Debido a las condiciones geográficas y a la necesidad de garantizar continuidad operativa del servicio, se implementó un esquema de redundancia basado en el protocolo RSTP (Rapid Spanning Tree Protocol), con el fin de mantener rutas alternativas de comunicación ante posibles fallos en los enlaces principales de la última milla.

Dentro de la arquitectura diseñada, los nodos backup operan como dispositivos de Capa 2, encargados del transporte transparente del tráfico correspondiente a cada segmento de usuarios mediante VLAN, mientras que la administración, el monitoreo y la gestión remota de la infraestructura se mantienen aislados a través de la VLAN 100 de Gestión [53].

3.4.12. Configuración del Backup_Rural

Configuración de la estación base para integración del backup

Como primera etapa, se incorporó el enlace físico destinado al Backup dentro de la Antena_Sectorial_Principal, con el fin de habilitar un nuevo canal de transporte hacia el nodo de extensión rural.

Para ello, se agregó la interfaz ether5 al dominio del Bridge_Sectorial, para que el puerto opere como enlace troncal para el transporte de tráfico etiquetado bajo el estándar IEEE 802.1Q [53].

El comando aplicado fue el siguiente:

```
# 1. Registrar la interfaz física ether5 en el dominio del Bridge
sectorial
```

```
/interface bridge port add bridge=Bridge_Sectorial interface=ether5
```

Posteriormente, se configuró una política de filtrado de ingreso sobre el puerto, que permite únicamente el tránsito de tramas etiquetadas (Tagged), con el propósito de evitar el ingreso de tráfico no autorizado dentro del backbone inalámbrico [53].

```
# 2. Configurar el filtrado perimetral de ingreso (Admitir únicamente
tramas etiquetadas 802.1Q)
```

```
/interface bridge port set [find interface=ether5] frame-types=admit-
only-vlan-tagged
```

Una vez agregado el puerto físico, se actualizó la matriz de conmutación correspondiente a la VLAN 10, para que el tráfico de datos del sector rural pueda propagarse hacia el backup implementado [53].

```
# 3. Modificar la matriz de la VLAN 10 (Datos Rurales) inyectando el
puerto ether5
```

```
/interface      bridge      vlan      set      [find      vlan-ids=10]
tagged=Bridge_Sectorial,ether1,ether2,ether5
```

De igual manera, se modificó la configuración de la VLAN 100 de Gestión, con el fin de mantener la supervisión y administración remota de los dispositivos desplegados dentro del enlace repetidor [53].

```
# 4. Actualizar la matriz de la VLAN 100 (Gestión) inyectando el puerto
ether5

/interface bridge vlan set [find vlan-ids=100]
tagged=Bridge_Sectorial,ether1,ether2,ether3,ether4,ether5
```

Esta configuración permitió integrar el Backup_Rural dentro de la infraestructura de distribución y habilitar el transporte simultáneo del tráfico de usuarios y del segmento de administración hacia las zonas de nodo de respaldo [53].

En la Figura 87 se evidencia la configuración aplicada en la Antena_Sectorial_Principal para la integración del enlace troncal correspondiente al Backup_Rural.

Figura 87. Configuración de integración del Backup_Rural en la Antena_Sectorial_Principal

```
Antena-Sectorial-Principal - PuTTY
[admin@Antena_Sectorial_Principal] > # 1. Aadir el puerto fsico ether5 al dominio
del Bridge (Esto elimina el mensaje en rojo)
[admin@Antena_Sectorial_Principal] > /interface bridge port add bridge=Bridge_S
ectorial interface=ether5
[admin@Antena_Sectorial_Principal] >
[admin@Antena_Sectorial_Principal] > # 2. Configurar el filtrado troncal de ingr
eso en ether5 (Solo tramas etiquetadas por seguridad)
[admin@Antena_Sectorial_Principal] > /interface bridge port set [find interface=
ether5] frame-types=admit-only-vlan-tagged
[admin@Antena_Sectorial_Principal] >
[admin@Antena_Sectorial_Principal] > # 3. Reescribir la matriz de etiquetas para
la VLAN 10 incorporando ether5
[admin@Antena_Sectorial_Principal] > /interface bridge vlan set [find vlan-ids=1
00] tagged=Bridge_Sectorial,ether1,ether2,ether5
[admin@Antena_Sectorial_Principal] >
[admin@Antena_Sectorial_Principal] > # 4. Reescribir la matriz de etiquetas de G
estión (VLAN 100) incorporando ether5
[admin@Antena_Sectorial_Principal] > /interface bridge vlan set [find vlan-ids=1
00] tagged=Bridge_Sectorial,ether1,ether2,ether3,ether4,ether5
```

Configuración del nodo de respaldo rural (BACKUP_ZONAL_1)

El presente apartado describe el procedimiento de configuración del nodo BACKUP_ZONAL_1, implementado con el propósito de garantizar la continuidad del servicio ante posibles fallos o degradaciones del enlace principal hacia zonas rurales con limitaciones de propagación o pérdida parcial de la línea de vista (LOS).

Dentro de la arquitectura propuesta, este dispositivo opera en la Capa 2 del modelo OSI, funcionando como un puente transparente encargado de recibir el tráfico proveniente de la Antena_Sectorial_Principal y retransmitirlo hacia el CPE_Rural, lo que permite el transporte simultáneo de la VLAN 10 (Datos rurales) y la VLAN 100 (Gestión de infraestructura) [53].

Asimismo, se habilitó el protocolo RSTP (Rapid Spanning Tree Protocol), con el fin de prevenir bucles de red y garantizar la redundancia lógica dentro del enlace de última milla [53].

1. Configuración de identidad, Bridge, interfaces físicas y matriz VLAN

Como primera etapa, se definió la identidad lógica del backup dentro de la topología WISP, con el fin de facilitar su identificación durante las tareas de monitoreo y administración de red [53].

Para ello, se aplicó el siguiente comando [53]:

```
# 1. Definir la identidad nominal del dispositivo repetidor rural

/system identity set name="BACKUP_ZONAL_1"
```

Posteriormente, se inicializó el puente lógico principal (Bridge_Backup) con el protocolo RSTP habilitado y se mantuvo inicialmente desactivado el filtrado de VLAN, con el fin de permitir el aprovisionamiento seguro de las interfaces físicas [53].

```
# 2. Inicializar el Bridge estructural con soporte del protocolo RSTP
activo

/interface bridge add name=Bridge_Backup protocol-mode=rstp vlan-
filtering=no
```

Una vez creado el Bridge, se integraron las interfaces físicas ether1 y ether2, correspondientes al enlace de subida (Uplink) desde la antena principal y al enlace de bajada (Downlink) hacia el sector rural [53].

```
# 3. Integrar las interfaces físicas miembros al dominio del Bridge

# ether1: Uplink desde la Antena Central | ether2: Downlink de
contingencia hacia CPE_Rural

/interface bridge port add bridge=Bridge_Backup interface=ether1
```

```
/interface bridge port add bridge=Bridge_Backup interface=ether2
```

Adicionalmente, se implementó una política de endurecimiento perimetral que permite únicamente el tránsito de tramas etiquetadas (Tagged) bajo el estándar IEEE 802.1Q, con lo cual se mitigan posibles intentos de inyección de tráfico no autorizado [53].

```
# 4. Forzar el descarte de tramas sin etiqueta (Seguridad contra VLAN Hopping)
```

```
/interface bridge port set [find interface=ether1] frame-types=admit-only-vlan-tagged
```

```
/interface bridge port set [find interface=ether2] frame-types=admit-only-vlan-tagged
```

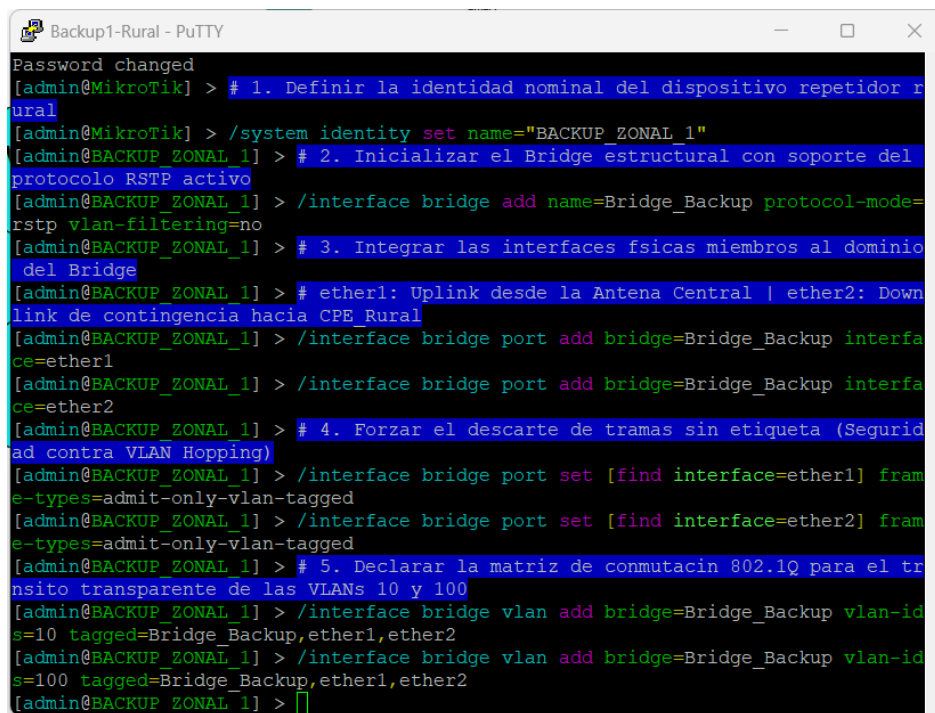
Finalmente, se declaró la matriz de conmutación correspondiente a las VLAN 10 y VLAN 100, con el fin de permitir el transporte transparente del tráfico rural y de gestión a través del nodo de respaldo [53].

```
# 5. Declarar la matriz de conmutación 802.1Q para el tránsito transparente de las VLAN 10 y 100
```

```
/interface bridge vlan add bridge=Bridge_Backup vlan-ids=10 tagged=Bridge_Backup,ether1,ether2
```

```
/interface bridge vlan add bridge=Bridge_Backup vlan-ids=100 tagged=Bridge_Backup,ether1,ether2
```

En la Figura 88 se evidencia la configuración aplicada a la identidad del backup, creación del Bridge_Backup, integración de interfaces físicas y declaración de las VLAN de transporte implementadas en el nodo de respaldo.

Figura 88. Configuración estructural del BACKUP_ZONAL_1


```

Backup1-Rural - PuTTY
Password changed
[admin@MikroTik] > # 1. Definir la identidad nominal del dispositivo repetidor r
ural
[admin@MikroTik] > /system identity set name="BACKUP_ZONAL_1"
[admin@BACKUP_ZONAL_1] > # 2. Inicializar el Bridge estructural con soporte del
protocolo RSTP activo
[admin@BACKUP_ZONAL_1] > /interface bridge add name=Bridge_Backup protocol-mode=
rstp vlan-filtering=no
[admin@BACKUP_ZONAL_1] > # 3. Integrar las interfaces físicas miembros al dominio
del Bridge
[admin@BACKUP_ZONAL_1] > # ether1: Uplink desde la Antena Central | ether2: Down
link de contingencia hacia CPE_Rural
[admin@BACKUP_ZONAL_1] > /interface bridge port add bridge=Bridge_Backup interfa
ce=ether1
[admin@BACKUP_ZONAL_1] > /interface bridge port add bridge=Bridge_Backup interfa
ce=ether2
[admin@BACKUP_ZONAL_1] > # 4. Forzar el descarte de tramas sin etiqueta (Segurid
ad contra VLAN Hopping)
[admin@BACKUP_ZONAL_1] > /interface bridge port set [find interface=ether1] fram
e-types=admit-only-vlan-tagged
[admin@BACKUP_ZONAL_1] > /interface bridge port set [find interface=ether2] fram
e-types=admit-only-vlan-tagged
[admin@BACKUP_ZONAL_1] > # 5. Declarar la matriz de conmutación 802.1Q para el tr
nsito transparente de las VLANs 10 y 100
[admin@BACKUP_ZONAL_1] > /interface bridge vlan add bridge=Bridge_Backup vlan-id
s=10 tagged=Bridge_Backup,ether1,ether2
[admin@BACKUP_ZONAL_1] > /interface bridge vlan add bridge=Bridge_Backup vlan-id
s=100 tagged=Bridge_Backup,ether1,ether2
[admin@BACKUP_ZONAL_1] >

```

2. Configuración de direccionamiento IP, DNS y activación del filtrado VLAN

Una vez configurada la estructura de conmutación del backup, se procedió a implementar la interfaz lógica de gestión sobre la VLAN 100, con el fin de integrar el dispositivo dentro del segmento de administración centralizado de la red.

Para ello, se creó una interfaz virtual de gestión y se asignó una dirección IP estática perteneciente al rango administrativo implementado en la infraestructura WISP [53].

La configuración aplicada fue la siguiente:

6. Instanciar la subinterfaz virtual y el direccionamiento IP de Gestión de infraestructura

```

/interface vlan add name=VLAN_Gestion vlan-id=100 interface=Bridge_Backup
/ip address add address=10.0.100.9/24 interface=VLAN_Gestion
/ip route add gateway=10.0.100.1

```

Posteriormente, se configuró el servicio de resolución de nombres (DNS), con el fin de habilitar la conectividad de los servicios requeridos para la administración del dispositivo [53].

7. Aprovisionamiento de servidores DNS para permitir la resolución de nombres de Capa 7

```
/ip dns set servers=8.8.8.8,1.1.1.1 allow-remote-requests=yes
```

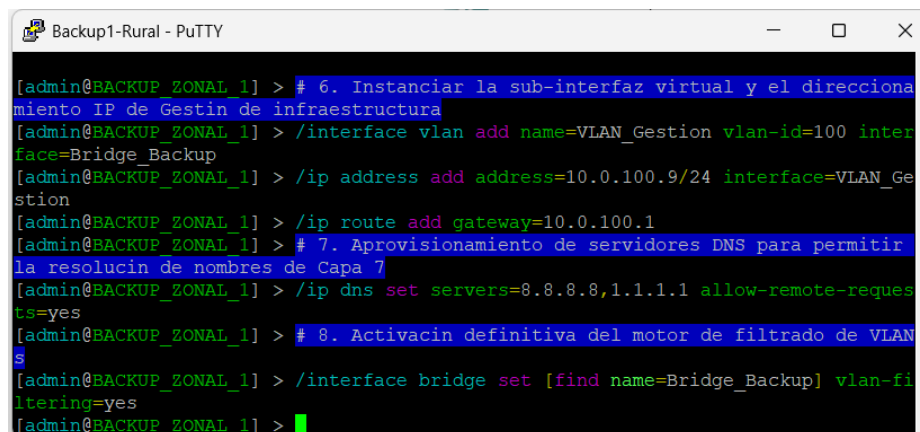
Finalmente, se habilitó el filtrado definitivo de VLAN dentro del Bridge, con lo cual se activó el funcionamiento estructurado del repetidor bajo el estándar IEEE 802.1Q [53].

8. Activación definitiva del motor de filtrado de VLAN

```
/interface bridge set [find name=Bridge_Backup] vlan-filtering=yes
```

En la Figura 89 se evidencia la configuración de direccionamiento IP, servicios DNS y activación del filtrado VLAN implementados en el BACKUP_ZONAL_1.

Figura 89. Configuración de gestión y filtrado del BACKUP_ZONAL_1



```
Backup1-Rural - PuTTY

[admin@BACKUP_ZONAL_1] > # 6. Instanciar la sub-interfaz virtual y el direccionamiento IP de Gestión de infraestructura
[admin@BACKUP_ZONAL_1] > /interface vlan add name=VLAN_Gestion vlan-id=100 interface=Bridge_Backup
[admin@BACKUP_ZONAL_1] > /ip address add address=10.0.100.9/24 interface=VLAN_Gestion
[admin@BACKUP_ZONAL_1] > /ip route add gateway=10.0.100.1
[admin@BACKUP_ZONAL_1] > # 7. Aprovisionamiento de servidores DNS para permitir la resolución de nombres de Capa 7
[admin@BACKUP_ZONAL_1] > /ip dns set servers=8.8.8.8,1.1.1.1 allow-remote-requests=yes
[admin@BACKUP_ZONAL_1] > # 8. Activación definitiva del motor de filtrado de VLAN
[admin@BACKUP_ZONAL_1] > /interface bridge set [find name=Bridge_Backup] vlan-filtering=yes
[admin@BACKUP_ZONAL_1] >
```

Configuración del anillo de respaldo RSTP en el CPE_Rural

Con el propósito de garantizar la continuidad del servicio ante posibles fallos de conectividad en el enlace principal del sector rural, se implementó un esquema de redundancia de red basado en el protocolo RSTP (Rapid Spanning Tree Protocol) sobre el dispositivo CPE_Rural.

Dentro de esta arquitectura, el equipo terminal del cliente quedó interconectado mediante dos rutas de comunicación en Capa 2: el enlace principal proveniente de la

Antena_Sectorial_Principal a través de la interfaz ether1, y un enlace alternativo de contingencia proveniente del BACKUP_ZONAL_1 mediante la interfaz ether3.

Como primera etapa, se eliminaron las asociaciones previas de los puertos involucrados dentro del Bridge, con el fin de limpiar las configuraciones heredadas y evitar inconsistencias en el proceso de convergencia del protocolo [53].

La configuración aplicada fue la siguiente:

```
# 1. Desacoplar los puertos de asignaciones previas para limpiar el mapa
dinámico
```

```
/interface bridge port remove [find interface=ether1]
```

```
/interface bridge port remove [find interface=ether3]
```

Posteriormente, se habilitó el protocolo RSTP sobre el Bridge_CPE y se mantuvo temporalmente desactivado el filtrado VLAN, con el fin de permitir la reconfiguración de los enlaces redundantes [53].

```
# 2. Forzar el modo de operación RSTP en el puente del terminal de usuario

/interface bridge set [find name=Bridge_CPE] protocol-mode=rstp vlan-
filtering=no
```

Una vez habilitado el protocolo, se definió una jerarquía de caminos mediante prioridades de puerto, estableciendo como enlace principal el puerto ether1 (camino directo desde la antena sectorial) y como enlace de respaldo el puerto ether3 (camino alternativo desde el backup rural) [53].

```
# 3. Configurar la jerarquía estricta de caminos mediante prioridades de
puerto:
```

```
# ether1 (Enlace Directo de Sectorial) -> Prioridad alta preferencial
(0x80 = 128 decimal)
```

```
# ether3 (Enlace desde backup zonal) -> Prioridad baja de respaldo (0x90
= 144 decimal)
```

```
/interface bridge port add bridge=Bridge_CPE interface=ether1
priority=0x80
```

```
/interface bridge port add bridge=Bridge_CPE interface=ether3
priority=0x90
```

Posteriormente, se actualizó la matriz de conmutación de la VLAN 10, con el fin de permitir el tránsito del tráfico rural por ambos enlaces físicos implementados [53].

4. Registrar de forma estática la autorización de la VLAN 10 sobre ambos enlaces

```
/interface bridge vlan set [find vlan-ids=10]
tagged=Bridge_CPE,ether1,ether3
```

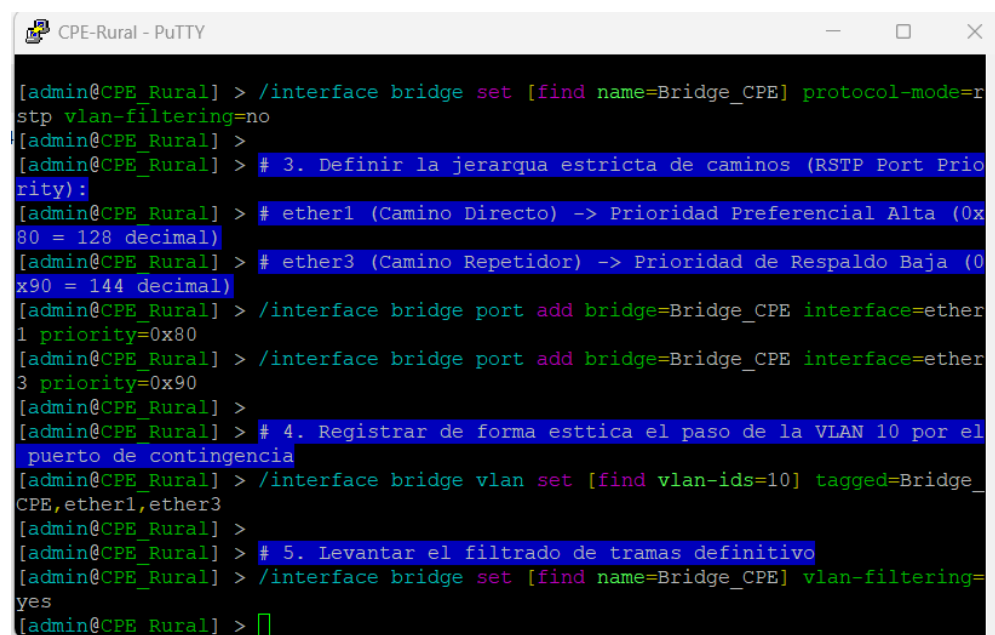
Finalmente, se habilitó nuevamente el filtrado de VLAN, con lo cual se consolidó la operación definitiva del Bridge_CPE bajo el esquema de redundancia implementado [53].

5. Levantar el motor de filtrado definitivo en el CPE del abonado

```
/interface bridge set [find name=Bridge_CPE] vlan-filtering=yes
```

En la Figura 90 se evidencia la configuración aplicada para la implementación del anillo de respaldo basado en RSTP en el dispositivo CPE_Rural, incluyendo la definición de prioridades de puerto y la habilitación del mecanismo de redundancia de enlaces.

Figura 90. Configuración del anillo de respaldo RSTP en el CPE_Rural



```
CPE-Rural - PuTTY

[admin@CPE_Rural] > /interface bridge set [find name=Bridge_CPE] protocol-mode=r
stp vlan-filtering=no
[admin@CPE_Rural] >
[admin@CPE_Rural] > # 3. Definir la jerarquía estricta de caminos (RSTP Port Prio
rity):
[admin@CPE_Rural] > # ether1 (Camino Directo) -> Prioridad Preferencial Alta (0x
80 = 128 decimal)
[admin@CPE_Rural] > # ether3 (Camino Repetidor) -> Prioridad de Respaldo Baja (0
x90 = 144 decimal)
[admin@CPE_Rural] > /interface bridge port add bridge=Bridge_CPE interface=ether
1 priority=0x80
[admin@CPE_Rural] > /interface bridge port add bridge=Bridge_CPE interface=ether
3 priority=0x90
[admin@CPE_Rural] >
[admin@CPE_Rural] > # 4. Registrar de forma esttica el paso de la VLAN 10 por el
puerto de contingencia
[admin@CPE_Rural] > /interface bridge vlan set [find vlan-ids=10] tagged=Bridge_
CPE,ether1,ether3
[admin@CPE_Rural] >
[admin@CPE_Rural] > # 5. Levantar el filtrado de tramas definitivo
[admin@CPE_Rural] > /interface bridge set [find name=Bridge_CPE] vlan-filtering=
yes
[admin@CPE_Rural] > []
```

3.4.13. Configuración de los nodos de respaldo Urbano y Empresas

Los nodos de respaldo correspondientes a los sectores Urbano y Empresas replican de manera íntegra el procedimiento descrito en el apartado anterior para el Backup_Rural. En ambos casos se incorporó una interfaz física adicional al Bridge_Sectorial de la estación base con la política frame-types=admit-only-vlan-tagged, se actualizó la matriz de conmutación de la VLAN de usuario y de la VLAN 100 de gestión para incluir dicho puerto, y se desplegó un nodo MikroTik CHR configurado como puente transparente de Capa 2 con el protocolo RSTP habilitado sobre el Bridge_Backup. Sobre el CPE de cada sector se estableció el lazo redundante mediante prioridades de puerto, asignando el valor 0x80 al enlace directo desde la sectorial (ether1) y 0x90 al enlace de contingencia proveniente del nodo de respaldo (ether3), de modo que este último permanece en estado de bloqueo hasta que se produzca un fallo en la ruta principal.

En la siguiente Tabla 38 se detallan los parámetros que diferencian a cada uno de los tres nodos de respaldo implementados.

Tabla 38. *Parámetros diferenciales de los nodos de respaldo por sector*

Parámetro	Backup Rural	Backup Urbano	Backup Empresas
Identidad del nodo	BACKUP_ZONAL_1	BACKUP_ZONAL_2	BACKUP_ZONAL_3
VLAN de usuario transportada	10	20	30
Interfaz añadida al Bridge_Sectorial	ether5	ether6	ether7
IP de gestión (VLAN 100)	10.0.100.9/24	10.0.100.19/24	10.0.100.29/24
CPE con lazo redundante	CPE_Rural (Bridge_CPE)	CPE_Urbano (Bridge_Urbano)	CPE_Empresas (Bridge_Corporativo)
Enlace principal / respaldo	ether1 (0x80) / ether3 (0x90)	ether1 (0x80) / ether3 (0x90)	ether1 (0x80) / ether3 (0x90)
Puerta de enlace de gestión	10.0.100.1	10.0.100.1	10.0.100.1

3.4.14. Topología final de la infraestructura WISP implementada

La topología final desarrollada integra los tres escenarios de servicio propuestos dentro de la infraestructura WISP: sector rural (VLAN 10), sector urbano (VLAN 20) y sector empresarial

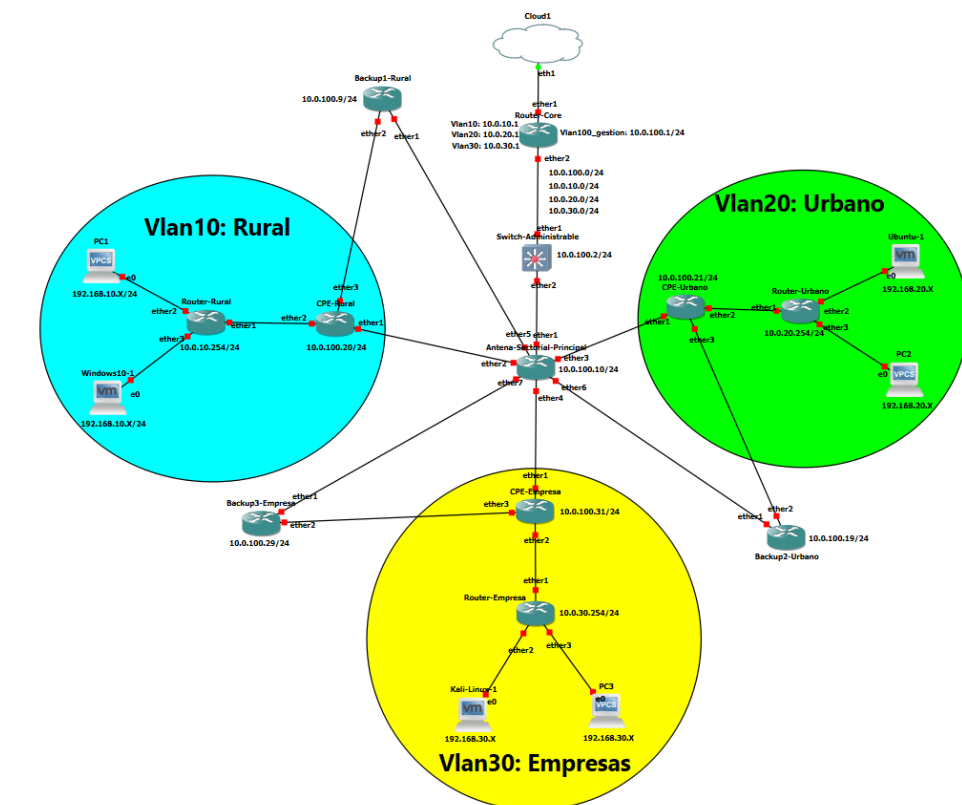
(VLAN 30), manteniendo la segmentación lógica del tráfico mediante el estándar IEEE 802.1Q y la administración centralizada a través de la VLAN 100 de gestión [53].

La arquitectura implementada se encuentra conformada por un Router Core, un Switch Administrable, una Antena Sectorial Principal, dispositivos CPE de usuario, routers de abonado, terminales finales y nodos backup configurados bajo el protocolo RSTP (Rapid Spanning Tree Protocol) para garantizar redundancia y continuidad del servicio ante posibles fallos de conectividad en el enlace principal [53].

Asimismo, se validó la correcta entrega de servicios mediante equipos finales físicos simulados (VPCS) y máquinas virtuales (Windows 10, Ubuntu Desktop y Kali Linux), verificando la asignación dinámica de direccionamiento IP, conectividad de red y acceso a internet dentro de cada segmento implementado.

En la Figura 91 se evidencia la topología final de la infraestructura WISP implementada en el entorno de simulación GNS3.

Figura 91. Topología final de la infraestructura WISP implementada



3.5. Desarrollo de la simulación en Atoll

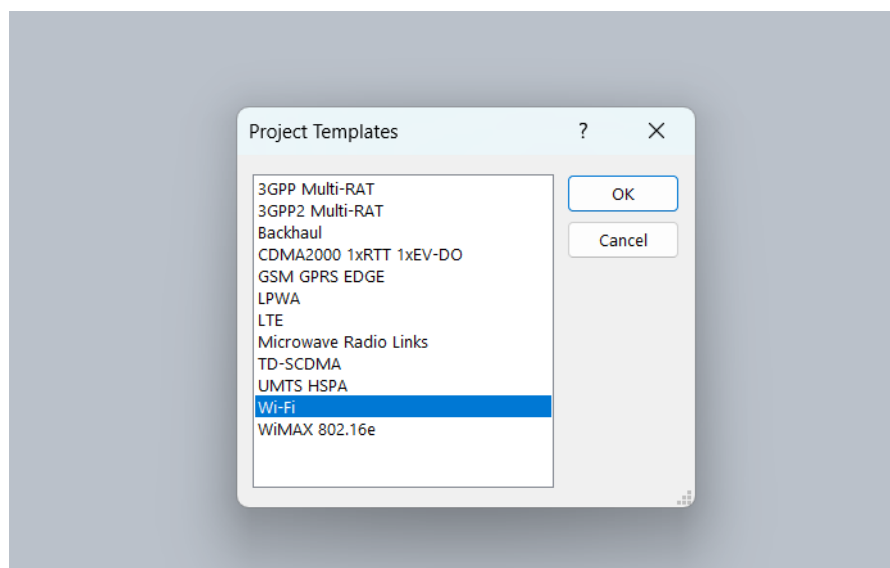
El software Atoll es una plataforma de planificación de redes de radiofrecuencia que permite simular el comportamiento de señales inalámbricas sobre un entorno geográfico real. Para el presente estudio, se utilizó Atoll en su modalidad de proyecto Wi-Fi con el fin de modelar la red WISP que cubre la península de Santa Elena, integrando datos de elevación del terreno, clasificación de uso de suelo y la configuración técnica de cada equipo de la red. A continuación, se describe paso a paso el procedimiento completo llevado a cabo.

3.5.1. Configuración inicial del proyecto

Al iniciar Atoll por primera vez, es necesario definir el tipo de tecnología sobre el que se trabajará. En este caso, se seleccionó la plantilla de proyecto Wi-Fi desde el menú Project Templates, el cual despliega una lista de tecnologías disponibles, incluyendo 3GPP Multi-RAT, LTE y WiMAX, entre otras. La selección de Wi-Fi establece el entorno de simulación adecuado para redes de acceso inalámbrico en las bandas de 2.4 GHz y 5 GHz [67].

En la Figura 92 se evidencia la selección de la plantilla de proyecto Wi-Fi dentro del menú Project Templates de Atoll.

Figura 92. Selección de la plantilla de proyecto Wi-Fi en Atoll



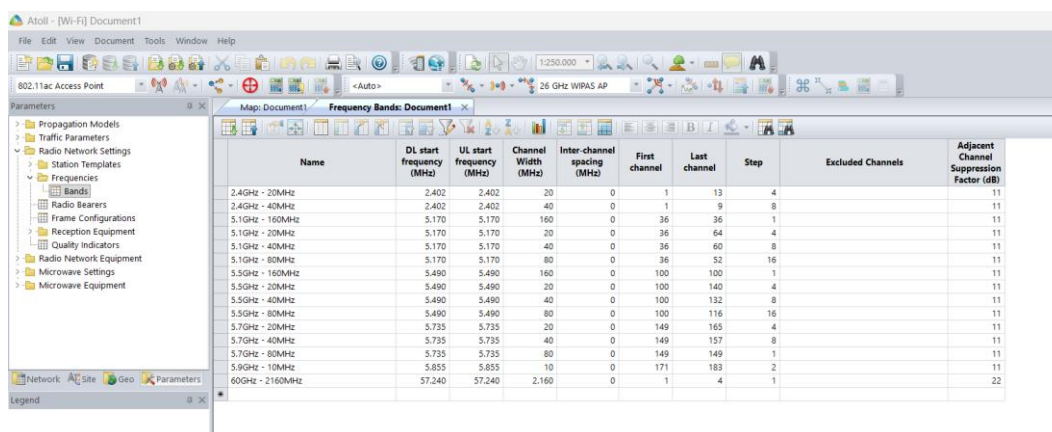
3.5.2. Configuración del canal y ancho de banda

Antes de colocar cualquier antena en el mapa, se deben definir los parámetros globales de frecuencia de la tecnología Wi-Fi. Este procedimiento se realiza desde el panel de parámetros globales de Atoll, siguiendo la secuencia descrita a continuación [67]:

1. En el panel izquierdo de la interfaz, se accede a la pestaña Parameters.
2. Se despliega la carpeta Radio Network Settings.
3. Se selecciona la opción Frequency.
4. Se hace clic derecho sobre Bands y se selecciona Open table para visualizar y configurar las bandas de frecuencia disponibles.

En la Figura 93 se evidencia la tabla de bandas de frecuencia desplegada en Atoll, donde se puede observar la configuración de las frecuencias disponibles para el proyecto.

Figura 93. *Tabla de bandas de frecuencia en Atoll (Radio Network Settings > Frequency > Bands)*



Name	DL start frequency (MHz)	UL start frequency (MHz)	Channel Width (MHz)	Inter-channel spacing (MHz)	First channel	Last channel	Step	Excluded Channels	Adjacent Channel Suppression Factor (dB)
2.4GHz - 20MHz	2.402	2.402	20	0	1	13	4		11
2.4GHz - 40MHz	2.402	2.402	40	0	1	9	8		11
5.1GHz - 160MHz	5.170	5.170	160	0	36	36	1		11
5.1GHz - 20MHz	5.170	5.170	20	0	36	64	4		11
5.1GHz - 40MHz	5.170	5.170	40	0	36	60	8		11
5.1GHz - 80MHz	5.170	5.170	80	0	36	52	16		11
5.5GHz - 160MHz	5.490	5.490	160	0	100	100	1		11
5.5GHz - 20MHz	5.490	5.490	20	0	100	140	4		11
5.5GHz - 40MHz	5.490	5.490	40	0	100	132	8		11
5.5GHz - 80MHz	5.490	5.490	80	0	100	116	16		11
5.7GHz - 20MHz	5.735	5.735	20	0	149	165	4		11
5.7GHz - 40MHz	5.735	5.735	40	0	149	157	8		11
5.7GHz - 80MHz	5.735	5.735	80	0	149	149	1		11
5.9GHz - 10MHz	5.855	5.855	10	0	171	183	2		11
60GHz - 2160MHz	57.240	57.240	2.160	0	1	4	1		22

Para el presente proyecto WISP, se priorizó la banda de 5.5 GHz correspondiente al estándar UNII-2, utilizada por los equipos de las marcas MikroTik y Ubiquiti en enlaces de larga distancia. La tabla de bandas permite configurar los siguientes parámetros [67]:

- Channel Width (MHz): Define el ancho de banda del canal. Se utilizó 20 MHz para las zonas rural, urbana y empresarial (VLAN 10, VLAN 20 y VLAN 30), por su mayor estabilidad ante interferencias en distancias largas.

- First / Last Channel: Corresponde a los números de canal equivalentes a los utilizados en equipos reales, tales como el canal 149 o 165.
- DL / UL start frequency: Indica la frecuencia exacta en MHz en la que comienza la transmisión de la antena en cada dirección (downlink y uplink).

3.5.3. Obtención e importación de datos geográficos

Para lograr una simulación de propagación precisa, Atoll requiere dos tipos de datos geográficos: el modelo digital de elevación del terreno (DTM/DEM) y la capa de uso de suelo (Clutter). Ambos datos son fundamentales para que el simulador calcule la línea de vista entre los nodos y la atenuación adicional provocada por la vegetación, edificaciones y otros obstáculos físicos del entorno.

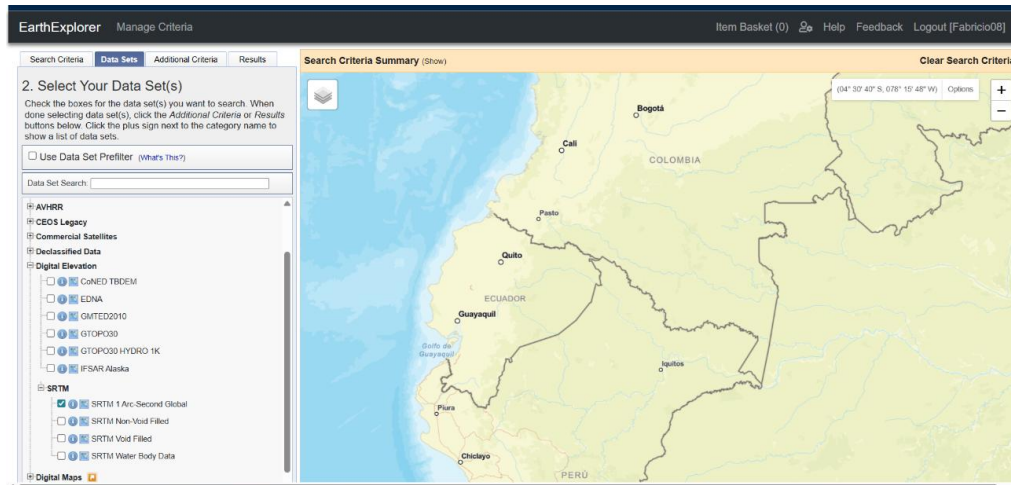
Datos de elevación del terreno – USGS EarthExplorer

El modelo digital de elevación se obtuvo de la plataforma USGS EarthExplorer (earthexplorer.usgs.gov), utilizando el dataset SRTM 1 Arc-Second Global, que proporciona datos de altimetría de forma gratuita con una resolución de 30 metros, cubriendo la totalidad del territorio ecuatoriano. El procedimiento de descarga fue el siguiente [58]:

- En la plataforma EarthExplorer, se accedió a la pestaña Data Sets y se verificó que la casilla SRTM 1 Arc-Second Global estuviese seleccionada dentro de la categoría Digital Elevation [58].

En la Figura 94 se evidencia la selección del dataset SRTM 1 Arc-Second Global dentro de la categoría Digital Elevation de USGS EarthExplorer.

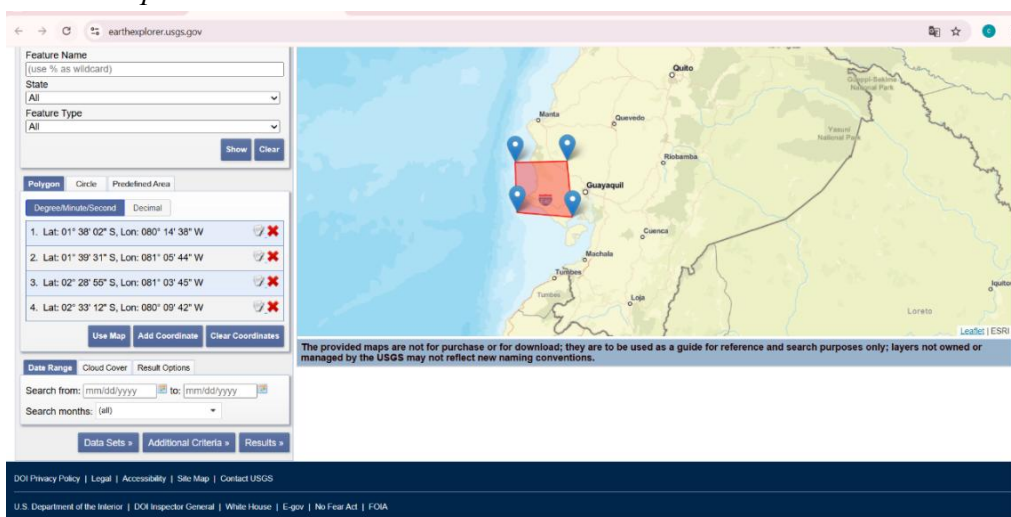
Figura 94. Selección del dataset SRTM 1 Arc-Second Global en USGS EarthExplorer



- En la pestaña Search Criteria, se utilizó la herramienta Use Map para definir el área de búsqueda centrando el mapa sobre la península de Santa Elena, Ecuador [58].

En la Figura 95 se evidencia la definición del área de búsqueda mediante coordenadas sobre la península de Santa Elena dentro de la plataforma EarthExplorer.

Figura 95. Definición del área de búsqueda mediante coordenadas sobre la península de Santa Elena en EarthExplorer

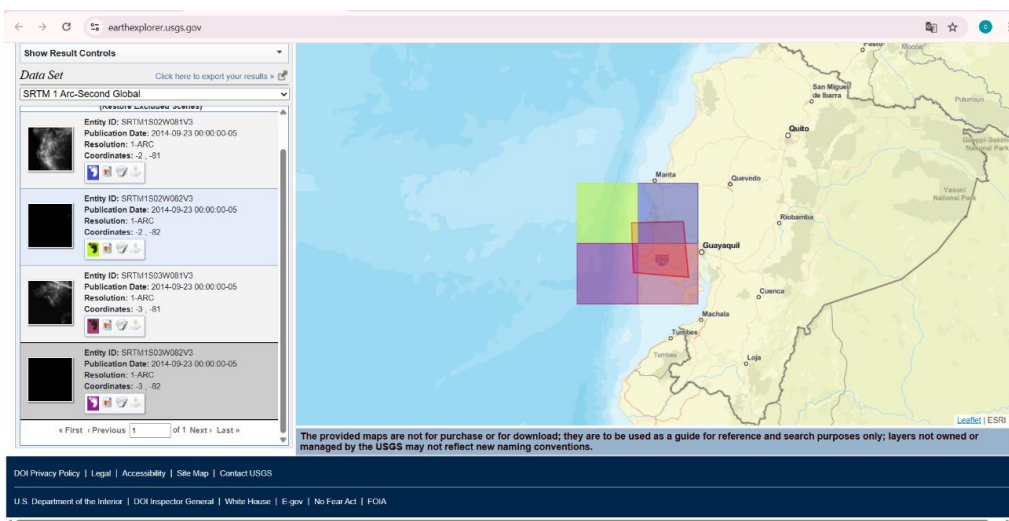


- En la pestaña Results, se identificó el tile correcto haciendo clic en el ícono Show Footprint de cada resultado hasta encontrar el que cubriera la totalidad de la

península de Santa Elena y se extendiese hacia el interior, en dirección a Guayaquil [58].

En la Figura 96 se evidencia la identificación del tile SRTM correcto resaltado sobre el mapa, el cual abarca la zona de estudio de manera completa.

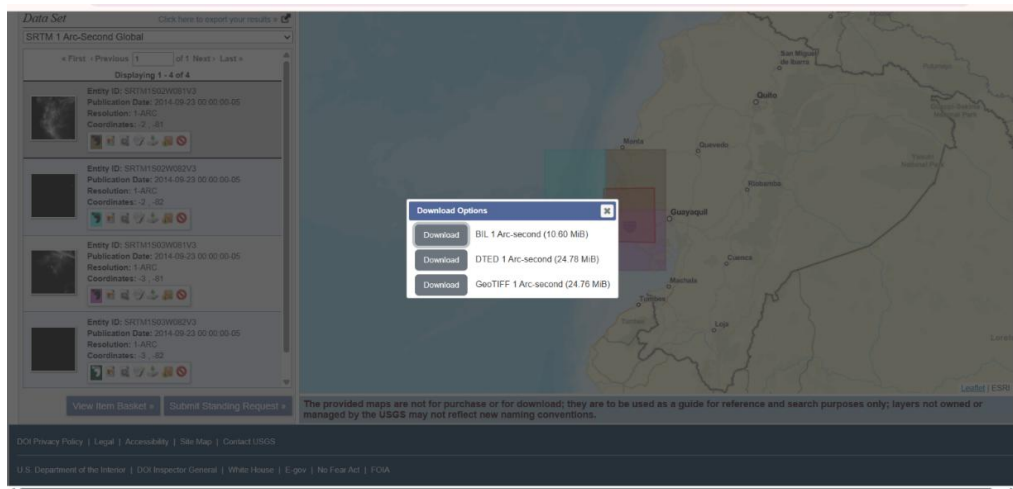
Figura 96. *Identificación del tile SRTM correcto sobre la península de Santa Elena en la pestaña Results*



- Se procedió a la descarga seleccionando exclusivamente el formato GeoTIFF 1 Arc-second, cuyo peso es de aproximadamente 25 MB. Este archivo .tif contiene los datos de altura que Atoll utilizará para calcular la línea de vista entre las torres ubicadas en el Cerro El Tablazo y los clientes de la VLAN 10 (Rural) [58].

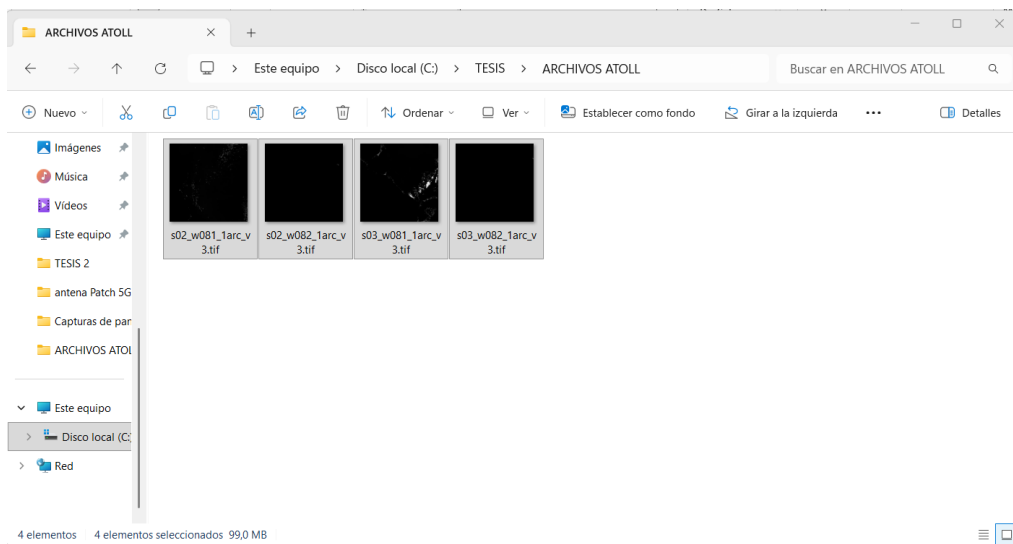
En la Figura 97 se evidencian las opciones de descarga disponibles para el tile seleccionado, destacando el formato GeoTIFF 1 Arc-second utilizado en este proyecto.

Figura 97. Opciones de descarga del tile SRTM en formato GeoTIFF



En la Figura 98 se evidencian los cuatro archivos GeoTIFF descargados desde USGS EarthExplorer, correspondientes a los tiles que cubren la península de Santa Elena.

Figura 98. Archivos GeoTIFF descargados desde USGS EarthExplorer para la zona de Santa Elena



Preprocesamiento en Global Mapper

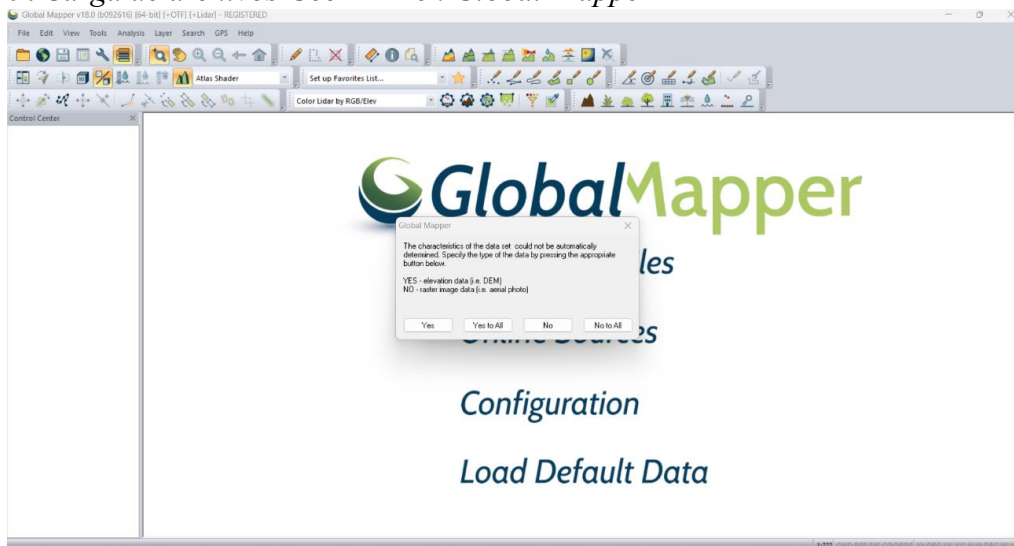
Atoll no puede importar directamente los archivos GeoTIFF de USGS en coordenadas geográficas (grados decimales), por lo que es necesario reproyectarlos al sistema UTM Zona 17S

(WGS84) utilizando el software Global Mapper 18.1, que trabaja en metros, unidad requerida por el simulador. El proceso fue el siguiente [58]:

- Se abrió Global Mapper 18.1 y se arrastraron los cuatro archivos .tif descargados al área de trabajo. Al solicitarse la confirmación del tipo de datos, se seleccionó Yes to All para identificarlos como datos de elevación (DEM) [58].

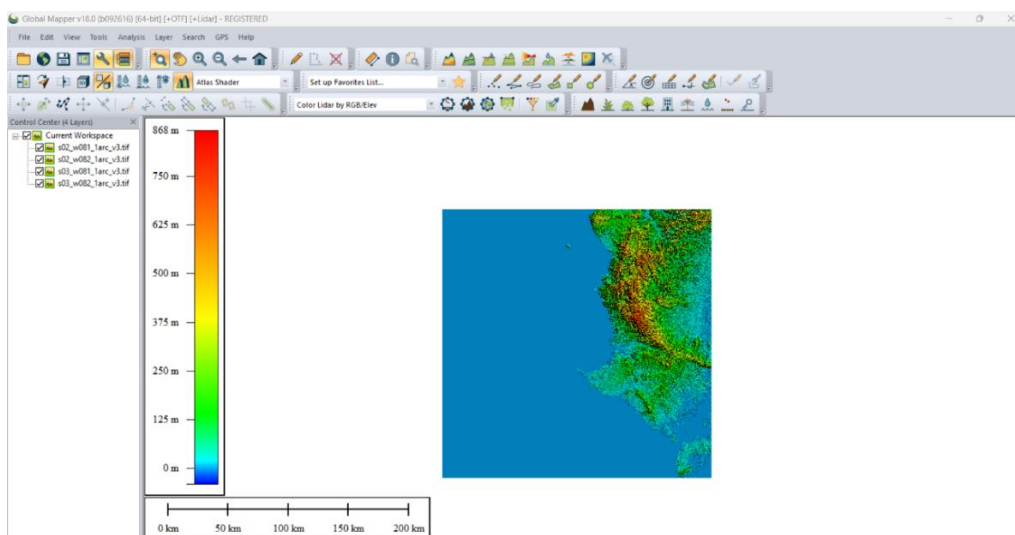
En la Figura 99 se evidencia el cuadro de confirmación que aparece al cargar los archivos GeoTIFF en Global Mapper, donde se selecciona Yes to All para reconocerlos como datos de elevación.

Figura 99. Carga de archivos GeoTIFF en Global Mapper



En la Figura 100 se evidencia el relieve tridimensional de la península de Santa Elena correctamente cargado y visualizado en Global Mapper tras la importación de los archivos SRTM.

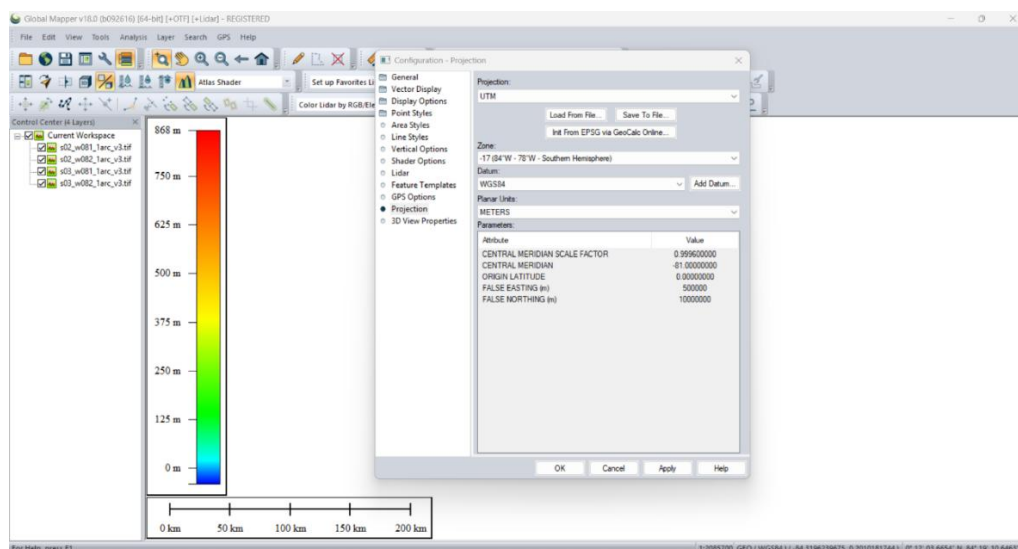
Figura 100. Visualización del relieve de la península de Santa Elena en Global Mapper tras cargar los archivos SRTM



- Se accedió a Tools > Configure... y, en la pestaña Projection, se cambió la proyección de Geographic a UTM. En el campo Zone se seleccionó la zona -17 (84W – 78W) – Southern Hemisphere y en Datum se verificó que estuviera establecido WGS84. Al aceptar, el mapa se reproyecta correctamente para Ecuador [58].

En la Figura 101 se evidencia la ventana de configuración de proyección en Global Mapper, donde se muestra la selección de UTM Zona 17S con datum WGS84 aplicada al proyecto.

Figura 101. Configuración de la proyección UTM Zona 17S (WGS84) en Global Mapper para exportar el relieve en metros



- Desde el menú File > Export > Export Elevation Grid Format..., se seleccionó el formato Vertical Mapper Grid File (.grd). En las opciones de exportación se marcó la casilla Generate PRJ (Projection) File para que Atoll pueda reconocer automáticamente el sistema de coordenadas. El archivo fue guardado con el nombre `Relieve_SantaElena_UTM17S.grd` [58].

En la Figura 102 se evidencia la ventana de opciones de exportación del software Global Mapper, donde se seleccionó el formato Vertical Mapper Grid File (.grd) para la generación del modelo de elevación compatible con el software de planificación. Posteriormente, en la Figura 103 se evidencia la activación de la opción para generar el archivo de proyección geográfica (.prj), permitiendo conservar la referencia espacial y garantizar la correcta georreferenciación de los datos exportados.

Figura 102. Selección del formato de exportación Vertical Mapper Grid File en Global Mapper

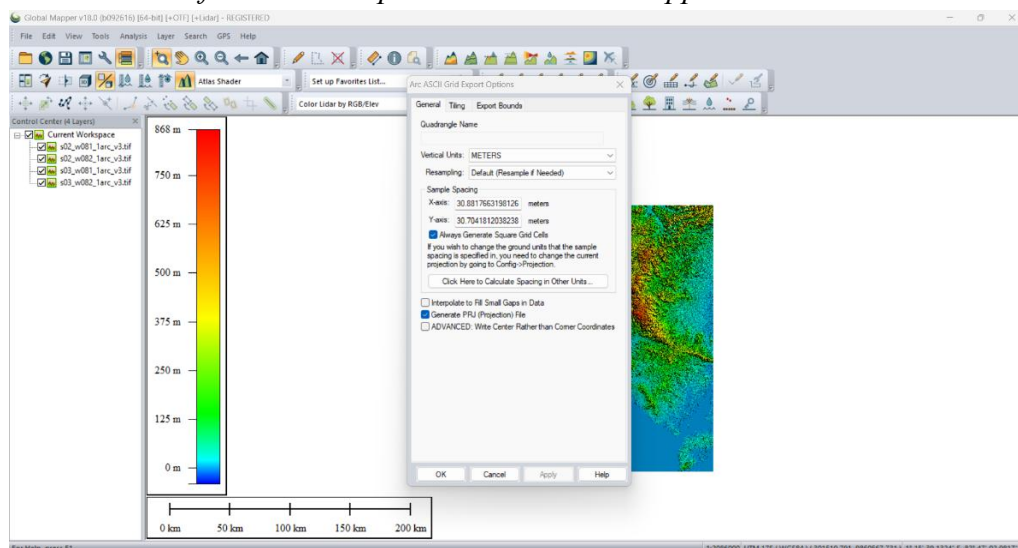
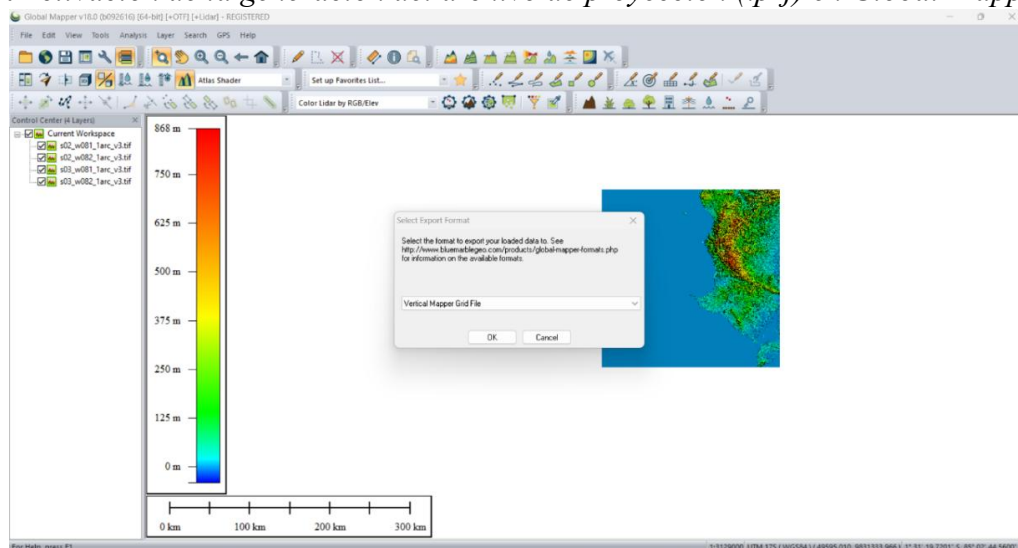


Figura 103. Activación de la generación del archivo de proyección (.prj) en Global Mapper



Datos de uso de suelo (Clutter) – ESA WorldCover

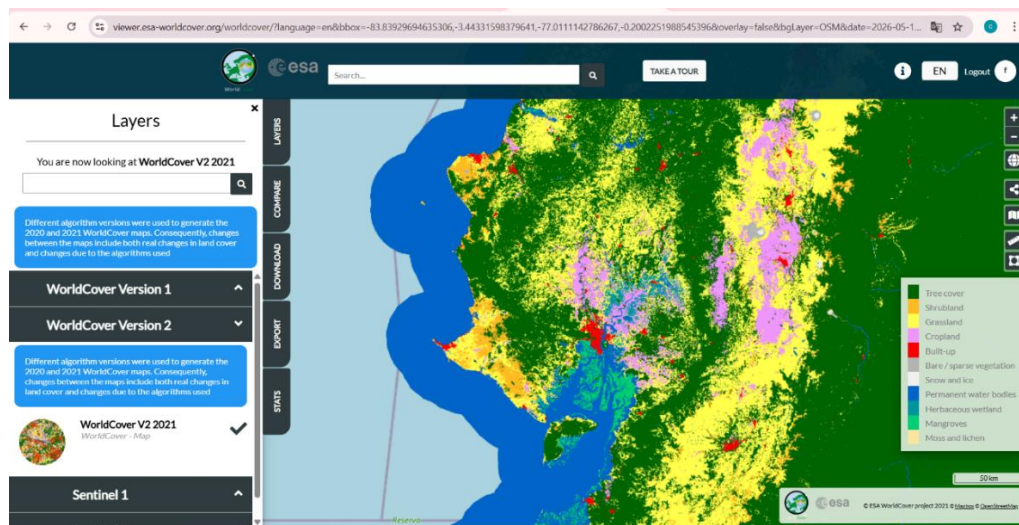
La capa de Clutter permite a Atoll identificar los obstáculos físicos presentes en el terreno (edificaciones, vegetación, cuerpos de agua) y calcular la atenuación y difracción que estos provocan sobre la señal de radiofrecuencia. Para este proyecto se utilizó la base de datos ESA WorldCover con una resolución de 10 metros.

El proceso de obtención fue el siguiente [68]:

- Se accedió al visor oficial de ESA WorldCover en viewer.esa-worldcover.org. Dado que los datos son de uso científico y educativo, es obligatorio registrarse en la plataforma Terrascope seleccionando la categoría Education y validando el correo electrónico de activación.
- En el panel lateral Layers, se seleccionó WorldCover Version 2 (2021), la cual ofrece mayor precisión en la detección de zonas urbanas desarrolladas recientemente.
- Se centró el mapa sobre la península de Santa Elena, asegurando la visibilidad de los puntos estratégicos de la red.

En la Figura 104 se evidencia la capa ESA WorldCover V2 2021 desplegada sobre la península de Santa Elena, mostrando la distribución de los diferentes tipos de cobertura de suelo.

Figura 104. Visualización de la capa ESA WorldCover V2 2021 sobre la península de Santa Elena

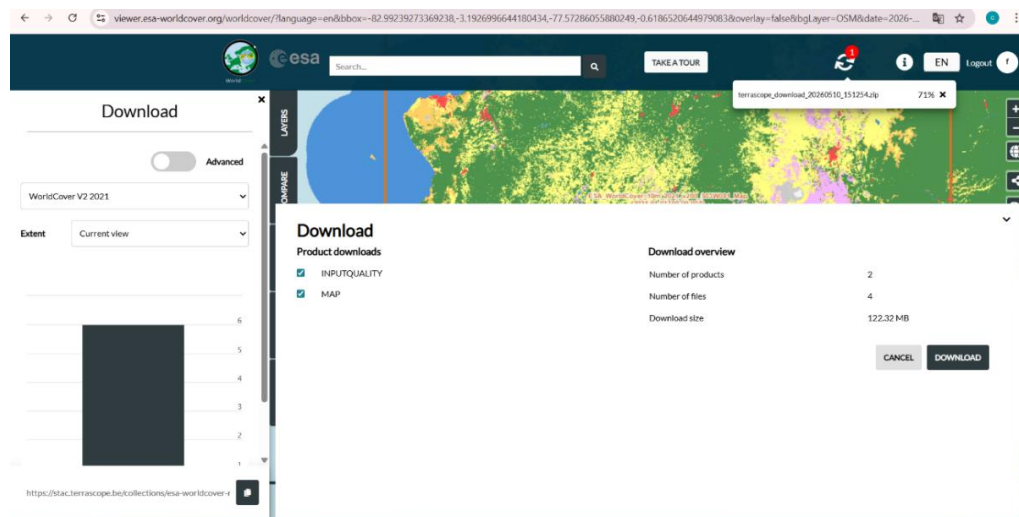


- En la pestaña vertical DOWNLOAD del menú principal, se utilizó la herramienta de dibujo de rectángulos (Bounding Box) para delimitar el área de descarga cubriendo los cantones de Salinas, La Libertad y Santa Elena. Se confirmó la

descarga y se obtuvo un archivo comprimido (.zip) con el mapa de clasificación de suelos [68].

En la Figura 105 se evidencia la configuración del Bounding Box y el panel de descarga de ESA WorldCover, indicando el tamaño del archivo generado para el área seleccionada.

Figura 105. Definición del Bounding Box y opciones de descarga en ESA WorldCover para la zona de Santa Elena

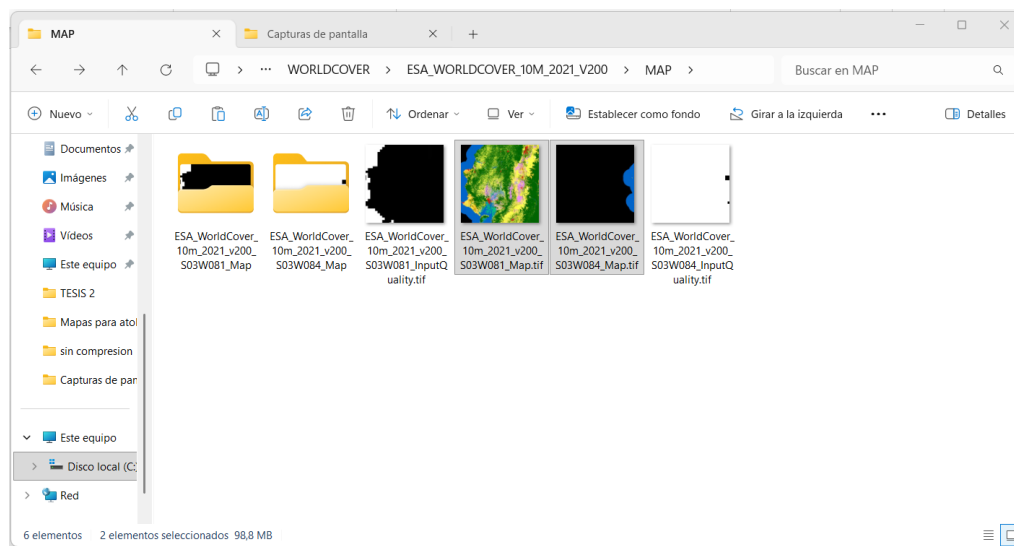


Preprocesamiento del Clutter en Global Mapper

Una vez descargados los archivos de ESA WorldCover, se abrieron en Global Mapper únicamente los archivos cuyos nombres terminan en Map.tif, que corresponden al mapa de clasificación de coberturas de suelo. Se aplicó la misma configuración de proyección UTM Zona 17S descrita anteriormente [68].

En la Figura 106 se evidencian los archivos descargados de ESA WorldCover, señalando cuáles corresponden al tipo Map.tif que deben ser utilizados en el procesamiento.

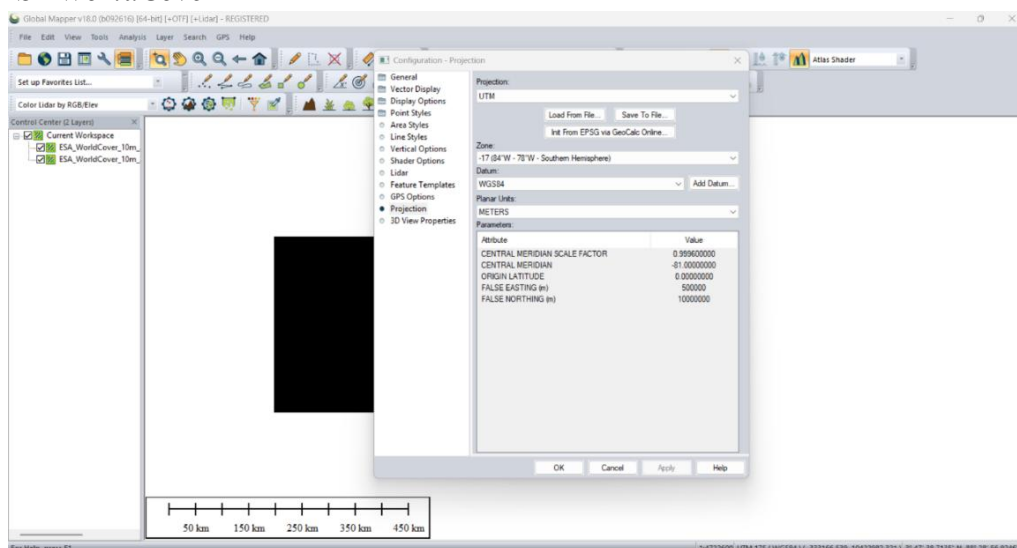
Figura 106. Archivos descargados de ESA WorldCover



- Se accedió a Tools > Configure... y, en la pestaña Projection, se cambió la proyección de Geographic a UTM. En el campo Zone se seleccionó la zona -17 (84W – 78W) – Southern Hemisphere y en Datum se verificó que estuviera establecido WGS84. Al aceptar, el mapa se reproyecta correctamente para Ecuador [68].

En la Figura 107 se evidencia la configuración de la proyección UTM Zona 17S aplicada en Global Mapper para los archivos de cobertura de ESA WorldCover, garantizando la compatibilidad con Atoll.

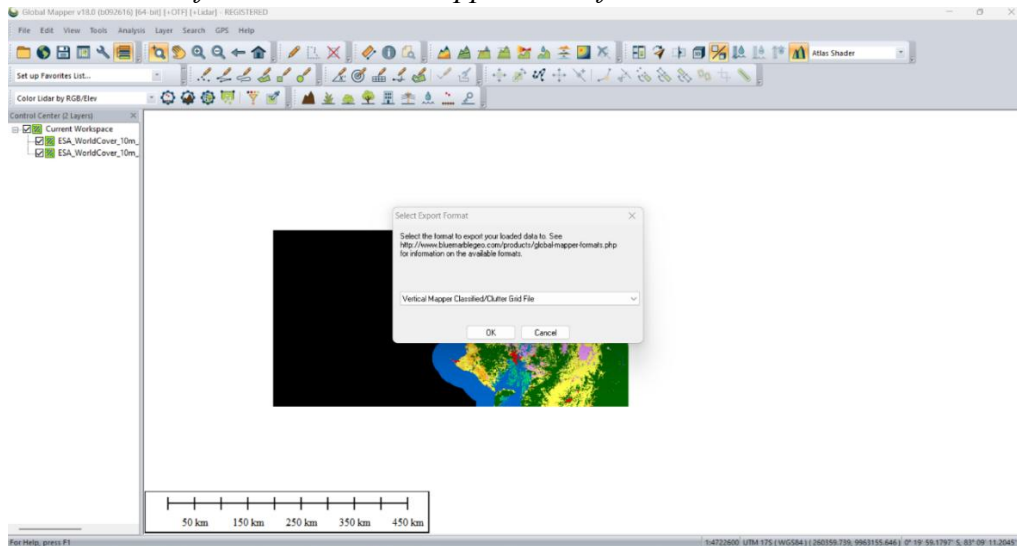
Figura 107. Configuración de proyección UTM Zona 17S en Global Mapper para los archivos de cobertura ESA WorldCover



Para la exportación compatible con Atoll, se ejecutaron los siguientes pasos:

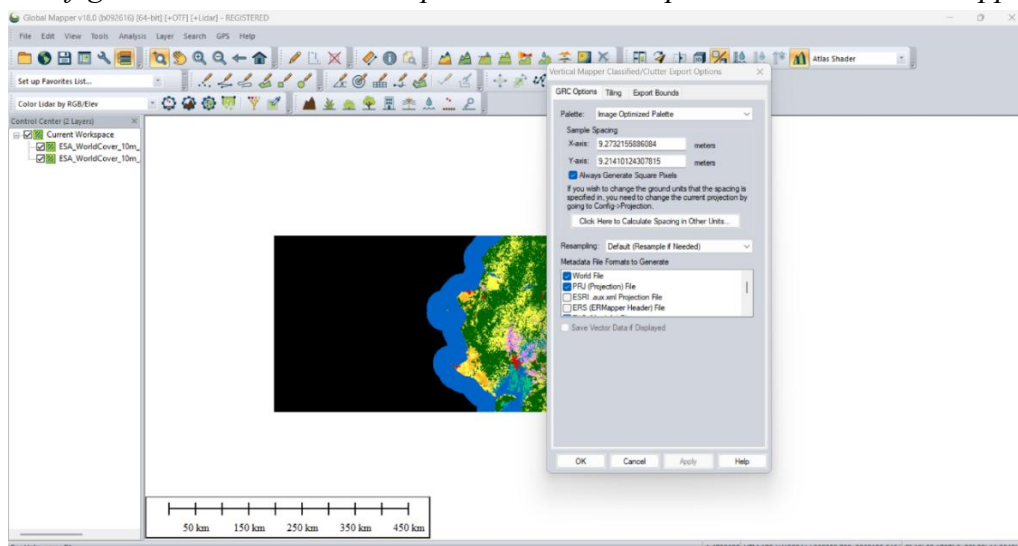
- Desde la ruta File > Export > Export Raster/Image Format..., se seleccionó el formato Vertical Mapper Classified/Clutter Grid File, como se evidencia en la Figura 108 [68].

Figura 108. Selección del formato Vertical Mapper Classified/Clutter Grid File en Global Mapper



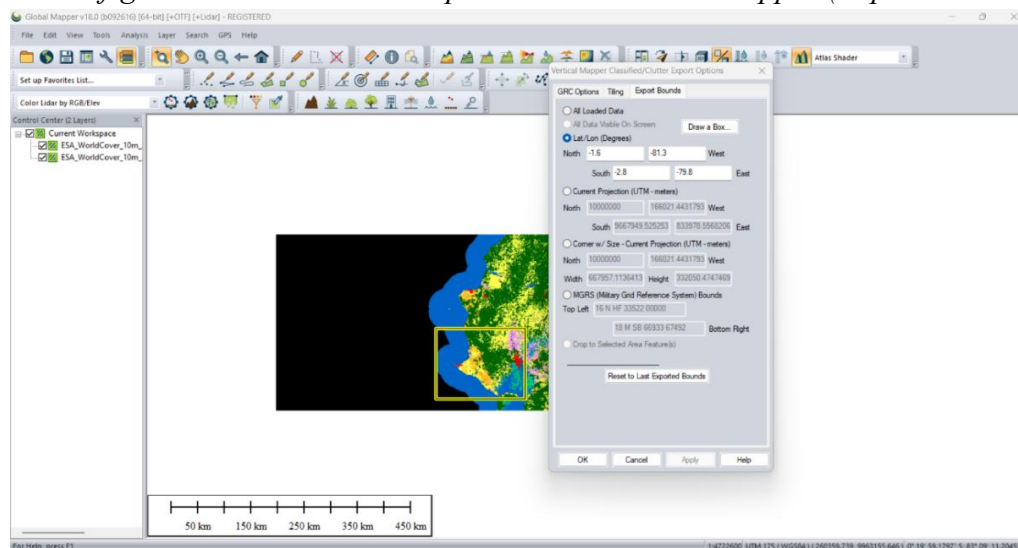
- Posteriormente, en la Figura 109 se observa la activación de las opciones PRJ (Projection) File, World File y TAB (MapInfo) File, permitiendo mantener la georreferenciación y compatibilidad de los datos espaciales para su posterior implementación en Atoll.

Figura 109. Configuración de archivos complementarios de exportación en Global Mapper



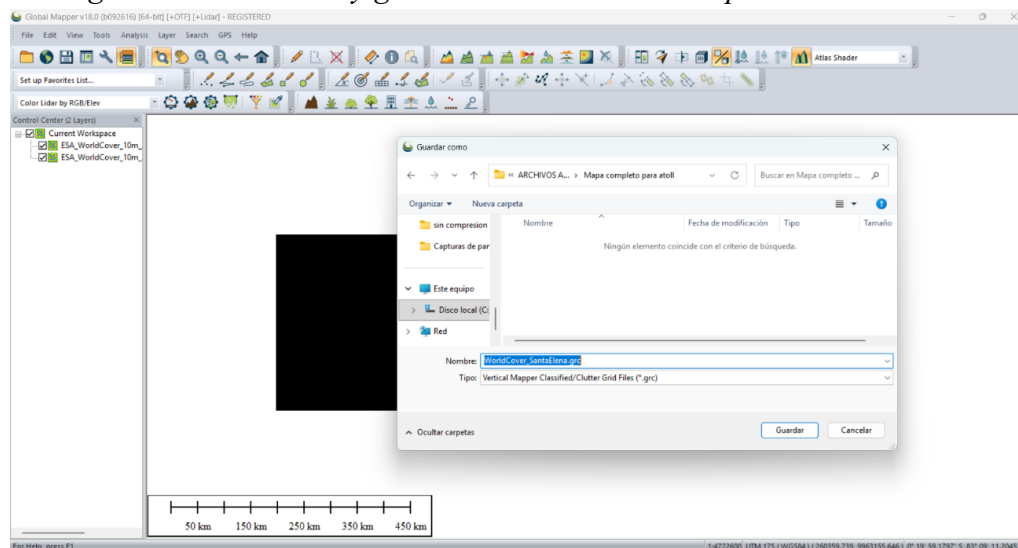
- En la pestaña Export Bounds, se verificaron y ajustaron manualmente las coordenadas del área de exportación correspondientes a Santa Elena: Norte: -1.6, Oeste: -81.3, Sur: -2.8, Este: -79.8 (en Lat/Lon Degrees), tal como se evidencia en la Figura 110 [68].

Figura 110. Configuración de límites de exportación en Global Mapper (Export Bounds)



- El archivo se guardó con el nombre WorldCover_SantaElena.grc en la carpeta del proyecto, como se evidencia en la siguiente Figura 111.

Figura 111. Asignación del nombre y guardado del archivo de exportación en Global Mapper



3.5.4. Configuración del proyecto en Atoll e importación de mapas

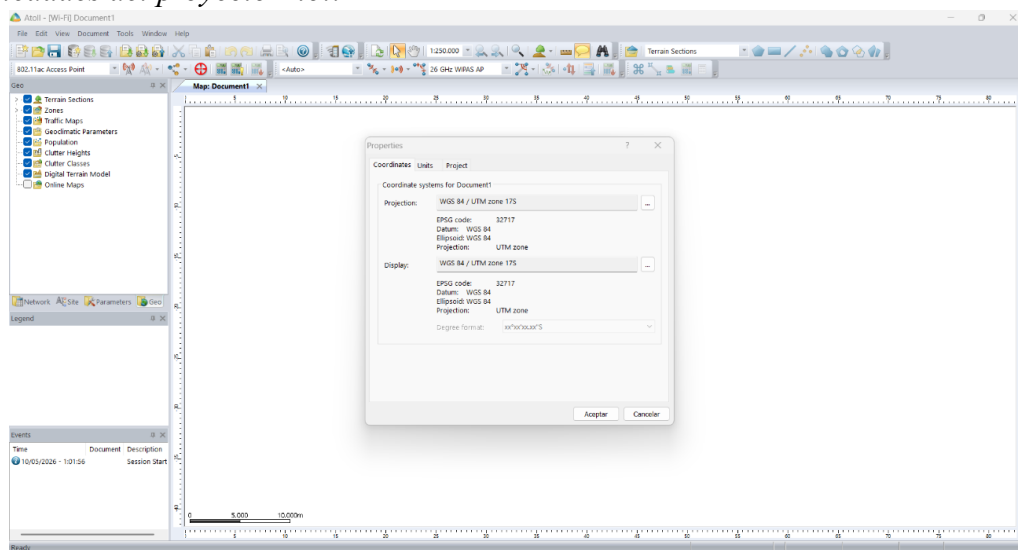
Definición del sistema de coordenadas

Antes de importar cualquier dato geográfico, Atoll debe configurarse para trabajar en el sistema de coordenadas métrico correspondiente al área de estudio. Para esto se realizó el siguiente procedimiento [58]:

- Se accedió a Document > Properties.
- En la pestaña Coordinates, se hizo clic en el botón de los tres puntos (...) junto a Projection.
- Se seleccionó WGS 84 / UTM zone 17S (Código EPSG: 32717).
- La misma proyección fue asignada en el campo Display. Al aceptar, las reglas de la pantalla cambiaron a coordenadas métricas, confirmando la correcta configuración.

En la Figura 112 se evidencia la ventana de propiedades del proyecto Atoll con el sistema de coordenadas WGS84 / UTM Zone 17S (EPSG: 32717) correctamente configurado tanto en Projection como en Display [58].

Figura 112. Configuración del sistema de coordenadas WGS84 / UTM Zone 17S (EPSG: 32717) en las propiedades del proyecto Atoll

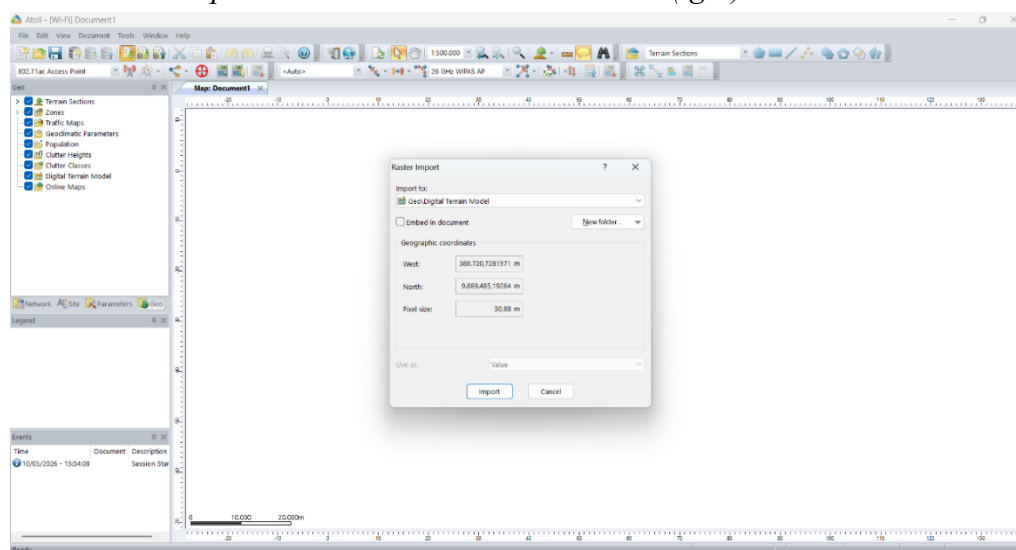


Importación del modelo digital de elevación de USGS EarthExplorer

Con el proyecto correctamente configurado, se procedió a importar el archivo de elevación obtenido desde EarthExplorer y exportado desde Global Mapper. Desde la barra de menú de Atoll se accedió a la opción de importación de datos ráster y se cargó el archivo *Relieve_SantaElena_UTM17S.grd*. El software Atoll reconoció automáticamente el sistema de coordenadas mediante el archivo .prj adjunto y desplegó el relieve tridimensional de la península de Santa Elena sobre el área de trabajo [58].

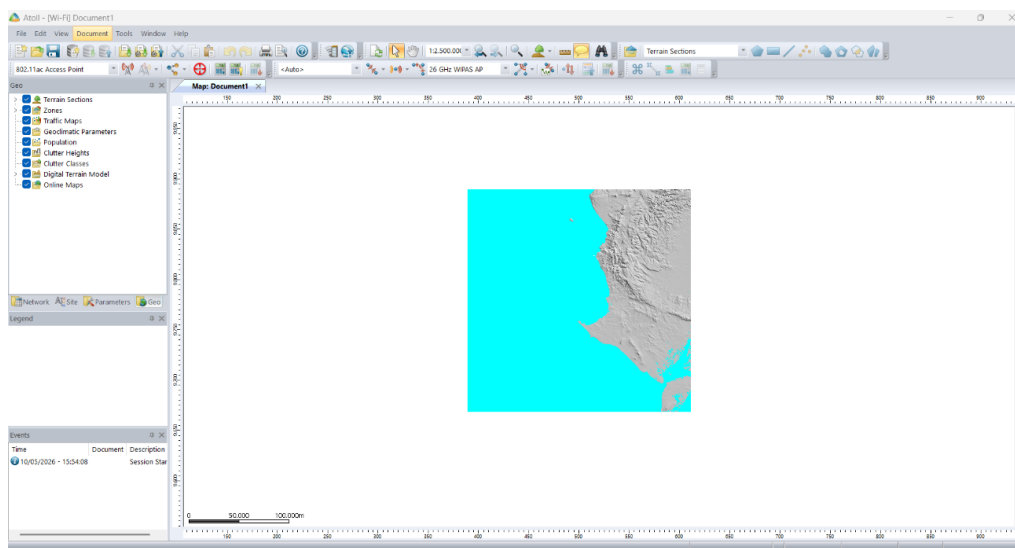
En la Figura 113 se evidencia la ventana de importación ráster de Atoll, donde se muestran los parámetros del archivo de elevación detectados automáticamente por el software.

Figura 113. *Ventana de importación del archivo de elevación (.grd) en Atoll*



En la Figura 114 se evidencia el mapa de elevación del terreno de la península de Santa Elena desplegado correctamente sobre el área de trabajo de Atoll.

Figura 114. *Mapa de elevación del terreno de la península de Santa Elena correctamente cargado en Atoll*

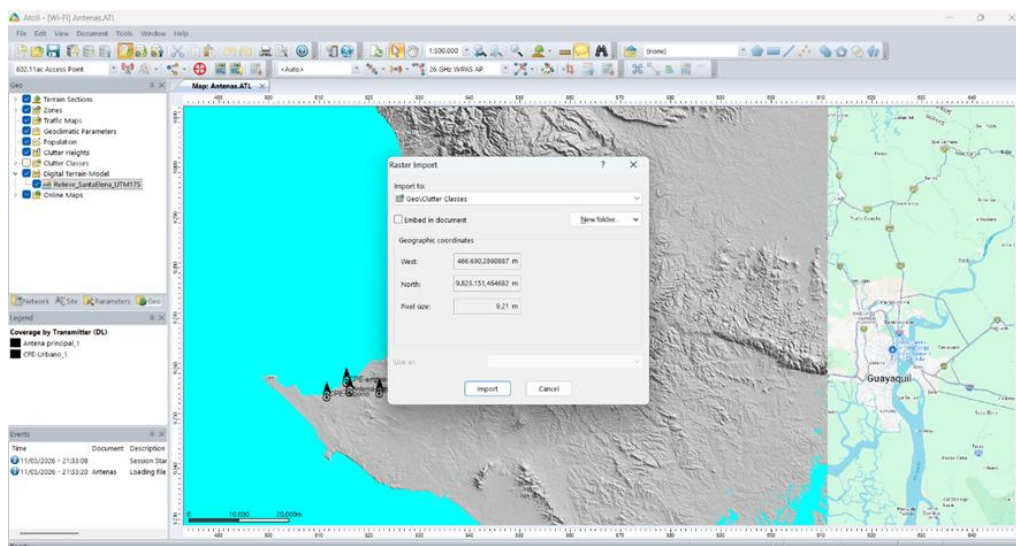


Importación de la capa de uso de suelo (Clutter) de WorldCover

De manera análoga, se procedió a importar el archivo de uso de suelo obtenido desde WorldCover y exportado previamente desde Global Mapper. Se cargó el archivo WorldCover_SantaElena.grc, generado en Global Mapper, y Atoll lo clasificó automáticamente como una capa de tipo Geo/Clutter Classified, desplegando el mapa de cobertura de suelos con los distintos tipos de terreno representados en colores [58].

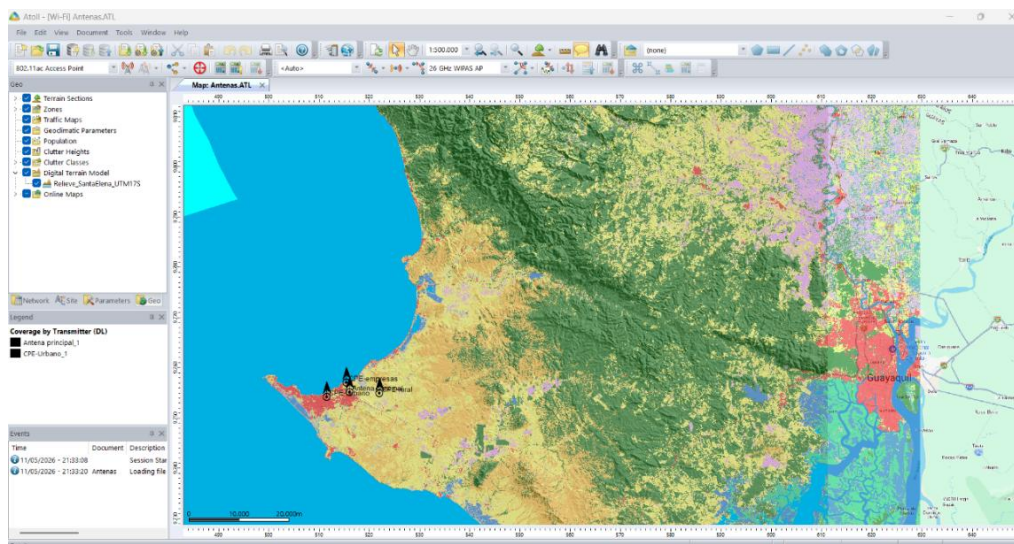
En la Figura 115 se evidencia la ventana de importación del archivo de Clutter en Atoll, donde se confirman los parámetros geográficos de la capa antes de cargarla en el proyecto.

Figura 115. *Ventana de importación del archivo de Clutter (.grc) en Atoll*



En la Figura 116 se evidencia el mapa de uso de suelo obtenido de ESA WorldCover cargado sobre la península de Santa Elena en Atoll, con los diferentes tipos de cobertura diferenciados por color.

Figura 116. *Mapa de uso de suelo (ESA WorldCover) cargado en Atoll sobre la península de Santa Elena*



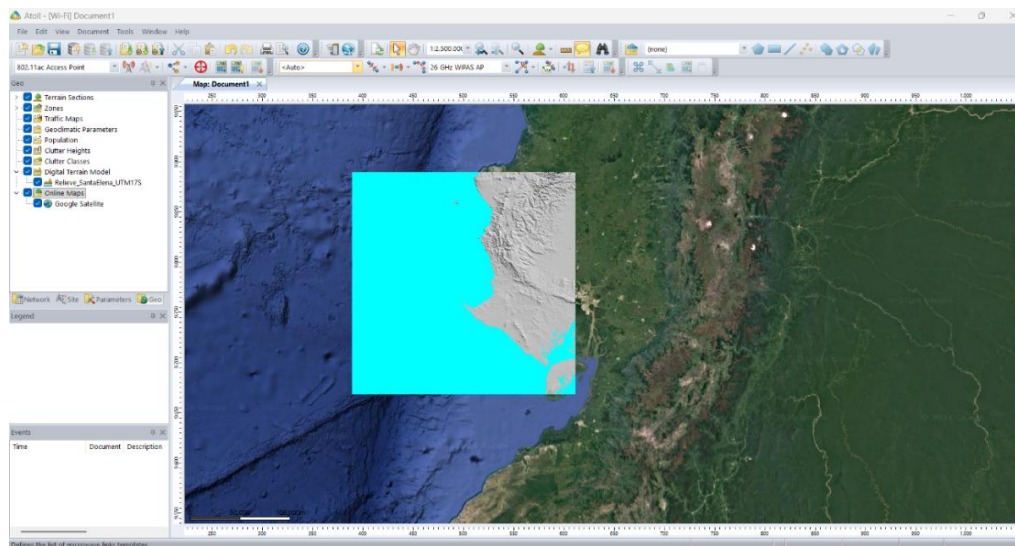
Configuración de mapas en línea

Para facilitar la ubicación geográfica de los nodos de la red, se añadieron mapas de referencia en línea. Primero se cargó el mapa base recomendado por Atoll (OpenStreetMap Standard Map) desde la opción Online Maps > New. Adicionalmente, se añadió una capa de imágenes satelitales de Google siguiendo el mismo procedimiento y configurando la URL del servidor de teselas [58]:

<http://mt1.google.com/vt/lyrs=s&x=%x&y=%y&z=%z>

En la Figura 117 se evidencia la ventana de configuración del servidor de mapa satelital de Google en la opción Online Maps de Atoll, con la URL del servicio de teselas ingresada.

Figura 117. Configuración del servidor de mapa satelital (Google Satellite) en la opción Online Maps de Atoll



3.5.5. Configuración de las clases de obstáculos (Clutter Classes)

Una vez importados los mapas, se procedió a caracterizar físicamente cada clase de cobertura de suelo para que el motor de simulación de Atoll calcule correctamente la atenuación de la señal en función del entorno. Este procedimiento se realizó desde el panel Explorer, carpeta Geo > Clutter Classes > Properties [58].

Paso 1: Configuración de parámetros físicos (pestaña Description)

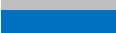
En esta pestaña se definió la altura promedio de cada tipo de obstáculo sobre el terreno (columna Height) y se tradujeron los índices de paleta (Pal Idx) asignados por ESA WorldCover a nombres descriptivos en español para facilitar la lectura de los informes de simulación [68].

Paso 2: Configuración de pérdidas por penetración (Indoor Loss)

Para estimar la cobertura en interiores en la frecuencia de operación de 5 GHz, se configuró la pérdida de penetración por tipo de obstáculo haciendo clic en la columna Indoor Loss (dB) de cada clase. Se definió la frecuencia de trabajo en 5100 MHz y se asignaron valores diferenciados según la densidad del entorno: 15 dB para zonas densamente construidas y 10 dB para zonas rurales y boscosas, compensando la atenuación producida por las paredes de bloque y ladrillo típicas de la región [68].

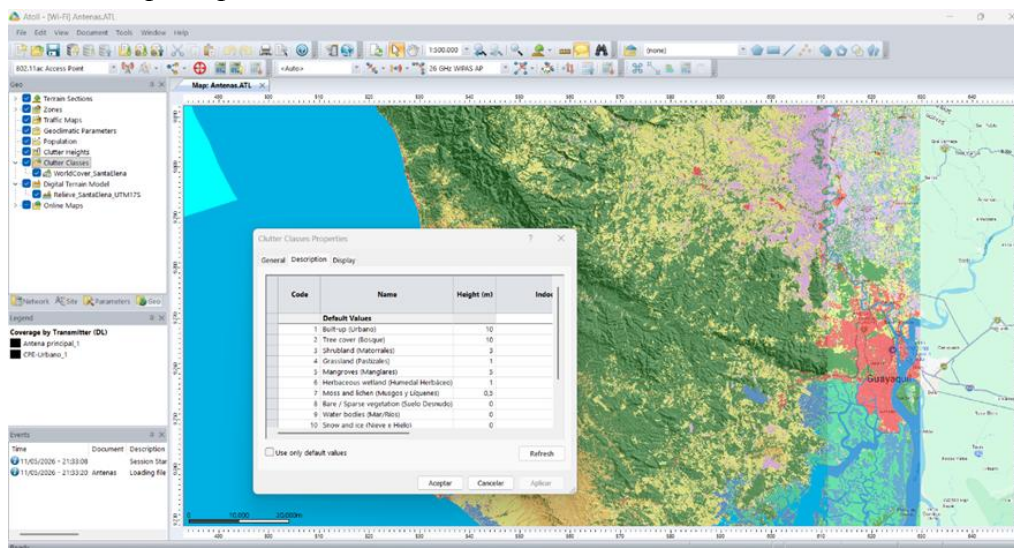
En la Tabla 39 se presentan los parámetros de configuración completos asignados a cada clase de Clutter implementada en el proyecto para la península de Santa Elena.

Tabla 39. Configuración de clases de obstáculos (Clutter Classes) en Atoll para la península de Santa Elena

Color	Code (Pal Idx)	Name (Traducción)	Height (m)	Indoor Loss (dB)
	1	Urbano / Edificios	10	15
	2	Bosque / Árboles	10	10
	3	Matorrales	3	8
	4	Pastizales	1	8
	5	Manglares	5	12
	6	Humedal Herbáceo	1	5
	7	Musgos y Líquenes	0.5	0
	8	Suelo Desnudo	0	0
	9	Agua (Océano)	0	0
	10	Hielo (Nieve)	0	0
	11	Cultivos	1.5	8

En la Figura 118 se evidencia la ventana de propiedades de Clutter Classes en Atoll, donde se aprecian los valores de altura e Indoor Loss configurados para cada tipo de cobertura de suelo.

Figura 118. Ventana de propiedades de Clutter Classes en Atoll mostrando la configuración de alturas e Indoor Loss por tipo de cobertura

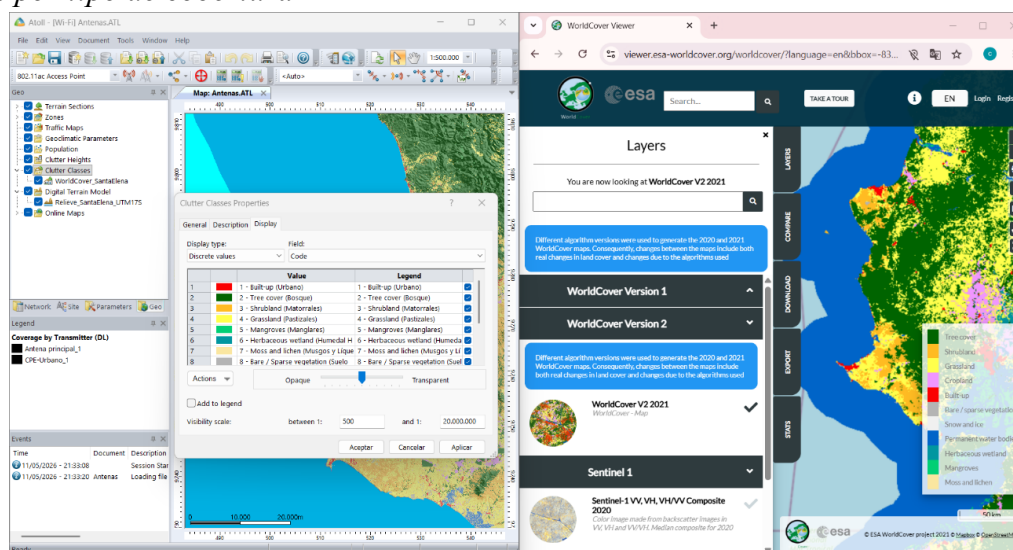


Paso 3: Verificación visual y aplicación

En la pestaña Display se verificó que los colores asignados al mapa coincidieran con la realidad geográfica de la zona (color rojo para las zonas pobladas, azul para el océano). Finalmente, se hizo clic en Apply y posteriormente en OK para que el motor de cálculo actualizara la base de datos geográfica [68].

En la Figura 119 se evidencia la verificación visual de la capa de Clutter en Atoll, confirmando que los colores asignados a cada clase de cobertura corresponden correctamente con la geografía real de la península de Santa Elena.

Figura 119. Verificación visual de la capa de Clutter en Atoll, confirmando la correcta asignación de colores por tipo de cobertura

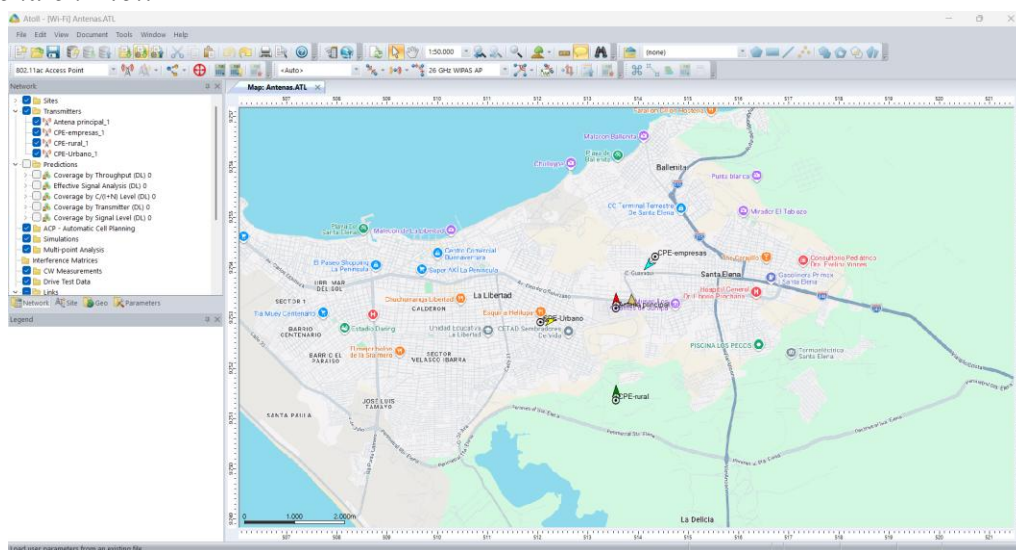


3.5.6. Colocación y configuración de antenas

Con el entorno geográfico completamente configurado, se procedió a la colocación de las antenas en el mapa mediante el ícono de torre disponible en la barra de herramientas. Se insertaron los nodos de la red en las ubicaciones geográficas reales de la península de Santa Elena, guiándose por el mapa satelital de Google Maps integrado en el proyecto. Se posicionó la antena principal en las instalaciones de la UPSE (Universidad Estatal Península de Santa Elena) y las antenas de usuario (CPE) en sus respectivas zonas de cobertura: CPE-Urbano, CPE-Empresas y CPE-Rural [58].

En la Figura 120 se evidencia la distribución geográfica de las antenas de la red WISP colocadas sobre el mapa satelital de la península de Santa Elena en Atoll.

Figura 120. Distribución de las antenas de la red WISP sobre el mapa satelital de la península de Santa Elena en Atoll



Configuración de los modelos de antena

Una vez colocados los nodos de la red sobre el mapa satelital, el siguiente paso consistió en configurar los modelos de antena reales que serían asignados a cada transmisor. Para ello, dentro del panel izquierdo de Atoll se accedió a la pestaña Parameters y, dentro de esta, al apartado Radio Network Equipment, donde se ubica la carpeta Antenas. Mediante doble clic sobre esta carpeta se ingresó a la tabla de modelos de antena, en la cual se procedió a definir los nuevos modelos correspondientes al equipamiento real utilizado en el diseño de la red WISP.

Para la antena principal se configuró el modelo Ubiquiti LiteAP LAP-120, en su variante omnidireccional, ya que esta antena irradia la señal en las tres direcciones hacia los sectores de cobertura (CPE-Urbano, CPE-Empresas y CPE-Rural) desde el nodo central ubicado en la UPSE. En la Tabla 40 se detallan los parámetros configurados para este modelo dentro de Atoll.

Tabla 40. *Parámetros de antena Ubiquiti LiteAP LAP-120*

Parámetro	Valor
Name	LiteAP LAP-120 Omnidireccional 16 dBi
Gain (dBi)	16
Manufacturer	Ubiquiti
Pattern Electrical Tilt (°)	0
Physical Antenna	LAP-120 Omni
Half-power Beamwidth	360
Min Frequency (MHz)	5.150
Max Frequency (MHz)	5.875

Posteriormente, se configuró el modelo de antena NanoStation Loco 5AC, en su variante direccional, correspondiente al equipo de usuario (CPE) instalado en cada uno de los sectores de la red. A diferencia de la antena principal, este modelo concentra su energía en una dirección específica, orientada hacia la antena principal, lo que permite establecer el enlace punto a punto entre cada CPE y el nodo central. En la Tabla 41 se muestran los parámetros configurados para este modelo.

Tabla 41. *Parámetros de antena NanoStation Loco5AC para las CPE*

Parámetro	Valor
Name	NanoStation Loco5AC Direccional 13 dBi
Gain (dBi)	13
Manufacturer	Ubiquiti
Pattern Electrical Tilt (°)	0
Physical Antenna	Loco5AC
Half-power Beamwidth	45
Min Frequency (MHz)	5.150
Max Frequency (MHz)	5.875

Con la configuración de ambos modelos de antena, quedaron definidos los parámetros técnicos que serían utilizados por cada transmisor de la red durante el proceso de simulación. En la Figura 121 se presentan los parámetros reales de las antenas configuradas dentro del simulador Atoll.

Figura 121. *Parámetros reales de antenas configurados en el simulador Atoll*

Name	Gain (dBi)	Manufacturer	Comments	Pattern	Pattern Electrical Tilt (°)	Physical Antenna	Half power Beamwidth	Min Frequency (MHz)	Max Frequency (MHz)	Pattern Electric Azimuth
2400MHz Omni 2.2dBi	2.2	Kathrein			36	Kathrein 80010430	360	1.710	6.000	
2400MHz Omni 5.7dBi	5.7	Kathrein			39.5	Kathrein 80010249	360	1.425	3.800	
2400MHz Omni 0dBi	0	Kathrein			41	Kathrein 80010709	360	1.710	2.700	
2400MHz Omni 5.8dBi	5.8	Kathrein			44	Kathrein 80010249	360	1.425	3.800	
2500MHz Omni 0dBi	0	Kathrein			46	Kathrein 80010709	360	1.710	2.700	
2500MHz Omni 2.2dBi	2.2	Kathrein			45.5	Kathrein 80010430	360	1.710	6.000	
2500MHz Omni 5.8dBi	5.8	Kathrein			48.5	Kathrein 80010249	360	1.425	3.800	
5150MHz Omni 13dBi	13	Kathrein			0	Kathrein 80010430	120	1.710	6.000	
5150MHz Omni 16dBi	16	Kathrein			0	Kathrein 80010249	120	3.150	6.000	
5200MHz Omni 2.2dBi	2.2	Kathrein			68	Kathrein 80010430	360	1.710	6.000	
5200MHz Omni 5.8dBi	5.8	Kathrein			65	Kathrein 80010249	360	5.150	6.000	
5200MHz Omni 5.8dBi	5.8	Kathrein			66	Kathrein 80010249	360	5.150	6.000	
5300MHz Omni 2.2dBi	2.2	Kathrein			67.5	Kathrein 80010430	360	1.710	6.000	
5300MHz Omni 5.8dBi	5.8	Kathrein			65	Kathrein 80010249	360	5.150	6.000	
5300MHz Omni 5.8dBi	5.8	Kathrein			67.5	Kathrein 80010249	360	5.150	6.000	
5400MHz Omni 2.2dBi	2.2	Kathrein			56	Kathrein 80010430	360	1.710	6.000	
5400MHz Omni 5.8dBi	5.8	Kathrein			66.5	Kathrein 80010249	360	5.150	6.000	
5500MHz Omni 2.2dBi	2.2	Kathrein			50	Kathrein 80010430	360	1.710	6.000	
5500MHz Omni 5.8dBi	5.8	Kathrein			0	Kathrein 80010249	360	5.150	6.000	
5550MHz Omni 5.8dBi	5.8	Kathrein			67	Kathrein 80010249	360	5.150	6.000	
5600MHz Omni 2.2dBi	2.2	Kathrein			49	Kathrein 80010430	360	1.710	6.000	
5600MHz Omni 5.8dBi	5.8	Kathrein			66.5	Kathrein 80010249	360	5.150	6.000	
5650MHz Omni 5.8dBi	5.8	Kathrein			66.5	Kathrein 80010249	360	5.150	6.000	
5700MHz Omni 2.2dBi	2.2	Kathrein			48	Kathrein 80010430	360	1.710	6.000	
5700MHz Omni 5.8dBi	5.8	Kathrein			52	Kathrein 80010249	360	5.150	6.000	
5750MHz Omni 5.8dBi	5.8	Kathrein			28	Kathrein 80010249	360	5.150	6.000	
5800MHz Omni 2.2dBi	2.2	Kathrein			47.5	Kathrein 80010430	360	1.710	6.000	
5800MHz Omni 5.8dBi	5.8	Kathrein			53	Kathrein 80010249	360	5.150	6.000	
5850MHz Omni 5.8dBi	5.8	Kathrein			29.5	Kathrein 80010249	360	5.150	6.000	
5900MHz Omni 2.2dBi	2.2	Kathrein			48	Kathrein 80010430	360	1.710	6.000	
6034 Directional Multibeam 20dBi	20	None			0	6034 Directional Multibeam	13	56.000	64.000	
LEAP LAP-120 Directional 16dBi	16	Ubiquiti			0	LAP-120	122	5.150	5.875	
NanoStation LocoSAC Directional 19dBi	19	Ubiquiti			0	LAP-120 Omni	360	5.150	5.875	
NanoStation LocoSAC Omnidirectional 13	13	Ubiquiti			0	LocoSAC	43	5.150	5.875	
					0	LocoSAC Omni	360	5.150	5.875	

Configuración de la antena principal (Antena_principal_1)

Desde la carpeta Network > Transmitters del panel Explorer, se accedió a las propiedades de la Antena_principal_1 con clic derecho > Properties. La configuración se realizó en dos pestañas [69]:

- **Pestaña Cell:**

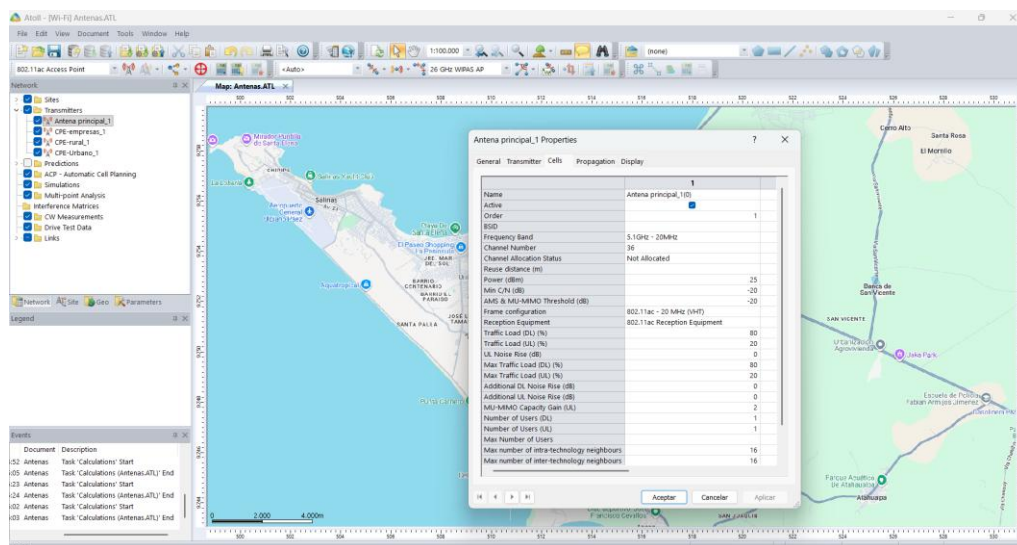
En la Tabla 42 se presentan los parámetros de celda configurados para la antena principal, incluyendo la banda de frecuencia, número de canal, tipo de trama y niveles de potencia y tráfico.

Tabla 42. *Parámetros de celda configurados para la antena principal en Atoll*

Parámetro	Valor configurado
Frequency Band	5.1 GHz – 20 MHz
Channel Number	36
Frame configuration	802.11ac – 20 MHz (VHT)
Power (dBm)	25 dBm
Min C/N (dB)	-20 dB
Traffic Load DL (%)	80 %
Traffic Load UL (%)	20 %

En la Figura 122 se evidencia la pestaña Cell de la Antena principal en Atoll, con todos los parámetros de celda ingresados según los valores de la Tabla 42.

Figura 122. Configuración de la pestaña Cell de la antena principal en Atoll



- **Pestaña Transmitter:**

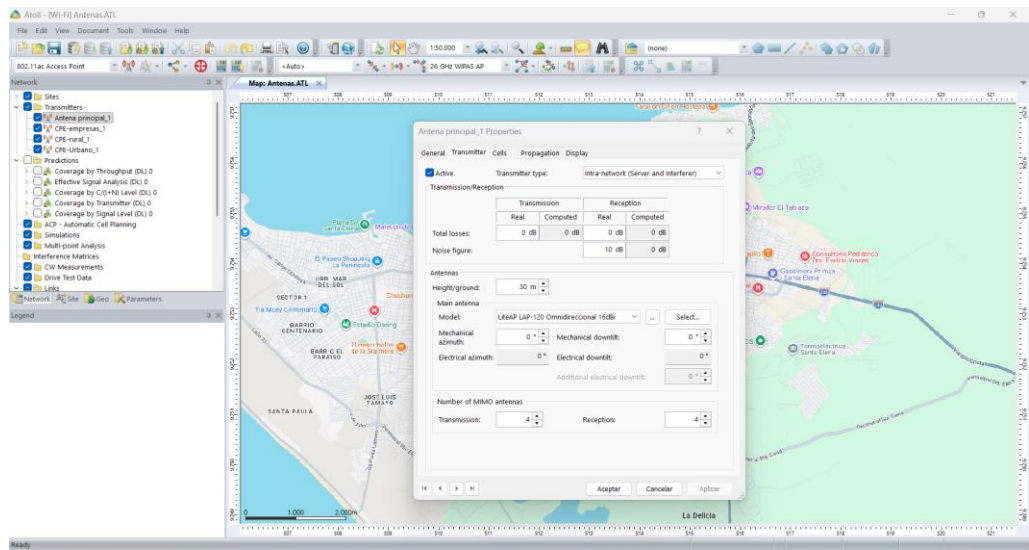
En la Tabla 43 se presentan los parámetros del transmisor configurados para la antena principal, correspondientes al modelo de antena, altura de instalación y configuración MIMO.

Tabla 43. Parámetros de transmisor configurados para la antena principal en Atoll

Parámetro	Valor configurado
Modelo de antena	LiteAP LAP-120 Omni 16 dBi
Fabricante	Ubiquiti
Height/ground	30 m
MIMO Transmission	4 antenas
MIMO Reception	4 antenas
Total losses	0 dB
Noise figure	10 dB

En la Figura 123 se evidencia la pestaña Transmitter de la Antena principal en Atoll, donde se aprecia la selección del modelo de antena Ubiquiti y la configuración de altura y MIMO.

Figura 123. Configuración de la pestaña Transmitter de la antena principal en Atoll



Configuración de la antena CPE-Urbano

De manera análoga, se accedió a las propiedades de la CPEUrbano_1 y se aplicó la siguiente configuración [69]:

- Pestaña Cell:

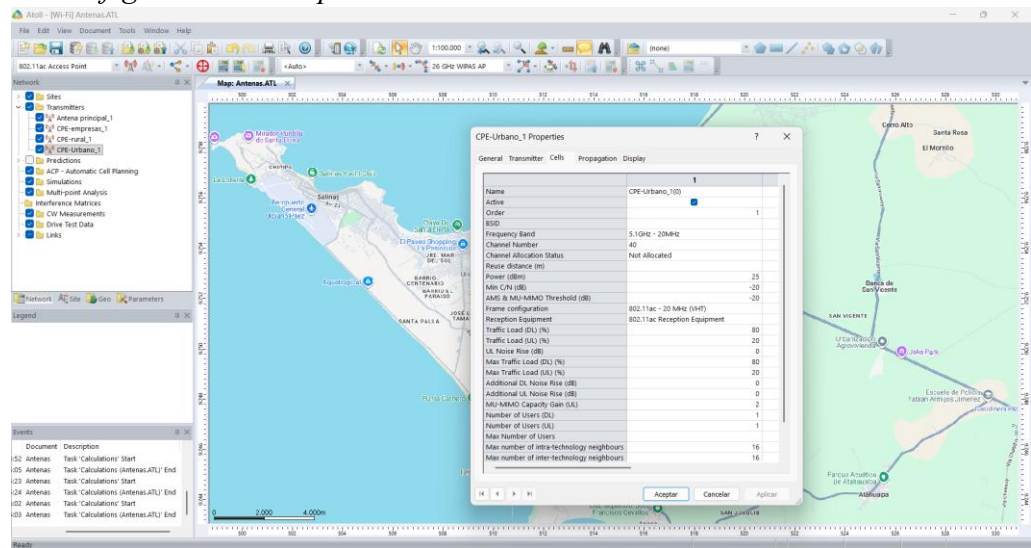
En la Tabla 44 se presentan los parámetros de celda asignados a la antena CPE-Urbano, utilizando el canal 40 para diferenciarla de los demás nodos de la red.

Tabla 44. Parámetros de celda configurados para la antena CPE-Urbano en Atoll

Parámetro	Pestaña	Valor
Frequency Band	Cells	5.1 GHz – 20 MHz
Channel Number	Cells	40
Frame configuration	Cells	802.11ac – 20 MHz (VHT)
Power (dBm)	Cells	25 dBm

En la Figura 124 se evidencia la pestaña Cell de la antena CPE-Urbano en Atoll, mostrando la asignación del canal 40 y la configuración de trama 802.11ac.

Figura 124. Configuración de la pestaña Cell de la antena CPE-Urbano en Atoll



• **Pestaña Transmitter:**

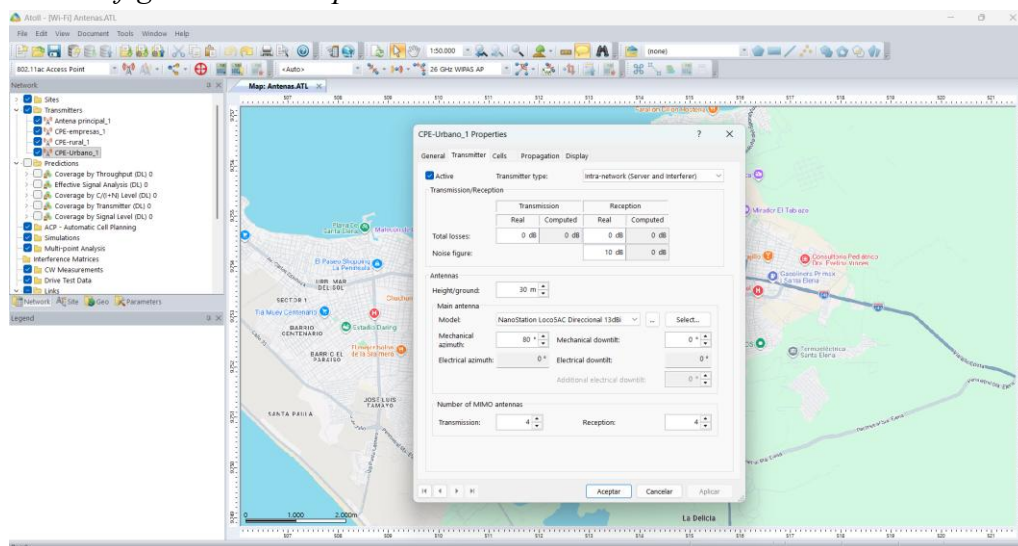
En la Tabla 45 se presentan los parámetros del transmisor de la antena CPE-Urbano, con una altura de instalación de 30 metros. En este caso se empleó una antena direccional de 13 dBi y se modificó el campo Mechanical azimuth según el ángulo de direccionamiento requerido.

Tabla 45. Parámetros de transmisor configurados para la antena CPE-Urbano en Atoll

Parámetro	Pestaña	Valor
Modelo de antena	Transmitter	NanoStation Direccional 13 dBi
Height/ground	Transmitter	30 m
Mechanical azimuth	Transmitter	80°

En la Figura 125 se evidencia la pestaña Transmitter de la antena CPE-Urbano en Atoll, con el modelo de antena y la altura de instalación configurados.

Figura 125. Configuración de la pestaña Transmitter de la antena CPE-Urbano en Atoll



Configuración de la antena CPE-Empresas

Para la antena CPE-Empresas_1, la configuración fue la siguiente [69]:

- **Pestaña Cell:**

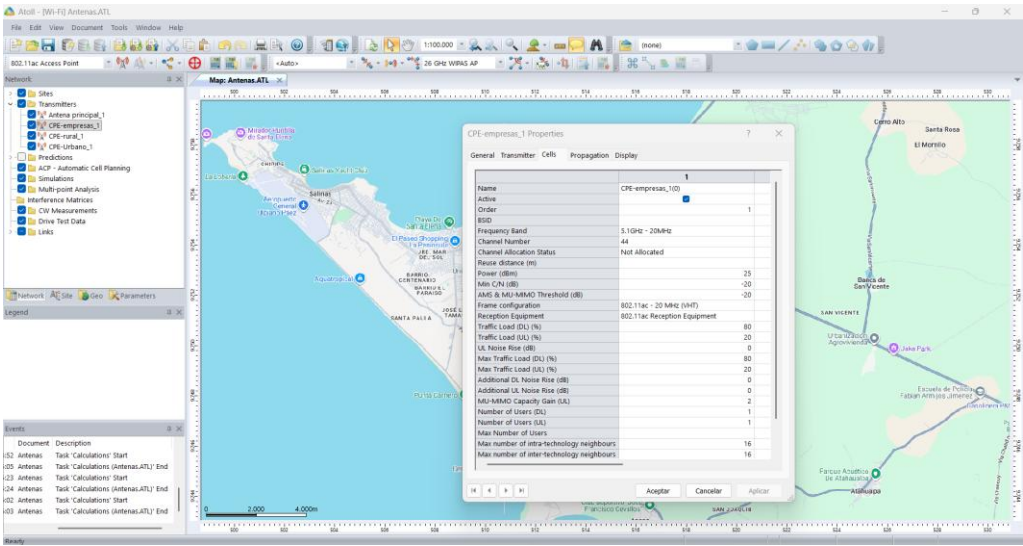
En la Tabla 46 se presentan los parámetros de celda de la antena CPE-Empresas, asignada al canal 44 para garantizar la no interferencia con los demás nodos.

Tabla 46. Parámetros de celda configurados para la antena CPE-Empresas en Atoll

Parámetro	Pestaña	Valor
Frequency Band	Cells	5.1 GHz – 20 MHz
Channel Number	Cells	44
Frame configuration	Cells	802.11ac – 20 MHz (VHT)
Power (dBm)	Cells	25 dBm

En la Figura 126 se evidencia la pestaña Cell de la antena CPE-Empresas en Atoll, donde se observa la asignación del canal 44 diferenciado de los demás nodos.

Figura 126. Configuración de la pestaña Cell de la antena CPE-Empresas en Atoll



• **Pestaña Transmitter:**

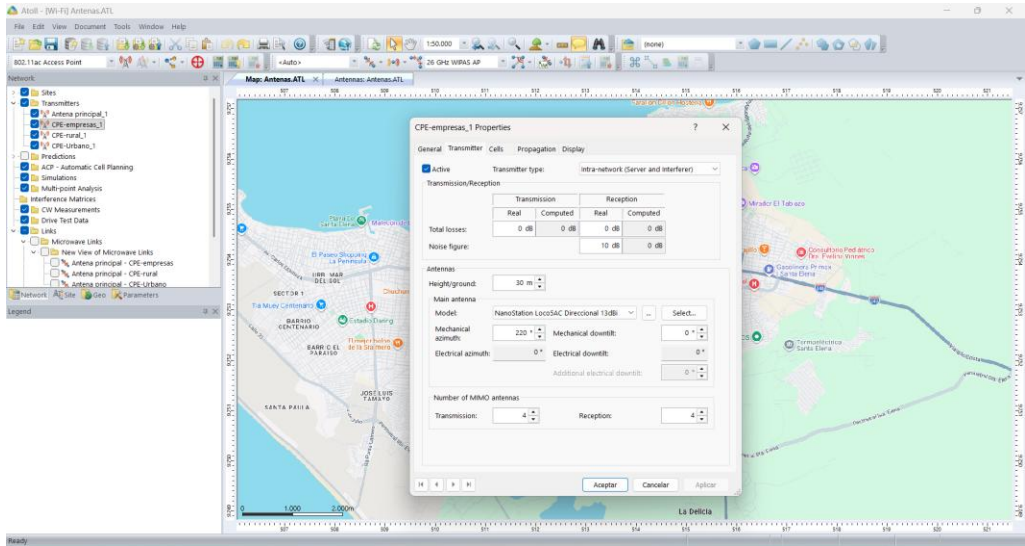
En la Tabla 47 se presentan los parámetros del transmisor de la antena CPE-Empresas, con la misma configuración de modelo y altura que el nodo CPE anterior. En este apartado también se modifica el campo Mechanical azimuth según el ángulo de dirección de la antena.

Tabla 47. Parámetros de transmisor configurados para la antena CPE-Empresas en Atoll

Parámetro	Pestaña	Valor
Modelo de antena	Transmitter	NanoStation Direccional 13 dBi
Height/ground	Transmitter	30 m
Mechanical azimuth	Transmitter	220°

En la Figura 127 se evidencia la pestaña Transmitter de la antena CPE-Empresas en Atoll con los parámetros de instalación configurados.

Figura 127. Configuración de la pestaña Transmitter de la antenna CPE-Empresas en Atoll



Configuración de la antenna CPE-Rural

Finalmente, la antenna CPE-Rural_1 fue configurada con los siguientes parámetros:

- **Pestaña Cell:**

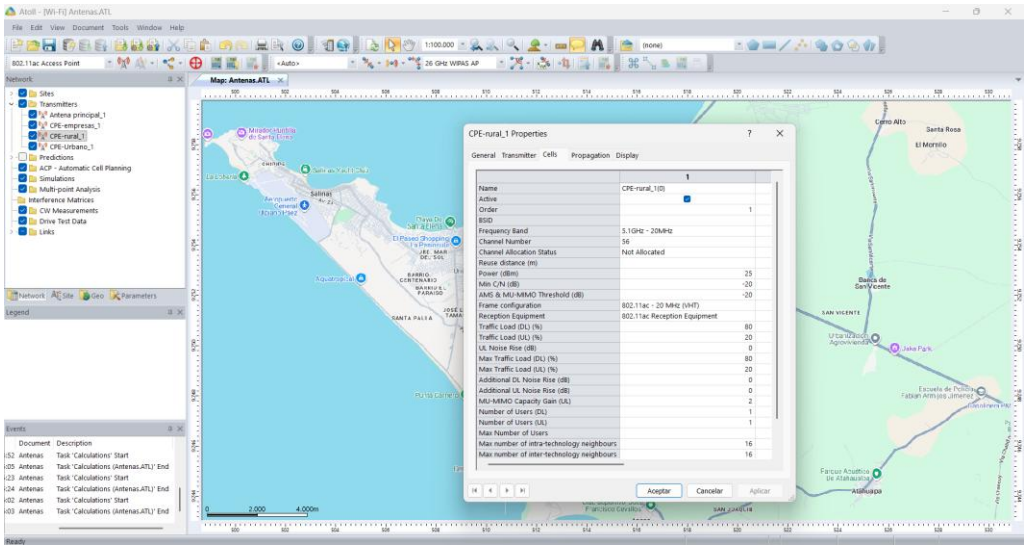
En la Tabla 48 se presentan los parámetros de celda de la antenna CPE-Rural, asignada al canal 56, el cual corresponde a una frecuencia más alejada del espectro utilizado por los demás nodos, favoreciendo la operación en entornos rurales con menor ruido ambiental.

Tabla 48. Parámetros de celda configurados para la antenna CPE-Rural en Atoll

Parámetro	Pestaña	Valor
Frequency Band	Cells	5.1 GHz – 20 MHz
Channel Number	Cells	56
Frame configuration	Cells	802.11ac – 20 MHz (VHT)
Power (dBm)	Cells	25 dBm

En la Figura 128 se evidencia la pestaña Cell de la antenna CPE-Rural en Atoll, con el canal 56 asignado para su operación en la zona de cobertura rural del proyecto.

Figura 128. Configuración de la pestaña Cell de la antena CPE-Rural en Atoll



• **Pestaña Transmitter:**

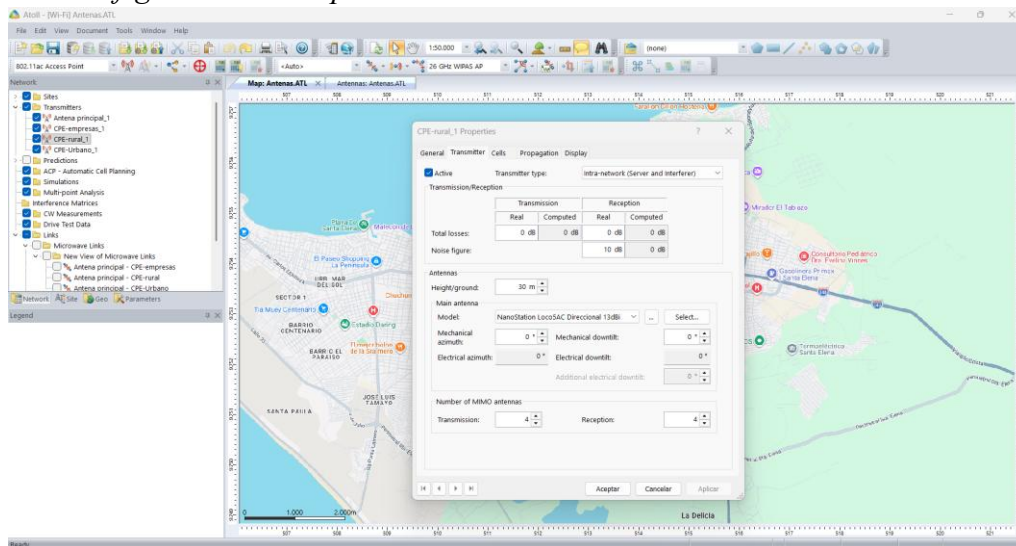
En la Tabla 49 se presentan los parámetros del transmisor de la antena CPE-Rural, con la misma configuración de modelo y altura empleada en los demás equipos CPE del proyecto.

Tabla 49. Parámetros de transmisor configurados para la antena CPE-Rural en Atoll

Parámetro	Pestaña	Valor
Modelo de antena	Transmitter	NanoStation Direccional 13 dBi
Height/ground	Transmitter	30 m

En la Figura 129 se evidencia la pestaña Transmitter de la antena CPE-Rural en Atoll, confirmando la altura de instalación y el modelo de antena seleccionado.

Figura 129. Configuración de la pestaña Transmitter de la antena CPE-Rural en Atoll



3.5.7. Creación de los enlaces punto a multipunto (PTMP)

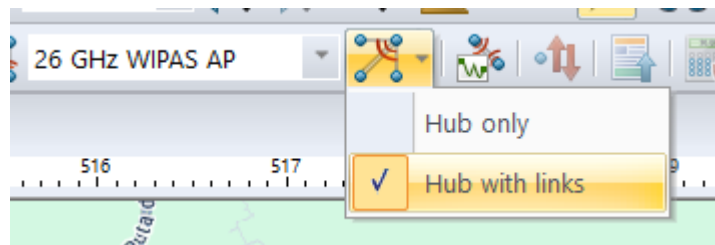
Una vez configuradas todas las antenas, se procedió a crear los enlaces punto a multipunto (PTMP) desde la antena principal hacia cada una de las antenas CPE. Este tipo de enlace modela el comportamiento real de una red WISP, donde un punto de acceso central distribuye la señal hacia múltiples clientes [58].

El procedimiento fue el siguiente [58]:

- Desde la barra de herramientas superior de Atoll, se seleccionó la opción New PMP, denominación que el simulador emplea para los enlaces punto a multipunto (PTMP).
- En el menú desplegable se eligió la opción Hub with links, la cual establece la antena principal como nodo central (hub) y genera automáticamente los enlaces hacia todas las antenas CPE configuradas.

En la Figura 130 se evidencia el menú desplegable de la opción New PMP en Atoll, donde se selecciona Hub with links para establecer la topología punto a multipunto de la red.

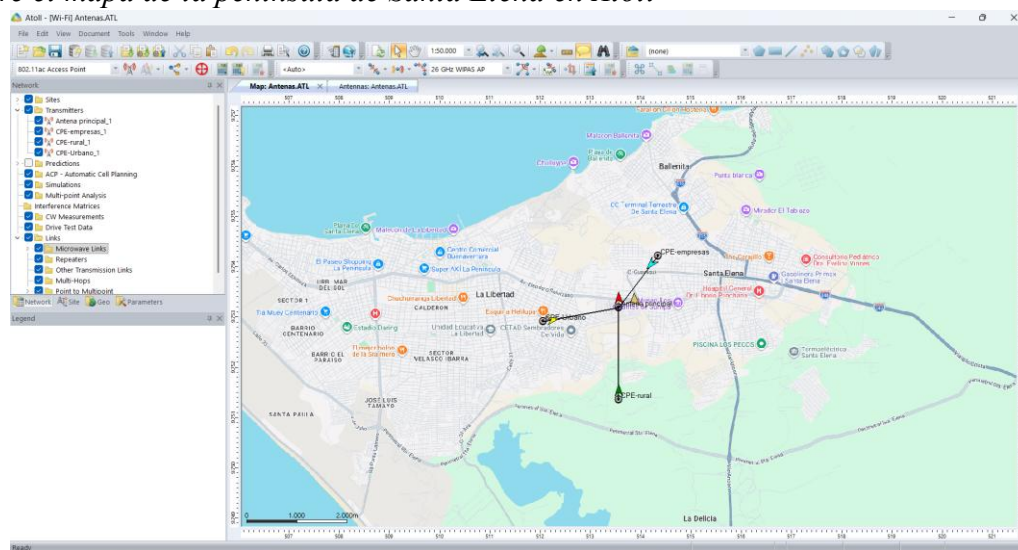
Figura 130. Selección de la opción *Hub with links* en el menú *New PMP* de la barra de herramientas de Atoll



- Una vez ejecutado el proceso, los enlaces quedaron representados en el mapa mediante líneas que conectan la antenna principal con cada CPE, lo que refleja la topología real de la red diseñada [58].

En la Figura 131 se evidencia la topología final de los enlaces PTMP establecidos en Atoll, donde se aprecian las conexiones entre la antenna principal y cada una de las antenas CPE distribuidas sobre la península de Santa Elena.

Figura 131. Vista final de los enlaces PTMP establecidos entre la antenna principal y las antenas CPE sobre el mapa de la península de Santa Elena en Atoll



Con esta configuración concluida, el entorno de simulación en Atoll quedó completamente preparado para ejecutar los análisis de cobertura, niveles de señal y modelos de propagación que se presentan en la siguiente sección de resultados.

3.6. Resumen del capítulo

En el presente capítulo se desarrolló la implementación de la infraestructura WISP propuesta mediante los entornos de simulación Atoll y GNS3, lo que permitió validar el diseño planteado para los sectores rural, urbano y empresarial.

Durante la fase de planificación en Atoll se realizaron los análisis de cobertura, perfil del terreno y distribución de enlaces inalámbricos, lo que permitió determinar la viabilidad técnica de la red y optimizar la ubicación de los diferentes nodos de comunicación [58].

Posteriormente, en GNS3 se implementó la topología lógica completa mediante dispositivos MikroTik, configurando VLAN, direccionamiento IP, servicios DHCP, NAT, mecanismos de administración y protocolos de redundancia RSTP para garantizar la continuidad operativa de la red [53].

Durante el proceso de implementación se presentó un inconveniente relacionado con la ejecución de la máquina virtual GNS3 VM en VMware Workstation. Como se observa en la Figura 49, el sistema generó un error de virtualización que impedía el arranque correcto de la máquina virtual. Tras el análisis realizado mediante las herramientas de diagnóstico del sistema operativo, se identificó que la causa del problema estaba asociada a la seguridad basada en la virtualización de Windows. Para solucionar este inconveniente, se deshabilitaron los servicios Hyper-V, Device Guard y Credential Guard mediante PowerShell y la herramienta DG Readiness Tool. Como resultado, la virtualización quedó correctamente deshabilitada, tal como se evidencia en la Figura 62, lo que permitió la ejecución normal de GNS3 VM y la continuidad del proceso de simulación [66].

Finalmente, se completó la implementación y configuración de la topología WISP propuesta mediante los entornos de simulación Atoll y GNS3, con la integración de los diferentes segmentos de red correspondientes a los sectores rural, urbano y empresarial; asimismo, se documentaron los procedimientos de configuración, los inconvenientes presentados durante el desarrollo y las soluciones aplicadas para garantizar la correcta integración de los dispositivos y servicios dentro de la infraestructura diseñada.

Capítulo 4: Resultados y validación de la red WISP propuesta

4.1. Introducción

El presente capítulo expone los resultados obtenidos a partir de las simulaciones realizadas en las dos plataformas empleadas durante el desarrollo del proyecto: GNS3, utilizada para la simulación lógica de la infraestructura de red, y Atoll, empleada para la planificación y predicción de cobertura radioeléctrica del sistema WISP propuesto para la provincia de Santa Elena.

En la primera parte se presentan las verificaciones funcionales ejecutadas sobre la topología simulada en GNS3, que abarcan la validación del direccionamiento IP, el servicio DHCP, la segmentación mediante VLAN, el acceso a internet, el análisis de tráfico con Wireshark, la medición estadística de latencia, las pruebas de rendimiento con WinBox y la validación de rutas redundantes mediante repetidores. Cada prueba fue diseñada para confirmar que los servicios configurados operan conforme a los requerimientos establecidos en el diseño de la red.

En la segunda parte se presentan los resultados de la planificación RF en Atoll, que incluyen el análisis de enlaces, cobertura de señal, zona de Fresnel, modelo de propagación y visualización 3D en Google Earth. Finalmente, se incluye un análisis comparativo entre los valores simulados y los obtenidos por el equipo de implementación real en campo.

4.2. Resultados de la simulación de la red WISP en GNS3

A continuación, se presentan los resultados derivados de la simulación lógica de la red WISP en el entorno GNS3. Las pruebas fueron ejecutadas de forma sistemática sobre cada uno de los segmentos de red que conforman la topología diseñada, con el fin de verificar el correcto funcionamiento de los servicios implementados en los routers MikroTik y en los equipos finales asignados a cada zona de cobertura.

4.2.1. Validación del direccionamiento IP

Una vez concluida la configuración de todos los dispositivos que conforman la topología simulada en GNS3, se procedió a verificar la correcta asignación de direcciones IP en los puntos de referencia más representativos de la red. Esta verificación se realizó en tres niveles jerárquicos:

el router principal (Router_Core), la Antena Sectorial Principal y los routers de acceso de cada zona (Router_Rural, Router_Urbano y Router_Empresas).

Para ejecutar esta validación se utilizó el comando propio del sistema operativo MikroTik RouterOS:

```
/ip address print
```

Este comando despliega en consola todas las interfaces configuradas en el dispositivo, junto con sus respectivas direcciones IP, redes asociadas e interfaces físicas o virtuales a las que pertenecen, lo cual permite verificar de forma directa y precisa el estado del direccionamiento en cada nodo.

Primer punto de referencia: Router_Core

En el Router_Core, que constituye el nodo central de la red y el punto de interconexión entre todos los segmentos VLAN, se pudo constatar la correcta asignación de todas las direcciones IP correspondientes a cada subred. Como se aprecia en la Figura 132, el router dispone de cuatro interfaces virtuales configuradas: VLAN10_Rural con la dirección 10.0.10.1/24, VLAN20_Urbano con la dirección 10.0.20.1/24, VLAN30_Empresas con la dirección 10.0.30.1/24 y VLAN100_Gestion con la dirección 10.0.100.1/24, esta última destinada exclusivamente a la administración remota de los dispositivos de red. Adicionalmente, se identifica la dirección dinámica asignada por el proveedor de acceso a internet en la interfaz ether1, correspondiente a la red 192.168.205.0/24, que habilita la salida hacia el exterior mediante el proceso de traducción de direcciones NAT.

Figura 132. Verificación del direccionamiento IP en el Router_Core

```
[admin@Router_Core] > /ip address print
Flags: D - DYNAMIC
Columns: ADDRESS, NETWORK, INTERFACE, VRF
# ADDRESS NETWORK INTERFACE VRF
0 10.0.10.1/24 10.0.10.0 VLAN10_Rural main
1 10.0.20.1/24 10.0.20.0 VLAN20_Urbano main
2 10.0.30.1/24 10.0.30.0 VLAN30_Empresas main
3 10.0.100.1/24 10.0.100.0 VLAN100_Gestion main
4 D 192.168.205.135/24 192.168.205.0 ether1 main
[admin@Router_Core] >
```

Segundo punto de referencia: Antena Sectorial Principal

En el segundo punto de verificación, correspondiente a la Antena Sectorial Principal, se comprobó la asignación de la dirección IP perteneciente a la VLAN 100 de gestión, que es la interfaz a través de la cual se administra este equipo de forma remota. Como se observa en la Figura 133, la dirección 10.0.100.10/24 fue correctamente asignada a la interfaz VLAN100_Gestion_Antena, lo que garantiza la accesibilidad de este nodo desde el plano de administración de la red sin interferir con el tráfico de datos de los usuarios.

Figura 133. Verificación del direccionamiento IP en la antena sectorial principal

```
[admin@Antena_Sectorial_Principal] > /ip address print
Columns: ADDRESS, NETWORK, INTERFACE, VRF
# ADDRESS NETWORK INTERFACE VRF
0 10.0.100.10/24 10.0.100.0 VLAN100_Gestion_Antena main
[admin@Antena_Sectorial_Principal] >
```

Tercer punto de referencia: Routers de acceso (Rural, Urbano y Empresas)

El tercer nivel de verificación se llevó a cabo sobre los routers de acceso o clientes, que actúan como puerta de enlace para los dispositivos finales en cada zona de cobertura. En primer lugar, el Router_Rural presenta la dirección 10.0.10.254/24 en la interfaz ether1, que corresponde al enlace de transporte con la red VLAN 10. Asimismo, dispone de la dirección 192.168.10.1/24 asignada al bridge Bridge_Hogar, que constituye la interfaz de distribución hacia los equipos de usuario del sector rural, tal como se muestra en la Figura 134.

Figura 134. Verificación del direccionamiento IP en el Router_Cliente_Rural

```
[admin@Router_Cliente_Rural] > /ip address print
Columns: ADDRESS, NETWORK, INTERFACE, VRF
# ADDRESS      NETWORK      INTERFACE    VRF
;;; Enlace de Internet - VLAN 10
0 10.0.10.254/24 10.0.10.0    ether1       main
1 192.168.10.1/24 192.168.10.0 Bridge_Hogar main
[admin@Router_Cliente_Rural] > []
```

A continuación, el Router_Urbano exhibe una configuración análoga para el segmento correspondiente a la VLAN 20. Tal como se aprecia en la Figura 135, las interfaces configuradas incluyen la dirección 10.0.20.254/24 en ether1 para el enlace de transporte y la dirección 192.168.20.1/24 en el bridge Bridge_Hogar para la distribución de conectividad a los usuarios de la zona urbana.

Figura 135. Verificación del direccionamiento IP en el Router_Cliente_Urbano

```
tdown
[admin@Router_Cliente_Urbano] > /ip address print
Columns: ADDRESS, NETWORK, INTERFACE, VRF
# ADDRESS      NETWORK      INTERFACE    VRF
;;; Enlace de Internet - Datos Urbanos
0 10.0.20.254/24 10.0.20.0    ether1       main
1 192.168.20.1/24 192.168.20.0 Bridge_Hogar main
[admin@Router_Cliente_Urbano] > []
```

Por último, el Router_Empresas presenta la configuración correspondiente al segmento VLAN 30. Según se evidencia en la Figura 136, la interfaz ether1 tiene asignada la dirección 10.0.30.254/24 para el enlace hacia la red troncal, mientras que el bridge Bridge_Corporativo_LAN dispone de la dirección 192.168.30.1/24 para la distribución de servicios de red hacia los equipos del entorno corporativo.

Figura 136. Verificación del direccionamiento IP en el Router_Empresas

```
[admin@Router_Empresa] > /ip address print
Columns: ADDRESS, NETWORK, INTERFACE, VRF
# ADDRESS      NETWORK      INTERFACE    VRF
;;; Enlace Dedicado - Datos Corporativos
0 10.0.30.254/24 10.0.30.0    ether1       main
;;; Gateway LAN - Servidores e Infraestructura
1 192.168.30.1/24 192.168.30.0 Bridge_Corporativo_LAN main
[admin@Router_Empresa] > []
```

Los resultados obtenidos en los tres niveles de verificación confirmaron que el plan de direccionamiento IP diseñado para la red WISP fue implementado de manera correcta en su

totalidad. Cada dispositivo dispone de las interfaces y direcciones necesarias para cumplir con su función dentro de la topología, ya sea como nodo de distribución, de transporte o de acceso al usuario final.

4.2.2. Validación del servicio DHCP

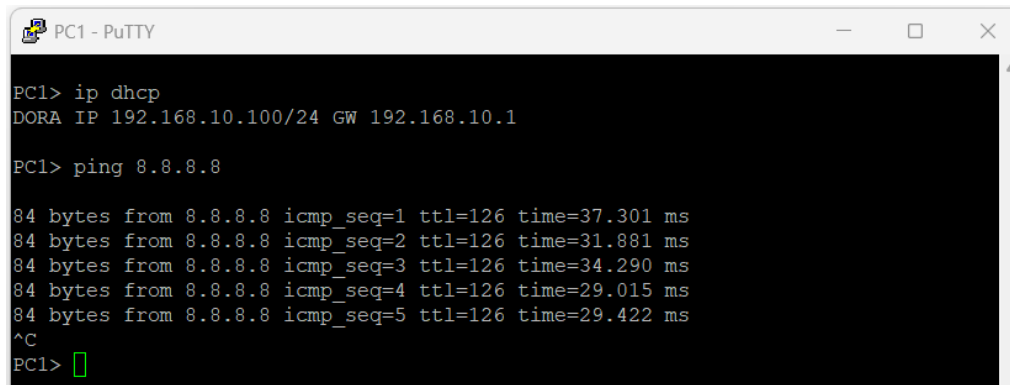
La correcta asignación dinámica de parámetros de red a los equipos de usuario constituye uno de los pilares fundamentales para garantizar el acceso al servicio sin intervención manual por parte del cliente. Por ello, una vez validado el direccionamiento estático de los nodos de infraestructura, se procedió a verificar el funcionamiento del servidor DHCP configurado en cada uno de los routers de acceso, comprobando que los dispositivos finales recibían correctamente la dirección IP, la máscara de subred, la puerta de enlace predeterminada y los servidores DNS asignados.

La validación se realizó de forma individual en cada una de las tres zonas de cobertura definidas en la topología, empleando tanto los equipos VPCS integrados en GNS3 como máquinas virtuales con sistemas operativos reales (Windows 10, Ubuntu y Kali Linux), con el propósito de representar de manera más fiel el comportamiento de los terminales de usuario en un entorno real.

VLAN 10 – Zona Rural

En la zona rural, la verificación se realizó sobre dos dispositivos: el equipo PC1 de GNS3 y la máquina virtual Windows 10. En el caso del PC1, se ejecutó el comando `ip dhcp` en la consola de VPCS, el cual desencadenó el proceso de descubrimiento DHCP (protocolo DORA: Discover, Offer, Request, Acknowledge). Como resultado, el servidor asignó exitosamente la dirección 192.168.10.100/24 junto con la puerta de enlace 192.168.10.1, tal como se muestra en la Figura 137. Para confirmar la conectividad, una vez obtenida la configuración, se ejecutó adicionalmente un ping hacia el servidor DNS público 8.8.8.8, obteniéndose respuestas satisfactorias con tiempos de respuesta comprendidos entre 29 y 37 ms, lo que evidenció salida efectiva hacia internet.

Figura 137. Asignación dinámica de dirección IP mediante DHCP en PC1 de la VLAN 10 Rural



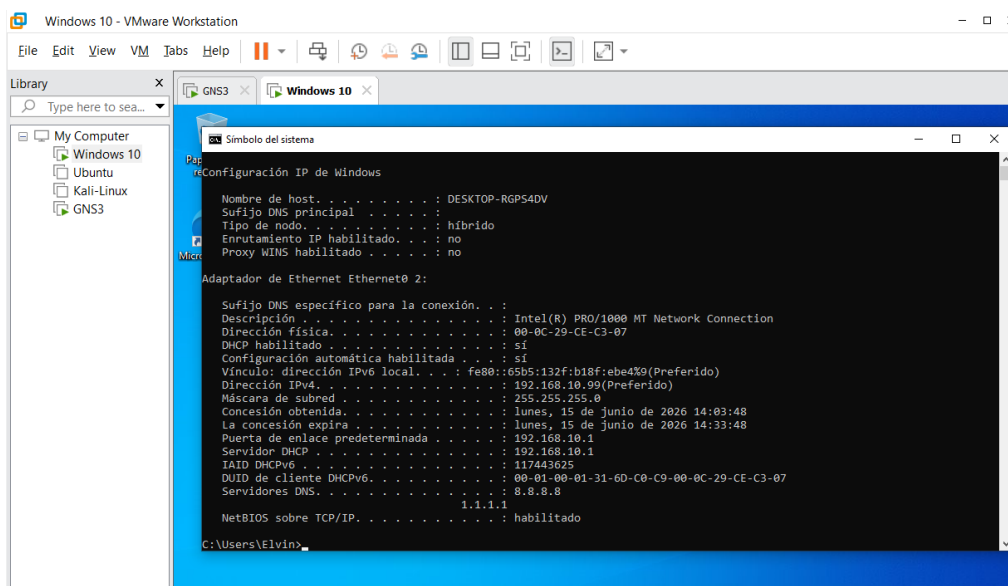
```
PC1> ip dhcp
DORA IP 192.168.10.100/24 GW 192.168.10.1

PC1> ping 8.8.8.8

84 bytes from 8.8.8.8 icmp_seq=1 ttl=126 time=37.301 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=126 time=31.881 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=126 time=34.290 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=126 time=29.015 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=126 time=29.422 ms
^C
PC1>
```

La máquina virtual Windows 10 permitió observar el proceso de asignación DHCP con un mayor nivel de detalle. A través del comando `ipconfig /all` ejecutado en el símbolo del sistema, se obtuvo la configuración completa del adaptador de red virtual, incluyendo la dirección IP asignada (192.168.10.99), la máscara de subred, la puerta de enlace, la dirección del servidor DHCP, el servidor DNS y las fechas de concesión del arrendamiento, tal como se aprecia en la Figura 138. Todos los parámetros fueron correctamente asignados de forma automática, confirmando el funcionamiento integral del servicio DHCP para este segmento.

Figura 138. Configuración completa de red en la máquina virtual Windows 10 de la VLAN 10 Rural

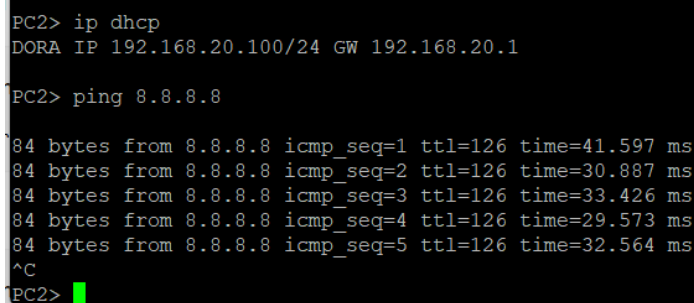


```
Windows 10 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search...
My Computer
  Windows 10
  Ubuntu
  Kali-Linux
  GNS3
GNS3 x Windows 10 x
Símbolo del sistema
reConfiguración IP de Windows
Nombre de host. . . . . : DESKTOP-RGPS4DV
Sufixo DNS principal. . . . . :
Tipo de nodo. . . . . : híbrido
Enrutamiento IP habilitado. . . . . : no
Proxy WINS habilitado. . . . . : no
Adaptador de Ethernet Ethernet0 2:
Sufixo DNS específico para la conexión. . . :
Descripción. . . . . : Intel(R) PRO/1000 MT Network Connection
Dirección física. . . . . : 00-0C-29-CE-C3-07
DHCP habilitado. . . . . : si
Configuración automática habilitada. . . . : si
Vínculo: dirección IPv6 local. . . : fe80::65b5:132f:b18f:eba4%9(Preferido)
Dirección IPv4. . . . . : 192.168.10.99(Preferido)
Máscara de subred. . . . . : 255.255.255.0
Concesión obtenida. . . . . : lunes, 15 de junio de 2026 14:03:48
La concesión expira. . . . . : lunes, 15 de junio de 2026 14:33:48
Puerta de enlace predeterminada. . . . . : 192.168.10.1
Servidor DHCP. . . . . : 192.168.10.1
IAID DHCPv6. . . . . : 117443625
DUID de cliente DHCPv6. . . . . : 00-01-00-01-31-6D-C0-C9-00-0C-29-CE-C3-07
Servidores DNS. . . . . : 8.8.8.8
                          1.1.1.1
NetBIOS sobre TCP/IP. . . . . : habilitado
C:\Users\Elvin>
```

VLAN 20 – Zona Urbana

En la zona urbana, la validación del servicio DHCP se llevó a cabo sobre el equipo PC2 de GNS3 y sobre la máquina virtual Ubuntu. En el PC2, la ejecución del comando `ip dhcp` confirmó la recepción automática de la dirección 192.168.20.100/24 y la puerta de enlace 192.168.20.1. Posteriormente, el ping hacia 8.8.8.8 arrojó tiempos de respuesta entre 29 y 41 ms sin pérdida de paquetes, tal como se ilustra en la Figura 139, validando tanto la asignación DHCP como la conectividad con el exterior.

Figura 139. *Asignación DHCP exitosa en PC2 de la VLAN 20 Urbana*



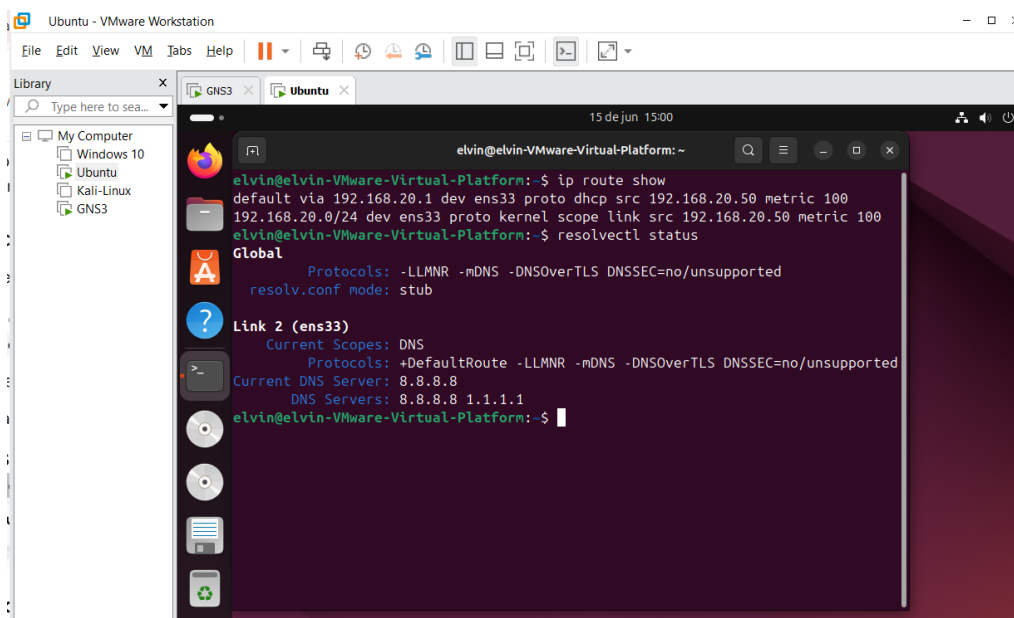
```
PC2> ip dhcp
DORA IP 192.168.20.100/24 GW 192.168.20.1

PC2> ping 8.8.8.8

84 bytes from 8.8.8.8 icmp_seq=1 ttl=126 time=41.597 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=126 time=30.887 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=126 time=33.426 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=126 time=29.573 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=126 time=32.564 ms
^C
PC2>
```

En la máquina virtual Ubuntu, la verificación se realizó a través de los comandos `ip route show` y `resolvectl status`, los cuales permitieron visualizar la ruta predeterminada aprendida vía DHCP (192.168.20.1 como gateway) y el servidor DNS asignado automáticamente (8.8.8.8), como se aprecia en la Figura 140. El sistema operativo Linux procesó correctamente todos los parámetros distribuidos por el servidor DHCP, sin requerir ninguna configuración manual por parte del usuario.

Figura 140. Verificación de los parámetros DHCP en la máquina virtual Ubuntu de la VLAN 20 Urbana



VLAN 30 – Zona Empresas

En la zona de empresas, la prueba DHCP se realizó sobre el equipo PC3 de GNS3 y la máquina virtual Kali Linux. El PC3 obtuvo mediante DHCP la dirección 192.168.30.199/24 (o 192.168.30.200/24 en sesiones previas, conforme a la dinámica del pool), con la puerta de enlace 192.168.30.1. La conectividad hacia internet fue confirmada mediante ping a 8.8.8.8, con tiempos de respuesta entre 27 y 41 ms sin pérdida de paquetes, como se muestra en la Figura 141.

Figura 141. Asignación DHCP y verificación de conectividad en PC3 de la VLAN 30 Empresas

```

PC3> ip dhcp
DDORA IP 192.168.30.199/24 GW 192.168.30.1

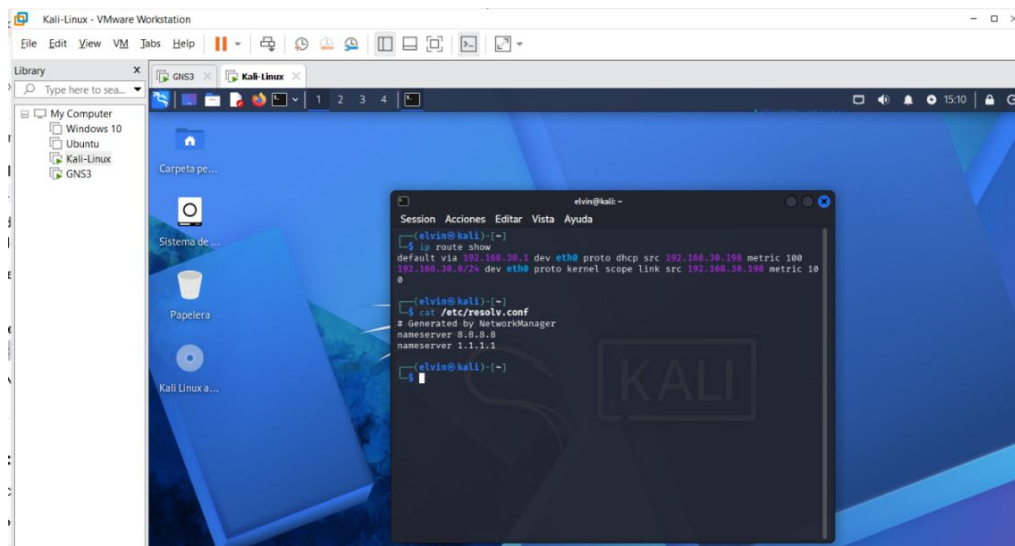
PC3> ping 8.8.8.8

84 bytes from 8.8.8.8 icmp_seq=1 ttl=126 time=40.949 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=126 time=36.001 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=126 time=36.154 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=126 time=32.906 ms
^C
PC3>
  
```

La máquina virtual Kali Linux complementó esta verificación mostrando la tabla de rutas y la configuración DNS a través de los comandos `ip route show` y `cat /etc/resolv.conf`

respectivamente. Como se observa en la Figura 142, la dirección 192.168.30.198/24 fue asignada correctamente junto con su ruta predeterminada hacia 192.168.30.1, y el archivo de resolución DNS refleja los servidores 8.8.8.8 y 1.1.1.1 configurados en el servidor DHCP del Router_Empresas.

Figura 142. Verificación de la configuración DHCP en la máquina virtual Kali Linux de la VLAN 30 Empresas



En los tres segmentos de red evaluados, el servidor DHCP asignó correctamente todos los parámetros de configuración de red sin necesidad de intervención manual por parte del usuario, lo que confirma la correcta implementación del servicio y su capacidad para dar soporte a los equipos finales de cada zona de cobertura de la red WISP propuesta.

4.2.3. Validación de la segmentación mediante VLAN

Con el propósito de verificar que la segmentación lógica de la red funciona de manera correcta y que cada segmento VLAN opera de forma independiente —permitiendo únicamente el tráfico autorizado entre zonas a través del Router_Core—, se realizaron pruebas de conectividad mediante el protocolo ICMP en cada una de las VLAN que conforman la topología: VLAN 100 de gestión, VLAN 10 Rural, VLAN 20 Urbana y VLAN 30 Empresas.

VLAN 100 – Red de Gestión

Las primeras pruebas se ejecutaron desde el Router_Core hacia los demás dispositivos de infraestructura, utilizando la VLAN 100 como canal de administración. Se verificó la conectividad hacia el Switch_Administrable (10.0.100.2), la Antena Sectorial Principal (10.0.100.10), el CPE_Rural (10.0.100.20), el CPE_Urbano (10.0.100.21) y el CPE_Empresas (10.0.100.31), como se aprecia en la Figura 143. Todas las respuestas fueron satisfactorias, con tiempos de respuesta que oscilaron entre 1 y 10 ms, confirmando la accesibilidad de todos los nodos de infraestructura desde el plano de gestión.

Figura 143. Pruebas de conectividad ICMP desde el Router_Core hacia todos los nodos de infraestructura a través de la VLAN 100 de gestión

```
[admin@Router_Core] > ping 10.0.100.2
SEQ HOST                                SIZE TTL TIME          STATUS
0 10.0.100.2                            56  64  7ms27us
sent=1 received=1 packet-loss=0% min-rtt=7ms27us avg-rtt=7ms27us
max-rtt=7ms27us

[admin@Router_Core] > ping 10.0.100.10
SEQ HOST                                SIZE TTL TIME          STATUS
0 10.0.100.10                            56  64  2ms282us
1 10.0.100.10                            56  64  1ms766us
2 10.0.100.10                            56  64  2ms932us
sent=3 received=3 packet-loss=0% min-rtt=1ms766us avg-rtt=2ms326us
max-rtt=2ms932us

[admin@Router_Core] > ping 10.0.100.20
SEQ HOST                                SIZE TTL TIME          STATUS
0 10.0.100.20                            56  64  10ms450us
sent=1 received=1 packet-loss=0% min-rtt=10ms450us avg-rtt=10ms450us
max-rtt=10ms450us

[admin@Router_Core] > ping 10.0.100.21
SEQ HOST                                SIZE TTL TIME          STATUS
0 10.0.100.21                            56  64  9ms528us
sent=1 received=1 packet-loss=0% min-rtt=9ms528us avg-rtt=9ms528us
max-rtt=9ms528us

[admin@Router_Core] > ping 10.0.100.31
SEQ HOST                                SIZE TTL TIME          STATUS
[admin@Router_Core] >
```

A continuación, se amplió el alcance de las pruebas incluyendo los routers de acceso de cada zona. El ping hacia Router_Rural (10.0.10.254), Router_Urbano (10.0.20.254) y Router_Empresas (10.0.30.254) arrojó respuestas con latencias promedio de 3.7 ms, 4.4 ms y 4.8 ms respectivamente, sin pérdida de paquetes en ningún caso, como se ilustra en la Figura 144.

Figura 144. Verificación de conectividad desde el Router_Core hacia los routers de acceso Rural, Urbano y Empresas mediante ping a través de sus respectivas VLAN

```
[admin@Router_Core] > ping 10.0.10.254
SEQ HOST                                SIZE TTL TIME          STATUS
0 10.0.10.254                          56  64 3ms959us
1 10.0.10.254                          56  64 3ms493us
sent=2 received=2 packet-loss=0% min-rtt=3ms493us avg-rtt=3ms726us
max-rtt=3ms959us

[admin@Router_Core] > ping 10.0.20.254
SEQ HOST                                SIZE TTL TIME          STATUS
0 10.0.20.254                          56  64 3ms662us
1 10.0.20.254                          56  64 5ms229us
sent=2 received=2 packet-loss=0% min-rtt=3ms662us avg-rtt=4ms445us
max-rtt=5ms229us

[admin@Router_Core] > ping 10.0.30.254
SEQ HOST                                SIZE TTL TIME          STATUS
0 10.0.30.254                          56  64 4ms649us
1 10.0.30.254                          56  64 5ms85us
sent=2 received=2 packet-loss=0% min-rtt=4ms649us avg-rtt=4ms867us
max-rtt=5ms85us

[admin@Router_Core] > █
```

Finalmente, se comprobó la comunicación con cada uno de los enlaces de respaldo que conforman la red de contingencia: Backup1_Rural (10.0.100.9), Backup2_Urbano (10.0.100.19) y Backup3_Empresas (10.0.100.29), como se puede observar en la Figura 145. Los tres dispositivos de respaldo respondieron satisfactoriamente a las solicitudes ICMP, con tiempos que se mantuvieron por debajo de los 12 ms, validando su presencia y disponibilidad en la red.

Figura 145. Verificación de conectividad desde el Router_Core hacia los dispositivos de respaldo de las zonas Rural, Urbana y Empresarial a través de la VLAN 100 de gestión

```
[admin@Router_Core] > ping 10.0.100.9
SEQ HOST                                SIZE TTL TIME          STATUS
0 10.0.100.9                          56  64 11ms828us
1 10.0.100.9                          56  64 5ms475us
sent=2 received=2 packet-loss=0% min-rtt=5ms475us avg-rtt=8ms651us
max-rtt=11ms828us

[admin@Router_Core] > ping 10.0.100.19
SEQ HOST                                SIZE TTL TIME          STATUS
0 10.0.100.19                          56  64 11ms850us
1 10.0.100.19                          56  64 2ms539us
sent=2 received=2 packet-loss=0% min-rtt=2ms539us avg-rtt=7ms194us
max-rtt=11ms850us

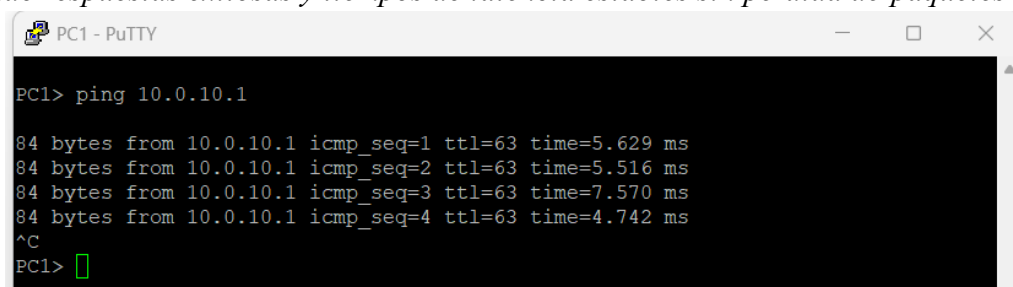
[admin@Router_Core] > ping 10.0.100.29
SEQ HOST                                SIZE TTL TIME          STATUS
0 10.0.100.29                          56  64 8ms390us
1 10.0.100.29                          56  64 3ms742us
sent=2 received=2 packet-loss=0% min-rtt=3ms742us avg-rtt=6ms66us
max-rtt=8ms390us

[admin@Router_Core] > █
```


VLAN 10 – Zona Rural

Para validar el correcto reconocimiento de la VLAN 10 por parte de los equipos del sector rural, se ejecutaron pruebas de ping desde PC1 hacia la dirección de gateway 10.0.10.1 asignada al Router_Core en este segmento. Los resultados de la Figura 146 muestran tiempos de respuesta comprendidos entre 4.7 y 7.6 ms con 0 % de pérdida de paquetes, lo que confirma que el tráfico de la zona rural es correctamente etiquetado y enrutado a través de la VLAN 10. De igual manera, la máquina virtual Windows 10 realizó la misma prueba desde su interfaz, obteniendo resultados análogos con tiempos mínimos de 3 ms, máximos de 5 ms y una media de 4 ms, como se aprecia en la Figura 147.

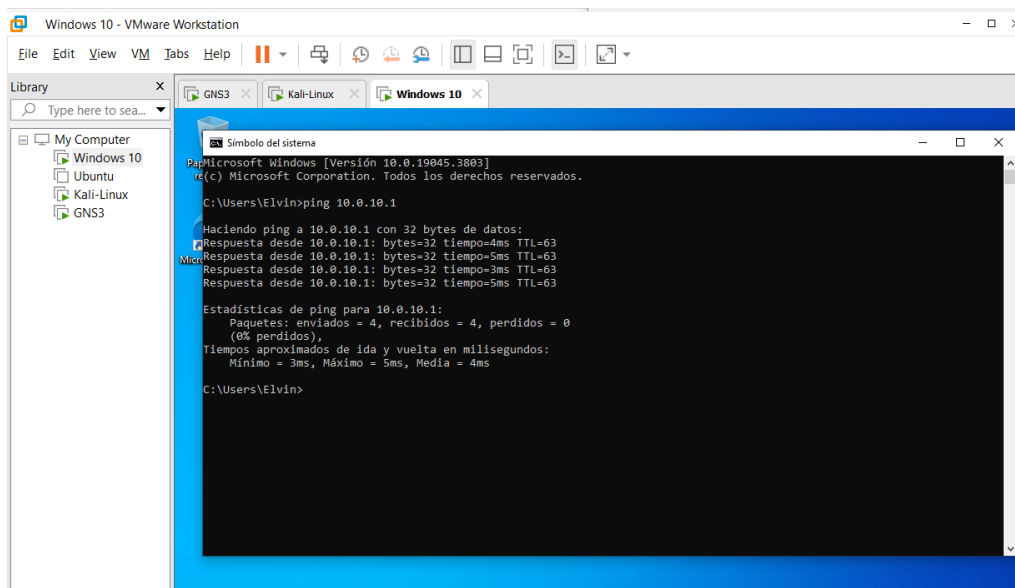
Figura 146. Prueba de ping desde PC1 de la VLAN 10 Rural hacia el gateway 10.0.10.1, mostrando respuestas exitosas y tiempos de latencia estables sin pérdida de paquetes



```
PC1> ping 10.0.10.1

84 bytes from 10.0.10.1 icmp_seq=1 ttl=63 time=5.629 ms
84 bytes from 10.0.10.1 icmp_seq=2 ttl=63 time=5.516 ms
84 bytes from 10.0.10.1 icmp_seq=3 ttl=63 time=7.570 ms
84 bytes from 10.0.10.1 icmp_seq=4 ttl=63 time=4.742 ms
^C
PC1>
```

Figura 147. Verificación de conectividad en la VLAN 10 Rural desde la máquina virtual Windows 10



```
Windows 10 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
Windows 10
Ubuntu
Kali-Linux
GNS3
GNS3
Kali-Linux
Windows 10
Símbolo del sistema
Microsoft Windows [Versión 10.0.19045.3803]
(c) Microsoft Corporation. Todos los derechos reservados.
C:\Users\Elvin>ping 10.0.10.1

Haciendo ping a 10.0.10.1 con 32 bytes de datos:
Respuesta desde 10.0.10.1: bytes=32 tiempo=4ms TTL=63
Respuesta desde 10.0.10.1: bytes=32 tiempo=5ms TTL=63
Respuesta desde 10.0.10.1: bytes=32 tiempo=3ms TTL=63
Respuesta desde 10.0.10.1: bytes=32 tiempo=5ms TTL=63

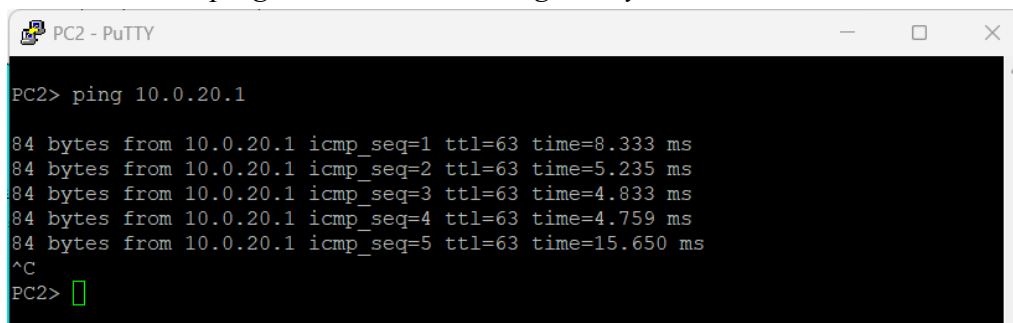
Estadísticas de ping para 10.0.10.1:
Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
Mínimo = 3ms, Máximo = 5ms, Media = 4ms

C:\Users\Elvin>
```

VLAN 20 – Zona Urbana

La validación de la VLAN 20 se efectuó desde PC2 y la máquina virtual Ubuntu hacia la dirección 10.0.20.1. La Figura 148 evidencia la correcta respuesta del gateway, con tiempos de latencia que oscilaron entre 4.8 y 15.6 ms. La máquina virtual Ubuntu, por su parte, ejecutó el ping estadístico, reportando en la Figura 149 un RTT mínimo de 4.42 ms, máximo de 6.24 ms y una media de 5.44 ms sobre 6 paquetes transmitidos y recibidos, con 0 % de pérdida, lo cual ratifica el correcto funcionamiento de la segmentación en la zona urbana.

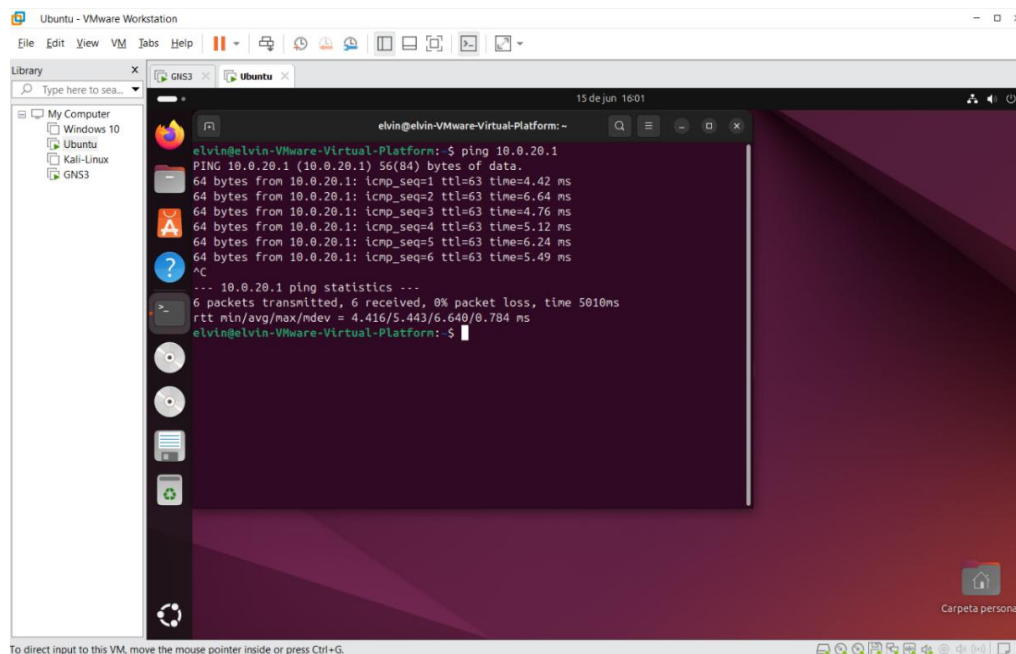
Figura 148. Prueba de ping desde PC2 hacia el gateway de la VLAN 20 Urbana



```
PC2> ping 10.0.20.1

84 bytes from 10.0.20.1 icmp_seq=1 ttl=63 time=8.333 ms
84 bytes from 10.0.20.1 icmp_seq=2 ttl=63 time=5.235 ms
84 bytes from 10.0.20.1 icmp_seq=3 ttl=63 time=4.833 ms
84 bytes from 10.0.20.1 icmp_seq=4 ttl=63 time=4.759 ms
84 bytes from 10.0.20.1 icmp_seq=5 ttl=63 time=15.650 ms
^C
PC2> 
```

Figura 149. Verificación de conectividad en la VLAN 20 Urbana desde la máquina virtual Ubuntu

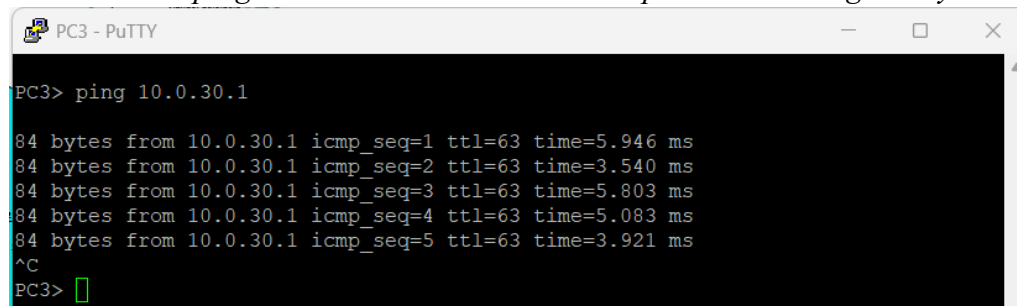


```
elvin@elvin-VMware-Virtual-Platform:~$ ping 10.0.20.1
PING 10.0.20.1 (10.0.20.1) 56(84) bytes of data:
64 bytes from 10.0.20.1: icmp_seq=1 ttl=63 time=4.42 ms
64 bytes from 10.0.20.1: icmp_seq=2 ttl=63 time=6.64 ms
64 bytes from 10.0.20.1: icmp_seq=3 ttl=63 time=4.76 ms
64 bytes from 10.0.20.1: icmp_seq=4 ttl=63 time=5.12 ms
64 bytes from 10.0.20.1: icmp_seq=5 ttl=63 time=6.24 ms
64 bytes from 10.0.20.1: icmp_seq=6 ttl=63 time=5.49 ms
^C
--- 10.0.20.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5010ms
rtt min/avg/max/mdev = 4.416/5.443/6.640/0.784 ms
elvin@elvin-VMware-Virtual-Platform:~$ 
```

VLAN 30 – Zona Empresas

Para el segmento empresarial, las pruebas de validación VLAN se realizaron desde PC3 y Kali Linux hacia la dirección de gateway 10.0.30.1. Los resultados de la Figura 150 muestran tiempos de respuesta entre 3.5 y 5.9 ms desde PC3, con 100 % de entrega de paquetes. Desde Kali Linux, la Figura 151 refleja una comunicación estable y bidireccional con el gateway, con 7 paquetes transmitidos y recibidos sin pérdida, y un RTT que se mantuvo en un rango de 5.3 a 7.9 ms, lo cual confirma la correcta segmentación y funcionamiento de la VLAN 30 para el segmento corporativo.

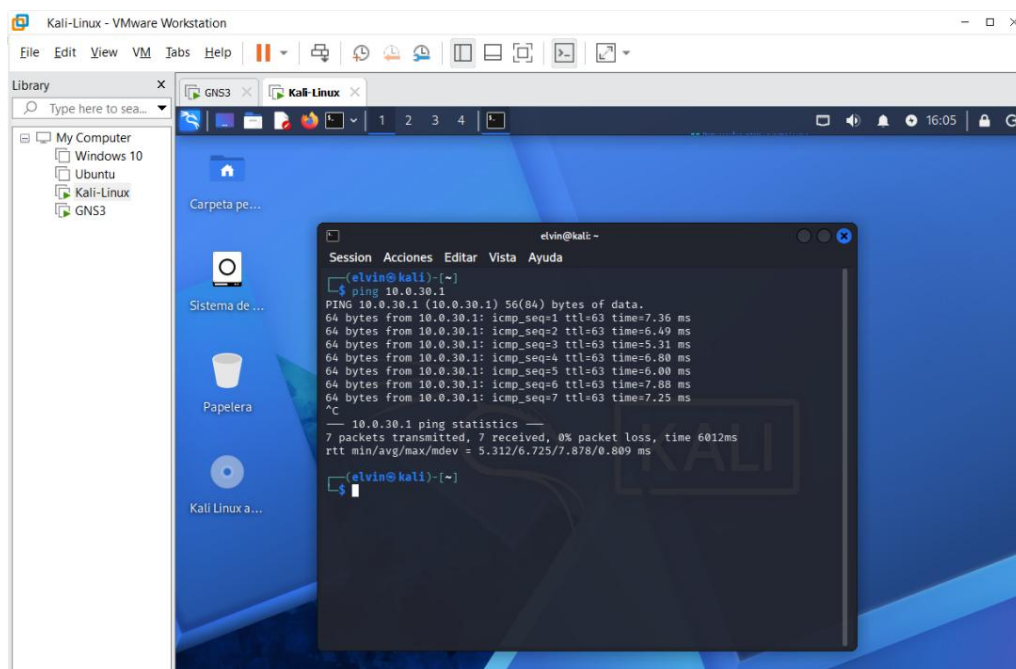
Figura 150. Prueba de ping desde PC3 de la VLAN 30 Empresas hacia el gateway 10.0.30.1



```
PC3> ping 10.0.30.1

84 bytes from 10.0.30.1 icmp_seq=1 ttl=63 time=5.946 ms
84 bytes from 10.0.30.1 icmp_seq=2 ttl=63 time=3.540 ms
84 bytes from 10.0.30.1 icmp_seq=3 ttl=63 time=5.803 ms
84 bytes from 10.0.30.1 icmp_seq=4 ttl=63 time=5.083 ms
84 bytes from 10.0.30.1 icmp_seq=5 ttl=63 time=3.921 ms
^C
PC3>
```

Figura 151. Verificación de la segmentación VLAN 30 Empresas desde la máquina virtual Kali Linux



```
elvin@kali: ~
$ ping 10.0.30.1
PING 10.0.30.1 (10.0.30.1) 56(84) bytes of data:
64 bytes from 10.0.30.1: icmp_seq=1 ttl=63 time=7.36 ms
64 bytes from 10.0.30.1: icmp_seq=2 ttl=63 time=6.49 ms
64 bytes from 10.0.30.1: icmp_seq=3 ttl=63 time=5.31 ms
64 bytes from 10.0.30.1: icmp_seq=4 ttl=63 time=6.80 ms
64 bytes from 10.0.30.1: icmp_seq=5 ttl=63 time=6.00 ms
64 bytes from 10.0.30.1: icmp_seq=6 ttl=63 time=7.88 ms
64 bytes from 10.0.30.1: icmp_seq=7 ttl=63 time=7.25 ms
^C
--- 10.0.30.1 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6012ms
rtt min/avg/max/mdev = 5.312/6.725/7.878/0.809 ms
elvin@kali: ~
$
```

Los resultados obtenidos en esta sección confirman que la segmentación lógica de la red mediante VLAN fue implementada y validada de forma exitosa. Cada zona opera de manera independiente sobre su propio segmento de red, mientras que el Router_Core gestiona el tráfico entre VLAN de acuerdo con las políticas de enrutamiento establecidas. Asimismo, la VLAN 100 de administración cumple su función de manera aislada, garantizando que el plano de gestión no interfiera con el tráfico de datos de los usuarios.

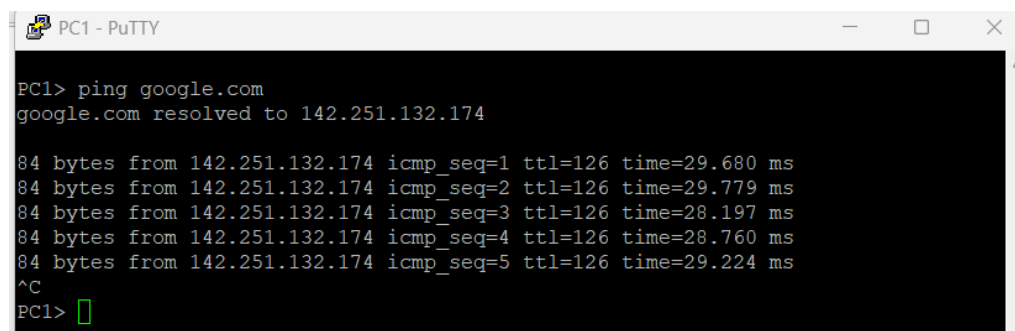
4.2.4. Verificación del acceso a internet

Una vez confirmada la segmentación interna de la red y la conectividad entre sus diferentes segmentos, se procedió a verificar que los equipos de usuario de cada zona tuvieran acceso efectivo a recursos externos a través de internet. Para ello, se realizaron pruebas de conectividad hacia el servidor DNS público de Google (8.8.8.8), así como búsquedas reales desde los navegadores web de las máquinas virtuales, con el fin de demostrar que el proceso de traducción de direcciones NAT configurado en el Router_Core opera correctamente para las tres VLAN.

VLAN 10 – Zona Rural

Desde el equipo PC1 de la zona rural, se ejecutó el comando ping google.com en la consola de GNS3. El sistema resolvió exitosamente el nombre de dominio a la dirección IP 142.251.132.174 y recibió respuestas con tiempos de latencia que oscilaron entre 28 y 30 ms, sin pérdida de paquetes, como se evidencia en la Figura 152. Este resultado confirma tanto la resolución DNS como el correcto funcionamiento del NAT para el tráfico saliente de la VLAN 10.

Figura 152. Verificación del acceso a internet desde PC1 de la VLAN 10 Rural mediante ping a google.com

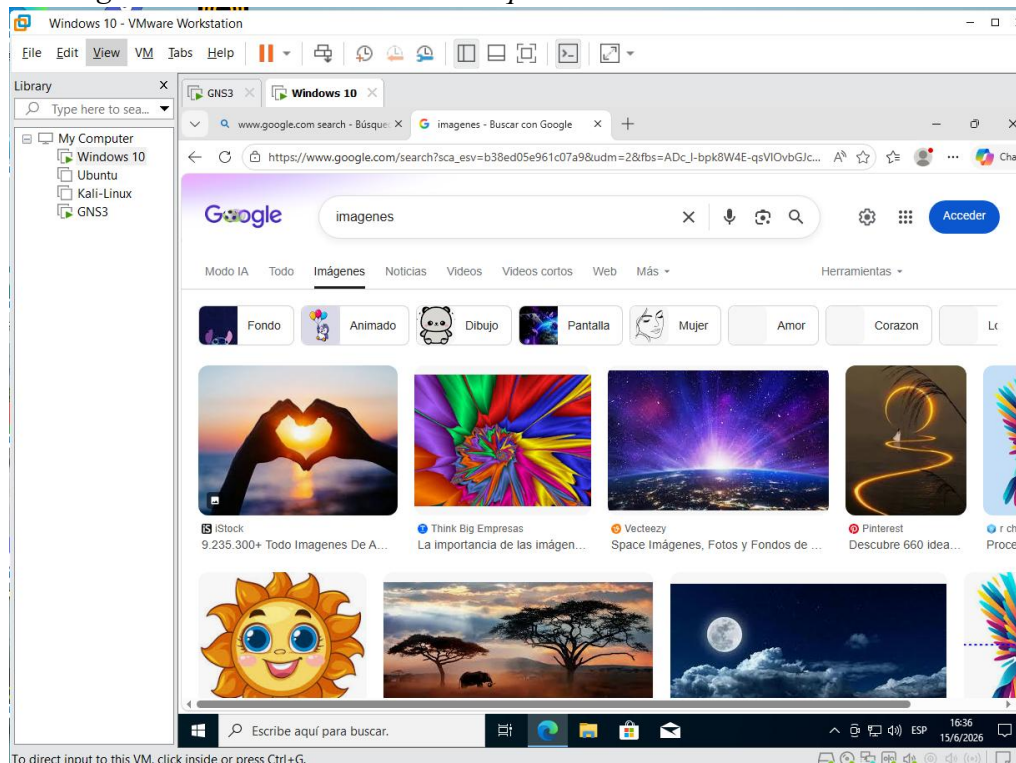


```
PC1> ping google.com
google.com resolved to 142.251.132.174

84 bytes from 142.251.132.174 icmp_seq=1 ttl=126 time=29.680 ms
84 bytes from 142.251.132.174 icmp_seq=2 ttl=126 time=29.779 ms
84 bytes from 142.251.132.174 icmp_seq=3 ttl=126 time=28.197 ms
84 bytes from 142.251.132.174 icmp_seq=4 ttl=126 time=28.760 ms
84 bytes from 142.251.132.174 icmp_seq=5 ttl=126 time=29.224 ms
^C
PC1> 
```

Complementariamente, desde la máquina virtual Windows 10 de la zona rural se realizó una navegación real a través del navegador web, accediendo al buscador de Google. Como se observa en la Figura 153, la página se cargó correctamente, lo que demuestra que la conectividad a internet es completamente funcional y no se limita únicamente al protocolo ICMP.

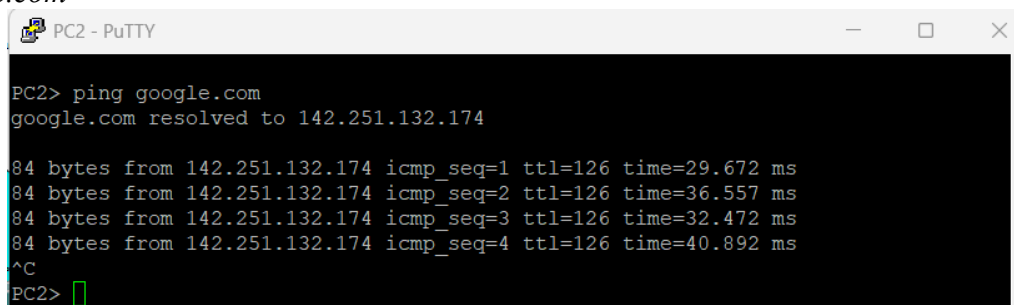
Figura 153. *Navegación web exitosa desde la máquina virtual Windows 10 de la VLAN 10 Rural*



VLAN 20 – Zona Urbana

En la zona urbana, el ping a google.com desde PC2 arrojó respuestas satisfactorias con tiempos entre 29 y 40 ms, confirmando la resolución DNS y la salida hacia internet tal como muestra la Figura 154. La máquina virtual Ubuntu también realizó una búsqueda real en Google, donde se cargó correctamente la página de resultados, como se aprecia en la Figura 155. Cabe señalar que en esta sesión se visualizó información relacionada con el Mundial de Fútbol 2026, lo que evidenció que la conexión a internet tenía acceso a contenido actualizado en tiempo real.

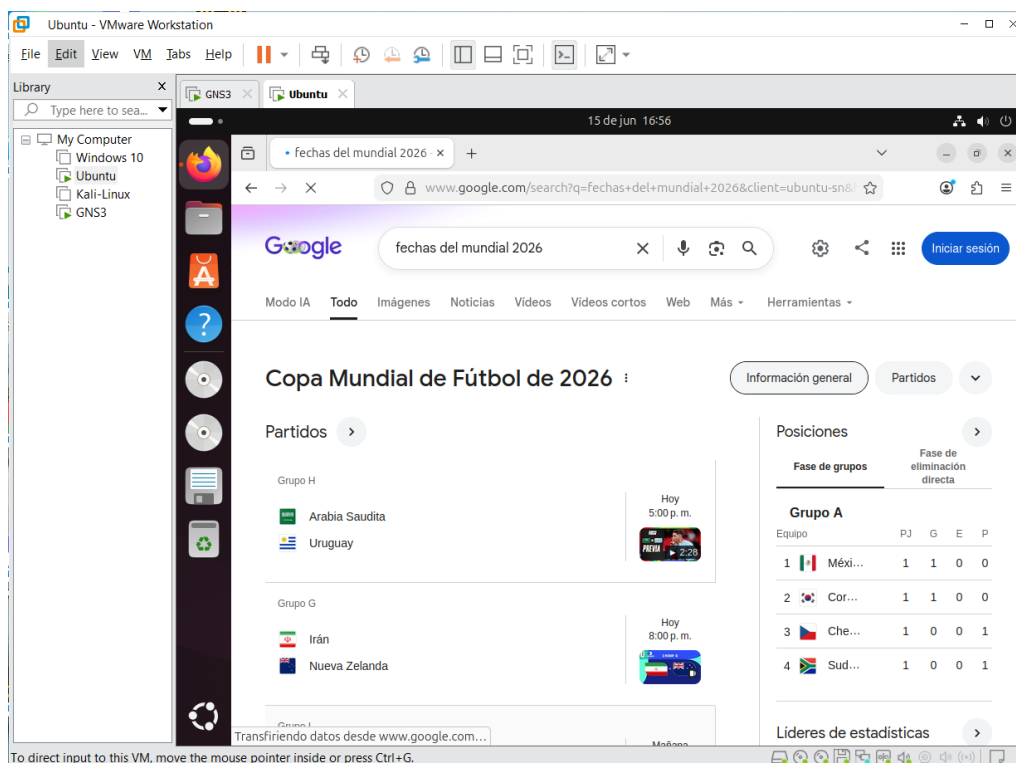
Figura 154. Verificación del acceso a internet desde PC2 de la VLAN 20 Urbana mediante ping a google.com



```
PC2> ping google.com
google.com resolved to 142.251.132.174

84 bytes from 142.251.132.174 icmp_seq=1 ttl=126 time=29.672 ms
84 bytes from 142.251.132.174 icmp_seq=2 ttl=126 time=36.557 ms
84 bytes from 142.251.132.174 icmp_seq=3 ttl=126 time=32.472 ms
84 bytes from 142.251.132.174 icmp_seq=4 ttl=126 time=40.892 ms
^C
PC2>
```

Figura 155. Navegación web desde la máquina virtual Ubuntu de la VLAN 20 Urbana

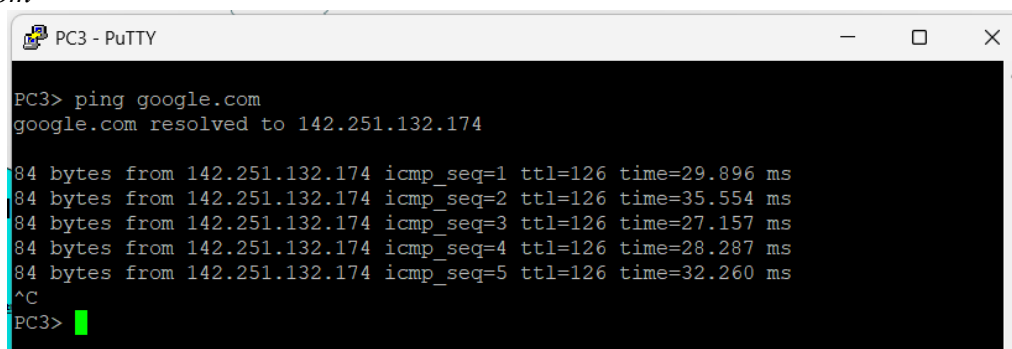


VLAN 30 – Zona Empresas

Para el segmento corporativo, el ping a google.com ejecutado desde PC3 produjo respuestas con tiempos entre 27 y 35 ms sin pérdida de paquetes, como se muestra en la Figura 156. La máquina virtual Kali Linux complementó esta prueba con una búsqueda real en el navegador, que también finalizó exitosamente, tal como se evidencia en la Figura 157. En este

caso, se cargó una búsqueda relacionada con EA Sports FC 26, confirmando el acceso a contenidos externos y validando que el tráfico del segmento empresarial también es correctamente procesado por el NAT del Router_Core.

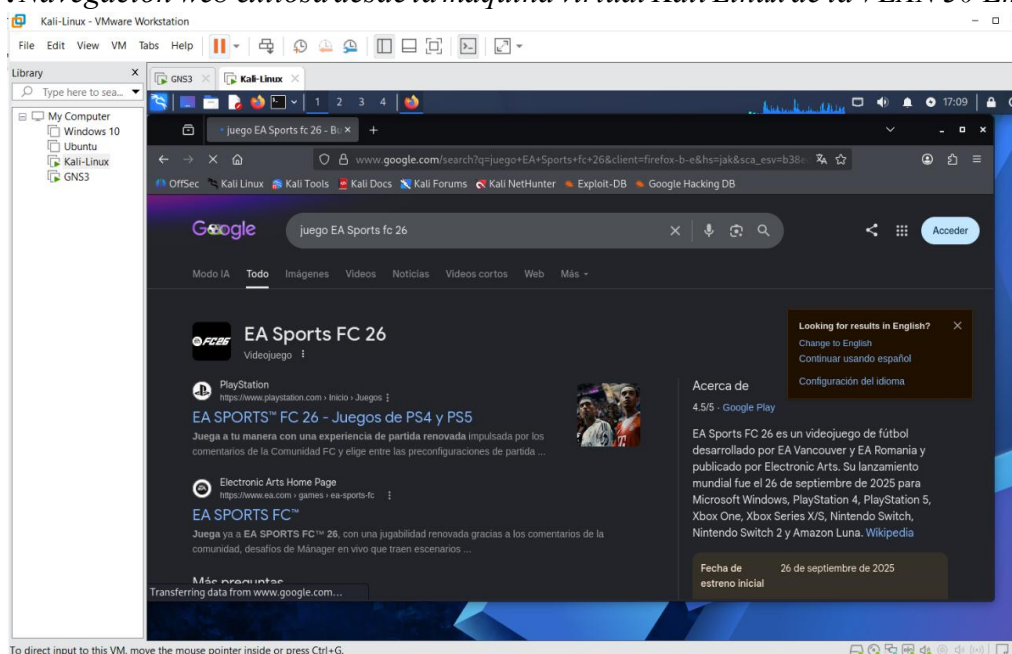
Figura 156. Verificación del acceso a internet desde PC3 de la VLAN 30 Empresas mediante ping a google.com



```
PC3> ping google.com
google.com resolved to 142.251.132.174

84 bytes from 142.251.132.174 icmp_seq=1 ttl=126 time=29.896 ms
84 bytes from 142.251.132.174 icmp_seq=2 ttl=126 time=35.554 ms
84 bytes from 142.251.132.174 icmp_seq=3 ttl=126 time=27.157 ms
84 bytes from 142.251.132.174 icmp_seq=4 ttl=126 time=28.287 ms
84 bytes from 142.251.132.174 icmp_seq=5 ttl=126 time=32.260 ms
^C
PC3>
```

Figura 157. Navegación web exitosa desde la máquina virtual Kali Linux de la VLAN 30 Empresas



Los resultados obtenidos en las tres VLAN confirman que la red permite el acceso a recursos externos mediante la traducción de direcciones NAT configurada en el Router_Core. Tanto las pruebas ICMP como la navegación web real demostraron que la conectividad a internet opera de forma correcta y estable para todos los segmentos de usuario de la red WISP propuesta.

4.2.5. Análisis de transmisión y recepción de paquetes

Con la finalidad de verificar en profundidad la correcta conectividad, el enrutamiento y el comportamiento del tráfico de datos en la infraestructura de red simulada, se realizó una captura y un análisis de paquetes mediante la herramienta Wireshark en las interfaces virtuales correspondientes a cada una de las VLAN. Este análisis permitió identificar los protocolos presentes en el tráfico, los tiempos de respuesta a nivel de paquete, el comportamiento de los mecanismos de control de capa 2 y la correcta operación de los protocolos de seguridad en la capa de transporte.

VLAN 10 – Zona Rural

Las capturas de tráfico de la VLAN 10 se realizaron desde el adaptador virtual VMnet10, vinculado a la máquina Windows 10 con dirección IP dinámica 192.168.10.99. El análisis del tráfico local, mostrado en la Figura 158, reveló el intercambio exitoso de paquetes ICMP (Echo request y Echo reply) entre el host y la dirección 10.0.10.1, lo que confirma la comunicación directa con el gateway del sector rural. Adicionalmente, se identificó tráfico fragmentado en paquetes de 1514 bytes hacia el servidor externo 23.58.246.115, resultado de la superación del MTU del enlace, y se observaron handshakes de los protocolos TLSv1.2 y TLSv1.3 (Server Hello), lo que evidencia que el cifrado en la capa de transporte opera correctamente para los usuarios de esta zona.

Figura 158. Captura de tráfico local en la VLAN 10 Rural (VMnet10)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.10.99	10.0.10.1	ICMP	74	Echo (ping) request id=0x0001, seq=36/9216, ttl=128
2	0.003124800	10.0.10.1	192.168.10.99	ICMP	74	Echo (ping) reply id=0x0001, seq=36/9216, ttl=63
3	0.018797700	23.58.246.115	192.168.10.99	IPv4	1514	Fragmented IP protocol (proto=TCP 6, off=0, ID=fe3e)
4	0.018838300	23.58.246.115	192.168.10.99	IPv4	1514	Fragmented IP protocol (proto=TCP 6, off=1480, ID=fe3e)
5	0.018854300	23.58.246.115	192.168.10.99	IPv4	1514	Fragmented IP protocol (proto=TCP 6, off=2960, ID=fe3e)
6	0.018874200	23.58.246.115	192.168.10.99	TLSv1.2	692	Server Hello, Certificate, Certificate Status, Server
7	0.748835700	8.8.8.4	192.168.10.99	IPv4	1514	Fragmented IP protocol (proto=TCP 6, off=0, ID=fe42)
8	0.748889500	8.8.8.4	192.168.10.99	TLSv1.2	641	Application Data, Application Data, Application Data
9	0.952347800	8.8.8.8	192.168.10.99	IPv4	1514	Fragmented IP protocol (proto=TCP 6, off=0, ID=fe44)
10	0.952387600	8.8.8.8	192.168.10.99	IPv4	1514	Fragmented IP protocol (proto=TCP 6, off=1480, ID=fe44)
11	0.952405700	8.8.8.8	192.168.10.99	IPv4	1514	Fragmented IP protocol (proto=TCP 6, off=2960, ID=fe44)
12	0.952423600	8.8.8.8	192.168.10.99	TLSv1.3	1110	Server Hello, Change Cipher Spec, Application Data

Frame	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.10.99	10.0.10.1	ICMP	74	Echo (ping) request id=0x0001, seq=36/9216, ttl=128

La segunda captura de la VLAN 10, presentada en la Figura 159, evidencia la verificación de conectividad externa mediante paquetes ICMP dirigidos hacia el servidor DNS público de Google (8.8.8.8), observándose un intercambio de ida y vuelta estable y sin pérdidas. Complementariamente, en el paquete número 10 de esta captura se identifica una trama del protocolo STP (Spanning Tree Protocol) enviada desde la dirección MAC 0c:96:5c:c9:00:02, lo que confirma que los mecanismos de prevención de bucles en la capa de enlace se encuentran activos y operando correctamente dentro del dominio de la VLAN 10.

Figura 159. Captura de tráfico de salida en la VLAN 10 Rural (VMnet10)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.10.99	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=623/28418, ttl=128
2	0.033335800	8.8.8.8	192.168.10.99	ICMP	74	Echo (ping) reply id=0x0001, seq=623/28418, ttl=126
3	0.593467000	172.178.240.163	192.168.10.99	IPv4	1514	Fragmented IP protocol (proto=TCP 6, off=0, ID=2bf2) [
4	0.593525000	172.178.240.163	192.168.10.99	IPv4	1514	Fragmented IP protocol (proto=TCP 6, off=1480, ID=2bf2
5	0.593542300	172.178.240.163	192.168.10.99	SSL	71	Continuation Data
6	0.621087400	40.126.29.9	192.168.10.99	IPv4	1514	Fragmented IP protocol (proto=TCP 6, off=0, ID=2bf5) [
7	0.621138000	40.126.29.9	192.168.10.99	SSL	1069	Continuation Data
8	1.018931900	192.168.10.99	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=624/28674, ttl=128
9	1.049673700	8.8.8.8	192.168.10.99	ICMP	74	Echo (ping) reply id=0x0001, seq=624/28674, ttl=126
10	1.757706500	0c:96:5c:c9:00:02	Nearest-Customer-Br...	STP	53	RST. Root = 32768/0/0c:96:5c:c9:00:01 Cost = 0 Port
11	2.038424800	192.168.10.99	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=625/28930, ttl=128
12	2.066780900	8.8.8.8	192.168.10.99	ICMP	74	Echo (ping) reply id=0x0001, seq=625/28930, ttl=126

Frame	Packet	Bytes on wire	Bytes captured	Protocol	Details
1	0000	0c 96 5c c9 00 01 00 0c	29	ce c3 07 08 00 45 00	...
2	0010	00 3c fc 8b 00 00 80 01	63	1a c0 a8 0a 63 08 08	...
3	0020	08 08 08 00 4a ec 00 01	02	6f 61 62 63 64 65 66	...
4	0030	67 68 69 6a 6b 6c 6d 6e	6f	70 71 72 73 74 75 76	ghijklmn...
5	0040	77 61 62 63 64 65 66 67	68	69	wabdefg...

VLAN 20 – Zona Urbana

El análisis de tráfico de la VLAN 20 se efectuó sobre el adaptador VMnet11, vinculado a la máquina virtual Ubuntu con dirección IP 192.168.20.50. En la captura de tráfico local de la Figura 160 se observa el intercambio continuo y exitoso de paquetes ICMP entre el host urbano y su gateway predeterminado (10.0.20.1), con respuestas ininterrumpidas que ratifican la conectividad local. Asimismo, se identificó tráfico TCP hacia el servidor externo 185.125.188.57 a través del puerto 443 (HTTPS), lo que confirma el inicio de sesiones web cifradas. La presencia regular de tramas STP emitidas por la MAC 0c:a0:9c:02:00:01 en las líneas 3 y 10 de la captura evidencia que los dispositivos de conmutación del sector urbano mantienen activos sus mecanismos de control de topología para evitar bucles de red.

Figura 160. Captura de tráfico local en la VLAN 20 Urbana (VMnet11)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.20.50	10.0.20.1	ICMP	98	Echo (ping) request id=0x0d0a, seq=21/5376, ttl=64 (r
2	0.006730600	10.0.20.1	192.168.20.50	ICMP	98	Echo (ping) reply id=0x0d0a, seq=21/5376, ttl=63 (r
3	0.582035700	0c:a0:9c:02:00:01	Nearest-Customer-Br...	STP	53	RST. Root = 32768/0/0c:a0:9c:02:00:01 Cost = 0 Port
4	1.000460500	192.168.20.50	10.0.20.1	ICMP	98	Echo (ping) request id=0x0d0a, seq=22/5632, ttl=64 (r
5	1.018520000	10.0.20.1	192.168.20.50	ICMP	98	Echo (ping) reply id=0x0d0a, seq=22/5632, ttl=63 (r
6	1.878092700	192.168.20.50	185.125.188.57	TCP	60	34468 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
7	1.887295900	185.125.188.57	192.168.20.50	TCP	54	[TCP ACKed unseen segment] 443 → 34468 [ACK] Seq=2134
8	2.002172700	192.168.20.50	10.0.20.1	ICMP	98	Echo (ping) request id=0x0d0a, seq=23/5888, ttl=64 (r
9	2.010634100	10.0.20.1	192.168.20.50	ICMP	98	Echo (ping) reply id=0x0d0a, seq=23/5888, ttl=63 (r
10	2.596321400	0c:a0:9c:02:00:01	Nearest-Customer-Br...	STP	53	RST. Root = 32768/0/0c:a0:9c:02:00:01 Cost = 0 Port
11	3.004115900	192.168.20.50	10.0.20.1	ICMP	98	Echo (ping) request id=0x0d0a, seq=24/6144, ttl=64 (r
12	3.011872400	10.0.20.1	192.168.20.50	ICMP	98	Echo (ping) reply id=0x0d0a, seq=24/6144, ttl=63 (r

Offset	Hex	ASCII
0000	0c a0 9c 02 00 01 00 0c	29 ab 3b 97 08 00 45 00
0010	00 54 5e f0 40 00 40 01	e8 dd c0 a8 14 32 0a 00
0020	14 01 08 00 fb ce 0d 0a	00 15 69 86 30 6a 00 00
0030	00 00 89 4e 0d 00 00 00	00 00 10 11 12 13 14 15
0040	16 17 18 19 1a 1b 1c 1d	1e 1f 20 21 22 23 24 25
0050	26 27 28 29 2a 2b 2c 2d	2e 2f 30 31 32 33 34 35
0060	36 37	67

La captura de tráfico de salida de la VLAN 20, presentada en la Figura 161, muestra las solicitudes ICMP hacia 8.8.8.8 y sus correspondientes respuestas, validando que la infraestructura de enrutamiento resuelve correctamente el paso de paquetes desde la red interna urbana hacia el exterior. Las tramas STP del bridge raíz (0c:a0:9c:02:00:01) continúan presentes en esta captura, fundamentando la estabilidad del diseño de red en la zona de mayor densidad de usuarios.

Figura 161. Captura de tráfico de salida en la VLAN 20 Urbana

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.20.50	8.8.8.8	ICMP	98	Echo (ping) request id=0x0d2c, seq=14/3584, ttl=64 (r
2	0.027972400	8.8.8.8	192.168.20.50	ICMP	98	Echo (ping) reply id=0x0d2c, seq=14/3584, ttl=126 (
3	0.290325000	192.168.20.50	185.125.188.54	TCP	60	41620 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
4	0.296569600	185.125.188.54	192.168.20.50	TCP	54	[TCP ACKed unseen segment] 443 → 41620 [ACK] Seq=3594
5	1.001691000	192.168.20.50	8.8.8.8	ICMP	98	Echo (ping) request id=0x0d2c, seq=15/3840, ttl=64 (r
6	1.034533100	8.8.8.8	192.168.20.50	ICMP	98	Echo (ping) reply id=0x0d2c, seq=15/3840, ttl=126 (
7	1.353654700	0c:a0:9c:02:00:01	Nearest-Customer-Br...	STP	53	RST. Root = 32768/0/0c:a0:9c:02:00:01 Cost = 0 Port
8	2.003627200	192.168.20.50	8.8.8.8	ICMP	98	Echo (ping) request id=0x0d2c, seq=16/4096, ttl=64 (r
9	2.042410500	8.8.8.8	192.168.20.50	ICMP	98	Echo (ping) reply id=0x0d2c, seq=16/4096, ttl=126 (
10	3.004712200	192.168.20.50	8.8.8.8	ICMP	98	Echo (ping) request id=0x0d2c, seq=17/4352, ttl=64 (r
11	3.034444200	8.8.8.8	192.168.20.50	ICMP	98	Echo (ping) reply id=0x0d2c, seq=17/4352, ttl=126 (
12	3.357556300	0c:a0:9c:02:00:01	Nearest-Customer-Br...	STP	53	RST. Root = 32768/0/0c:a0:9c:02:00:01 Cost = 0 Port

Offset	Hex	ASCII
0000	0c a0 9c 02 00 01 00 0c	29 ab 3b 97 08 00 45 00
0010	00 54 50 62 40 00 40 01	05 5d c0 a8 14 32 08 08
0020	08 08 08 00 83 34 0d 2c	00 0e bd 86 30 6a 00 00
0030	00 00 85 cd 05 00 00 00	00 00 10 11 12 13 14 15
0040	16 17 18 19 1a 1b 1c 1d	1e 1f 20 21 22 23 24 25
0050	26 27 28 29 2a 2b 2c 2d	2e 2f 30 31 32 33 34 35
0060	36 37	67

VLAN 30 – Zona Empresas

Las capturas de la VLAN 30 se realizaron a través del adaptador VMnet12, utilizando la máquina virtual Kali Linux con la dirección IP 192.168.30.198 como host de prueba. En la Figura 162 se observa la comunicación bidireccional constante entre el host y el gateway corporativo (10.0.30.1), con paquetes ICMP distribuidos de forma secuencial a lo largo de la captura y tiempos de respuesta óptimos. Las tramas STP presentes en las líneas 5 y 10, emitidas por la MAC de control 0c:4d:f5:c4:00:01, validan que el switch empresarial difunde correctamente los parámetros de topología para mantener la red protegida contra bucles lógicos.

Figura 162. Captura de tráfico local en la VLAN 30 Empresas (VMnet12)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.30.198	10.0.30.1	ICMP	98	Echo (ping) request id=0x0d25, seq=13/3328, ttl=64 (r
2	0.007403700	10.0.30.1	192.168.30.198	ICMP	98	Echo (ping) reply id=0x0d25, seq=13/3328, ttl=63 (r
3	1.002075400	192.168.30.198	10.0.30.1	ICMP	98	Echo (ping) request id=0x0d25, seq=14/3584, ttl=64 (r
4	1.009113500	10.0.30.1	192.168.30.198	ICMP	98	Echo (ping) reply id=0x0d25, seq=14/3584, ttl=63 (r
5	1.014327700	0c:4d:f5:c4:00:01	Nearest-Customer-Br...	STP	53	RST. Root = 32768/0/0c:4d:f5:c4:00:01 Cost = 0 Port
6	2.004131500	192.168.30.198	10.0.30.1	ICMP	98	Echo (ping) request id=0x0d25, seq=15/3840, ttl=64 (r
7	2.013106800	10.0.30.1	192.168.30.198	ICMP	98	Echo (ping) reply id=0x0d25, seq=15/3840, ttl=63 (r
8	3.005933600	192.168.30.198	10.0.30.1	ICMP	98	Echo (ping) request id=0x0d25, seq=16/4096, ttl=64 (r
9	3.011131600	10.0.30.1	192.168.30.198	ICMP	98	Echo (ping) reply id=0x0d25, seq=16/4096, ttl=63 (r
10	3.017402500	0c:4d:f5:c4:00:01	Nearest-Customer-Br...	STP	53	RST. Root = 32768/0/0c:4d:f5:c4:00:01 Cost = 0 Port
11	4.007777400	192.168.30.198	10.0.30.1	ICMP	98	Echo (ping) request id=0x0d25, seq=17/4352, ttl=64 (r
12	4.017279400	10.0.30.1	192.168.30.198	ICMP	98	Echo (ping) reply id=0x0d25, seq=17/4352, ttl=63 (r

Frame 1: Packet, 98 bytes on wire (784 bits), 98 bytes captured	0000	0c 4d f5 c4 00 01 00 0c	29 68 d9 64 08 00 45 00	.M.....
> Ethernet II, Src: VMware_68:d9:64 (00:0c:29:68:d9:64), Dst: 0c:4d:f5:c4:00:01	0010	00 54 01 a5 40 00 40 01	31 95 c0 a8 1e c6 0a 00	.T...@..
> Internet Protocol Version 4, Src: 192.168.30.198, Dst: 10.0.30.1	0020	1e 01 08 00 64 24 0d 25	00 0d 2c 87 30 6a 00 00	...d\$.%
> Internet Control Message Protocol	0030	00 00 61 e5 09 00 00 00	00 00 10 11 12 13 14 15	...a.....
	0040	16 17 18 19 1a 1b 1c 1d	1e 1f 20 21 22 23 24 25	...a.....
	0050	26 27 28 29 2a 2b 2c 2d	2e 2f 30 31 32 33 34 35	&'()*+,-
	0060	36 37		67

En cuanto al tráfico de salida de la VLAN 30, la Figura 163 muestra las solicitudes ICMP hacia 8.8.8.8, cuyas respuestas alternas confirman que el enrutador principal realiza la traducción y el reenvío de paquetes de forma exitosa, proveyendo al sector empresarial un acceso estable hacia internet. Las tramas STP del bridge raíz empresarial (0c:4d:f5:c4:00:01) siguen presentes incluso durante la transmisión hacia redes externas, asegurando que la alta disponibilidad y la mitigación de tormentas de broadcast se mantienen constantes en beneficio de la estabilidad operativa del segmento corporativo.

Figura 163. Captura de tráfico externo en la VLAN 30 Empresas (VMnet12)

Capturing from VMware Network Adapter VMnet12

Archivo

Edición

Visualización

Ir

Captura

Analizar

Estadísticas

Telefonía

Wireless

Herramientas

Ayuda

</

El análisis completo de tráfico realizado mediante Wireshark en las tres VLAN permitió confirmar el correcto funcionamiento de los protocolos de capa 2, 3 y 4 en la topología simulada. La convergencia del protocolo STP en todos los segmentos garantiza la ausencia de bucles de red, mientras que el enrutamiento inter-VLAN y el NAT aseguran la conectividad tanto interna como externa para todos los usuarios de la red WISP propuesta.

4.2.6. Análisis estadístico de latencia

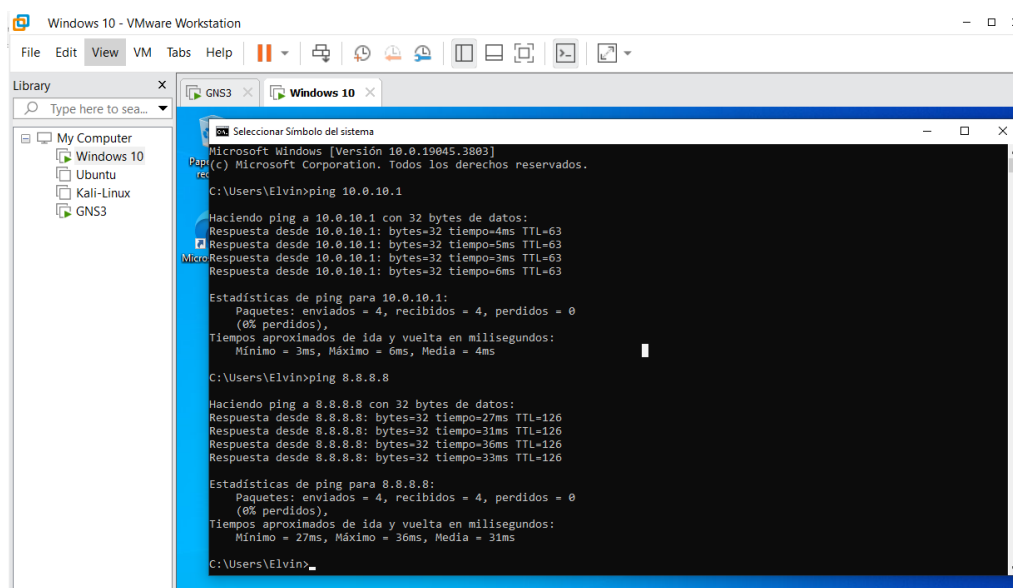
El análisis de latencia constituye uno de los indicadores más relevantes para evaluar la calidad de servicio de una red de comunicaciones. En este apartado se presentan los resultados obtenidos al medir los tiempos de respuesta entre los equipos finales de cada zona y sus respectivos gateways, así como hacia el servidor DNS público de Google (8.8.8.8) como referencia de conectividad externa. Las mediciones incluyen los valores mínimo, máximo y promedio de latencia, así como el número de paquetes transmitidos y recibidos en cada prueba.

Los resultados se obtuvieron desde los equipos de usuario de cada VLAN, empleando el comando ping estadístico en los sistemas operativos Windows 10, Ubuntu y Kali Linux, los cuales proporcionan una presentación más detallada de los indicadores de latencia en comparación con el cliente VPCS de GNS3.

VLAN 10 – Zona Rural

Las pruebas de latencia en la VLAN 10 se ejecutaron desde la máquina virtual Windows 10, realizando dos tipos de medición: hacia el gateway local (10.0.10.1) y hacia el servidor externo (8.8.8.8). Como se puede observar en la Figura 164, la latencia hacia el gateway local presentó un valor mínimo de 3 ms, un valor máximo de 6 ms y una media de 4 ms, con cuatro paquetes enviados y recibidos sin ninguna pérdida. Para la conectividad hacia internet (8.8.8.8), los valores registrados fueron: mínimo de 27 ms, máximo de 36 ms y media de 31 ms, igualmente sin pérdida de paquetes.

Figura 164. *Análisis estadístico de latencia en la VLAN 10 Rural desde Windows 10*



```

Microsoft Windows [Versión 10.0.19045.3803]
(c) Microsoft Corporation. Todos los derechos reservados.
C:\Users\Elvin>ping 10.0.10.1

Haciendo ping a 10.0.10.1 con 32 bytes de datos:
Respuesta desde 10.0.10.1: bytes=32 tiempo=4ms TTL=63
Respuesta desde 10.0.10.1: bytes=32 tiempo=5ms TTL=63
Respuesta desde 10.0.10.1: bytes=32 tiempo=3ms TTL=63
Respuesta desde 10.0.10.1: bytes=32 tiempo=6ms TTL=63

Estadísticas de ping para 10.0.10.1:
Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
Mínimo = 3ms, Máximo = 6ms, Media = 4ms

C:\Users\Elvin>ping 8.8.8.8

Haciendo ping a 8.8.8.8 con 32 bytes de datos:
Respuesta desde 8.8.8.8: bytes=32 tiempo=27ms TTL=126
Respuesta desde 8.8.8.8: bytes=32 tiempo=31ms TTL=126
Respuesta desde 8.8.8.8: bytes=32 tiempo=36ms TTL=126
Respuesta desde 8.8.8.8: bytes=32 tiempo=33ms TTL=126

Estadísticas de ping para 8.8.8.8:
Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
Mínimo = 27ms, Máximo = 36ms, Media = 31ms

C:\Users\Elvin>

```

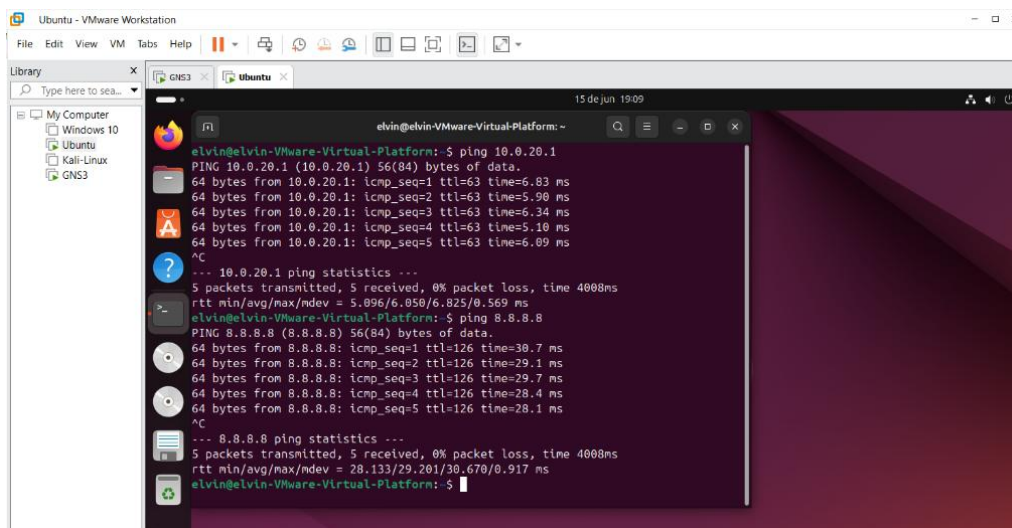
Los valores de latencia hacia el gateway local reflejan una comunicación de baja latencia propia de una red LAN simulada, mientras que los tiempos hacia internet incorporan el retardo acumulado por el trayecto a través del Router_Core, el proceso NAT, la interfaz de salida de GNS3 hacia el sistema anfitrión y el enlace real hacia el servidor externo. En ambos casos, la ausencia de pérdida de paquetes confirma la estabilidad del enlace en este segmento.

VLAN 20 – Zona Urbana

En la zona urbana, las mediciones de latencia se realizaron desde la máquina virtual Ubuntu. Hacia el gateway de la VLAN 20 (10.0.20.1), los resultados de la Figura 165 indican un

valor mínimo de 5.096 ms, máximo de 6.825 ms y media de 6.050 ms, con 5 paquetes enviados y recibidos sin pérdida. Para la conectividad hacia el servidor externo 8.8.8.8, los valores registrados fueron: mínimo de 28.133 ms, máximo de 30.670 ms y media de 29.201 ms, con 5 paquetes transmitidos y recibidos exitosamente.

Figura 165. *Análisis estadístico de latencia en la VLAN 20 Urbana desde Ubuntu*



```

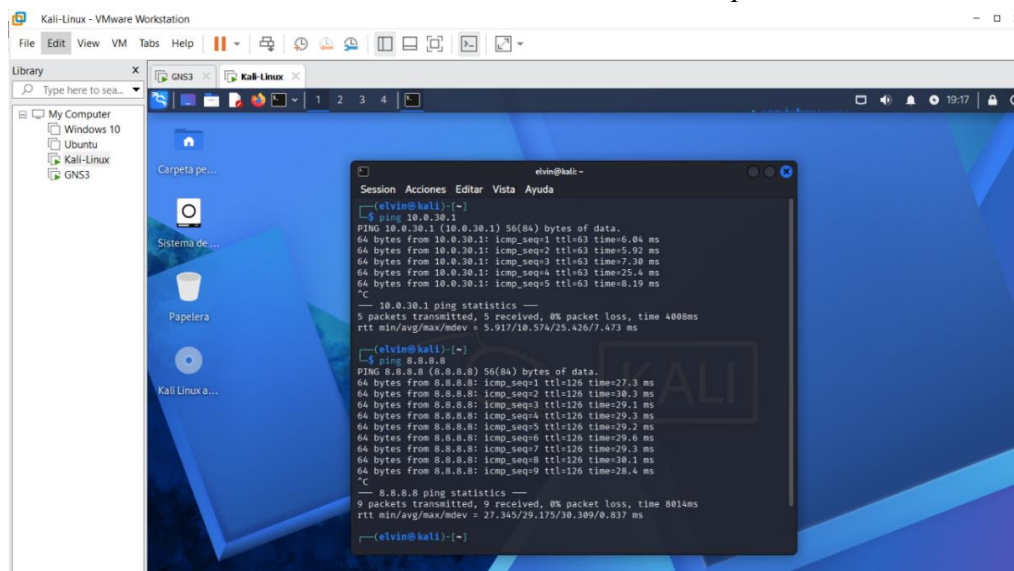
elvin@elvin-VMware-Virtual-Platform: ~
$ ping 10.0.20.1
PING 10.0.20.1 (10.0.20.1) 56(84) bytes of data:
64 bytes from 10.0.20.1: icmp_seq=1 ttl=63 time=6.83 ms
64 bytes from 10.0.20.1: icmp_seq=2 ttl=63 time=5.90 ms
64 bytes from 10.0.20.1: icmp_seq=3 ttl=63 time=5.34 ms
64 bytes from 10.0.20.1: icmp_seq=4 ttl=63 time=5.10 ms
64 bytes from 10.0.20.1: icmp_seq=5 ttl=63 time=6.09 ms
^C
--- 10.0.20.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 400ms
rtt min/avg/max/ndev = 5.096/6.050/6.825/0.569 ms
elvin@elvin-VMware-Virtual-Platform: ~
$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data:
64 bytes from 8.8.8.8: icmp_seq=1 ttl=126 time=30.7 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=126 time=29.1 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=126 time=29.7 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=126 time=28.4 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=126 time=28.1 ms
^C
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 400ms
rtt min/avg/max/ndev = 28.133/29.201/30.670/0.917 ms
elvin@elvin-VMware-Virtual-Platform: ~

```

Los tiempos registrados en la VLAN 20 son ligeramente superiores a los de la VLAN 10, lo cual es consistente con el mayor número de saltos que debe recorrer el tráfico urbano a través de la topología simulada. Sin embargo, los valores se mantienen dentro de rangos aceptables para una red de tipo WISP, sin comprometer la calidad de servicio percibida por el usuario.

VLAN 30 – Zona Empresas

Las mediciones de latencia correspondientes al segmento corporativo se obtuvieron desde la máquina virtual Kali Linux. Como se muestra en la Figura 166, la latencia hacia el gateway de la VLAN 30 (10.0.30.1) presentó valores más dispersos: mínimo de 5.917 ms, máximo de 25.426 ms y media de 10.574 ms, con 5 paquetes transmitidos y recibidos. Esta variabilidad, mayor respecto a las otras zonas, puede estar relacionada con la carga del sistema anfitrión durante las pruebas o con la prioridad de los recursos virtuales asignados a este segmento en el momento de la medición. Hacia el servidor externo 8.8.8.8, los valores fueron: mínimo de 27.345 ms, máximo de 30.309 ms y media de 29.175 ms, sobre 9 paquetes enviados y recibidos sin pérdida.

Figura 166. *Análisis estadístico de latencia en la VLAN 30 Empresas desde Kali Linux*

A modo de resumen consolidado, la siguiente Tabla 50 presenta los indicadores de latencia obtenidos para las tres zonas de cobertura de la red WISP propuesta:

Tabla 50. *Resumen comparativo de latencia por VLAN para tráfico local (gateway) y tráfico externo (8.8.8.8) en la red WISP simulada*

Segmento	Destino	Mín (ms)	Máx (ms)	Media (ms)
VLAN 10 Rural	10.0.10.1 (GW)	3	6	4
VLAN 10 Rural	8.8.8.8 (internet)	27	36	31
VLAN 20 Urbano	10.0.20.1 (GW)	5.096	6.825	6.050
VLAN 20 Urbano	8.8.8.8 (internet)	28.133	30.670	29.201
VLAN 30 Empresas	10.0.30.1 (GW)	5.917	25.426	10.574
VLAN 30 Empresas	8.8.8.8 (internet)	27.345	30.309	29.175

Los resultados permiten concluir que la latencia hacia los gateways locales de las tres zonas se mantiene en rangos inferiores a 11 ms para los casos típicos, lo cual resulta coherente con el comportamiento esperado en una red de acceso WISP de baja carga. La latencia hacia internet, que ronda entre 27 y 37 ms en las tres zonas, incorpora el retardo del trayecto completo desde el equipo de usuario hasta el servidor de Google, pasando por la infraestructura de simulación y el enlace real del sistema anfitrión. En todos los casos, la tasa de pérdida de paquetes fue del 0 %, lo que valida la estabilidad de las comunicaciones en el entorno simulado.

4.2.7. Evaluación del rendimiento de transferencia de datos

Para complementar los análisis de conectividad y latencia, se procedió a evaluar el rendimiento máximo de transferencia de datos que la infraestructura simulada es capaz de ofrecer entre el Router_Core y cada uno de los routers de acceso de las zonas de cobertura. Para ello se empleó WinBox, la herramienta gráfica de administración de MikroTik RouterOS, a través de la cual se accedió a la función Bandwidth Test (Tools > Bandwidth Test), que permite medir de forma activa el caudal de transmisión y recepción entre dos equipos MikroTik de la red.

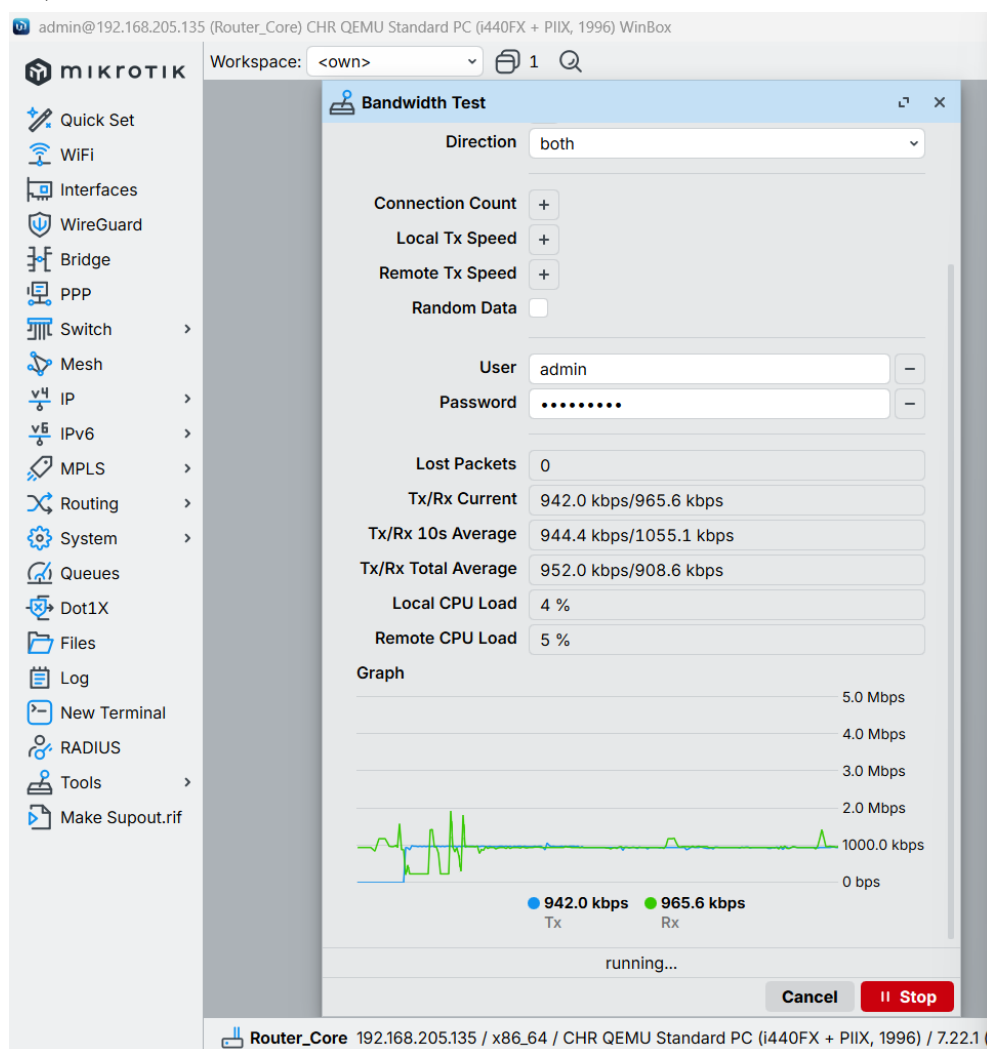
El procedimiento consistió en conectarse al Router_Core desde WinBox mediante su dirección IP (192.168.205.135) o dirección MAC y configurar el Bandwidth Test indicando como destino la dirección IP de administración del router de cada zona. La dirección de prueba se configuró en modo bidireccional (both), lo que permite medir simultáneamente el throughput de transmisión (Tx, representado en azul) y el de recepción (Rx, representado en verde).

Es importante destacar que los resultados de esta prueba están condicionados por las limitaciones propias de la versión gratuita de MikroTik RouterOS CHR (Cloud Hosted Router), que impone un límite de 1 Mbps (1000 kbps) por interfaz como restricción de velocidad. Este límite no representa el techo real de la red diseñada, sino únicamente la restricción de la licencia gratuita utilizada en el entorno de simulación. Para entornos de producción, sería necesario adquirir una licencia comercial en el portal oficial de MikroTik, que elimina esta restricción y permite aprovechar el ancho de banda completo del hardware.

VLAN 10 – Zona Rural (Router 10.0.10.254)

La prueba de Bandwidth Test dirigida al Router_Rural (10.0.10.254) arrojó un throughput de transmisión (Tx) de 942.0 kbps y un throughput de recepción (Rx) de 965.6 kbps, con un promedio de 10 segundos de 944.4/1055.1 kbps. Como se aprecia en la Figura 167, la carga de CPU local se reportó en 4 % y la remota en 5 %, lo que indica un uso de recursos mínimo durante la prueba. Los valores alcanzados se aproximan al límite de 1 Mbps impuesto por la licencia gratuita, confirmando que la topología virtual es capaz de transferir datos de forma eficiente entre el nodo central y el acceso rural.

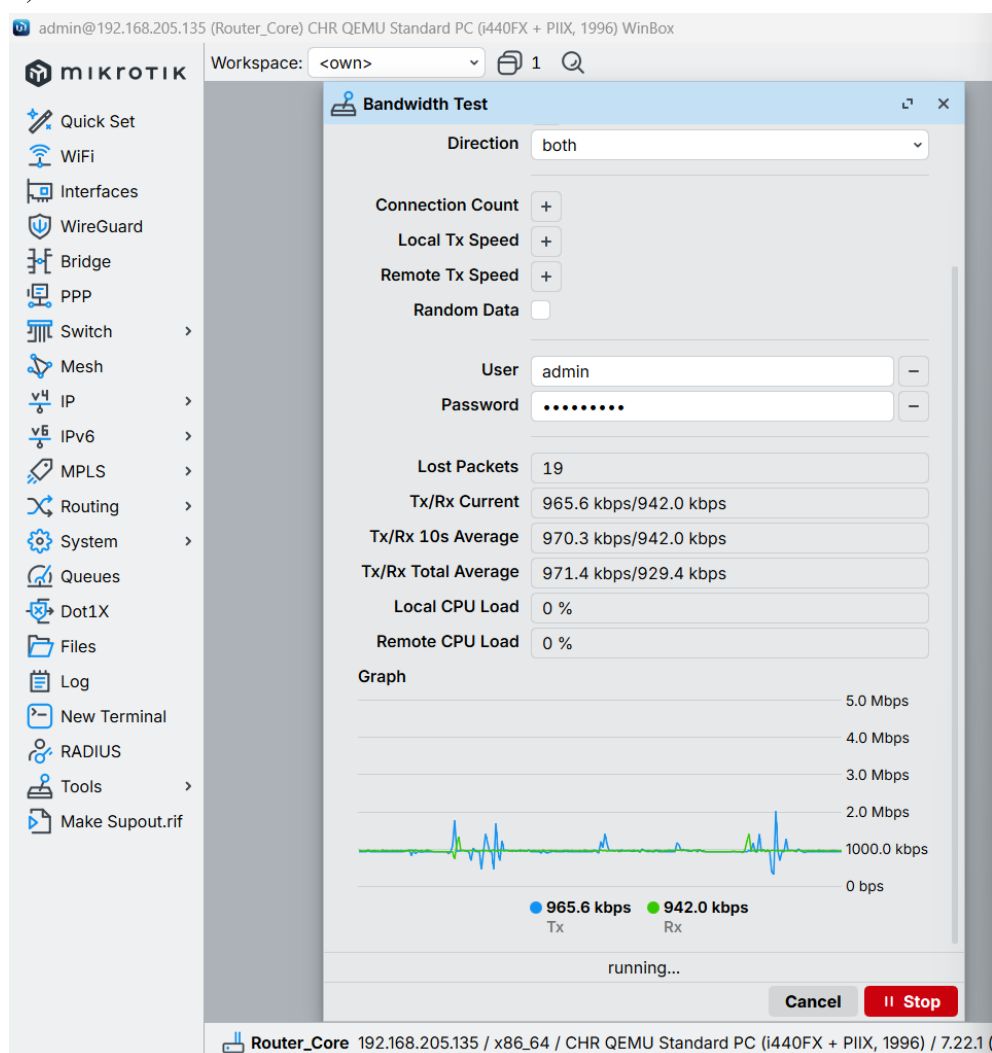
Figura 167. Resultado del Bandwidth Test desde el Router_Core hacia el Router_Cliente_Rural (10.0.10.254) mediante WinBox



VLAN 20 – Zona Urbana (Router 10.0.20.254)

La evaluación de rendimiento hacia el Router_Urbano (10.0.20.254) produjo un throughput actual de 965.6 kbps en transmisión y 942.0 kbps en recepción, con un promedio acumulado de 970.3/942.0 kbps, tal como se muestra en la Figura 168. En este caso, la carga de CPU en ambos extremos fue de 0 %, lo que evidencia que los recursos de cómputo no representan un cuello de botella en la transferencia. Se registraron 19 paquetes perdidos durante la prueba, valor atribuible a la dinámica de inicialización del test más que a una condición de degradación del enlace.

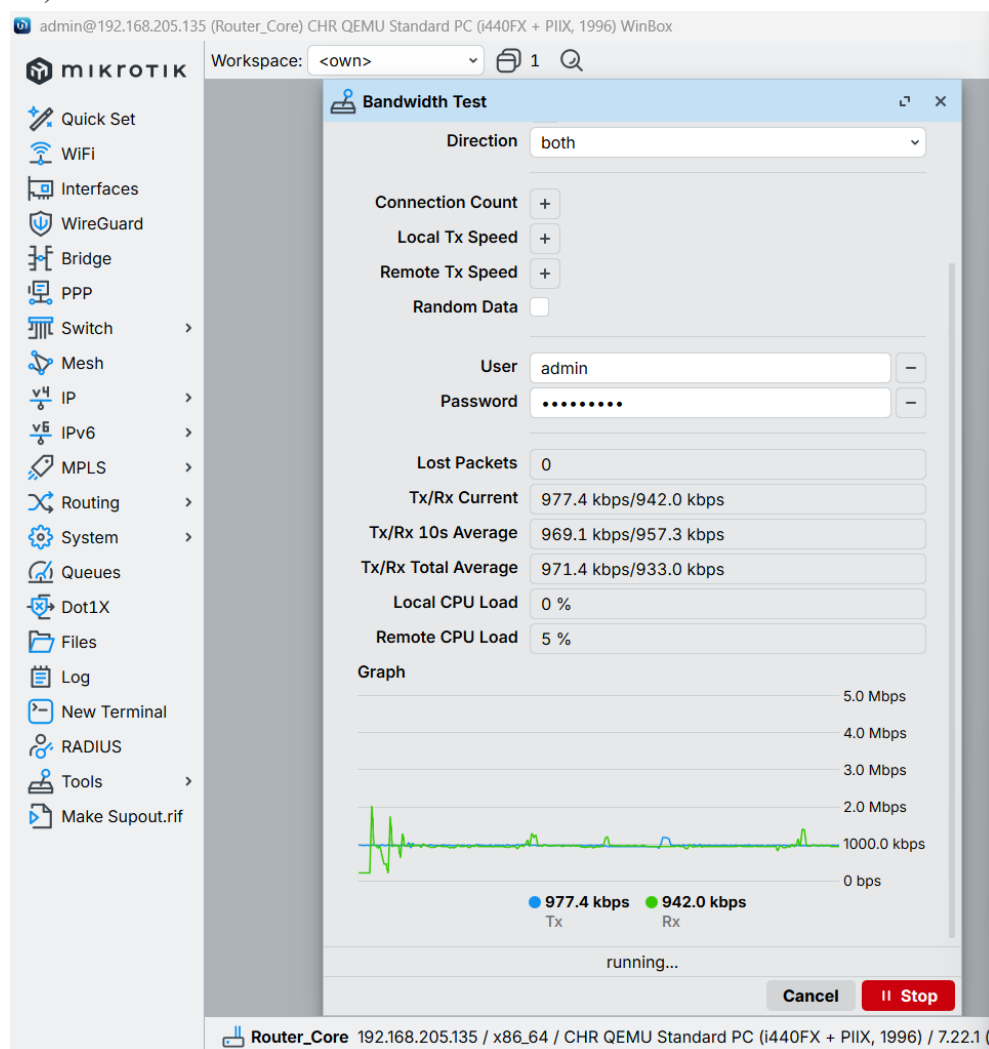
Figura 168. Resultado del Bandwidth Test desde el Router_Core hacia el Router_Cliente_Urbano (10.0.20.254) mediante WinBox



VLAN 30 – Zona Empresas (Router 10.0.30.254)

La prueba correspondiente al segmento empresarial, ejecutada hacia el Router_Empresas (10.0.30.254), reportó un throughput actual de 977.4 kbps en transmisión y 942.0 kbps en recepción, con un promedio de 10 segundos de 969.1/957.3 kbps, como se ilustra en la Figura 169. La carga de CPU local fue de 0 % y la remota de 5 %, sin paquetes perdidos durante la sesión de prueba, lo que refleja el comportamiento más estable entre las tres zonas evaluadas.

Figura 169. Resultado del Bandwidth Test desde el Router_Core hacia el Router_Empresas (10.0.30.254) mediante WinBox



En los tres segmentos evaluados, el Bandwidth Test confirmó que la red simulada opera al límite de transferencia permitido por la licencia gratuita de Mikrotik RouterOS CHR (aproximadamente 1 Mbps por interfaz). Todos los routers de acceso respondieron satisfactoriamente a la prueba, lo que valida la capacidad de la topología para sostener flujos de datos bidireccionales continuos entre el nodo central y cada zona de cobertura. En un escenario de producción real con licencia comercial, estos valores se incrementarían sustancialmente en función del hardware y el ancho de banda del enlace de backhaul disponible.

4.2.8. Validación de enlaces redundantes

Una de las características críticas de cualquier red de comunicaciones es su capacidad para mantener la operatividad del servicio ante la ocurrencia de fallos en alguno de sus componentes. En el diseño de la red WISP propuesta, esta tolerancia a fallos se garantiza mediante la incorporación de backups en cada una de las zonas de cobertura (Rural, Urbano y Empresas), los cuales actúan como rutas alternativas en caso de interrupción del enlace principal entre la Antena Sectorial Principal y las antenas CPE de cada sector.

Para demostrar el funcionamiento de este mecanismo de redundancia en el entorno simulado, se emuló la pérdida del enlace principal deshabilitando temporalmente la interfaz de la Antena Sectorial Principal que conecta hacia cada CPE, mediante el siguiente comando de MikroTik RouterOS:

```
/interface disable etherX::delay 30s; /interface enable etherX
```

Este comando deshabilita la interfaz indicada durante 30 segundos y la restaura de forma automática, simulando la condición de un obstáculo físico o una interrupción temporal del enlace de radio. De manera paralela, se ejecutó en cada equipo de usuario un ping continuo (ping 8.8.8.8 -t) para monitorear en tiempo real la pérdida y recuperación de la conectividad, observando el comportamiento de los repetidores al asumir el tráfico del enlace caído.

VLAN 10 – Validación del Backup1_Rural

Para la zona rural, se deshabilitó la interfaz ether2 de la Antena Sectorial Principal, que corresponde al enlace directo hacia el CPE_Rural (VLAN 10). Simultáneamente, se ejecutó un ping continuo a 8.8.8.8 desde PC1. Como se aprecia en la Figura 170, al producirse la interrupción del enlace se observa una pérdida de conectividad de aproximadamente 3 segundos, tras los cuales el tráfico es redirigido automáticamente a través del Backup1_Rural y se recupera la comunicación sin necesidad de intervención manual. Una vez transcurridos los 30 segundos configurados, el enlace principal es restaurado y el tráfico continúa fluyendo de forma estable.

Figura 170. Simulación de fallo del enlace principal hacia CPE_Rural mediante inhabilitación de ether2 en la antena sectorial principal

```

PC1 - PuTTY
84 bytes from 8.8.8.8 icmp_seq=14 ttl=126 time=29.938 ms
84 bytes from 8.8.8.8 icmp_seq=15 ttl=126 time=41.259 ms
84 bytes from 8.8.8.8 icmp_seq=16 ttl=126 time=28.606 ms
84 bytes from 8.8.8.8 icmp_seq=17 ttl=126 time=30.586 ms
84 bytes from 8.8.8.8 icmp_seq=18 ttl=126 time=27.387 ms
84 bytes from 8.8.8.8 icmp_seq=19 ttl=126 time=29.630 ms
84 bytes from 8.8.8.8 icmp_seq=20 ttl=126 time=26.552 ms
84 bytes from 8.8.8.8 icmp_seq=21 ttl=126 time=28.556 ms
84 bytes from 8.8.8.8 icmp_seq=22 ttl=126 time=28.066 ms
84 bytes from 8.8.8.8 icmp_seq=23 ttl=126 time=27.838 ms
84 bytes from 8.8.8.8 icmp_seq=24 ttl=126 time=29.107 ms
84 bytes from 8.8.8.8 icmp_seq=25 ttl=126 time=31.370 ms
84 bytes from 8.8.8.8 icmp_seq=26 ttl=126 time=25.947 ms
84 bytes from 8.8.8.8 icmp_seq=27 ttl=126 time=28.558 ms
84 bytes from 8.8.8.8 icmp_seq=28 ttl=126 time=29.473 ms
84 bytes from 8.8.8.8 icmp_seq=29 ttl=126 time=25.690 ms
84 bytes from 8.8.8.8 icmp_seq=30 ttl=126 time=33.617 ms
8.8.8.8 icmp_seq=31 timeout
8.8.8.8 icmp_seq=32 timeout
8.8.8.8 icmp_seq=33 timeout
84 bytes from 8.8.8.8 icmp_seq=34 ttl=126 time=36.545 ms
84 bytes from 8.8.8.8 icmp_seq=35 ttl=126 time=28.147 ms
84 bytes from 8.8.8.8 icmp_seq=36 ttl=126 time=28.295 ms

Antena-Sectorial-Principal - PuTTY
Press F1 for help

(3 messages not shown)
2026-05-24 08:14:41 system,error,critical router was rebooted without proper shutdown
2026-05-24 17:47:31 system,error,critical router was rebooted without proper shutdown
2026-05-24 18:02:47 system,error,critical router was rebooted without proper shutdown
2026-06-07 17:09:17 system,error,critical router was rebooted without proper shutdown
2026-06-15 17:22:40 system,error,critical router was rebooted without proper shutdown
2026-06-16 01:25:25 system,error,critical router was rebooted without proper shutdown
2026-06-16 01:25:27 system,error,critical kernel failure in previous boot
2026-06-16 01:26:04 system,error,critical Automatic supout.rif file generated due to service malfunction, please contact MikroTik support and supply the generated file
[admin@Antena_Sectorial_Principal] > /interface disable ether2; :delay 30s; /interface enable ether2

```

VLAN 20 – Validación del Backup2_Urbano

En la zona urbana, la prueba se realizó inhabilitando la interfaz ether3 de la Antena Sectorial Principal, que corresponde al enlace con el CPE_Urbano. El ping continuo ejecutado desde PC2 hacia 8.8.8.8, mostrado en la Figura 171, evidencia una interrupción de aproximadamente 2 segundos antes de que el Backup2_Urbano asuma el tráfico y restablezca la conectividad. El tiempo de convergencia fue inferior al registrado en la zona rural, lo que puede atribuirse a diferencias en la configuración de las rutas o en la respuesta de los dispositivos virtuales en ese instante específico de la simulación.

Figura 171. Simulación de fallo del enlace hacia CPE_Urbano mediante inhabilitación de ether3 en la antena sectorial principal

```

PC2 - PuTTY
DORA IP 192.168.20.100/24 GW 192.168.20.1
PC2> ping 8.8.8.8 -t
84 bytes from 8.8.8.8 icmp_seq=1 ttl=126 time=31.171 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=126 time=29.655 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=126 time=29.180 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=126 time=28.045 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=126 time=28.165 ms
84 bytes from 8.8.8.8 icmp_seq=6 ttl=126 time=30.404 ms
84 bytes from 8.8.8.8 icmp_seq=7 ttl=126 time=34.703 ms
84 bytes from 8.8.8.8 icmp_seq=8 ttl=126 time=29.501 ms
84 bytes from 8.8.8.8 icmp_seq=9 ttl=126 time=29.945 ms
84 bytes from 8.8.8.8 icmp_seq=10 ttl=126 time=29.781 ms
84 bytes from 8.8.8.8 icmp_seq=11 ttl=126 time=31.816 ms
84 bytes from 8.8.8.8 icmp_seq=12 ttl=126 time=28.775 ms
8.8.8.8 icmp_seq=13 timeout
8.8.8.8 icmp_seq=14 timeout
84 bytes from 8.8.8.8 icmp_seq=15 ttl=126 time=29.511 ms
84 bytes from 8.8.8.8 icmp_seq=16 ttl=126 time=29.353 ms
84 bytes from 8.8.8.8 icmp_seq=17 ttl=126 time=34.695 ms
84 bytes from 8.8.8.8 icmp_seq=18 ttl=126 time=29.879 ms

Antena-Sectorial-Principal - PuTTY
[admin@Antena_Sectorial_Principal] > /interface disable ether3; :delay 30s; /interface enable ether3

```

VLAN 30 – Validación del Backup3_Empresas

Para el segmento corporativo, la prueba de redundancia se llevó a cabo inhabilitando la interfaz ether4 de la Antena Sectorial Principal, que establece el enlace con el CPE_Empresas. El ping continuo a 8.8.8.8 desde PC3, presentado en la Figura 172, mostró igualmente una interrupción de aproximadamente 2 segundos hasta que el Backup3_Empresas activó su función de ruta alternativa y restableció la comunicación de forma estable. Al igual que en los casos anteriores, la restauración del enlace principal al cabo de los 30 segundos configurados no produjo ninguna interrupción adicional en el servicio.

Figura 172. Simulación de fallo del enlace hacia CPE_Empresas mediante inhabilitación de ether4 en la antena sectorial principal

```

PC3 - PuTTY
84 bytes from 8.8.8.8: icmp_seq=233 ttl=126 time=31.781 ms
84 bytes from 8.8.8.8: icmp_seq=234 ttl=126 time=32.911 ms
84 bytes from 8.8.8.8: icmp_seq=235 ttl=126 time=27.233 ms
84 bytes from 8.8.8.8: icmp_seq=236 ttl=126 time=28.845 ms
84 bytes from 8.8.8.8: icmp_seq=237 ttl=126 time=28.441 ms
84 bytes from 8.8.8.8: icmp_seq=238 ttl=126 time=29.132 ms
84 bytes from 8.8.8.8: icmp_seq=239 ttl=126 time=29.777 ms
84 bytes from 8.8.8.8: icmp_seq=240 ttl=126 time=29.044 ms
84 bytes from 8.8.8.8: icmp_seq=241 ttl=126 time=28.942 ms
84 bytes from 8.8.8.8: icmp_seq=242 ttl=126 time=30.186 ms
84 bytes from 8.8.8.8: icmp_seq=243 ttl=126 time=29.992 ms
84 bytes from 8.8.8.8: icmp_seq=244 ttl=126 time=29.499 ms
84 bytes from 8.8.8.8: icmp_seq=245 ttl=126 time=28.438 ms
84 bytes from 8.8.8.8: icmp_seq=246 ttl=126 time=28.984 ms
84 bytes from 8.8.8.8: icmp_seq=247 ttl=126 time=29.688 ms
8.8.8.8: icmp_seq=248: timeout
8.8.8.8: icmp_seq=249: timeout
84 bytes from 8.8.8.8: icmp_seq=250 ttl=126 time=32.313 ms
84 bytes from 8.8.8.8: icmp_seq=251 ttl=126 time=41.234 ms
84 bytes from 8.8.8.8: icmp_seq=252 ttl=126 time=29.573 ms
84 bytes from 8.8.8.8: icmp_seq=253 ttl=126 time=30.720 ms
84 bytes from 8.8.8.8: icmp_seq=254 ttl=126 time=46.521 ms
84 bytes from 8.8.8.8: icmp_seq=255 ttl=126 time=38.212 ms

Antena-Sectorial-Principal - PuTTY
[admin@Antena_Sectorial_Principal] > /interface disable ether4; :delay 30s; /interface enable ether4

```

Los resultados de las tres pruebas de redundancia confirmaron que los backups diseñados para cada zona de cobertura cumplen eficazmente con su función de proporcionar continuidad del servicio ante fallos en el enlace principal. Los tiempos de conmutación registrados, comprendidos entre 2 y 3 segundos, son aceptables para una red WISP de las características propuestas y demuestran la robustez del diseño en términos de tolerancia a fallos.

4.2.9. Validación integral de la topología propuesta

Los resultados obtenidos a partir del conjunto de pruebas realizadas en el entorno de simulación GNS3 permitieron validar el correcto funcionamiento de la topología WISP propuesta en todos sus aspectos fundamentales. A lo largo de las secciones precedentes se comprobó la correcta asignación del direccionamiento IP en los nodos de infraestructura y de acceso, el funcionamiento del servidor DHCP para los equipos de usuario de las tres zonas de cobertura, la correcta segmentación lógica mediante VLAN, el acceso a internet a través de la traducción NAT,

el comportamiento del tráfico a nivel de paquete mediante capturas Wireshark, los indicadores de latencia por segmento, el rendimiento máximo de transferencia mediante WinBox y la capacidad del diseño para mantener la continuidad del servicio ante la pérdida de un enlace principal.

El análisis de latencia evidenció tiempos de respuesta bajos y ausencia de pérdida de paquetes en condiciones normales de operación, mientras que las pruebas de Bandwidth Test confirmaron que la infraestructura virtual es capaz de operar al límite de transferencia de la plataforma de simulación empleada. Las pruebas de redundancia demostraron que el diseño de la red responde adecuadamente ante escenarios de fallo, garantizando la continuidad del servicio mediante la activación automática del backup en un tiempo de convergencia inferior a 3 segundos.

En conjunto, los resultados obtenidos validan que la infraestructura diseñada cumple con los requerimientos funcionales establecidos para la red WISP propuesta, garantizando la comunicación entre los distintos segmentos de la topología y proporcionando una base sólida para la posterior evaluación de cobertura y desempeño inalámbrico desarrollada en Atoll.

4.3. Resultados de la planificación y cobertura en Atoll

En esta sección se presentan los resultados obtenidos a partir de la simulación radioeléctrica ejecutada en el software Atoll, herramienta especializada en planificación de redes de telecomunicaciones inalámbricas. El proceso de simulación abarcó desde la verificación geométrica de los enlaces punto a punto hasta la generación de mapas de cobertura, análisis de niveles de señal recibida, capacidad de transmisión y relación portadora a interferencia. Todos los resultados fueron obtenidos bajo las condiciones topográficas reales de la provincia de Santa Elena, incorporando el modelo de elevación del terreno y las características técnicas de los equipos definidos en el diseño: la antena principal LiteAP LAP-120 de 16 dBi como nodo central y las estaciones remotas NanoStation Loco 5AC de 13 dBi como equipos de usuario (CPE) para cada uno de los tres segmentos de red (VLAN 10 – Rural, VLAN 20 – Urbana, VLAN 30 – Empresas).

Los análisis desarrollados permitieron validar cuantitativamente la viabilidad técnica del diseño propuesto y determinar los indicadores de rendimiento que sustentarán el correcto funcionamiento del WISP en las zonas de cobertura proyectadas.

4.3.1. Análisis de viabilidad de los enlaces inalámbricos

Como primer paso en la evaluación del sistema WISP, se procedió a verificar la viabilidad técnica de cada uno de los enlaces inalámbricos establecidos entre la antena principal y las estaciones de usuario remotas. Este análisis es fundamental, dado que la correcta operación de una red inalámbrica en la banda de 5 GHz depende en gran medida de dos condiciones esenciales: la existencia de línea de vista directa (LOS, por sus siglas en inglés, Line of Sight) entre los extremos del enlace y el despeje adecuado de la primera zona de Fresnel.

Para llevar a cabo esta verificación se empleó la herramienta de análisis de microondas integrada en Atoll (Microwave Link Analysis), que permite generar perfiles de elevación topográfica sobre la trayectoria exacta de cada enlace y evaluar de manera precisa el comportamiento del canal radioeléctrico. Los tres enlaces analizados corresponden a las conexiones entre la antena principal y cada una de las CPE asociadas a las VLAN del diseño: CPE-Rural (VLAN 10), CPE-Urbano (VLAN 20) y CPE-Empresas (VLAN 30). El procedimiento de configuración del perfil en dicha herramienta fue idéntico para los tres enlaces analizados y se detalla en el Anexo A; en este apartado se presentan únicamente los resultados obtenidos.

Evaluación de línea de vista (LOS)

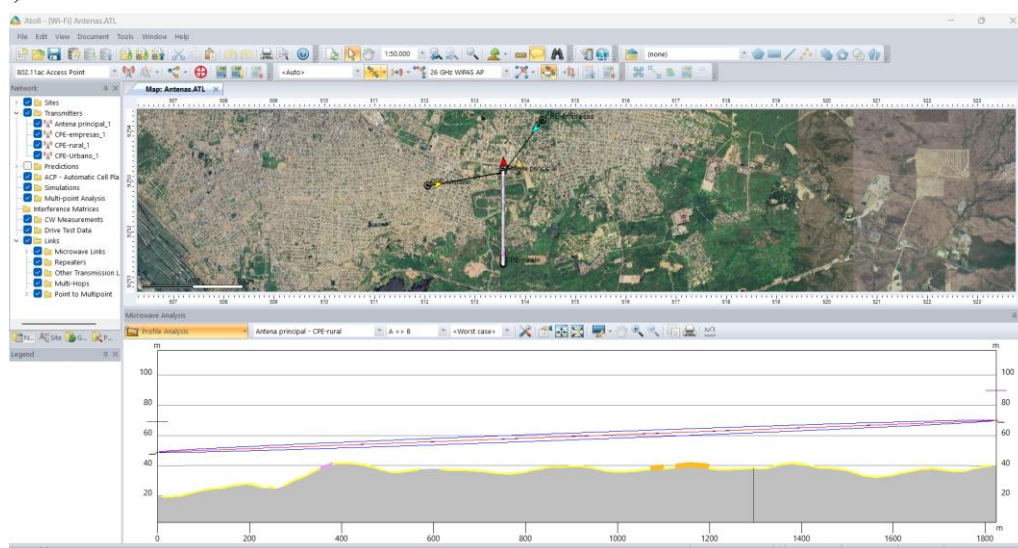
La evaluación de la línea de vista constituye la verificación más básica y, al mismo tiempo, más crítica en el diseño de un enlace inalámbrico de microondas. Un enlace LOS garantiza que el haz electromagnético viaje sin obstrucciones directas entre el transmisor y el receptor, maximizando la potencia de la señal recibida y minimizando las pérdidas adicionales por difracción o reflexión en el trayecto. Para cada uno de los tres sectores se configuró la herramienta Profile Analysis de Atoll indicando las coordenadas y alturas de instalación de las antenas extremas, a fin de obtener el perfil topográfico real del enlace.

VLAN 10 – Sector Rural (CPE-Rural)

Resultado del perfil topográfico: Una vez configuradas las alturas de las antenas, Atoll generó automáticamente el perfil de elevación del terreno sobre la trayectoria del enlace. Como se puede observar en la Figura 173, el enlace entre la antena principal y el CPE-Rural presenta una distancia de propagación de 1,826 km, con un corredor de trayectoria notablemente despejado. El

perfil topográfico evidencia que, si bien a lo largo del trayecto existen elementos como zonas de pastizales, matorrales y cultivos, ninguno de estos obstáculos penetra en la zona del haz electromagnético principal. La colocación estratégica de ambas antenas en puntos de relieve elevado fue determinante para obtener este resultado, ya que les permite operar por encima del nivel medio del terreno y los obstáculos circundantes, asegurando una trayectoria de propagación limpia y eficiente.

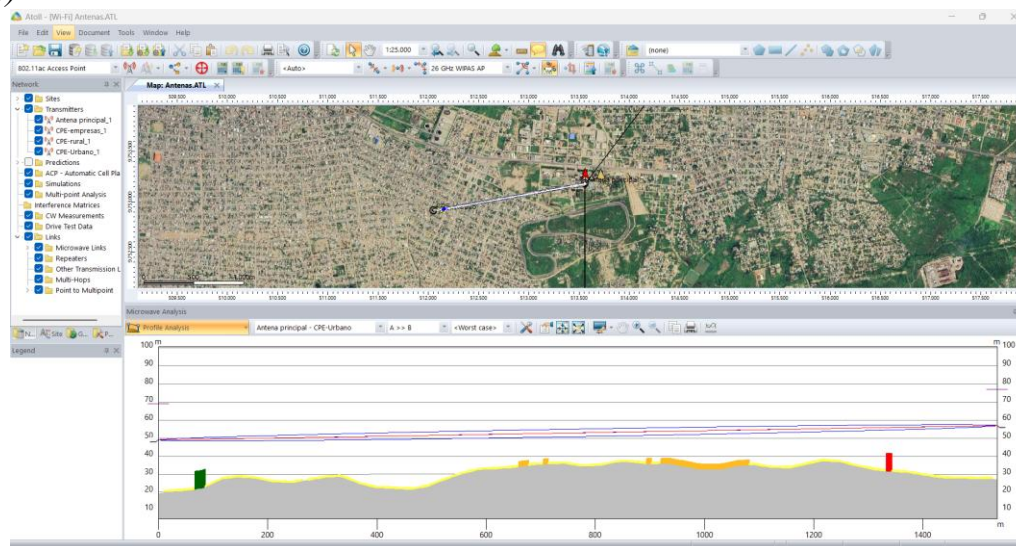
Figura 173. Perfil topográfico del enlace inalámbrico entre la antena principal y el CPE-Rural (VLAN 10)



VLAN 20 – Sector Urbano (CPE-Urbano)

Resultado del perfil topográfico: El perfil generado para el enlace urbano, mostrado en la Figura 174, indica que este trayecto tiene una distancia de propagación de **1,532 km**. A pesar de que el área urbana implica la presencia de edificaciones, infraestructura vial y vegetación de menor altura, el perfil topográfico confirma que el corredor de propagación se mantiene libre de obstrucciones directas. Los elementos del entorno, tales como matorrales, pastizales, zonas urbanas y pequeñas masas boscosas dispersas, se encuentran por debajo del nivel del haz electromagnético principal, lo que garantiza la existencia de línea de vista directa entre ambos extremos del enlace. La distancia apropiada de este enlace, junto con la configuración omnidireccional y direccional correspondiente de las antenas, contribuye a mantener pérdidas por espacio libre controladas, resultando en niveles de señal recibida favorables para este trayecto.

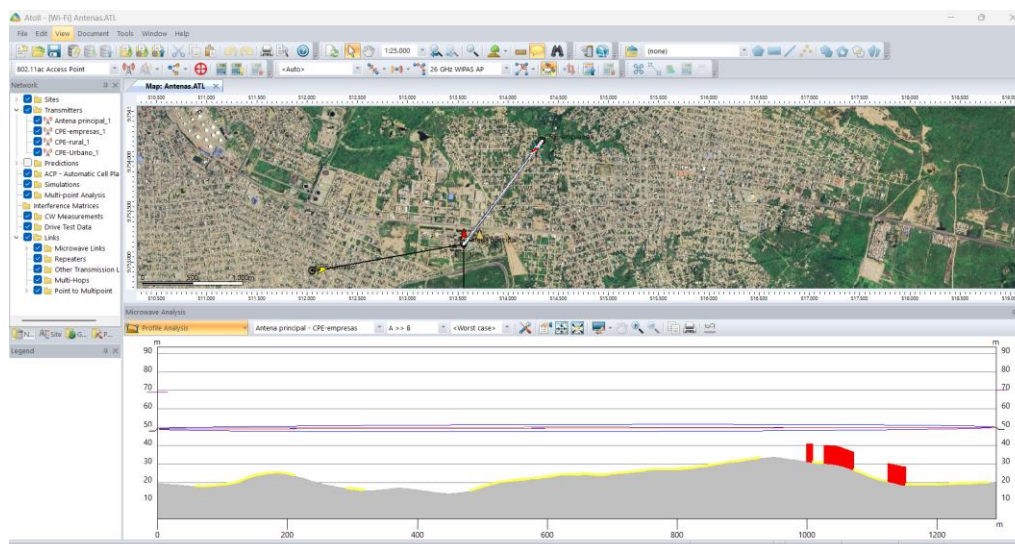
Figura 174. Perfil topográfico del enlace inalámbrico entre la antena principal y el CPE-Urbano (VLAN 20)



VLAN 30 – Sector Empresarial (CPE-Empresas)

Resultado del perfil topográfico: La Figura 175 presenta el perfil topográfico del enlace hacia el sector empresarial, el cual alcanza una distancia de **1,288 km**, siendo la menor de las tres trayectorias analizadas. No obstante, esta menor distancia representa además una ventaja significativa en términos de pérdidas por espacio libre, ya que resulta en niveles de señal recibida considerablemente más altos que los obtenidos en los trayectos más largos. Si bien en la trayectoria se identifican obstáculos puntuales como zonas urbanas de alta densidad, matorrales y áreas de pastizales, todos ellos se ubican por debajo del corredor de propagación definido por las alturas de instalación seleccionadas. Esto confirma la existencia de línea de vista directa entre la antena principal y el CPE-Empresas, garantizando que la señal no experimente pérdidas adicionales significativas por difracción en este enlace.

Figura 175. *Perfil topográfico del enlace inalámbrico entre la antena principal y el CPE-Empresas (VLAN 30)*



En resumen, el análisis de línea de vista realizado para los tres enlaces del sistema WISP demuestra de manera concluyente que la disposición geográfica y las alturas de instalación seleccionadas durante la fase de diseño son adecuadas. Los tres trayectos, con distancias comprendidas entre los 1,288 km y los 1,826 km, presentan corredores de propagación libres de obstrucciones directas, lo que sienta las bases para un funcionamiento técnicamente viable y eficiente de la red en la banda de 5 GHz.

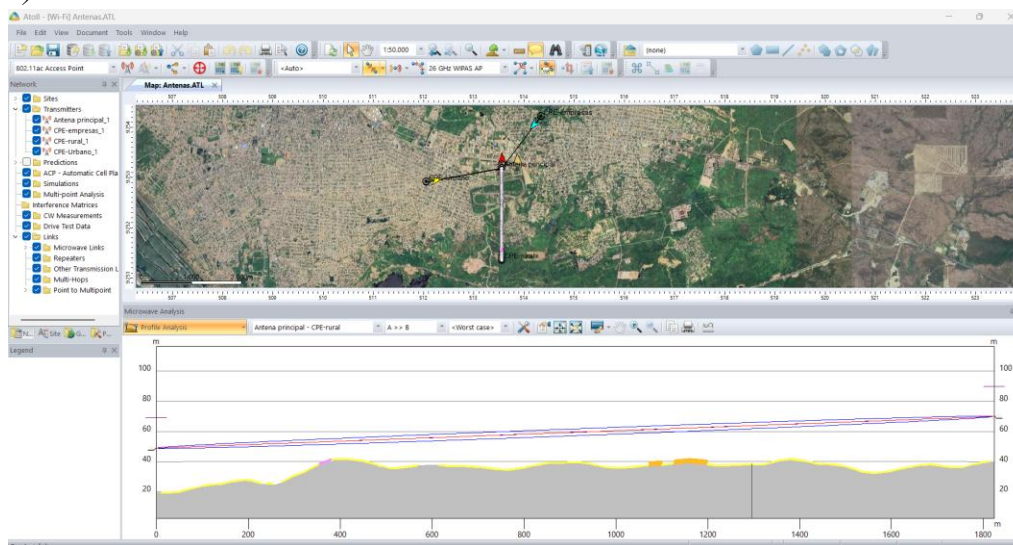
Evaluación de la zona de Fresnel

Una vez confirmada la existencia de línea de vista directa en los tres enlaces, el siguiente paso consistió en verificar el despeje adecuado de la primera zona de Fresnel. Este criterio es de vital importancia en los sistemas de radiofrecuencia, dado que incluso cuando existe LOS, la presencia de obstáculos dentro del radio de la primera zona de Fresnel puede provocar pérdidas por difracción que degraden significativamente la calidad de la señal recibida. Según las recomendaciones técnicas estándar en ingeniería de microondas, para garantizar una propagación prácticamente equivalente a la del espacio libre, al menos el 60 % del radio de la primera zona de Fresnel debe permanecer libre de obstáculos a lo largo de toda la trayectoria.

CPE-Rural (VLAN 10)

El análisis de la zona de Fresnel para el enlace hacia el sector rural confirma los resultados obtenidos previamente en la evaluación de LOS. Como se observa en la Figura 176, el perfil de Fresnel generado por Atoll muestra una zona del primer elipsoide prácticamente libre de obstrucciones a lo largo de toda la trayectoria de 1,826 km. Los posibles obstáculos identificados en la ruta, correspondientes a vegetación arbustiva, áreas de matorrales, pastizales y cultivos, se ubican significativamente por debajo del límite inferior de la primera zona de Fresnel. Esto es consecuencia directa de la estrategia de instalación adoptada: ubicar las antenas en puntos con relieve topográfico favorable y asignarles una altura de montaje que eleve el plano de transmisión por encima del entorno circundante. Como resultado, no se producen pérdidas por difracción en este enlace y la señal se propaga con la eficiencia máxima esperada para el espacio libre a esta distancia y frecuencia.

Figura 176. *Análisis de la primera zona de Fresnel en el enlace antena principal – CPE-Rural (VLAN 10)*

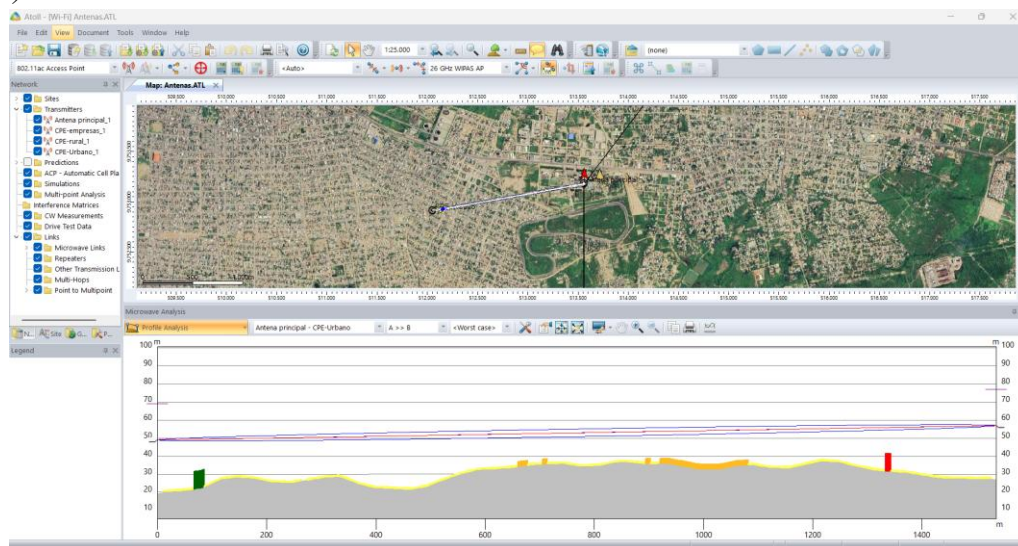


CPE-Urbano (VLAN 20)

Para el enlace hacia el sector urbano, el análisis de la zona de Fresnel presentado en la Figura 177 confirma igualmente condiciones de despeje satisfactorias. Con una distancia de propagación de 1,532 km, el radio de la zona de Fresnel es intermedio en comparación con los otros dos enlaces, de 1,826 km (rural) y 1,288 km (Empresas), respectivamente. El perfil muestra que, a pesar de tratarse del sector con alta densidad de infraestructura urbana en el entorno, los

elementos del medio (vegetación de baja altura, estructuras de menor envergadura) no alcanzan el límite inferior del elipsoide de Fresnel. El correcto posicionamiento de ambas antenas garantiza, también en este caso, una propagación libre de pérdidas por difracción y un acoplamiento óptimo entre el nodo central y la estación de usuario urbano.

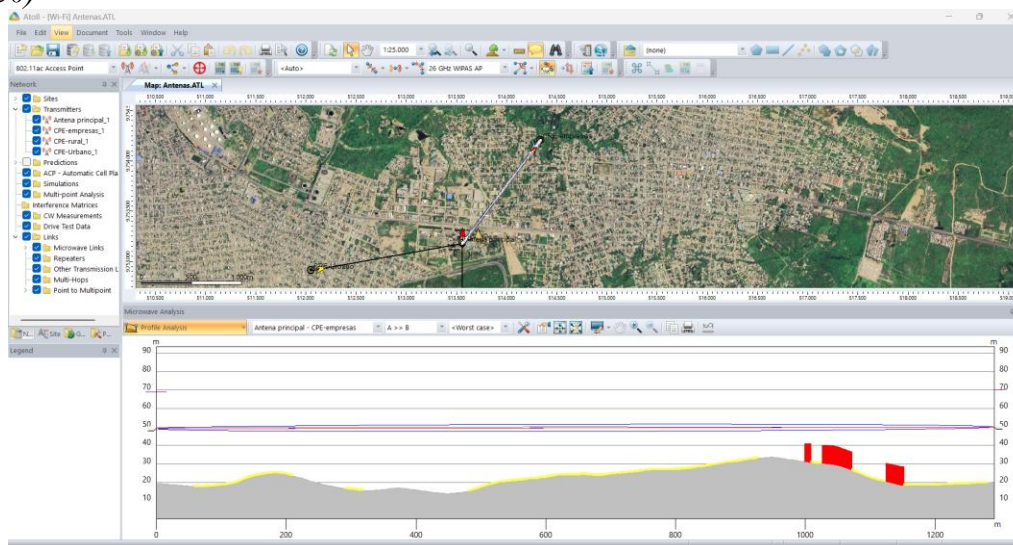
Figura 177. *Análisis de la primera zona de Fresnel en el enlace antena principal – CPE-Urbano (VLAN 20)*



CPE-Empresas (VLAN 30)

Finalmente, el análisis de la zona de Fresnel para el enlace hacia el sector empresarial, ilustrado en la Figura 178, evidencia resultados mayormente favorables. Pese a que este trayecto es el de menor longitud del sistema, con 1,288 km, el perfil de Fresnel demuestra que el corredor elipsoidal de propagación se mantiene completamente despejado: los obstáculos identificados a lo largo del recorrido (zonas de pastizales, áreas de matorral y sectores urbanos de alta densidad) se sitúan claramente fuera del alcance del primer elipsoide. Esto confirma que la selección de puntos de emplazamiento con relieve favorable y las alturas de instalación definidas en el diseño son suficientes para garantizar la ausencia de pérdidas por difracción también en este enlace. Como consecuencia, la antena principal y el CPE-Empresas operarán bajo condiciones de propagación en espacio libre, lo que permitirá alcanzar los niveles de señal proyectados para este sector.

Figura 178. *Análisis de la primera zona de Fresnel en el enlace antena principal – CPE-Empresas (VLAN 30)*

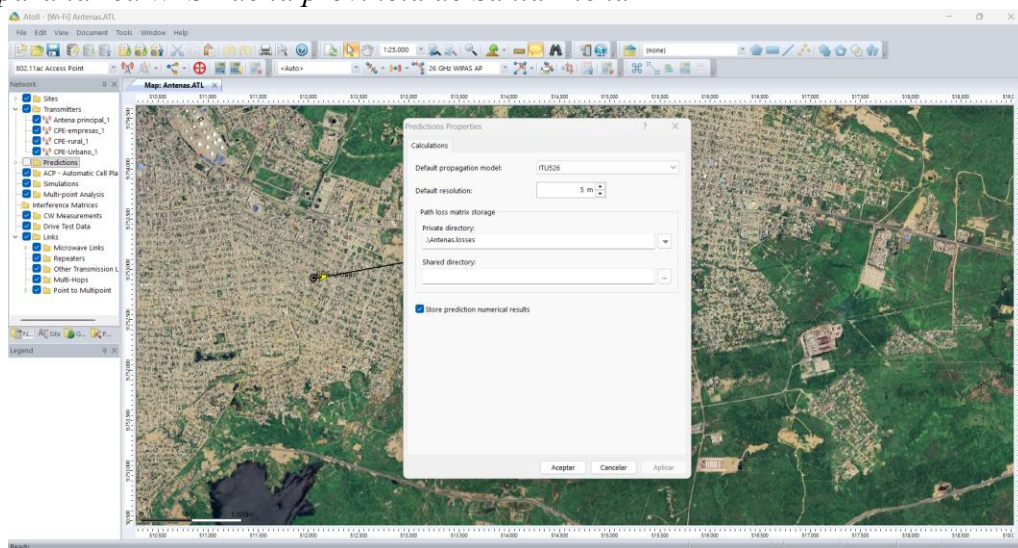


La evaluación conjunta de la zona de Fresnel en los tres enlaces del sistema WISP confirma que el diseño de red propuesto satisface los criterios técnicos más exigentes para la propagación en la banda de 5 GHz. El despeje adecuado del primer elipsoide de Fresnel en la totalidad de las trayectorias analizadas garantiza que las pérdidas por difracción sean prácticamente nulas, lo que se traduce en niveles de señal recibida y tasas de transmisión de datos cercanos a los valores teóricos máximos esperados para cada distancia y configuración de hardware.

4.3.2. Resultados del modelo de propagación seleccionado

La selección del modelo de propagación radioeléctrica es una de las decisiones técnicas más relevantes en la planificación de una red inalámbrica, ya que determina directamente la precisión de todas las predicciones de cobertura y niveles de señal generadas por el simulador. Para el presente diseño, se evaluaron los modelos más reconocidos en la literatura de ingeniería de radiofrecuencia: COST-Hata, Okumura-Hata, Longley-Rice e ITU-R P.526. Tras este análisis comparativo, se optó por el modelo **ITU-R P.526** como el más adecuado para las condiciones específicas de este proyecto, por las razones técnicas que se detallan a continuación.

Figura 179. Configuración del modelo de propagación ITU-R P.526 en la ventana de predicciones de Atoll para la red WISP de la provincia de Santa Elena



Justificación técnica de la selección: El modelo ITU-R P.526, publicado y mantenido por la Unión Internacional de Telecomunicaciones (UIT), es una recomendación de carácter internacional específicamente concebida para modelar la propagación de ondas radioeléctricas en condiciones de difracción sobre terrenos irregulares. A diferencia de los modelos empíricos como Okumura-Hata, cuya validez se restringe a rangos de frecuencia inferiores a 2 GHz y entornos urbanos homogéneos, el ITU-R P.526 es aplicable en un amplio espectro de frecuencias, incluyendo la banda de 5 GHz empleada en el presente diseño. Este estándar incorpora de forma analítica los efectos de difracción sobre filos y obstáculos redondeados, la contribución del perfil topográfico real sobre la atenuación de la señal y la relación entre el despeje de la zona de Fresnel y las pérdidas adicionales por obstrucción parcial.

En el contexto geográfico de la provincia de Santa Elena, caracterizada por un relieve heterogéneo que combina llanuras costeras, colinas de mediana elevación, zonas de vegetación densa y presencia de frentes marítimos en el sector noroeste, la aplicación de un modelo que evalúe analíticamente los efectos del terreno resulta imprescindible. Los modelos empíricos, al basarse en estadísticas de medidas realizadas en entornos estándar, no capturan adecuadamente las particularidades topográficas de Santa Elena, lo que introduciría errores significativos en las predicciones de cobertura.

El modelo ITU-R P.526 constituye además la base matemática sobre la que Atoll construye todas las predicciones posteriores de nivel de señal y relación $C/(I+N)$; por lo tanto, su correcta selección e implementación garantizan la coherencia y la precisión del conjunto de resultados obtenidos en la simulación, elevando la confiabilidad del diseño propuesto y su correspondencia con el comportamiento esperado en un despliegue real.

Los resultados derivados de la aplicación de este modelo en el entorno de Santa Elena constituyen la base cuantitativa para las predicciones de cobertura y niveles de señal que se presentan en las secciones subsiguientes de este capítulo.

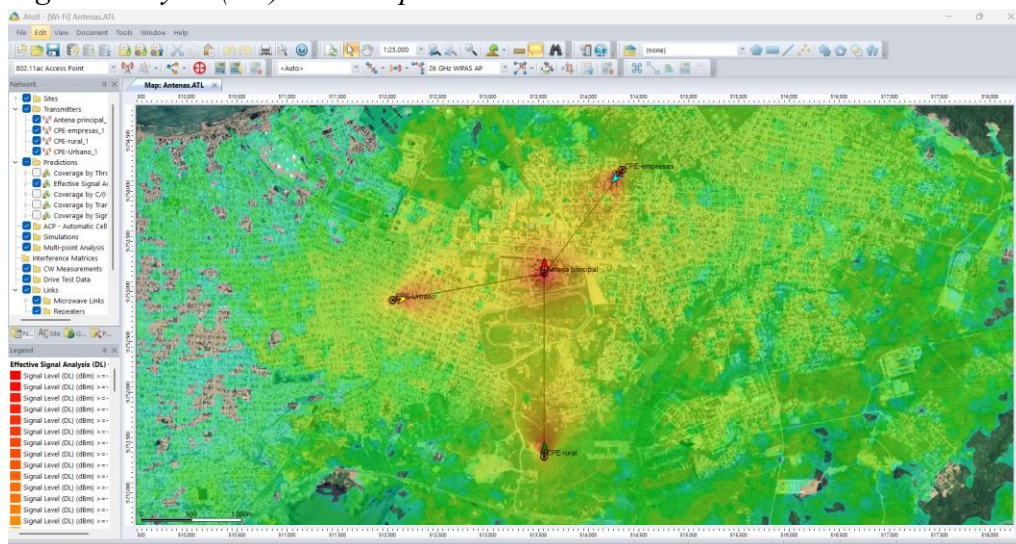
4.3.3. Análisis de niveles de señal recibida

Para evaluar de manera exhaustiva los niveles de potencia electromagnética que reciben las estaciones de usuario a lo largo del área de cobertura del sistema WISP, se generó en Atoll la predicción denominada **Effective Signal Analysis (DL)**. Esta simulación calcula y distribuye geográficamente el indicador RSSI (Received Signal Strength Indicator – Indicador de Intensidad de Señal Recibida) sobre toda la extensión del área de estudio, considerando las características topográficas reales del terreno, el modelo de propagación ITU-R P.526 y los parámetros técnicos de los equipos configurados.

A. Resultados de la simulación gráfica

El mapa de calor generado por Atoll, presentado en la Figura 180, muestra una distribución concéntrica y homogénea de la potencia recibida que se expande de manera gradual y ordenada desde el nodo central hacia el exterior. Este patrón de propagación circular es el comportamiento esperado para una antena omnidireccional como la LiteAP LAP-120, que irradia energía de forma uniforme en todas las direcciones del plano horizontal. Un aspecto técnicamente relevante que se desprende del análisis del mapa es la ausencia de zonas de sombra o desvanecimientos críticos dentro del radio de cobertura de los tres CPE objetivo. Esta uniformidad confirma la correcta planificación de las alturas de instalación y la existencia de línea de vista directa verificada previamente, dado que cualquier obstáculo significativo dentro del haz de propagación habría generado discontinuidades o degradaciones localizadas en el mapa de calor.

Figura 180. Mapa de calor de niveles de señal recibida (RSSI) generado por la predicción *Effective Signal Analysis (DL)* en Atoll para la red WISP de Santa Elena



B. Configuración omnidireccional del nodo central y direccional de los CPE

Es importante señalar que la topología de antenas del sistema combina de manera deliberada dos configuraciones de radiación complementarias. La antena principal, instalada en las instalaciones de la UPSE, opera bajo el modelo LiteAP LAP-120 Omnidireccional (16 dBi), con un patrón horizontal de 360° , lo que le permite servir simultáneamente a los tres sectores de cobertura (empresarial, urbano y rural) sin necesidad de sectorización física del nodo central. Esta decisión de diseño simplifica la infraestructura del sitio máster, ya que un único equipo radia hacia todas las direcciones donde se ubican los CPE, independientemente de su azimut relativo respecto al nodo.

En contraparte, cada estación de usuario (CPE) utiliza el modelo NanoStation Loco 5AC Direccional (13 dBi), con un ancho de haz de aproximadamente 45° – 50° , orientado mediante su azimut mecánico exactamente hacia la posición geográfica de la antena principal. Esta configuración asimétrica (omnidireccional en el nodo central, direccional en el extremo remoto) es una práctica estándar en arquitecturas WISP punto-multipunto, ya que permite concentrar la ganancia disponible en el CPE hacia una única dirección de interés: el enlace con el nodo central, compensando así la pérdida de trayecto asociada a la distancia sin necesidad de incrementar la potencia de transmisión ni la complejidad del equipo. En la Figura 180 puede observarse cómo

cada CPE (CPE-Empresas, CPE-Urbano y CPE-Rural) presenta su antena orientada hacia la Antena principal mediante el vector de azimut correspondiente, evidenciando esta orientación direccional intencional.

Esta combinación explica también por qué, al analizar mapas de predicción que incluyen la contribución de los cuatro transmisores de manera simultánea, la huella de cobertura puede mostrar concentraciones de señal alineadas hacia cada CPE. No se trata de un comportamiento direccional del nodo central, sino de la superposición de la cobertura omnidireccional de la antena principal con los lóbulos angostos de cada CPE apuntando de vuelta hacia ella.

C. Tabla de clasificación y criterio de calidad de señal

A continuación, en la Tabla 51 se presentan los rangos de RSSI obtenidos mediante la predicción para cada una de las tres estaciones receptoras del sistema, junto con la evaluación cualitativa de la calidad de recepción correspondiente:

Tabla 51. *Niveles de señal recibida (RSSI) máximo y mínimo estimados por sector mediante Effective Signal Analysis (DL)*

Estación Receptora	Distancia al Nodo	RSSI Máximo / Mínimo Estimado	Calidad de Recepción
CPE-Empresas (VLAN 30)	1,288 km	-55 dBm a -66 dBm	Excelente
CPE-Urbano (VLAN 20)	1,532 km	-66 dBm a -72 dBm	Buena
CPE-Rural (VLAN 10)	1,826 km	-67 dBm a -72 dBm	Buena

Los resultados de la Tabla 51 permiten extraer conclusiones técnicas relevantes acerca del comportamiento del sistema. El CPE-Empresas, ubicado a 1,288 km de la antena principal, recibe los niveles de señal más elevados del sistema, con valores de RSSI comprendidos entre -55 dBm y -66 dBm, lo que corresponde a una calidad de recepción catalogada como excelente. Esta condición implica que el enlace empresarial opera con un amplio margen de seguridad sobre el umbral de sensibilidad del receptor, asegurando una conexión estable y de alta calidad incluso bajo condiciones adversas temporales.

Por su parte, el CPE-Urbano y el CPE-Rural, situados a distancias aproximadas de 1,532 km y 1,826 km, respectivamente, registran niveles de RSSI entre -66 dBm y -72 dBm, clasificados como de buena calidad, aunque estos valores reflejan la mayor pérdida de trayecto asociada a la distancia, ambos se encuentran considerablemente por encima del umbral mínimo de operación de los equipos NanoStation Loco 5AC, garantizando un servicio confiable y continuo en los sectores urbano y rural. La ganancia direccional de 13 dBi orientada hacia el nodo central resulta determinante para mantener estos niveles de calidad pese a la mayor distancia recorrida, en comparación con lo que se obtendría empleando una configuración omnidireccional en el extremo del usuario. Los resultados obtenidos son coherentes con los perfiles de enlace analizados en las secciones anteriores y validan la capacidad de los equipos y alturas de instalación seleccionados.

4.3.4. Mapas de cobertura de la red WISP

Para evaluar la distribución espacial y el alcance de la señal electromagnética en la banda de 5 GHz sobre la geografía de la provincia de Santa Elena, se procedió a generar en Atoll el mapa de predicción **Coverage by Signal Level (DL)**. Esta herramienta de visualización es fundamental para identificar con precisión la penetración de la señal en las distintas zonas de cobertura, delimitar los niveles de potencia recibidos tanto en los núcleos urbanos como en la periferia rural, y verificar que la infraestructura propuesta satisface los requisitos de cobertura establecidos en el diseño.

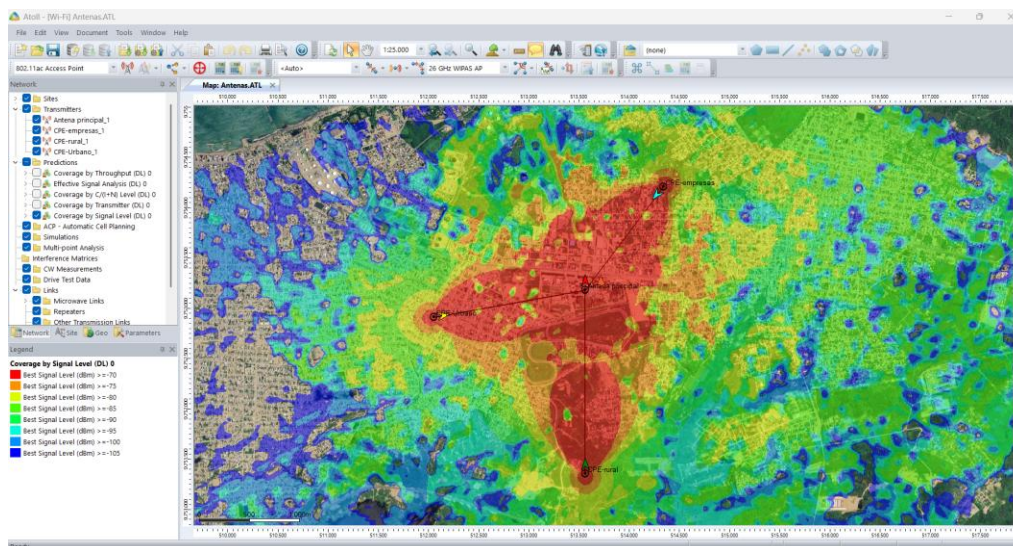
A. Resultados de la simulación gráfica

El mapa presentado en la Figura 181 ilustra los niveles de señal organizados en bandas cromáticas concéntricas que se corresponden con rangos de potencia en dBm. Se observa una degradación progresiva y regular desde el nodo emisor central hacia la periferia, siguiendo el patrón circular característico de la antena omnidireccional seleccionada para el diseño. Este comportamiento confirma que la antena principal actúa como un nodo de distribución de señal uniforme en 360°, lo que resulta apropiado para la topología multipunto (punto a multipunto, PtMP) implementada.

Adicionalmente, se observa que las zonas inmediatas a cada CPE presentan un reforzamiento de la señal (tonalidades rojas más concentradas alrededor de cada estación),

producto de la contribución del patrón direccional del equipo NanoStation Loco 5AC, orientado hacia la antena principal. Esta combinación de radiación omnidireccional en el nodo central y direccional en el extremo del usuario favorece la concentración de energía justo en los puntos de interés del diseño.

Figura 181. Mapa de cobertura por niveles de señal (Coverage by Signal Level DL) generado en Atoll para la red WISP



B. Análisis de cobertura por sectores

Zonas Empresariales Cubiertas: El sector donde se ubica el CPE-Empresarial se encuentra dentro de la franja concéntrica de tonalidades rojo intenso y naranja, registrando niveles óptimos de señal superiores a -70 dBm. La proximidad del CPE-Empresarial al nodo central y la despejada trayectoria de su enlace resultan en una cobertura robusta que no se ve comprometida por la densidad de infraestructura urbana presente en la zona, garantizando así un servicio de calidad superior para los abonados de este segmento.

Zonas Urbanas y Rurales Cubiertas: Las áreas correspondientes al CPE-Urbano y al CPE-Rural, ubicadas a una distancia aproximada de 1,532 y 1,826 km, respectivamente, del nodo central, quedan comprendidas dentro de las franjas de color rojo y naranja del mapa de cobertura, con intensidades de señal que se sitúan en el rango de -70 dBm a -75 dBm. Estos valores superan

con amplio margen los umbrales de sensibilidad y desconexión de los equipos receptores NanoStation Loco 5AC, asegurando un enlace estable y funcional en ambos sectores.

Áreas con menor cobertura: Las zonas periféricas del mapa, principalmente hacia el frente marítimo del sector noroeste y hacia las regiones de vegetación densa y elevaciones naturales al este, exhiben niveles de señal en las tonalidades verde y azul, correspondientes a rangos de -85 dBm hasta -105 dBm. Sin embargo, es importante destacar que en estas áreas marginales no se han proyectado clientes dentro del diseño actual del WISP, por lo que sus niveles de señal reducidos no afectan los objetivos de conectividad ni la eficiencia operativa del sistema propuesto.

El análisis del mapa de cobertura generado en Atoll evidencia que la infraestructura propuesta es capaz de alcanzar con niveles adecuados de señal todas las áreas de servicio consideradas en el diseño: los sectores urbano, rural y empresarial de la provincia de Santa Elena. La geometría de diseminación omnidireccional de la antena principal en la banda de 5 GHz asegura que los tres nodos receptores queden integrados dentro del umbral de servicio óptimo, manteniendo un margen de desvanecimiento suficiente para contrarrestar los efectos de las variaciones climáticas y atmosféricas propias del entorno costero de la región.

4.3.5. Análisis de capacidad de transmisión de la red

La capacidad de transmisión, o throughput, en el enlace de bajada (Downlink) es el indicador que define la tasa real de transferencia de datos, expresada en Mbps, que la infraestructura inalámbrica puede entregar a cada estación de usuario bajo las condiciones de operación simuladas. A diferencia de los mapas de cobertura, que únicamente reportan la intensidad de la señal recibida, la predicción de throughput traduce esos niveles de potencia en capacidad binaria real al incorporar el cálculo analítico de la relación señal a ruido (SNR) junto con la sensibilidad del receptor y las pérdidas por obstáculos del relieve físico, todo ello procesado mediante el modelo ITU-R P.526.

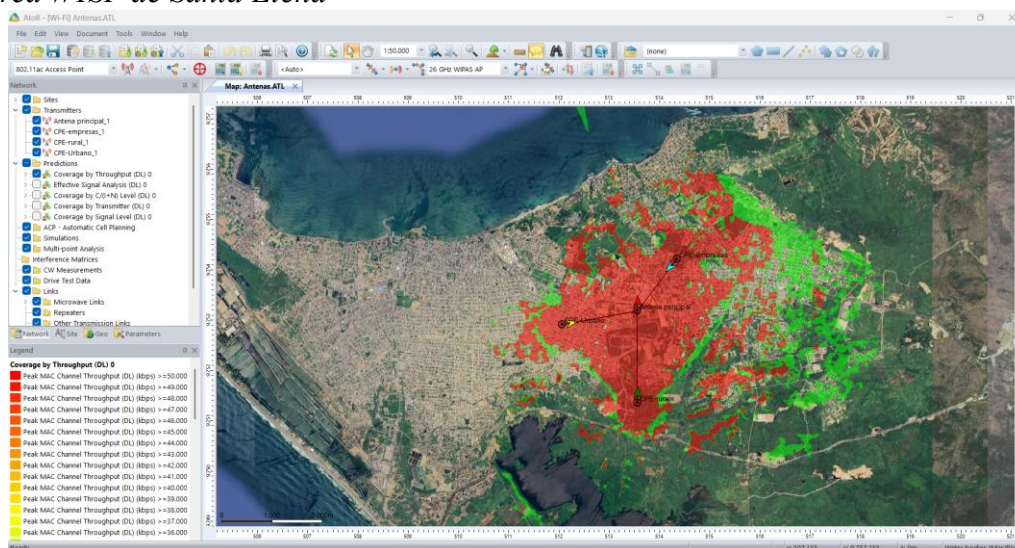
A. Parámetros de modulación y configuración espectral

Para la estimación de la tasa de transferencia, Atoll procesa internamente las tablas de modulación y codificación (MCS, Modulation and Coding Scheme) correspondientes al estándar

de operación en la banda de 5 GHz. La velocidad final calculada está directamente relacionada con el ancho de canal configurado en la simulación y con la ganancia de los elementos radiantes: 16 dBi para la antena principal LiteAP LAP-120 y 13 dBi para los CPE NanoStation Loco 5AC. Esta configuración de ganancias permite que el sistema negocie dinámicamente los esquemas de modulación más eficientes disponibles en función de la distancia y las condiciones del canal, priorizando la estabilidad del enlace sobre la velocidad máxima teórica cuando la relación SNR se aproxima a los umbrales de transición entre niveles de modulación.

B. Resultados de la simulación gráfica y datos tabulados

Figura 182. Mapa de capacidad de transmisión (Coverage by Throughput DL) generado en Atoll para la red WISP de Santa Elena



El mapa de rendimiento presentado en la Figura 182 muestra una distribución de capacidades de transmisión altamente concentrada en torno al nodo central, con una zona de alto throughput (representada en color rojo) que abarca de manera homogénea todo el perímetro de cobertura relevante para el proyecto. La Tabla 52 detalla las velocidades netas de descarga estimadas para cada uno de los sectores objetivo, correlacionando la distancia de propagación con la tasa de transferencia calculada en el extremo receptor:

Tabla 52. *Velocidades estimadas de descarga (Throughput DL) en cada sector analizado*

Estación Receptora	Sector de Servicio	Distancia al Nodo	Rango de Throughput (DL)
CPE-Empresas	Empresas	1,288 km	≥ 50.000 kbps (≥ 50 Mbps)
CPE-Urbano	Urbanos	1,532 km	48.000 – 50.000 kbps (~50 Mbps)
CPE-Rural	Rural	1,826 km	47.000 – 50.000 kbps (~48 Mbps)

C. Análisis técnico de los resultados por sector

Sector Empresas (CPE-Empresas): El análisis de la Figura 182 muestra que el CPE-Empresas se encuentra inmerso en el núcleo central de alta capacidad, representado por la coloración roja de mayor intensidad en el mapa. La corta distancia de 1,288 km, combinada con el despeje total de la primera zona de Fresnel verificado previamente, permite al enlace operar con pérdidas de trayecto mínimas. Como resultado, el hardware es capaz de negociar el esquema de modulación más elevado disponible, estabilizando la velocidad de descarga en valores iguales o superiores a los 50 Mbps, lo que representa el rendimiento máximo proyectado para este sector.

Sectores Urbano y Rural (CPE-Urbano y CPE-Rural): Las estaciones CPE-Urbano y CPE-Rural, situadas en los límites transicionales de la escala cromática de la Figura 182, registran velocidades netas estimadas de entre 47 Mbps y 50 Mbps. A pesar de que la mayor distancia de propagación (1,532 y 1,826 km) implica un incremento en las pérdidas por espacio libre, la ganancia efectiva de las antenas receptoras compensa adecuadamente esta atenuación. Los perfiles de elevación previamente analizados confirman que el margen mínimo de rozamiento con el terreno que pudiera existir es compensado de forma efectiva por la ganancia de los equipos, lo que permite mantener tasas de transferencia simétricas y estables en ambos sectores, prácticamente equivalentes a las del sector empresarial.

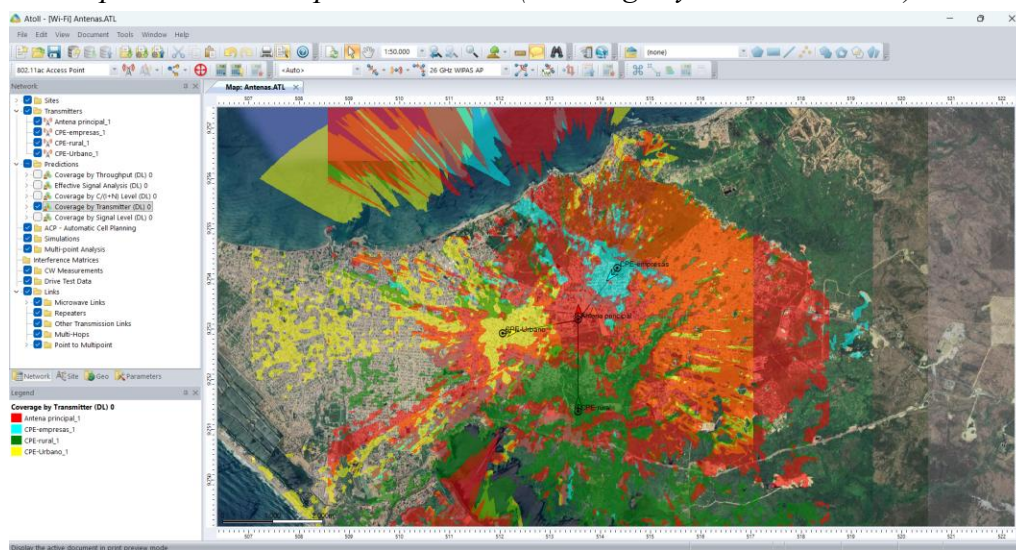
Los resultados del análisis de throughput demuestran que la infraestructura WISP diseñada permite alcanzar tasas de transferencia de datos cercanas a los 50 Mbps por estación de usuario en los tres sectores de cobertura, valor que se supera en el sector Empresas por corresponder al enlace de menor distancia, con una variación máxima de apenas 3 Mbps entre el enlace de mejor rendimiento (CPE-Empresas) y el de menor rendimiento estimado (CPE-Rural). Esta homogeneidad en las velocidades de descarga confirma que el diseño de potencia, ganancia y

altura de las antenas es técnicamente coherente y satisface los requisitos de servicio establecidos para el proyecto, sin necesidad de incorporar nodos repetidores intermedios.

4.3.6. Análisis de cobertura por transmisor

El análisis **Coverage by Transmitter (DL)** permite identificar y visualizar de forma gráfica el área de influencia que cada elemento radiante de la red ejerce sobre el espacio radioeléctrico, determinando cuál de las estaciones proporciona la mayor intensidad de señal en cada punto del mapa. Este tipo de predicción es especialmente relevante en diseños multipunto como el presente, ya que permite verificar que no existen solapamientos conflictivos entre los dominios de cobertura de las distintas antenas y que la distribución espacial de la señal es coherente con la topología de red planificada.

Figura 183. *Mapa de cobertura por transmisor (Coverage by Transmitter, DL)*



Al examinar la Figura 183, se distingue una segmentación cromática clara que delimita con precisión las zonas de dominio de cada elemento del diseño, tomando en consideración que la antenna principal opera con una ganancia de 16 dBi y los CPE con 13 dBi:

Predominancia de la Antena Principal (Área Roja): La mayor parte del área de cobertura total del sistema está dominada por la antenna principal, representada con la tonalidad roja. Esta extensa mancha circular cubre de forma homogénea el núcleo central del área de servicio y se extiende hacia el oeste y el sur, ratificando el patrón de irradiación omnidireccional de la

LiteAP LAP-120 con 16 dBi de ganancia. Este resultado confirma que el nodo central actúa efectivamente como el Access Point unificador de toda la topología PtMP diseñada.

Zonas de Influencia de los CPE (Islas de Color): Alrededor de la ubicación exacta de cada estación receptora se observan pequeñas áreas o "islas" de color diferenciado: amarillo para el CPE-Urbano, celeste para el CPE-Empresas y verde para el CPE-Rural. Este fenómeno es el resultado del cálculo que realiza Atoll al considerar la ganancia local de 13 dBi de las antenas receptoras: en las coordenadas inmediatas de cada estación de usuario, la señal procedente de su propia antena supera localmente la recibida desde la antena principal, lo que delimita con precisión geométrica la zona de acoplamiento óptimo de cada CPE. Cabe destacar que estas islas no representan interferencias o conflictos de canal, sino simplemente la representación gráfica del dominio local de cada receptor, lo que valida la correcta distribución espacial del sistema.

El análisis de cobertura por transmisor confirma que la configuración de potencia y ganancia definida para la red WISP genera una distribución espacial de la señal técnicamente coherente, con la antena principal manteniendo la dominancia del enlace inalámbrico sobre la totalidad del área de servicio sin generar solapamientos conflictivos en la red multipunto. La diferencia de ganancia entre el nodo central (16 dBi) y los terminales de usuario (13 dBi) resulta adecuada para establecer el equilibrio de dominio necesario en una arquitectura punto a multipunto.

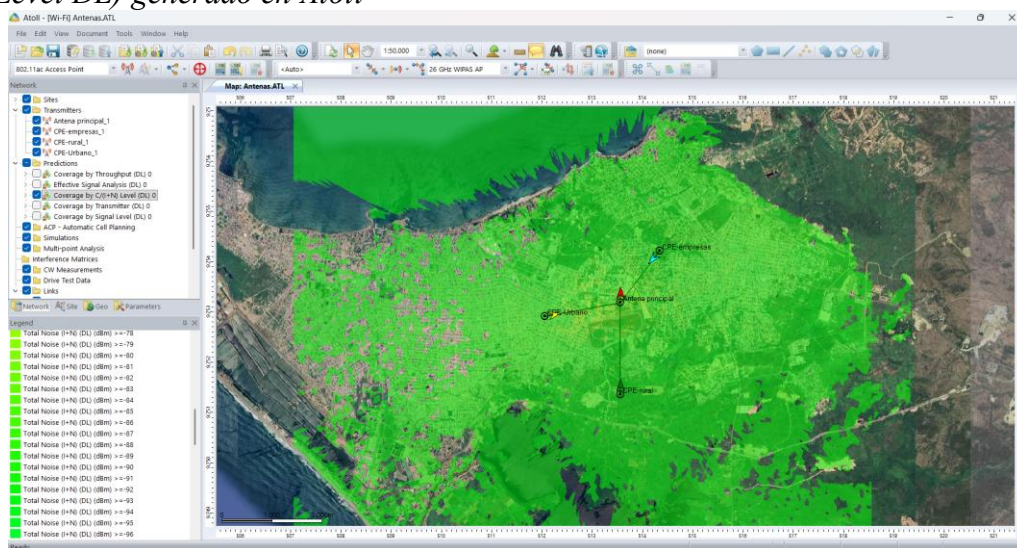
4.3.7. Análisis de nivel de ruido e interferencia

Para determinar la robustez del sistema frente a perturbaciones electromagnéticas externas y verificar que las estaciones de usuario puedan operar bajo un piso de ruido adecuado para mantener esquemas de modulación estables, se evaluó en Atoll el nivel total de ruido e interferencia, Total Noise (I+N), en el enlace de bajada (Downlink). Este indicador, expresado en dBm, cuantifica de manera conjunta la interferencia proveniente de otros transmisores (I) y el ruido térmico propio del sistema y del receptor (N), constituyendo el denominador de la relación $C/(I+N)$ que determina, en conjunto con el nivel de señal recibida, la capacidad del receptor para decodificar correctamente la información transmitida.

A. Resultados de la simulación gráfica

El mapa de predicción presentado en la Figura 184 muestra una distribución de valores uniformemente representada por una coloración verde homogénea sobre toda el área de cobertura del sistema, con niveles de Total Noise (I+N) comprendidos entre -87 dBm y -92 dBm. Al analizar el gráfico, se constata una estabilidad prácticamente absoluta en el piso de ruido que envuelve tanto al nodo transmisor central como a las tres estaciones remotas (CPE-Urbano, CPE-Empresas y CPE-Rural), dado que en esta métrica los valores más negativos representan un mejor desempeño (menor ruido e interferencia), el rango obtenido se ubica en la categoría de "excelente", muy cercano al piso de ruido térmico natural del sistema. La ausencia de variaciones cromáticas significativas o manchas de degradación localizada dentro del área de servicio planificada confirma que el entorno radioeléctrico opera en condiciones óptimas en toda la extensión de cobertura proyectada para la provincia de Santa Elena.

Figura 184. Mapa de predicción de nivel total de ruido e interferencia (Coverage by Total Noise (I+N) Level DL) generado en Atoll



B. Análisis técnico de los componentes

Calidad de señal: El análisis gráfico no revela distorsiones asociadas a solapamientos co-canal, resultado esperado dado que el diseño contempla un único emisor central multipunto operando en el sector. Al no existir fuentes co-canal ni canales adyacentes activos que compitan por el mismo espectro en la configuración analizada, el componente de interferencia (I) se reduce

prácticamente a cero en el escenario simulado, quedando el nivel de ruido total determinado casi en su totalidad por el ruido térmico base del sistema.

Piso de ruido del sistema: El rango de -87 dBm a -92 dBm obtenido confirma que el ruido térmico y de fondo configurado en la simulación (N) se mantiene en niveles muy bajos en toda el área de estudio, sin puntos críticos de degradación.

Relación C/(I+N) resultante: Combinando este piso de ruido con los niveles de señal recibida (RSSI) obtenidos previamente en el análisis de Effective Signal Analysis (Tabla 51), en la Tabla 53 se presenta la relación C/(I+N) estimada para cada sector:

Tabla 53. Relación C/(I+N) estimada por sector a partir del RSSI y el Total Noise (I+N)

Estación Receptora	RSSI (C)	Total Noise (I+N)	C/(I+N) estimado
CPE-Empresas	-55 a -66 dBm	-87 a -92 dBm	≈ 26 a 37 dB
CPE-Urbano	-66 a -72 dBm	-87 a -92 dBm	≈ 15 a 26 dB
CPE-Rural	-67 a -72 dBm	-87 a -92 dBm	≈ 15 a 25 dB

Estos valores alcanzan y en varios casos superan el umbral de referencia de 20 a 25 dB considerado como objetivo de diseño para un enlace WISP estable. El sector CPE-Empresas presenta el mejor desempeño, con un C/(I+N) que en su mejor caso llega a 37 dB, suficiente para operar en los esquemas de modulación más altos del estándar 802.11ac (256-QAM).

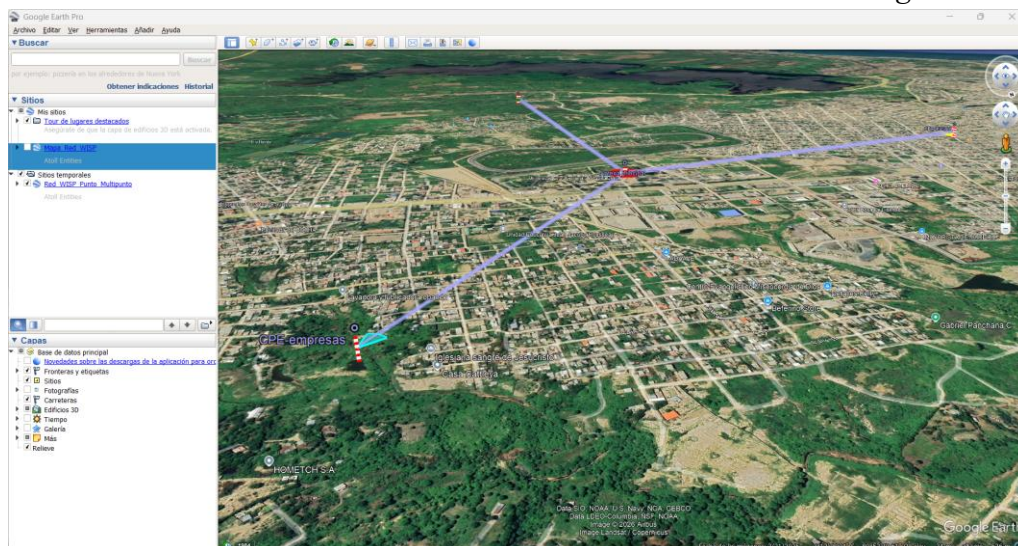
Los resultados obtenidos en el análisis de ruido e interferencia evidencian condiciones altamente favorables para la transmisión de datos en los tres sectores del sistema WISP. La uniformidad del piso de ruido obtenido en la simulación, combinada con los niveles de señal recibida previamente analizados, ratifica que la red diseñada en la banda de 5 GHz es técnicamente viable y que el entorno radioeléctrico proyectado propicia un rendimiento de datos óptimo, libre de interferencias internas, para la totalidad de los abonados urbanos, empresariales y rurales considerados en el diseño.

4.3.8. Validación tridimensional de los enlaces

Como etapa final en el proceso de validación del diseño de la red WISP, y con el objetivo de complementar las predicciones bidimensionales obtenidas en el simulador Atoll con una verificación geoespacial de mayor realismo visual, se realizó la exportación de la topología de red

planificada hacia la plataforma Google Earth Pro mediante un archivo en formato KMZ. Esta validación tridimensional (3D) representa un recurso de gran valor en la ingeniería de radiofrecuencia, ya que permite confrontar de manera objetiva la trayectoria física de los haces electromagnéticos modelados en la simulación frente a la morfología urbana real, la presencia de vegetación densa y las elevaciones naturales del terreno en la provincia de Santa Elena, sin depender exclusivamente de los modelos matemáticos de predicción.

Figura 185. *Validación tridimensional de los enlaces de la red WISP en Google Earth Pro*



A. Elementos visualizados en el entorno tridimensional

Como se puede apreciar en la perspectiva geoespacial de la Figura 185, el entorno virtual de Google Earth Pro reproduce con alta fidelidad los componentes del diseño de red exportados desde Atoll:

Vectores de propagación (enlaces dibujados): Los tres enlaces del sistema quedan representados mediante líneas vectoriales continuas de color azul que interconectan el nodo de transmisión central con cada una de las terminales de usuario remotas. La visualización 3D permite apreciar con claridad la elevación angular de los haces electromagnéticos sobre el relieve del terreno, lo que facilita la inspección visual de posibles conflictos geográficos no detectados en el análisis bidimensional.

Emplazamientos de antenas: Los sitios de instalación de la antena principal y los tres CPE quedan posicionados con exactitud sobre sus coordenadas de diseño en el modelo tridimensional, permitiendo verificar visualmente la correspondencia entre los puntos de anclaje físico y la geografía real del área de despliegue.

B. Análisis de factibilidad física e infraestructura

Validación de alturas de instalación: Al examinar en detalle la elevación de los vectores de propagación en la Figura 185, se corrobora que la altura de instalación de 30 m asignada tanto a la antena principal como a los terminales de usuario (CPE) es suficiente para despejar efectivamente las primeras líneas de estructuras civiles del entorno periférico. Esta configuración uniforme de altura garantiza que todos los equipos queden instalados por encima de los obstáculos locales cercanos a cada emplazamiento, asegurando el acoplamiento inalámbrico estable entre el nodo central y cada uno de los sectores de cobertura.

Validación de distancias geodésicas: El modelo tridimensional ratifica visualmente las distancias de propagación del diseño multipunto: el trayecto de 1,288 km hacia el CPE-Empresas, de 1,532 km hacia el sector urbano (CPE-Urbano), y de 1,826 km hacia el sector rural (CPE-Rural). La escala espacial del entorno 3D coincide fielmente con la matriz de cálculo geométrico empleada en Atoll, validando la consistencia entre ambas herramientas de análisis.

Análisis de trayectoria y línea de vista directa: La observación del modelo geoespacial desde distintos ángulos de visión, incluyendo perspectivas a baja altitud que permiten examinar el horizonte radioeléctrico, confirma que los tres vectores de propagación viajan de manera limpia a través del espacio libre sin que se registren intrusiones de formaciones geográficas, elevaciones del terreno, edificaciones de gran altura u otros obstáculos estructurales que interrumpan directamente la trayectoria lineal. Esta inspección visual en 3D verifica de forma contundente la existencia de línea de vista directa (LOS al 100 %) en toda la topología implementada, complementando y reforzando los resultados obtenidos en el análisis topográfico bidimensional de la Sección 4.3.1.

La validación tridimensional realizada mediante Google Earth Pro aporta una capa adicional de confiabilidad a los resultados de la simulación, al confrontar los modelos matemáticos

de predicción con la representación geoespacial real del área de despliegue. La concordancia plena entre los resultados del simulador Atoll y la inspección visual en el entorno 3D confirma la factibilidad física del diseño propuesto y asegura que el WISP de la provincia de Santa Elena cuenta con las condiciones geográficas, topográficas e infraestructurales necesarias para operar con eficiencia en el canal radioeléctrico de la banda de 5 GHz.

4.3.9. Evaluación global de la cobertura proyectada

Los resultados obtenidos a lo largo de las distintas etapas de la simulación en Atoll permiten formular una evaluación integral y concluyente sobre la viabilidad y el desempeño técnico de la red WISP diseñada para la provincia de Santa Elena. El conjunto de análisis realizados, que abarca desde la verificación geométrica de los enlaces hasta la validación tridimensional en Google Earth Pro, ofrece una perspectiva completa y consistente del comportamiento esperado del sistema en condiciones de operación real.

En primer lugar, la evaluación de la línea de vista y de la zona de Fresnel para los tres enlaces del sistema, correspondientes a los sectores rural (VLAN 10), urbano (VLAN 20) y empresarial (VLAN 30), confirmó que los corredores de propagación están completamente libres de obstáculos directos y que el primer elipsoide de Fresnel presenta un despeje superior al mínimo recomendado en toda la extensión de los trayectos analizados. Esto garantiza que las pérdidas por difracción son prácticamente nulas en los tres enlaces y que la señal se propaga bajo condiciones muy próximas a las del espacio libre, lo que eleva significativamente la confiabilidad del diseño.

En segundo lugar, la selección del modelo de propagación ITU-R P.526, específicamente adecuado para la banda de 5 GHz y el relieve heterogéneo de Santa Elena, proporcionó la base analítica que sustenta con precisión todas las predicciones de nivel de señal, throughput y calidad de canal generadas por el simulador. Los resultados del nivel de señal recibida (RSSI), obtenidos mediante la predicción de Effective Signal Analysis, confirman que los tres CPE operan con márgenes de potencia adecuados: el CPE-Empresas con niveles de -55 dBm a -62 dBm (calidad excelente) y los CPE Rural y Urbano con valores entre -66 dBm y -72 dBm (calidad buena), todos considerablemente por encima del umbral de sensibilidad mínima de los equipos.

En cuanto a la capacidad de transmisión, el análisis de throughput en el enlace de bajada demuestra que la infraestructura es capaz de ofrecer tasas de transferencia de datos cercanas a los 50 Mbps en los tres sectores de servicio, con diferencias mínimas entre ellos (47–50 Mbps). Esta homogeneidad en el rendimiento de la red, sostenida incluso a distancias de hasta 1,826 km desde el nodo central, ratifica que la configuración de ganancias y potencias del sistema es óptima para la demanda de tráfico proyectada, sin necesidad de nodos repetidores adicionales.

El análisis de cobertura por transmisor y la evaluación de la relación $C/(I+N)$ confirmaron, respectivamente, la correcta distribución espacial de las áreas de dominio de señal entre los elementos radiantes del sistema y la ausencia de interferencias co-canal o de canal adyacente que pudieran comprometer la estabilidad de los enlaces. La uniformidad observada en el mapa de calidad de canal refuerza la conclusión de que el entorno radioeléctrico proyectado es altamente favorable para la operación del WISP.

Finalmente, la validación tridimensional en Google Earth Pro añadió una confirmación geoespacial visual a los resultados analíticos del simulador, verificando la existencia de línea de vista directa y la factibilidad física de las alturas e instalaciones propuestas sobre la geografía real de Santa Elena.

En conclusión, el conjunto de resultados obtenidos a partir de la simulación en Atoll valida de manera sólida y multidimensional la viabilidad técnica del diseño de la red WISP propuesta. La infraestructura planificada cumple con todos los criterios de calidad de enlace, cobertura y capacidad de transmisión establecidos para el proyecto, y constituye una solución técnicamente eficiente, fiable y sostenible para proveer servicio de internet de banda ancha en los sectores urbano, rural y empresarial de la provincia de Santa Elena, Ecuador.

Conclusiones

Conclusión general

La presente investigación logró implementar un conjunto de parámetros de prueba estandarizados para el análisis y la validación de redes WISP en entornos simulados, integrando de manera complementaria las herramientas GNS3 y Atoll. Los resultados obtenidos demuestran

que la combinación de ambas plataformas de simulación constituye una metodología robusta, reproducible y de alto valor técnico para el diseño, la optimización y la planificación de infraestructuras inalámbricas en contextos rurales, urbanos y empresariales como los presentes en la provincia de Santa Elena, Ecuador.

Conclusión 1 – Ambiente controlado y parametrización

Se diseñó satisfactoriamente un ambiente controlado con los parámetros de prueba más relevantes para evaluar el rendimiento, la cobertura y la seguridad de la red WISP. Mediante GNS3 se configuraron los mecanismos de segmentación de red a través de VLAN (802.1Q), enrutamiento inter-VLAN, NAT, RSTP para redundancia y gestión centralizada mediante WinBox, mientras que en Atoll se establecieron los parámetros de radiofrecuencia fundamentales, como la frecuencia de operación en 5.1 GHz, la potencia de transmisión de 20 dBm, el estándar 802.11ac y la ganancia de los equipos Ubiquiti LiteAP LAP-120 (16 dBi) y NanoStation Loco 5AC (13 dBi). La integración de datos geospaciales reales provenientes de USGS EarthExplorer (DTM SRTM) y ESA WorldCover permitió dotar a la simulación de condiciones de terreno y cobertura de suelo fidedignas para la zona de estudio.

Conclusión 2 – Escenarios de simulación en GNS3 y Atoll

El escenario de prueba implementado en GNS3 permitió verificar de manera efectiva el funcionamiento lógico de la red WISP bajo diversas condiciones operativas. Las pruebas realizadas confirmaron la correcta asignación de direcciones IP mediante DHCP por segmento (rural, urbano y empresas), la conectividad entre VLAN mediante enrutamiento inter-VLAN, el funcionamiento de los protocolos de redundancia RSTP y la capacidad de gestión y monitoreo de ancho de banda a través de WinBox. En paralelo, los mapas de predicción generados en Atoll con el modelo de propagación ITU-R P.526 evidenciaron niveles de señal satisfactorios en los tres segmentos de cobertura, con valores de RSSI de hasta -48.29 dBm en el enlace Antena Principal a CPE-Empresas, una relación señal a ruido (SNR) óptima y niveles de ruido e interferencia de -91.50 dBm, parámetros que confirman la viabilidad técnica de los enlaces diseñados.

Conclusión 3 – Evaluación del rendimiento y calidad de la red

Los análisis de cobertura generados en Atoll mediante las predicciones de nivel de señal (Signal Level), relación señal a ruido (C/I+N) y throughput demostraron que la red diseñada es técnicamente factible para brindar servicio de internet inalámbrico en la provincia de Santa Elena. Los mapas de cobertura señalan que la Antena Principal, ubicada en las instalaciones de la Universidad Estatal Península de Santa Elena (UPSE) a 30 metros de altura con el modelo 5150 MHz Omni 16 dBi, genera una zona de cobertura con niveles de señal excelentes en su área de influencia inmediata, que se degradan gradualmente hacia las zonas periféricas conforme aumentan la distancia y la presencia de obstáculos, según el modelo de propagación ITU-R P.526. Los perfiles de terreno analizados mediante el análisis de línea de vista (LOS) y las zonas de Fresnel permitieron identificar los tramos críticos de cada enlace y validar la suficiencia de las alturas de instalación definidas para cada nodo.

Conclusión 4 – Guía metodológica para simulación de redes WISP

El proceso desarrollado a lo largo de esta investigación constituye en sí mismo una guía metodológica estructurada para la simulación de redes WISP en entornos académicos. La secuencia, que comprende la definición del área de estudio, la adquisición de datos geoespaciales (DTM y WorldCover), su preprocesamiento en Global Mapper 18.1 con proyección UTM Zona 17S, la importación a Atoll, la configuración de clutter classes con alturas reales de obstáculos, la parametrización de los transmisores y la generación de predicciones de cobertura, representa un flujo de trabajo replicable, documentado y adaptable a diferentes escenarios geográficos. De igual manera, la configuración de la topología lógica en GNS3, con sus respectivas pruebas de verificación, constituye un referente metodológico para la formación de ingenieros en telecomunicaciones.

Recomendaciones

Recomendaciones técnicas

- Para futuras implementaciones, se sugiere evaluar la incorporación del estándar 802.11ax (Wi-Fi 6) en los nodos CPE, ya que ofrece mayores tasas de throughput, mejor eficiencia espectral mediante OFDMA y mayor capacidad para gestionar

múltiples usuarios simultáneos, aspectos críticos para el segmento empresarial de la red WISP.

- Se recomienda realizar mediciones de campo reales (drive test o walk test) en los puntos de instalación definidos para los nodos de la red, con el objetivo de calibrar el modelo de propagación ITU-R P.526 con datos empíricos locales y reducir la incertidumbre inherente a cualquier simulación de cobertura radioeléctrica.
- Para el segmento rural, se sugiere evaluar el uso de antenas sectoriales con mayor apertura de haz o antenas de alta ganancia tipo grilla (grid), dado que el análisis de perfiles de terreno evidenció la presencia de obstrucciones en algunos tramos del enlace, lo que podría comprometer la calidad del servicio en condiciones adversas de propagación.
- Se recomienda implementar un sistema de monitoreo de red (NMS) como Zabbix, PRTG o LibreNMS integrado a la topología GNS3, con el fin de simular la supervisión en tiempo real del estado de los equipos, consumo de ancho de banda por VLAN y generación de alertas ante degradación del servicio.

Recomendaciones académicas y metodológicas

- Se recomienda que futuras investigaciones extiendan la metodología propuesta hacia el cálculo y validación de la tasa de error de bits (BER) en función de los valores de SNR obtenidos en Atoll, utilizando modelos matemáticos de canal como AWGN o Rayleigh, con el fin de caracterizar de manera más completa la calidad de los enlaces inalámbricos simulados.
- La metodología desarrollada en esta investigación puede ser adoptada como material de referencia en las asignaturas de Telecomunicaciones Inalámbricas, Redes de Datos y Planificación de Redes de la carrera de Ingeniería en Telecomunicaciones, dado que integra herramientas de uso profesional (GNS3 y Atoll) con datos geoespaciales reales y parámetros técnicos documentados.

- Para fortalecer la validación de los resultados, se recomienda incorporar en trabajos futuros un análisis comparativo de modelos de propagación (Longley-Rice, COST 231-Hata y Okumura-Hata) sobre la misma área de estudio, evaluando las diferencias en los mapas de cobertura predichos y su correlación con mediciones reales, lo que aportaría mayor rigor científico a la metodología propuesta.

Referencias

Bibliografía

- [1] P. G. Pérez Caisaguano, abril 2018. [En línea]. Available: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://dspace.ups.edu.ec/bitstream/123456789/15471/1/UPS%20-%20ST003525.pdf.
- [2] O. D. Pastrano Ibarra, 2022. [En línea]. Available: https://repositorio.puce.edu.ec/server/api/core/bitstreams/8ed62410-f07a-4648-81e4-beec42786d52/content.
- [3] E. S. Castro Ullauri, marzo 2015. [En línea]. Available: https://dspace.ups.edu.ec/bitstream/123456789/10297/1/UPS-GT001192.pdf.
- [4] A. W. Párraga Lara y J. C. Aspiazu Rovira, 2021. [En línea]. Available: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://dspace.ups.edu.ec/bitstream/123456789/20805/1/UPS-GT003348.pdf.
- [5] C. W. Suárez González, 2021. [En línea]. Available: https://repositorio.upse.edu.ec/handle/46000/7715.
- [6] M. A. Ponce Monterrosas, 2014. [En línea]. Available: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/http://132.248.9.195/ptd2014/mayo/0712735/0712735.pdf.

- [7] A. A. Manzano Angulo, 2023. [En línea]. Available: chrome-extension://efaidnbmnnnibpcajpcgiclfndmkaj/https://dspace.ups.edu.ec/bitstream/123456789/26228/1/UPS-GT004700.pdf.
- [8] J. Jiménez, «RZ redes zones,» 18 noviembre 2024. [En línea]. Available: https://www.redeszone.net/tutoriales/redes-cable/programas-similar-red/.
- [9] J. A. Santos Mercado, 2022. [En línea]. Available: chrome-extension://efaidnbmnnnibpcajpcgiclfndmkaj/https://dspace.ups.edu.ec/bitstream/123456789/23263/1/UPS%20-%20TTS913.pdf.
- [10] R. B. Pérez, s.f.. [En línea]. Available: chrome-extension://efaidnbmnnnibpcajpcgiclfndmkaj/https://uvadoc.uva.es/bitstream/handle/10324/38784/TFG-G3730.pdf?sequence=1&isAllowed=y.
- [11] A. E. Cruz Quilca y R. D. Gordon Pérez, «Desarrollo de guías practicas para la simulacion de redes con equipos mikrotik utilizando GNS3,» junio 2021. [En línea]. Available: https://bibdigital.epn.edu.ec/handle/15000/21717?utm_source.
- [12] E. Ochoa Torres y M. I. Castro Olaya, 7 marzo 2014. [En línea]. Available: chrome-extension://efaidnbmnnnibpcajpcgiclfndmkaj/https://www.redalyc.org/pdf/2570/257059812012.pdf.
- [13] E. N. M. d. Hogares, Abril 2021. [En línea]. Available: chrome-extension://efaidnbmnnnibpcajpcgiclfndmkaj/https://www.ecuadorencifras.gob.ec/documentos/web-inec/Estadisticas_Sociales/TIC/2020/202012_Principales_resultados_Multiproposito_TIC.pdf?utm_source.
- [14] «Data Reportal,» 3 marzo 2025. [En línea]. Available: https://datareportal.com/reports/digital-2025-ecuador.

- [15] L. I. Quiñones, febrero 2016. [En línea]. Available: chrome-extension://efaidnbmnnnibpcajpcgclefindmkaj/https://upcommons.upc.edu/bitstream/handle/2117/83015/PFC%20Luis%20Iglesias.pdf.
- [16] A. Walton, «CCNA,» s.f. [En línea]. Available: https://ccnadesdecero.es/que-es-gns3-como-usarlo/?utm_source.
- [17] «Forsk,» s.f. [En línea]. Available: https://www.forsk.com/atoll-overview?utm_source.
- [18] A. Escudero Pascual, s.f. [En línea]. Available: chrome-extension://efaidnbmnnnibpcajpcgclefindmkaj/https://nsrc.org/wrc/trac/wirelessu/raw-attachment/wiki/WALC2009/02_es_estandares-inalambricos_guia_v02 %5B1 %5D.pdf.
- [19] P. Gil y G. García, s.f. [En línea]. Available: chrome-extension://efaidnbmnnnibpcajpcgclefindmkaj/https://rua.ua.es/dspace/bitstream/10045/45467/1/2014_Gil_etal_FIE_rev.pdf.
- [20] R. E. Ríos, julio 2019. [En línea]. Available: chrome-extension://efaidnbmnnnibpcajpcgclefindmkaj/https://upcommons.upc.edu/bitstream/handle/2117/169237/5G%20Network%20Planning%20and%20Optimization%20Using%20Atoll%20-%20Master%27s%20Thesis%20-%20Riviel%20Rios.pdf?sequence=4&isAllowed=y.
- [21] A. A. Andrade Mafla, marzo 2013. [En línea]. Available: chrome-extension://efaidnbmnnnibpcajpcgclefindmkaj/https://bibdigital.epn.edu.ec/bitstream/15000/6099/1/CD-4805.pdf.
- [22] «Networks Training,» s.f. [En línea]. Available: https://www.networkstraining.com/gns3-vs-eve-ng-vs-cisco-packet-tracer/.
- [23] «Redes Zone,» s.f. [En línea]. Available: https://www.redeszone.net/tutoriales/redes-cable/programas-simular-red/.
- [24] J. Rejon, «mundotelematico.com,» 14 mayo 2019. [En línea]. Available: https://www.mundotelematico.com/simulador-de-red-gns3/.

- [25] «ScienceDirect,» 2018. [En línea]. Available: <https://www.sciencedirect.com/topics/computer-science/vmware-workstation#definition>.
- [26] D. Córdoba, «Junco TIC,» 19 febrero 2019. [En línea]. Available: <https://juncotic.com/gns3-virtualbox-simulando-redes-tcp-ip/>.
- [27] «GNS3,» s.f.. [En línea]. Available: <https://docs.gns3.com/docs/getting-started/installation/download-gns3-vm/>.
- [28] «MB Services,» s.f.. [En línea]. Available: <https://mbservices.cl/throughput-que-es-y-como-optimizarlo-en-tu-empresa/#:~:text=Throughput:%20Es%20la%20cantidad%20real,de%20datos%20debido%20a%20errores..>
- [29] «Indusface,» s.f.. [En línea]. Available: <https://www.indusface.com/learning/what-is-latency/>.
- [30] S. Butani, «IDT EXPRESS,» 13 JUNIO 2023. [En línea]. Available: <https://idtexpress.com/es/blog/what-is-jitter-typical-causes-ways-to-reduce-it/>.
- [31] «NetSpot,» s.f.. [En línea]. Available: <https://www.netspotapp.com/es/wifi-troubleshooting/signal-to-noise-ratio.html>.
- [32] «Studocu,» s.f.. [En línea]. Available: <https://www.studocu.com/ec/document/universidad-de-las-fuerzas-armadas-de-ecuador/comunicacion-y-cod-digital/cost-231-propagation/7044929>.
- [33] «RF Wireless World,» s.f.. [En línea]. Available: <https://www.rfwireless-world.com/terminology/okumura-hata-model-cost-231-extension>.
- [34] J. A. Bernal Botello y J. C. Bocanegra Luna, 3 NOVIEMBRE 2021. [En línea]. Available: <https://repositorio.unitec.edu.co/bitstream/handle/20.500.12962/2014/Dise%C3%B1o%20y%20simulaci%C3%B3n%20de%20un%20enlace%20terrestre%20punto%20a%20punto%20para%20un%20cliente%20privado.pdf?sequence=1&isAllowed=y#:~:text=Aplicando%20decibeles%2C%20resulta>.

- [35] G. Piero Perrino, MARZO s.f. [En línea]. Available:
https://upcommons.upc.edu/bitstream/handle/2099.1/18251/PFC_-_Gian_Piero_Perrino.pdf#:~:text=radioel%C3%A9ctricos%20en%20el%20entorno%20profesional%2C%20como%20es,con%20su%20nuevo%20m%C3%B3dulo%20LTE%20disponible%2C%20se..
- [36] W. H. Pazuzhi Idrovo, s.f. [En línea]. Available:
<https://dspace.ups.edu.ec/bitstream/123456789/12127/1/UPS-CT006042.pdf>
- [37] L. Díaz Cervantes, s.f. [En línea]. Available: <https://1library.co/document/z1l1leq-evaluacion-herramienta-gns-conectividad-enrutadores-reales.html>.
- [38] L. Golightly, «Deploying secure distributed systems: Comparative analysis of GNS3 and SEED Internet Emulator,» 3 agosto 2023. [En línea]. Available: <https://www.mdpi.com/2624-800X/3/3/24>.
- [39] L. Iglesias Quiñones, FEBRERO 2016. [En línea]. Available:
<https://upcommons.upc.edu/bitstream/handle/2117/83015/PFC%20Luis%20Iglesias.pdf>
- [40] F. A. Carrasco Cabrera, 6 NOVIEMBRE 2020. [En línea]. Available:
<http://repositorio.ucsg.edu.ec/bitstream/3317/15699/1/T-UCSG-POS-MTEL-179.pdf>
- [41] «Source Force,» s.f. [En línea]. Available: <https://sourceforge.net/software/compare/SolarWinds-NetFlow-Traffic-Analyzer-vs-Wireshark-vs-tcpdump/>.
- [42] «El Hacker Net,» 7 10 2024. [En línea]. Available: <https://blog.elhacker.net/2024/10/ntopng-monitor-analizador-trafico-red-avanzado.html>.
- [43] L. Deri, 06 2015. [En línea]. Available:
<https://sharkfest.wireshark.org/retrospective/sfus/presentations15/16.pdf>
- [44] «LabEx,» s.f. [En línea]. Available: <https://labex.io/es/tutorials/wireshark-capture-and-analyze-network-traffic-with-wireshark-415956>.

- [45] «6sense,» s.f. [En línea]. Available: <https://6sense.com/tech/network-monitoring/wireshark-vs-ntopng>.
- [46] «Capterra,» s.f. [En línea]. Available: <https://www.capterra.com/compare/172324-209737/NetFlow-Analyzer-vs-Wireshark>.
- [47] «Campus Internacional Ciberseguridad,» s.f. [En línea]. Available: <https://www.campusciberseguridad.com/blog/guia-completa-de-wireshark-para-analisis-y-monitoreo-de-redes/#:~:text=Wireshark%20es%20una%20herramienta%20fundamental,causa%20ra%C3%ADz%20de%20un%20fallo..>
- [48] «NetFlow,» s.f. [En línea]. Available: <https://www.manageengine.com/latam/netflow/que-es-netflow.html>.
- [49] M. I. Gandía Carriedo, s.f. [En línea]. Available: <https://es.slideshare.net/slideshow/herramientas-de-monitorizacin-de-flujos-qu-tenemos-qu-necesitamos/180669780>.
- [50] D. Sinchi Torres, «Scribd,» s.f. [En línea]. Available: <https://es.scribd.com/document/386446238/Modelos-Propagacio-n>.
- [51] J. L. Oña Riera, 2025. [En línea]. Available: <https://dspace.espol.edu.ec/bitstream/123456789/65822/1/T-115117%20POSTG119%200%c3%91A%20RIERA%20JOSE.pdf>.
- [52] Medina, «Instalar Router Mikrotik CHr en GNS3,» Youtube, 2024.
- [53] «Mikrotik,» [En línea]. Available: <https://help.mikrotik.com/docs/spaces/ROS/pages/328151/First+Time+Configuration>.
- [54] Spatial Zone, «Como descargar imagenes Landsat de USGS Earth Explorer gratis [video],» Youtube, 2023.
- [55] Vikas Ghadamode, «RS & GIS QA14- ESA World Cover 2021 and 2020 || Download Free Global 10 m resolution LULC [video],» Youtube, 2022.

- [56] MasterGIS, «10 Motivos para aprender Global Mapper | Master SIG [video],» Youtube, 2017.
- [57] Muhammad Sadeq, «Create Maps with Global Mapper for Atoll,» Youtube, 2024.
- [58] Mega Datum, «Atoll - Map | Atoll Mapas,» Youtube, 2015.
- [59] Villafuerte, «GNS3 tarea1 creacion de vlans entre switch Mikrotik,» Youtube, 2021.
- [60] A. Gamarra, 2018. [En línea]. Available:
https://mum.mikrotik.com/presentations/AR18/presentation_6297_1542974948.pdf.
- [61] N. Bautista, 30 agosto 2019. [En línea]. Available:
https://dl.ubnt.com/datasheets/LiteAP_ac/LiteAP_AC_DS.pdf.
- [62] N. Bautista, 20 diciembre 2019. [En línea]. Available:
https://dl.ubnt.com/datasheets/NanoStation_AC/NanoStation_AC_DS.pdf.
- [63] I. R. Gongora, 13 mayo 2025. [En línea]. Available: <https://blog.sensando.mx/que-es-ieee-802-1q-y-como-funciona-el-etiquetado-de-vlan/>.
- [64] C. Castaño, 14 Julio 2024. [En línea]. Available: <https://prezi.com/p/lf7z4upbphmv/ieee-8021w-rapid-spanning-tree-protocol-rstp/>.
- [65] La Oficina de Sistemas, «Cómo instalar GNS3 Y GNS3 VM en WMware WorkStation para simular redes,» Youtube, 2025.
- [66] La Oficina de Sistemas, «VMware Workstation AMD-V/RVI is not Supported GNS3: Solucionalo fácil,» Youtube, 2025.
- [67] Casa iTech, «Comment faire l'installation complète du logiciel Atoll,» Youtube, 2022.
- [68] Global Mapper, «Global Mapper 23 Reclassificacao raster do Land cover da ESA,» Youtube, 2021.
- [69] Flores, «Tutorial video 04 de 20 Atoll - Configuracion del modelo de propagación y del site,» Youtube, 2021.

- [70] P. L. A. VLADIMIR, 2021. [En línea]. Available: chrome-extension://efaidnbmninnbpcjpcglclefindmkaj/https://dspace.ups.edu.ec/bitstream/123456789/20805/1/UPS-GT003348.pdf.
- [71] «NETWORK INFORMATION LIBRARY,» [En línea]. Available: https://nil.uniza.sk/en/connecting-gns3-virtualbox-host/.
- [72] «CHEAP WINDOWS VPS,» [En línea]. Available: https://cheapwindowsvps.com/blog/mastering-complex-network-simulations-with-gns3/.
- [73] «virtualbox.org,» [En línea]. Available: https://forums.virtualbox.org/viewtopic.php?t=91009.
- [74] «help left,» [En línea]. Available: https://www.helpleft.com/es/internet/what-is-a-bit-error-rate.html.
- [75] «PROGRAMADOR CLIC,» [En línea]. Available: https://programmerclick.com/article/7213244069/.
- [76] S. D. LUZ, «REDES ZONE,» 25 MAYO 2025. [En línea]. Available: https://www.redeszone.net/tutoriales/redes-cable/iperf3-medir-velocidad-lan-wifi-internet/.
- [77] B. LEON, «GURU99,» 28 ABRIL 2025. [En línea]. Available: https://www.guru99.com/es/best-ping-monitoring-tools.html.
- [78] «ESEYE,» 16 OCTUBRE 2024. [En línea]. Available: https://www.eseye.com/resources/iot-explained/understanding-signal-quality-rssi-rsrp-and-rsrq/#:~:text=una%20en%20IoT.-,Indicador%20de%20intensidad%20de%20la%20se%C3%B1al%20recibida%20(RSSI),la%20calidad%20de%20la%20se%C3%B1al..
- [79] «ROM MAYER,» [En línea]. Available: https://rom-mayer.cl/redes-inalambricas-2/.
- [80] «MDPI,» 2022. [En línea]. Available: https://www.researchgate.net/publication/363701747_Average_BER_Performance_Estimation_of_Relayed_Thz_Links_with_Losses_Molecular_Attenuation_Adverse_Weather_Conditions_Turbulence_and_Generalized_Pointing_Errors/fulltext/632b0584071ea12e364e9206/Average-BE.

- [81] E. F. MATEO, JUNIO 2018. [En línea]. Available:
<https://upcommons.upc.edu/bitstream/handle/2117/129150/Figueras%20Mateo%20Eduard%20%5BTFG%5D.pdf?sequence=1>.
- [82] «IELECTEL,» [En línea]. Available: https://ielectel.com/compuerta-logica-xor/#google_vignette.
- [83] «TECNOLOBLOG,» [En línea]. Available: <https://www.tecnoloblog.com/que-es-fpga/>.
- [84] Universitat Politècnica de valencia - UPV, «Atoll - conceptos básicos || UPV».
- [85] «CCNA,» s.f.. [En línea]. Available: <https://ccnadesdecero.es/perdida-de-paquetes-packet-loss/>.

Anexo. Procedimiento de configuración completa de la red WISP

Con el propósito de garantizar la replicabilidad del prototipo, el procedimiento de configuración paso a paso de la totalidad de los dispositivos que integran la red WISP se encuentra disponible en un repositorio digital de acceso público. Dicho repositorio contiene el detalle íntegro de los comandos ejecutados y las capturas de pantalla correspondientes a cada dispositivo, incluidos los sectores Urbano y Empresas y los nodos de respaldo Urbano y Empresas, cuyos parámetros se presentan de forma resumida en los apartados 3.4.11 y 3.4.13 del presente documento.

Enlace al repositorio:

[https://drive.google.com/file/d/1EAMFBRsJ9Hr0PrtyW5kxm1HTqZtr7sGo/view?usp=s_haring]