



**UNIVERSIDAD ESTATAL
PENÍNSULA DE SANTA ELENA**

FACSISTEL

INGENIERÍA EN TELECOMUNICACIONES

TRABAJO DE INTEGRACIÓN CURRICULAR

**Implementación de una red de acceso en WISP utilizando
protocolos de red para garantizar calidad y seguridad**

Jeffry Paúl Rodríguez De La A

Dirigido por:

Ing. Luis Miguel Amaya Fariño, Mgtr.

LA LIBERTAD – 2026

AGRADECIMIENTO

A Dios, por brindarme la salud, sabiduría y fortaleza necesarias para superar cada obstáculo a lo largo de mi formación académica y culminar este proyecto de titulación.

A la Universidad Estatal Península de Santa Elena y a la Carrera de Ingeniería en Telecomunicaciones, por haberme abierto las puertas de sus aulas y laboratorios, brindándome las herramientas necesarias para mi desarrollo profesional.

Expreso mi sincero agradecimiento a mi tutor de tesis y al docente especialista, por su valiosa guía, tiempo y criterio técnico en la revisión de este documento.

De igual manera, reconozco el esfuerzo de mis compañeros de proyecto y amigos, por las extensas jornadas de trabajo y aprendizaje compartido.

Finalmente, a mi familia, cuyo apoyo incondicional y motivación constante fue el pilar fundamental para alcanzar este logro.

Jeffry Paúl Rodríguez De La A



**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, Mgtr.
TUTOR

Ing. Fernando Chamba Macas, Mgtr.
DOCENTE ESPECIALISTA

Ing. Luis Amaya Fariño, Mgtr.
DOCENTE GUÍA UIC

Ing. Corina Raquel Gonzabay De La A, Mgtr.
SECRETARIA



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

AUTORIZACIÓN

Yo, Jeffry Paúl Rodríguez De La A

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

Cedo los derechos en línea patrimoniales de 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 3 días del mes de agosto del año 2026

EL AUTOR

Jeffry Paúl Rodríguez De La A



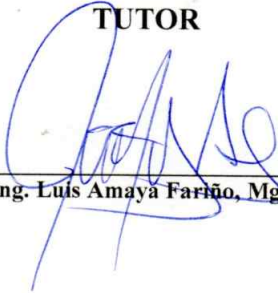
**UNIVERSIDAD ESTATAL PENÍNSULA
DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES**

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 el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por Jeffry Paúl Rodríguez De La A, como requerimiento para la obtención del título de Ingeniero en telecomunicaciones.

La Libertad, a los 3 días del mes de agosto del año 2026

TUTOR



Ing. Luis Amaya Fariño, Mgtr.



**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 titulación denominado Implementación de una red de acceso en WISP utilizando protocolos para garantizar calidad y seguridad, presentado por el estudiante, Jeffry Paúl Rodríguez De La A fue enviado al Sistema Antiplagio, presentando un porcentaje de similitud correspondiente al 9%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.



Certificado de análisis
Compilatio Magister+ | UPSE-ECU

TRABAJO_DE_INTEGRACION_CURICULAR_JEFFRY_RODRIGUEZ_DE_LA_A
ID : 868626e68a16e9fc675d36fce53b77f28834589b



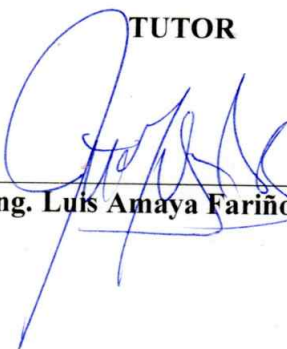
9%

Textos sospechosos

Nombre del fichero :
TRABAJO_DE_INTEGRACION_CURICULAR_JEFFRY_RODRIGUEZ_DE_LA_A.txt
Tamaño del archivo original : 7,56 MB
Número de palabras : 35.694

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 Mgtr.



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

DECLARACIÓN DE RESPONSABILIDAD

Yo, Jeffry Paúl Rodríguez De La A

DECLARO QUE:

El trabajo de Titulación, Implementación de un sistema de comunicaciones segura para la gestión crítica utilizando redes dinámicas de un previo a la obtención del título en Ingeniero en Tecnologías de la Información, ha sido desarrollado respetando derechos intelectuales de terceros conforme 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 Titulación referido.

La Libertad, a los 3 días del mes de agosto del año 2026

EL AUTOR

Jeffry Paúl Rodríguez De La A

DEDICATORIA

Este logro académico se lo dedico a mis padres, por su amor incondicional, sus constantes oraciones y su esfuerzo desinteresado para brindarme un futuro mejor. Gracias por ser mi mayor ejemplo de trabajo y perseverancia.

A mis hermanos y demás familiares, por ser mi refugio, mi motivación en los momentos de cansancio y por celebrar cada paso hacia esta meta.

A todas las personas que creyeron en mí y me brindaron una palabra de aliento a lo largo de este camino.

Jeffry Paúl Rodríguez De La A

Índice

0.1. Resumen	16
1. CAPÍTULO 1: MARCO TEÓRICO	17
1.1. Introducción	17
1.2. Antecedentes	17
1.3. Planteamiento del problema	19
1.4. Justificación	20
1.5. Descripción del proyecto	20
1.6. Proceso de implementación	21
1.7. Beneficios de la implementación	22
1.8. Objetivos	24
1.8.1. Objetivo general	24
1.8.2. Objetivos específicos	24
1.9. Resultados esperados	24
1.10. Metodología	25
2. CAPÍTULO 2: FUNDAMENTACIÓN TEÓRICA	26
2.1. Introducción	26
2.2. Conceptos fundamentales de telecomunicaciones	26
2.2.1. Espectro electromagnético	26
2.2.2. Espectro radioeléctrico	27
2.2.3. Línea de vista	29
2.2.4. Zona de Fresnel	29
2.2.5. Topología de red	31
2.2.6. Componentes de una topología de red	31
2.2.7. Topología física frente a topología lógica	32
2.2.8. Tipos de topologías de red	33
2.2.9. Clasificación de redes según su distancia	36

2.3.	¿Qué es una red WISP?	38
2.3.1.	Componentes de una red WISP	39
2.3.2.	Requisitos para un WISP	40
2.3.3.	Marco normativo y regulatorio	40
2.3.4.	Requisitos y viabilidad técnica	41
2.4.	Infraestructura en redes de acceso	42
2.5.	Servicios de una red WISP	43
2.6.	Estándares	44
2.6.1.	Estándar IEEE 802.11	44
2.6.2.	IEEE 802.1Q	46
2.6.3.	ANSI/TIA-568	46
2.6.4.	RFC 1918	48
2.7.	Protocolos	49
2.7.1.	IP (Internet Protocol)	49
2.7.2.	TCP (Transmission Control Protocol)	49
2.7.3.	UDP (User Datagram Protocol)	49
2.7.4.	DNS (Domain Name System)	49
2.7.5.	DHCP (Dynamic Host Configuration Protocol)	50
2.7.6.	RSTP (Rapid Spanning Tree Protocol)	50
2.7.7.	Protocolo PPPoE (Point-to-Point Protocol over Ethernet)	50
2.7.8.	SSH (Secure Shell)	51
2.8.	Tecnologías	51
2.8.1.	airMAX	51
2.8.2.	RouterOS	51
2.9.	Mecanismos de control de tráfico y calidad de servicio	52
2.9.1.	Clasificación, diferenciación y marcado de tráfico (Firewall Mangle)	52
2.9.2.	Algoritmos de distribución equitativa del canal (Per Connection Queueing - PCQ)	54
2.9.3.	Asignación jerárquica de recursos (Hierarchical Token Bucket - HTB)	55

2.10. Mecanismos de seguridad y mitigación de vulnerabilidades	57
2.10.1. NAT (Network Address Translation)	57
2.10.2. Filtrado de paquetes y mitigación de amenazas (Firewall Filter)	58
2.10.3. Aislamiento lógico e inter-VLAN de abonados	60
2.10.4. Robustecimiento del plano de control	61
2.11. Fenómenos físicos de la propagación de onda	62
2.11.1. Reflexión	62
2.11.2. Refracción	66
2.11.3. Difracción	69
2.11.4. Dispersión	71
2.11.5. Interferencias	71
2.11.6. Absorción	73
2.11.7. Atenuación	74
2.12. Ataques cibernéticos en redes inalámbricas	76
2.12.1. Denegación de servicio	76
2.12.2. Hombre en el medio	77
2.12.3. Ataques por fuerza bruta	78
2.12.4. Espionaje	79
2.12.5. Suplantación de MAC	80
3. CAPÍTULO 3: PROPUESTA DEL PROYECTO	81
3.1. Arquitectura y diseño lógico de la red	81
3.2. Topología lógica y flujo de datos	81
3.2.1. Núcleo (Core Layer)	82
3.2.2. Capa de distribución (Distribution Layer)	83
3.2.3. Capa de acceso (Access Layer)	84
3.2.4. Integración de la red completa	85
3.2.5. Segmentación de red mediante redes locales virtuales (VLANs)	86
3.2.6. Esquema de direccionamiento IP (IPv4)	87
3.2.7. Transición del modelo de red: Migración de DHCP a PPPoE	88

3.3.	Especificaciones y requerimientos técnicos de hardware	89
3.3.1.	Estación base: Transmisión y recepción centralizada	89
3.3.2.	Terminal de usuario / Estación de abonado	90
3.3.3.	Enrutador central / Administrador de red	91
3.3.4.	Especificaciones de medio de transmisión	92
3.4.	Configuración de calidad de servicio (QoS)	92
3.4.1.	Clasificación y marcado de tráfico (Mangle)	93
3.4.2.	Jerarquía de prioridades (Queue Tree)	93
3.4.3.	Implementación de subcolas para el sector empresarial	94
3.5.	Protocolos de seguridad e integridad de datos	95
3.5.1.	Aislamiento de clientes y capa inalámbrica	95
3.5.2.	Filtrado de tráfico y seguridad en el core	95
3.6.	Procedimiento de implementación técnica	96
3.6.1.	Fase 1: Configuración del enrutador central (Core MikroTik)	97
3.6.2.	Fase 2: Configuración del switch y distribución	99
3.6.3.	Fase 3: Configuración de antenas (Enlaces inalámbricos)	100
3.6.4.	Fase 4: Configuración de MikroTik (Cliente)	102
3.6.5.	Fase 5: Pruebas de validación y QoS	102

4. CAPÍTULO 4: RESULTADOS 103

4.1.	Identificación de elementos de la red	103
4.2.	Implementación bajo normativas y estándares	103
4.3.	Pruebas de rendimiento	103
4.3.1.	Pruebas internas de la red con iPerf3	103
4.3.2.	Prueba de red sin priorización de tráfico	104
4.3.3.	Prueba red no saturada con priorización de tráfico	105
4.3.4.	Prueba con red saturada con priorización de tráfico	105
4.4.	Pruebas de rendimiento usando nperf	105
4.4.1.	Prueba 1: Red no saturada	106
4.4.2.	Prueba 2: Red saturada	107

4.5.	Análisis de resultados y discusión en QoS	108
4.5.1.	Análisis de resultados Iperf previo a la aplicación de QoS	108
4.5.2.	Análisis de resultados Iperf posterior a la aplicación de QoS	109
4.5.3.	Análisis de resultados nPerf	110
4.5.4.	Análisis del canal de descarga (Download)	110
4.5.5.	Análisis del canal de subida (Upload)	111
4.6.	Verificación del comportamiento de las colas de prioridad	112
4.6.1.	Verificación de tráfico constante de todos los abonados	112
4.6.2.	Verificación de subcolas del área empresarial	112
4.6.3.	Inyección de tráfico UDP con descarga	113
4.7.	Verificación de seguridad de clientes	114
4.7.1.	Etapa 1: Control de acceso y autenticación mediante servidor PPPoE	114
4.7.2.	Etapa 2: Aislamiento e intercepción de tráfico inter-VLAN	114
4.7.3.	Etapa 3: Auditoría de hardening e inactivación de servicios	116
4.8.	Análisis de resultados y discusión en seguridad	117
4.9.	Recomendaciones	118
4.10.	Conclusiones	119

Índice de figuras

1.	Representación geométrica de la primera zona de Fresnel.	29
2.	Efecto de obstrucción en el radio de la zona de Fresnel.	30
3.	Topologías de red convencionales.	33
4.	Clasificación de redes según su alcance.	36
5.	Mapa conceptual de los requisitos técnicos y normativos para un WISP	40
6.	Distribución de pines y códigos de colores normalizados para conectores RJ-45.	47
7.	Frente de onda plano incidente	63
8.	Reflexión del frente de onda y generación de ondas secundarias	63
9.	Formación del frente de onda reflejado	64
10.	Geometría para la deducción de la ley de reflexión	65
11.	Geometría para la deducción de la ley de la refracción	66
12.	Geometría para la deducción de la ley de la refracción	67
13.	Ley de refracción	68
14.	Difracción	69
15.	Denegación de servicio	76
16.	MitM	77
17.	Ataques por fuerza bruta	78
18.	Eavesdropping	79
19.	MAC Spoofing	80
20.	Topología de la capa de núcleo (Core Layer).	82
21.	Topología e interconexión de la capa de distribución.	83
22.	Topología y direccionamiento de la capa de acceso.	84
23.	Topología lógica integral y flujo de datos extremo a extremo de la red WISP. . .	85
24.	Diagrama de puertos del switch	100
25.	Resultados de pruebas nPerf en escenario de uso individual para diferentes planes de cliente.	106

26.	Resultados de pruebas nPerf en escenario saturado para diferentes planes de cliente.	107
27.	Comportamiento de las colas con tráfico constante en todos los perfiles.	112
28.	Distribución de tráfico interno en las subcolas del perfil Empresa.	113
29.	Comportamiento del Queue Tree ante la inyección de tráfico UDP con descarga activa.	113
30.	VLANs habilitadas en el dispositivo.	127
31.	Configuración de los puertos de acceso en la interfaz del conmutador.	128
32.	Asignación y etiquetado de los puertos troncales (VLAN Trunk).	128
33.	Segmento primario de direccionamiento IP e interfaces lógicas.	129
34.	Configuración de enrutamiento y gestión IP del switch.	129
35.	Parámetros inalámbricos de operación en modo punto de acceso (AP).	130
36.	Configuración de las interfaces de red y enrutamiento del sistema inalámbrico. .	130
37.	Habilitación y optimización de servicios de transmisión y seguridad.	131
38.	Conectorización, guiado y organización de cordones de parcheo en el conmutador de distribución.	132
39.	Instalación y energización del enrutador residencial del abonado en el panel de distribución.	133
40.	Fijación mecánica, montaje y alineación azimutal de la estación base sectorial. .	134
41.	Instalación y orientación del equipo transceptor inalámbrico (CPE) en el nodo terminal del cliente.	135
42.	Implementación física de la infraestructura central y distribución del prototipo WISP.	136

Índice de tablas

1.	Distribución convencional del espectro radioeléctrico y sus aplicaciones típicas.	28
2.	Segmentación de red mediante VLANs	86
3.	Dispositivos y direccionamiento IP de la topología lógica	87
4.	Comparativa técnica en la transición del modelo de red: DHCP vs. PPPoE . . .	88
5.	Especificaciones técnicas de la estación base LiteAP GPS (LAP-GPS)	90
6.	Especificaciones técnicas del terminal de abonado Loco NanoStation 5AC . . .	91
7.	Especificaciones técnicas del router principal MikroTik hEX (RB750Gr3) . . .	92
8.	Especificaciones técnicas del hardware seleccionado para la red WISP	93
9.	Jerarquía de prioridades y garantía de ancho de banda	94
10.	Asignación de puertos y etiquetado VLAN en el Switch.	99
11.	Matriz de parámetros de radiofrecuencia para AP y CPE.	101
12.	Rendimiento en red sin QoS ni priorización por VLANs (Iperf)	108
13.	Comparativa de rendimiento UDP mediante iPerf3	109
14.	Comparativa de rendimiento de red mediante nPerf	110
15.	Porcentajes de eficiencia y degradación en la tasa de descarga (Download) . . .	110
16.	Porcentajes de eficiencia y degradación en la tasa de subida (Upload)	111
17.	Resultados de la prueba de control de acceso y autenticación PPPoE.	114
18.	Evaluación de conectividad PING entre la VLAN 10 (Gestión) y los diferentes segmentos de clientes antes y después de aplicar reglas de firewall.	115
19.	Resultados de hardening e inactivación de servicios de gestión.	116
20.	Matriz de verificación y validación de la estrategia de seguridad en la red . . .	117

0.1 Resumen

Este proyecto tiene como tema central la implementación de una red de acceso de tipo WISP (Wireless Internet Service Provider), con el propósito de simular un entorno real de conectividad inalámbrica que garantice calidad y seguridad en el servicio. El objetivo principal es evaluar el rendimiento de la red mediante la aplicación de estándares y protocolos específicos. Se emplea una metodología de investigación aplicada, descriptiva y explicativa, utilizando equipos reales como antenas Ubiquiti y routers MikroTik. Para ello, se diseña una red punto a multipunto dividida en tres tipos de abonados (doméstico, empresarial y VIP), aplicando configuraciones personalizadas para cada perfil. Entre los resultados obtenidos destacan mejoras en el rendimiento, la estabilidad y la segmentación del servicio, así como la reducción de interferencias. En conclusión, el proyecto evidencia la importancia de una planificación técnica adecuada y se consolida como una herramienta pedagógica valiosa para la formación de futuros profesionales en telecomunicaciones.

Palabras clave: WISP, red de acceso, punto a multipunto, calidad de servicio, MikroTik, Ubiquiti.

1 CAPÍTULO 1: MARCO TEÓRICO

1.1 Introducción

En esta era digital, el internet es uno de los pilares fundamentales tanto en lo económico como en lo educativo. Sin embargo, en varias comunidades rurales y zonas periurbanas, la falta de infraestructura de telecomunicaciones limita el acceso a este servicio, lo que genera una brecha significativa que dificulta el acceso de sus habitantes a la educación en línea, el teletrabajo y el comercio electrónico [1].

Para enfrentar esta problemática de conectividad, las redes de los proveedores de servicio de internet inalámbrico (WISP, por sus siglas en inglés) surgen como una alternativa viable y económica. Este tipo de redes permite la distribución del servicio mediante tecnología de radiofrecuencia, evitando el despliegue de cableado físico e infraestructura compleja y costosa, como la fibra óptica o el cobre.

Este proyecto plantea el diseño e implementación de un prototipo WISP con una arquitectura de árbol dentro de un entorno controlado para dar servicio a tres abonados. Esto no solo valida la efectividad de una red WISP, sino que también permite contar con una herramienta educativa para los estudiantes de telecomunicaciones y carreras afines.

1.2 Antecedentes

El origen de la tecnología inalámbrica se remonta a una necesidad militar durante la Segunda Guerra Mundial, cuando la actriz e inventora Hedy Lamarr y el compositor George Antheil desarrollaron un sistema de comunicación secreta basado en el salto de frecuencia para evitar la interceptación de torpedos. Posteriormente, en 1985, la Comisión Federal de Comunicaciones de Estados Unidos (FCC) liberó el uso no licenciado de las bandas de frecuencia en 2.4 GHz, lo que impulsó exponencialmente el desarrollo de las redes y dispositivos inalámbricos. Años después, en 1997, el IEEE publicó el primer estándar 802.11 (popularizado como Wi-Fi), sentando las bases para el surgimiento de los proveedores de servicios de internet inalámbrico [2].

Durante los inicios de internet, la conectividad inalámbrica se consideraba un objeti-

vo distante; sin embargo, con el tiempo se transformó en una necesidad fundamental del día a día. Ante el acelerado crecimiento en la demanda de conectividad, los WISP emergieron como una solución estratégica cuya ventaja principal radica en ofrecer cobertura en zonas de difícil acceso o donde la infraestructura basada en cobre o fibra óptica resulta inviable [3].

En el año 2021, Párraga y Aspiazu implementaron un módulo funcional de una red WISP en el laboratorio de Telecomunicaciones de la Universidad Politécnica Salesiana, aplicando conceptos de enrutamiento IP, configuración de routers y sistemas de transmisión por antena. Su objetivo principal fue proporcionar un prototipo didáctico para la simulación y el aprendizaje de un proveedor inalámbrico, sirviendo como marco de referencia para el diseño de redes de acceso al abonado [4].

Asimismo, Aguilar, Guerrero y Rendón (2004) desarrollaron la estructura integral de una red WISP, abarcando la configuración del acceso inalámbrico y una proyección de crecimiento de usuarios a cinco años. Su estudio contempló aspectos técnicos, legales, regulatorios y económicos, consolidándose como una referencia clave en el diseño de redes inalámbricas de última milla [5].

Por su parte, Suárez González (2021) analizó la implementación de una red comunitaria WISP en la comuna Bellavista del Cerro, aplicando protocolos de red para proveer servicio de internet como respuesta a la emergencia sanitaria por el COVID-19 en el Ecuador. En su trabajo evaluó aspectos de infraestructura y simulación mediante herramientas como Cisco Packet Tracer y VirtualBox. Dicha investigación demostró la factibilidad técnica y social de una red punto a multipunto, destacando la correcta selección de antenas y la segmentación del servicio como factores determinantes para un modelo funcional [6].

En resumen, la evolución de las tecnologías inalámbricas, desde sus inicios militares hasta la estandarización comercial, ha facilitado la adopción de modelos WISP para reducir la brecha digital. Trabajos previos como los de Párraga y Aspiazu, Aguilar y Suárez han demostrado la viabilidad técnica, pedagógica y social de este tipo de infraestructuras, constituyendo la base formal y metodológica para el presente proyecto.

1.3 Planteamiento del problema

En la actualidad, el acceso a internet es considerado un recurso básico, equiparable a servicios esenciales como el agua potable o la energía eléctrica, debido a su carácter indispensable para el desarrollo social, económico y educativo. Sin embargo, en zonas periféricas y sectores rurales, la conectividad sigue representando un desafío significativo. El despliegue de tecnologías tradicionales de distribución guiada, como la fibra óptica, suele resultar inviable en estos entornos debido a los elevados costos de infraestructura, la gran distancia respecto a los nodos principales, la topografía irregular del terreno y la falta de canalización adecuada, factores que encarecen considerablemente la obra. Esta limitación perpetúa la brecha digital, dejando a numerosas familias al margen de oportunidades educativas, laborales y tecnológicas.

Ante este panorama, las redes inalámbricas se consolidan como una alternativa altamente eficiente y económicamente viable, tanto para los usuarios como para los proveedores. Su arquitectura optimiza los costos de despliegue al requerir únicamente equipamiento receptor en las instalaciones del abonado y nodos centrales encargados de la administración, gestión y enrutamiento del tráfico.

En consecuencia, el presente proyecto propone el diseño e implementación de un prototipo de red WISP a escala dentro de un entorno de laboratorio controlado. La red contará con tres perfiles de abonado con diferentes asignaciones de ancho de banda y parámetros de calidad de servicio (QoS), utilizando tecnologías robustas que garanticen la estabilidad de la red, tales como el protocolo airMAX en los enlaces inalámbricos y la configuración de equipos mediante el sistema operativo RouterOS de MikroTik. De este modo, la propuesta no solo valida técnicamente el diseño de una red de acceso de última milla, sino que también se posiciona como una guía metodológica y didáctica para los estudiantes de Ingeniería en Telecomunicaciones y carreras afines.

1.4 Justificación

La propuesta de este proyecto surge al analizar el panorama de conectividad en diversas zonas de la provincia de Santa Elena, donde el acceso a internet sigue siendo limitado debido a que las operadoras tradicionales suelen descartar el despliegue de infraestructura guiada por sus elevados costos de inversión. Frente a este contexto, las redes WISP representan una alternativa técnica y económicamente viable. Por ello, resulta fundamental contar con espacios académicos de prueba donde se simulen y analicen estas arquitecturas de red bajo criterios rigurosos de ingeniería.

Desde la perspectiva académica y técnica, la implementación de este prototipo dentro del laboratorio de la carrera permite validar las configuraciones en un entorno controlado, garantizando el uso eficiente y normado del espectro radioeléctrico. Asimismo, la puesta en marcha de este modelo físico facilita la observación en tiempo real del comportamiento de protocolos y técnicas de red esenciales, tales como la segmentación de tráfico mediante VLAN, la gestión de acceso a través de autenticación PPPoE y la asignación de recursos mediante colas de prioridad (QoS); conceptos teóricos que adquieren mayor solidez mediante la experimentación práctica. De este modo, la plataforma física queda consolidada como un banco de pruebas para la realización de futuras prácticas estudiantiles e investigaciones.

Finalmente, la documentación detallada del proceso metodológico, del dimensionamiento y de los scripts de configuración se constituye como una guía de referencia para la comunidad académica y profesional. Este aporte busca optimizar los tiempos de implementación y reducir el margen de error técnico en proyectos de redes inalámbricas de acceso de última milla.

1.5 Descripción del proyecto

El proyecto contempla la implementación de un proveedor de servicios de internet inalámbrico (WISP), enfocado en la alineación de parámetros de calidad de servicio (QoS) y seguridad mediante la aplicación de protocolos de red avanzados. La arquitectura está basada en una topología punto a multipunto (PtMP) y consta de tres perfiles de abonado completamente

aislados entre sí, utilizando la segmentación de red por VLAN y esquemas de autenticación basados en credenciales individuales.

En el nodo central se ubica el enrutador principal, responsable de la gestión y administración de la red. Este equipo se encarga de direccionar el tráfico de datos entre los abonados e internet, aplicando reglas de cortafuegos (firewall), marcado de paquetes (mangle) y priorización del tráfico mediante colas de ancho de banda (Simple Queues/Queue Tree) para dar soporte a aplicaciones en tiempo real.

Respecto a la infraestructura de transmisión inalámbrica, la estación base dispone de una antena sectorial configurada bajo el protocolo TDMA (Time Division Multiple Access). Esta tecnología resulta fundamental en entornos WISP, debido a que optimiza la eficiencia del canal radioeléctrico y mitiga el problema del nodo oculto. Adicionalmente, el enlace opera en la banda de frecuencia de 5 GHz, lo que proporciona mayor ancho de banda y menor susceptibilidad a interferencias externas en comparación con bandas saturadas.

Finalmente, en el extremo del usuario se encuentran los equipos en las instalaciones del cliente (CPE, por sus siglas en inglés), los cuales actúan como estaciones remotas encargadas de establecer la conectividad con la estación base y entregar el servicio al abonado final.

1.6 Proceso de implementación

■ Fase 1: Planificación y diseño de la arquitectura

En esta etapa inicial se realiza la simulación y el análisis de cobertura para definir los equipos del laboratorio. El dimensionamiento considera parámetros críticos del enlace inalámbrico, tales como la existencia de línea de vista (LoS, por sus siglas en inglés), la potencia de transmisión, la estimación del ancho de banda, la topología física y lógica más adecuada para satisfacer el tráfico simulado.

■ Fase 2: Configuración lógica y servicios de red

En esta fase se configura el enrutador principal (MikroTik), estableciendo los segmentos de red aislados mediante VLAN para cada perfil de abonado. Asimismo, se define el direccionamiento IP, los rangos de distribución (pools), las reglas de seguridad en el cortafuegos, el

marcado de paquetes (mangle) y las políticas de calidad de servicio (QoS), con el propósito de optimizar la asignación de recursos y el enrutamiento.

- **Fase 3: Configuración de la infraestructura inalámbrica**

Corresponde a la parametrización de las antenas Ubiquiti. La estación base (Access Point) y las estaciones remotas (CPE) se establecen en modo *bridge* transparente para preservar las etiquetas VLAN del segmento lógico. Adicionalmente, se habilita el protocolo propietario TDMA (airMAX) para reducir la latencia, evitar colisiones y optimizar el uso del espectro radioeléctrico.

- **Fase 4: Montaje e integración física**

Comprende el ensamblaje y la interconexión de los componentes dentro del laboratorio de pruebas. Se ubican las antenas respetando la alineación y polarización para maximizar la ganancia del enlace y minimizar pérdidas por desadaptación. De igual manera, se realiza el cableado estructurado y la distribución de energía hacia el nodo principal de enrutamiento.

- **Fase 5: Pruebas de conectividad y evaluación de rendimiento**

Consiste en la validación funcional de la infraestructura desplegada. Se ejecutan pruebas de latencia y alcance mediante herramientas de diagnóstico ICMP (ping y traceroute), seguidas de pruebas de estrés y ancho de banda (utilizando iPerf3 y la herramienta integrada Bandwidth Test) para evaluar la estabilidad, el cumplimiento de los perfiles de QoS y el comportamiento de la red ante escenarios de alta saturación.

- **Fase 6: Monitoreo, gestión y optimización**

En la fase final se integran herramientas de supervisión para analizar el comportamiento del tráfico y el estado de los enlaces en tiempo real. Esto permite identificar cuellos de botella, verificar el consumo de los abonados y realizar los ajustes finos necesarios para garantizar la estabilidad del servicio.

1.7 Beneficios de la implementación

La integración de una arquitectura inalámbrica basada en topología punto a multipunto permite ofrecer conectividad a múltiples usuarios sin la necesidad de desplegar infraestructura física guiada. En el entorno de pruebas, la implementación de una única estación base

sectorial demuestra la capacidad de distribuir el servicio de internet de manera eficiente hacia tres abonados independientes. Esta flexibilidad operativa representa la ventaja competitiva principal de un modelo WISP frente a tecnologías como la fibra óptica o el par de cobre, especialmente en escenarios de topografía compleja.

Por su parte, la adopción del protocolo de acceso múltiple TDMA (airMAX) optimiza sustancialmente la gestión del canal radioeléctrico durante escenarios de alta saturación. Las evaluaciones de carga evidencian que, ante la demanda simultánea del ancho de banda máximo por parte de los tres perfiles de abonado, el sistema mantiene una latencia estable y previene el uso excesivo del recurso por un único nodo. Asimismo, la configuración de políticas de marcación y colas de prioridad (QoS) garantiza la estabilidad del tráfico crítico en tiempo real (como la voz sobre IP y la videoconferencia) del segmento empresarial, independientemente del tráfico de alta densidad generado en otros segmentos de la red.

En materia de seguridad e integridad del tráfico, la combinación de segmentación lógica mediante VLAN y túneles de autenticación punto a punto (PPPoE) establece un aislamiento efectivo a Nivel 2 y Nivel 3 entre los usuarios. Este esquema de seguridad perimetral impide el tráfico no autorizado inter-abonado y restringe el acceso no autenticado a los dispositivos de gestión de la infraestructura, proporcionando una capa de protección robusta frente a arquitecturas de red convencionales.

1.8 Objetivos

1.8.1 *Objetivo general*

Implementar una red de acceso siguiendo los respectivos estándares, normativas y protocolos de red para un proveedor de servicio de internet inalámbrico evaluando su rendimiento en calidad de servicio y ancho de banda en un ambiente controlado.

1.8.2 *Objetivos específicos*

- Identificar los elementos necesarios que componen un proveedor de servicio de internet inalámbrico.
- Implementar infraestructura de red de acceso siguiendo estándares y normativas para un proveedor de servicio de internet inalámbrico.
- Realizar prueba de rendimiento de la red evaluando la calidad de servicio y ancho de banda utilizado por cada abonado.
- Aplicar protocolos de red, para mejorar la eficiencia y estabilidad de la red de acceso.
- Evaluar el impacto de los protocolos de red en términos de calidad de servicio, velocidad, comparando los resultados antes y después de la implementación.

1.9 Resultados esperados

Se espera que, después de la implementación de la red WISP, se logren los resultados con base en los objetivos específicos. En primer lugar, un listado detallado de los equipos a utilizar. En segundo lugar, una correcta implementación de la red de acceso junto con los estándares, protocolos y normativas para una red inalámbrica. Como tercer resultado, gracias a las mediciones obtenidas, se espera detectar de forma clara los principales problemas de la red WISP sin protocolos que garanticen la calidad del servicio; esto da paso al cuarto objetivo donde, mediante los protocolos aplicados para el QoS, se espera tener una red eficiente y estable para el cliente. Como punto final, una vez aplicadas las optimizaciones, se espera el correcto funcionamiento de la red aun cuando se encuentre congestionada por el tráfico.

1.10 Metodología

■ Investigación aplicada

Se enfoca en la aplicación práctica de los conocimientos teóricos adquiridos en la carrera de Telecomunicaciones, mediante la cual se implementará una red inalámbrica punto a multipunto con el uso de equipos reales y protocolos de red para evaluar su desempeño. La finalidad es obtener una solución funcional que pueda ser replicada o usada como base para implementaciones futuras.

■ Investigación descriptiva

Esta investigación permite detallar las características técnicas de los dispositivos utilizados, la topología de red, los protocolos aplicados y los resultados obtenidos. Asimismo, se elaborará un registro detallado de cada etapa del proceso, facilitando su comprensión y replicación.

■ Investigación explicativa

Se utilizará para analizar las causas y efectos del rendimiento de la red antes y después de aplicar protocolos de seguridad y calidad de servicio (QoS). Esto incluye la comparación de métricas como la velocidad de conexión, la estabilidad de la señal, la segmentación de tráfico y el desempeño de las VLAN.

2 CAPÍTULO 2: FUNDAMENTACIÓN TEÓRICA

2.1 Introducción

En este capítulo se establecen las bases conceptuales que sustentan el desarrollo de una red WISP orientada a entregar un acceso inalámbrico seguro y con altos estándares de calidad. Se analizarán aspectos fundamentales para una red inalámbrica, tales como el comportamiento de las ondas de radio, la línea de vista, la zona de Fresnel y otros factores que afectan el rendimiento de la red.

2.2 Conceptos fundamentales de telecomunicaciones

“Una onda de radio es una perturbación física producida por un intercambio energético provocado por fuerzas eléctricas y magnéticas que cambian periódicamente, desplazándose con el tiempo” [7].

2.2.1 *Espectro electromagnético*

La propagación se define como el mecanismo mediante el cual se transporta energía en el espacio y en el tiempo. Por su parte, una onda electromagnética corresponde a la propagación simultánea de campos eléctricos y magnéticos oscilantes, generados por cargas eléctricas en movimiento.

En el área de las telecomunicaciones, el espectro electromagnético se utiliza para la transmisión de información a través de medios no guiados. Las frecuencias empleadas dependen directamente del comportamiento de la onda al interactuar con distintos medios y materiales, dando origen a la radiocomunicación o comunicación inalámbrica.

2.2.2 *Espectro radioeléctrico*

El espectro radioeléctrico hace referencia al conjunto de frecuencias que se usan en las comunicaciones inalámbricas. Estas se dividen y se mencionan según su longitud de onda. A continuación, se mencionan las usadas en telecomunicaciones.

- **Banda VLF:** Se denomina así a las frecuencias muy bajas, entre 10 kHz y 30 kHz. Esta banda se caracteriza por una propagación de onda de tierra, con atenuación débil, siendo una de las bandas más estables; se usa para enlaces de radio a gran distancia.
- **Banda LF:** Esta banda usa frecuencias bajas, entre 30 y 300 kHz. Su uso es similar al de la banda VLF, aunque, al ser menos estable, se emplea comúnmente para enlaces de radio y como banda auxiliar para comunicaciones marítimas y aéreas.
- **Banda MF:** La banda MF está ubicada entre 300 kHz y 3 MHz. Esta es una banda similar a la precedente, pero con una absorción elevada durante el día y propagación predominantemente ionosférica durante la noche; se usa para la radiodifusión.
- **Banda HF:** Para frecuencias entre 3 y 30 MHz, es una banda con propagación predominantemente ionosférica, con fuertes variaciones estacionales y en las diferentes horas del día y de la noche; se usa para comunicaciones de todo tipo a media y larga distancia.
- **Banda VHF:** Ubicada entre 30 y 300 MHz, es una banda con propagación directa y, esporádicamente, propagación ionosférica; se usa para enlaces de radio a corta distancia, televisión y frecuencia modulada.
- **Banda UHF:** Banda entre 300 MHz y 3 GHz, con propagación exclusivamente directa y posibilidad de enlaces por reflexión o a través de satélites artificiales.
- **Banda SHF:** Funciona entre 3 y 30 GHz, con las mismas características que la banda UHF; se usa para radares y enlaces de radio.
- **Banda EHF:** Funciona entre 30 y 300 GHz, con las mismas características y usos que la banda SHF.

Información extraída del artículo de Javier Luque Ordóñez [8].

Tabla 1*Distribución convencional del espectro radioeléctrico y sus aplicaciones típicas.*

Sigla	Denominación	Longitud de Onda	Gama de Frecuenc.	Uso Típico
VLF	Very Low Frequencies Frecuencias muy bajas	30.000 m a 10.000 m	10 kHz a 30 kHz	Enlaces de radio a gran distancia.
LF	Low Frequencies Frecuencias bajas	10.000 m a 1.000 m	30 kHz a 300 kHz	Enlaces de radio a gran distancia, ayuda a la navegación aérea y marítima.
MF	Medium Frequencies Frecuencias medias	1.000 m a 100 m	300 kHz a 3 MHz	Radiodifusión.
HF	High Frequencies Frecuencias altas	100 m a 10 m	3 MHz a 30 MHz	Comunicaciones de todo tipo a media y larga distancia.
VHF	Very High Frequencies Frecuencias muy altas	10 m a 1 m	30 MHz a 300 MHz	Enlaces de radio a corta distancia, televisión, frecuencia modulada.
UHF	Ultra High Frequencies Frecuencias ultra altas	1 m a 10 cm	de 300 MHz a 3 GHz	Enlaces de radio, radar, ayuda a la navegación aérea, televisión.
SHF	Super High Frequencies Frecuencias superaltas	10 cm a 1 cm	de 3 GHz a 30 GHz	Radar, enlaces de radio.
EHF	Extra High Frequencies Frecuencias extra-altas	1 cm a 1 mm	30 GHz a 300 GHz	Como la precedente.
EHF	Extra High Frequencies Frecuencias extra-altas	1 mm a 0,1 mm	300 GHz a 3.000 GHz	Como la precedente.

Nota. Clasificación y distribución convencional adaptada de la reglamentación estándar del espectro radioeléctrico. Obtenido de [9].

2.2.3 Línea de vista

La línea de vista (LoS, por sus siglas en inglés) hace referencia a la trayectoria libre de obstáculos entre las antenas transmisora y receptora. Al desplegar una infraestructura inalámbrica, es fundamental minimizar la cantidad de materiales en la trayectoria de la señal para garantizar una recepción óptima, dado que elementos como el metal o el hormigón generan severas atenuaciones y reflexiones. En particular, la presencia de estructuras metálicas cercanas a la antena provoca reflexiones radioeléctricas que originan desvanecimiento por multicamino (multipath), ocasionando la cancelación parcial o total de la señal principal y reduciendo la calidad del enlace.

Por esta razón, resulta imprescindible instalar las antenas a una altura adecuada que evite bloqueos temporales por el tránsito de vehículos, personas u otros objetos dinámicos. Un emplazamiento a baja altura afecta significativamente la disponibilidad y el rendimiento del enlace cada vez que la línea de vista experimenta una obstrucción.

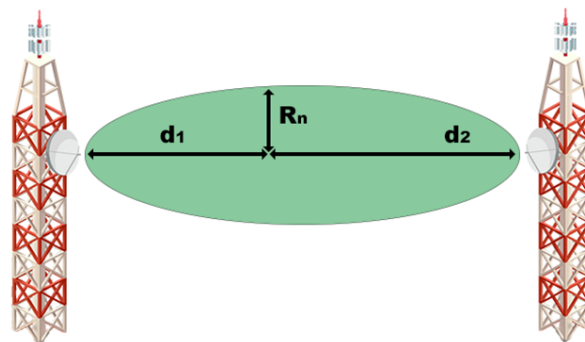
2.2.4 Zona de Fresnel

“Las Zonas de Fresnel son elipsoides que poseen distintos radios cada vez mayores” [10].

A continuación se presenta la ecuación que permite estimar la zona de Fresnel:

Figura 1

Representación geométrica de la primera zona de Fresnel.



Nota. Demostración de la región elipsoidal entre el transmisor y el receptor. Tomado de [10].

En la figura 1 se muestra la forma de la zona de Fresnel; la ecuación que permite estimarla es:

$$R_n = \sqrt{\frac{n * \lambda * d_1 * d_2}{d}} \quad (1)$$

Donde

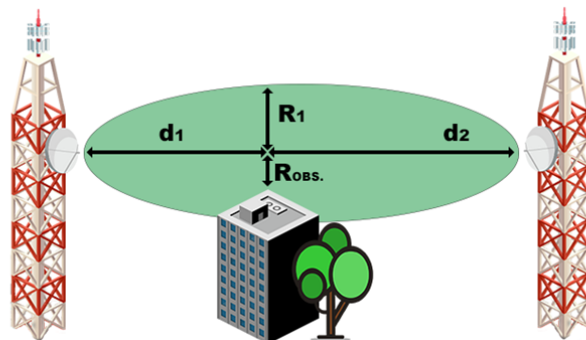
- R_n . – Es la zona de Fresnel
- n . – Es el número de radio de Fresnel
- λ . – Es la longitud de onda del radio enlace
- d_1 . – Distancia desde la antena transmisora al punto en el cual se quiere calcular el radio de Fresnel, en metros
- d_2 . - Distancia restante a la antena receptora, en metros
- d . - Distancia entre la antena receptora y transmisora, en metros.

Por lo general, el cálculo de la zona de Fresnel es en entornos ideales, es decir con línea de vista perfecta, pero en la realidad la mayoría de los enlaces presentan uno o más obstáculos como se muestra en la figura 2, y, para garantizar la estabilidad del enlace, se toma el 60 % de la zona como aceptable, siendo:

$$R = 0,6R_n$$

Figura 2

Efecto de obstrucción en el radio de la zona de Fresnel.



Nota. Impacto de un obstáculo físico invadiendo el radio crítico de despeje de la onda de radio.

Adaptado de D'Angelo [10].

Además, durante el diseño se realiza un estudio de canalización, en el cual se asignan frecuencias a cada enlace para evitar solapamientos con otras redes. Se debe seleccionar cuidadosamente el ancho de banda por canal y la potencia de transmisión, ya que un uso excesivo puede generar interferencias.

2.2.5 Topología de red

La topología de red se refiere a la disposición física y lógica de los nodos y enlaces en una red de computadoras, la cual define la estructura y el modo en que fluyen los datos entre los dispositivos [11].

En este contexto, las redes están constituidas por conjuntos de nodos interconectados; cada nodo integra dispositivos activos como enrutadores, conmutadores, puntos de acceso o estaciones terminales. Por lo tanto, la topología permite describir formalmente cómo se organizan estos componentes entre sí y la dinámica mediante la cual se realiza el transporte de datos a través del medio de transmisión.

2.2.6 Componentes de una topología de red

Dentro del estudio de las topologías de red, se distinguen dos componentes principales: los nodos y los enlaces.

- **Nodos:** Corresponden a los puntos de conexión dentro de la red con capacidad para procesar, enviar y recibir datos. Entre ellos se incluyen dispositivos como estaciones de trabajo, teléfonos móviles, enrutadores, conmutadores, puntos de acceso y otros equipos activos de red.
- **Enlaces:** Constituyen los medios de transmisión que permiten el flujo de información entre los nodos. Estos pueden ser de naturaleza guiada (como cables de cobre, coaxiales o fibra óptica) o no guiada/inalámbrica (utilizando el espectro radioeléctrico como medio de propagación).

2.2.7 Topología física frente a topología lógica

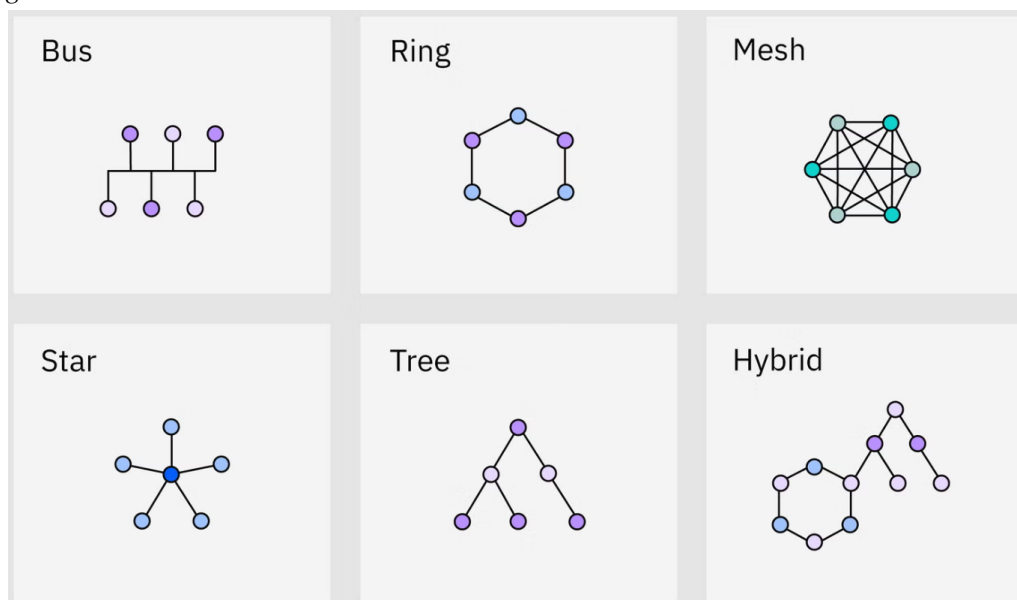
En el diseño y análisis de redes de datos, es fundamental distinguir entre la topología física y la topología lógica. Aunque ambas describen la estructura de la red, lo hacen desde enfoques conceptuales distintos:

- **Topología física:** Se refiere a la disposición espacial y estructural de los componentes de la red. Funciona como un mapa que representa de forma concreta la ubicación de los nodos, los dispositivos de interconexión y los medios de transmisión (como el cableado de cobre, la fibra óptica o los enlaces radioeléctricos).
- **Topología lógica:** Describe la manera en que los datos fluyen a través de la red, independientemente de la distribución física de los dispositivos. En esta topología se definen las rutas que siguen los paquetes de información, las etiquetas de red (como las VLAN) y los protocolos que regulan la transmisión. A diferencia de la topología física, la lógica no necesariamente coincide con el esquema de cableado o cobertura radioeléctrica, ya que las trayectorias de datos están determinadas por los conmutadores, enrutadores y políticas de enrutamiento aplicadas.

2.2.8 Tipos de topologías de red

Figura 3

Topologías de red convencionales.



Nota. Diagrama comparativo de las estructuras físicas y lógicas de red en entornos de telecomunicaciones. Imagen obtenida de [11].

Si bien el diseño de cada red es único debido a las necesidades específicas del entorno, la mayoría de las arquitecturas basan su configuración en una o más topologías. A continuación, se describen los diferentes tipos de topologías físicas utilizados en el despliegue de infraestructuras de telecomunicaciones, clasificación detallada por IBM [11].

Topología punto a punto (PtP). La topología punto a punto es la estructura de red más elemental, ya que conecta únicamente dos nodos mediante un solo enlace dedicado para el intercambio bidireccional de datos. Aunque destaca por su simplicidad de configuración y alto rendimiento de ancho de banda entre ambos extremos, su aplicación resulta limitada cuando se requiere interconectar múltiples usuarios o nodos.

Topología de bus. En la topología de bus, todos los dispositivos se conectan a un único canal o cable central compartido por el cual circula la información. Si bien es una opción

económica y sencilla de desplegar, presenta importantes desventajas: la falla del cable principal interrumpe el servicio en toda la red, existe un mayor riesgo de colisiones de tráfico y la velocidad disminuye drásticamente a medida que se añaden nuevos nodos.

Topología de anillo. En una red en anillo, los equipos se disponen en una trayectoria cerrada donde cada nodo se enlaza directamente con otros dos adyacentes. Aunque ofrece un flujo de datos ordenado, su principal vulnerabilidad radica en la dependencia de cada integrante: si un nodo o enlace falla, se interrumpe la comunicación global. Para solucionar este inconveniente existen las arquitecturas de doble anillo, las cuales añaden una vía concéntrica de respaldo en dirección opuesta para brindar redundancia y alta disponibilidad.

Topología de estrella. En la topología de estrella, todos los equipos terminales se conectan de manera independiente a un dispositivo concentrador central (como un hub o un conmutador de red). Esta estructura facilita la administración, la detección de fallas y la integración de nuevos nodos, ofreciendo aislamiento de averías. Sin embargo, su principal debilidad radica en la dependencia del elemento central, cuyo colapso interrumpe el servicio de toda la red.

Topología de árbol. Esta topología organiza los dispositivos de forma jerárquica combinando las estructuras en estrella y bus. Parte de un nodo raíz principal que se conecta a sub-nodos o conmutadores intermedios, permitiendo centralizar una gran cantidad de equipos y gestionar el tráfico eficientemente. A pesar de que facilita el diagnóstico de fallas a nivel de segmento, mantiene un punto único de falla (Single Point of Failure): si el conmutador raíz colapsa, los segmentos dependientes quedan inoperativos.

Topología de malla. Una red en malla se caracteriza por la redundancia de conexiones directas entre sus nodos. En su versión completa (full mesh), cada dispositivo se enlaza con todos los demás, ofreciendo múltiples rutas de transporte de datos y alta tolerancia a fallos. En la versión parcial (partial mesh), solo ciertos nodos estratégicos disponen de enlaces redundantes para optimizar costos. Aunque es una estructura altamente segura y tolerante a fallas, su implementación física implica un elevado costo de infraestructura, por lo que su uso

suele reservarse para enlaces troncales críticos o redes inalámbricas (Wireless Mesh).

Topología híbrida. La topología híbrida resulta de la combinación de dos o más estructuras de red diferentes (por ejemplo, la integración de una topología en estrella con una en malla) para adaptarse a los requerimientos específicos de diseño. Este modelo permite aprovechar las fortalezas de cada topología individual, como la escalabilidad y la redundancia, aunque incrementa la complejidad del diseño, la configuración y el mantenimiento.

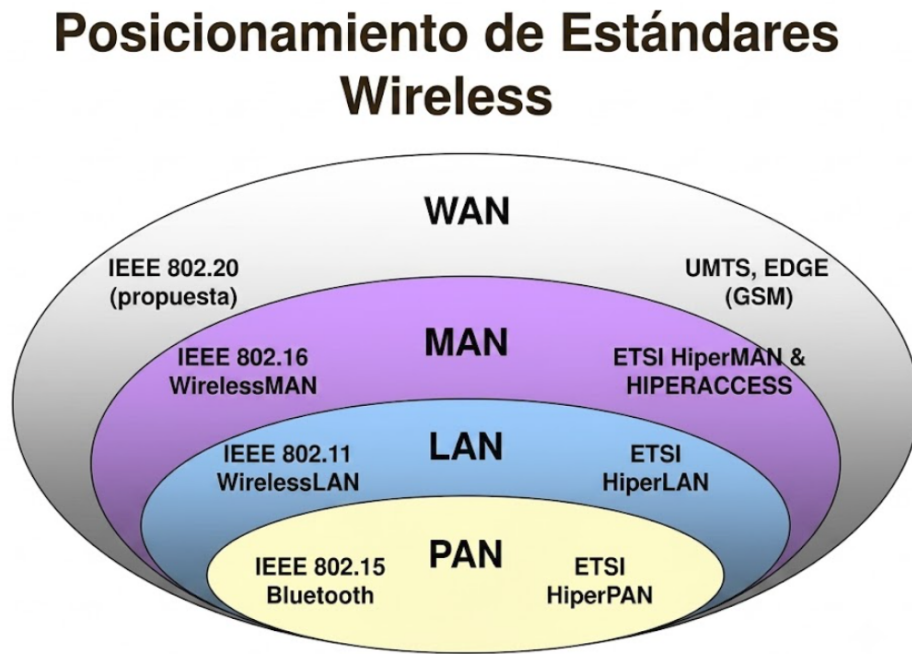
Arquitectura punto a multipunto (PtMP). Las arquitecturas punto a multipunto (PtMP) son ampliamente utilizadas en los proveedores de servicios de internet inalámbrico (WISP) debido a su alta eficiencia, facilidad de despliegue y escalabilidad. Este esquema consta de un nodo central (estación base o Access Point) equipado con antenas de alta ganancia y cobertura sectorial usualmente instaladas en torres de telecomunicaciones que gestiona la comunicación simultánea con múltiples estaciones remotas (CPE) asociadas a los abonados.

A diferencia de las conexiones punto a punto (PtP), que requieren un par de antenas por cada enlace individual, la arquitectura PtMP permite distribuir el servicio a múltiples clientes desde un solo punto emisor. Esto reduce significativamente los costos de infraestructura en el nodo central y facilita la expansión de la red, ya que la incorporación de un nuevo usuario únicamente requiere la instalación y parametrización del equipo cliente remoto.

2.2.9 Clasificación de redes según su distancia

Figura 4

Clasificación de redes según su alcance.



Nota. Posicionamiento de redes según su distancia geográfica. Tomada de [12].

Independientemente de si el despliegue se realiza mediante medios guiados (cableado estructurado) o no guiados (enlaces inalámbricos), las redes de datos se clasifican de acuerdo con su alcance geográfico o área de cobertura. La complejidad y los costos de infraestructura aumentan en proporción al espacio que se requiere abarcar, haciendo que la implementación de medios guiados para grandes extensiones resulte inviable y poco rentable para la mayoría de las organizaciones.

De acuerdo con [13], las redes de datos se categorizan en las siguientes tipologías:

Red de área personal (PAN, *Personal Area Network*). Posee un área de cobertura reducida, limitada a unos pocos metros alrededor del usuario (equivalente al alcance del protocolo Bluetooth o Zigbee). Son estructuras destinadas a entornos compactos e interconexión

de dispositivos de uso personal. Para extender el alcance y evitar el tendido de cables, es habitual realizar la transición hacia redes locales inalámbricas.

Red de área local (LAN, *Local Area Network*). Constituye la infraestructura estándar implementada en edificaciones, entornos corporativos o viviendas. Su objetivo es interconectar estaciones de trabajo y dispositivos compartidos (servidores, impresoras, puntos de acceso) para el intercambio interno de datos. Dependiendo de su diseño físico y tecnología empleada, su alcance abarca habitualmente desde decenas de metros hasta un kilómetro.

Red de área de campus (CAN, *Campus Area Network*). Se aplica cuando la superficie a cubrir excede los límites de una sola edificación y abarca recintos compuestos por múltiples inmuebles o naves industriales. Su arquitectura se basa en la interconexión de varias redes LAN independientes distribuidas estratégicamente, permitiendo el intercambio de datos a alta velocidad y el acceso centralizado a los recursos de red a lo largo de todo el complejo.

Red de área metropolitana (MAN, *Metropolitan Area Network*). Diseñada para dar cobertura a zonas urbanas o metropolitanas extensas, superando sensiblemente el radio de las configuraciones previas. Su aplicación es común en redes gubernamentales, infraestructuras de videovigilancia ciudadana y en los despliegues de fibra óptica (FTTH) de las empresas de telecomunicaciones. Por lo general, una red MAN se encarga de interconectar múltiples redes LAN dentro de un perímetro de hasta 50 kilómetros.

Red de área amplia (WAN, *Wide Area Network*). Es la infraestructura desplegada por los proveedores de servicios de internet (ISP) para resolver las necesidades de conectividad a gran escala. Su alcance supera los límites urbanos y regionales, permitiendo la interconexión entre diferentes ciudades, países o continentes para la conformación de redes globales.

Red de área de almacenamiento (SAN, *Storage Area Network*). Red de alta velocidad dedicada al ámbito corporativo y centros de datos (Data Centers). Su propósito principal es desacoplar el tráfico de almacenamiento masivo del tráfico de la red LAN convencional, evitando la saturación del ancho de banda del usuario final. Esta arquitectura centraliza las unidades de almacenamiento, permitiendo a los servidores acceder a ellas con latencias míni-

mas a nivel de bloque.

Red de área local virtual (VLAN, *Virtual Local Area Network*). A diferencia de los modelos anteriores definidos por límites físicos, las VLAN constituyen agrupaciones lógicas de dispositivos dentro de una misma infraestructura física, gestionadas mediante protocolos (como el estándar IEEE 802.1Q) y configuración de puertos en conmutadores. Esta tecnología permite segmentar redes, aislar dominios de difusión (broadcast), reducir el tráfico innecesario y elevar el nivel de seguridad perimetral sin modificar el cableado existente.

2.3 ¿Qué es una red WISP?

Un proveedor de servicios de internet inalámbrico (WISP, por sus siglas en inglés: *Wireless Internet Service Provider*) es una entidad encargada de suministrar acceso a internet a través de enlaces inalámbricos por radiofrecuencia, en lugar de emplear infraestructura guiada como el par de cobre o la fibra óptica. Este tipo de proveedores gestiona el transporte de datos entre los usuarios finales y el nodo central mediante el despliegue de equipamiento especializado, tales como enrutadores, conmutadores y sistemas radiantes (antenas).

Este modelo de transmisión inalámbrica ha experimentado un crecimiento notable, principalmente en zonas rurales y de difícil acceso, escenarios donde la comunicación por radiofrecuencia representa la alternativa más viable en términos de relación costo-beneficio [14].

A diferencia de los proveedores tradicionales basados en medios guiados, un WISP emplea topologías inalámbricas de cobertura extendida, tales como enlaces punto a punto (PtP) y punto a multipunto (PtMP). En esta arquitectura, el uso de bandas de frecuencia no licenciadas adquiere especial relevancia debido a los marcos regulatorios establecidos por los organismos gubernamentales de telecomunicaciones, como la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL). No obstante, para enlaces dedicados de gran distancia, como los enlaces troncales o estaciones repetidoras interprovinciales, se suele optar por bandas de frecuencia licenciadas para mitigar interferencias. Gracias a esta flexibilidad en el medio de transmisión, las redes WISP ofrecen un despliegue ágil y con costos de inversión inicial reducidos.

La arquitectura fundamental de una red WISP consta de una estación base o nodo central donde se instalan las antenas emisoras de sector o de cobertura omnidireccional y múltiples nodos receptores. Estos últimos corresponden a los equipos en las instalaciones del cliente (CPE), estaciones repetidoras o puntos de acceso. La recepción de la señal y la entrega del servicio en el extremo del abonado se realiza finalmente mediante la interfaz de enrutadores domésticos o residenciales [15].

2.3.1 Componentes de una red WISP

Dentro de la arquitectura WISP, coexiste una variedad de elementos tecnológicos interconectados que aseguran una transmisión de datos eficiente, estable y segura. Los componentes principales de esta infraestructura se desglosan a continuación:

Estaciones base (Nodos centrales). Constituyen el núcleo de la red de distribución radioeléctrica. Están equipadas con antenas sectoriales o multisectoriales de alta ganancia y amplio rango de cobertura, encargadas de propagar la señal hacia los diferentes usuarios. Asimismo, integran dispositivos de enrutamiento y conmutación avanzados, los cuales gestionan el tráfico de los clientes mediante la aplicación de políticas de seguridad, control de ancho de banda y priorización a través de calidad de servicio (QoS).

Equipos en las instalaciones del cliente (CPE y enrutadores domésticos). En el extremo receptor o de última milla se instalan los equipos locales del usuario, conocidos como CPE (*Customer Premises Equipment*). Estas estaciones remotas captan la señal emitida por la estación base y la entregan hacia un enrutador doméstico en el interior del domicilio. Dichos enrutadores gestionan la conectividad lógica de la red interna del usuario, aplicando traducción de direcciones de red (NAT), filtrado de tráfico y esquemas de autenticación para garantizar una salida segura hacia internet.

Sistemas de gestión, monitoreo y alimentación eléctrica. La estabilidad operativa del ecosistema WISP depende de herramientas complementarias críticas, entre las que destacan las plataformas de monitoreo de red, los sistemas de análisis de tráfico y las herramientas de gestión del espectro radioeléctrico para mitigar interferencias. En el plano físico,

la infraestructura de energía desempeña un rol fundamental mediante el uso de inyectores de alimentación a través de ethernet (PoE, *Power over Ethernet*), los cuales permiten energizar los equipos de radiotransmisión mediante el mismo cable de datos UTP/STP, simplificando los despliegues en intemperie.

2.3.2 Requisitos para un WISP



Figura 5

Mapa conceptual de los requisitos técnicos y normativos para un WISP

En la figura 5 se observan los pilares fundamentales requeridos para el despliegue de una red inalámbrica de distribución. Este ecosistema se divide estrictamente en dos vertientes: los lineamientos normativos y las especificaciones técnicas indispensables para su operación.

2.3.3 Marco normativo y regulatorio

Regulación nacional e internacional. El uso del espectro radioeléctrico está estrictamente regulado por organismos estatales en cada país. En Ecuador, esta función le corresponde a la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), entidad encargada de normar, fiscalizar y otorgar los permisos para el uso de frecuencias [16].

Dado que los WISP operan principalmente en bandas de uso libre, deben hacerlo bajo condiciones específicas, orientadas a regular la potencia máxima de emisión, la canalización y las características de las antenas. Asimismo, ARCOTEL establece los procedimientos de registro para los proveedores de servicios de internet, requiriendo su inscripción formal como prestadores de servicios de telecomunicaciones. De igual forma, se exige el cumplimiento de

la normativa sobre protección de datos personales, políticas de uso aceptable y, en determinados casos, metas de conectividad en zonas prioritarias. El incumplimiento de estas regulaciones puede acarrear sanciones económicas o la suspensión del servicio. Por esta razón, los operadores WISP deben mantener su infraestructura alineada con el marco legal vigente en el país, así como con los estándares internacionales de telecomunicaciones promovidos por el IEEE para transmisiones de datos en medios no guiados.

Gestión del espectro y frecuencias. Aunque la mayoría de los despliegues inalámbricos operan en bandas de uso libre tales como la frecuencia de 2.4 GHz, caracterizada por su mayor alcance de propagación, o la de 5 GHz, orientada a mayores velocidades de transmisión, el operador está obligado a respetar minuciosamente las normativas vigentes. Estas regulaciones incluyen los límites de potencia radiada isotrópica efectiva (PIRE/EIRP), la canalización autorizada y los parámetros de emisión para evitar penalizaciones administrativas e interferencias perjudiciales en el espectro.

Políticas de seguridad y privacidad. Desde la perspectiva legal y de cara al usuario, se exige la implementación de políticas transparentes de privacidad y contratos de uso aceptable del servicio. Con el fin de asegurar la protección de datos personales y la integridad de la información de los abonados, es obligatorio desplegar mecanismos robustos de seguridad lógica, tales como el cifrado WPA2/WPA3 y esquemas de autenticación en la red de acceso.

2.3.4 Requisitos y viabilidad técnica

Planificación de enlaces radioeléctricos. El éxito operativo de un WISP radica en la aplicación de buenas prácticas de ingeniería durante la planificación de sus radioenlaces. Esto incluye la ejecución obligatoria de estudios topográficos para garantizar una línea de vista (LoS) totalmente despejada, así como el cálculo matemático preciso de la primera zona de Fresnel, asegurando la ausencia de obstrucciones físicas que puedan degradar la potencia y la estabilidad de la señal.

Optimización del espectro y mitigación de ruido. El área técnica debe realizar análisis continuos del espectro radioeléctrico en las zonas de cobertura. Este diagnóstico permite

identificar y mapear los canales saturados, facilitando una asignación eficiente de frecuencias operativas que minimice el impacto del ruido ambiental en el rendimiento global de la red.

Continuidad del servicio y respaldo energético. Para mitigar el riesgo de interrupciones imprevistas y garantizar los acuerdos de nivel de servicio, la infraestructura de las estaciones base debe contar con sistemas redundantes de respaldo de energía. La implementación de sistemas de alimentación ininterrumpida (UPS), bancos de baterías de ciclo profundo o soluciones fotovoltaicas (paneles solares) asegura la resiliencia y disponibilidad del nodo central ante apagones o fluctuaciones en la red eléctrica pública.

2.4 Infraestructura en redes de acceso

La infraestructura de red constituye la combinación de componentes de hardware y software que hacen posible el funcionamiento de las redes de comunicaciones modernas [17].

Para asegurar que la red se mantenga operativa, la mayoría de las organizaciones integran la gestión de su infraestructura dentro de su planificación estratégica. Esto involucra el uso de herramientas de supervisión, tareas de mantenimiento preventivo y soluciones de seguridad diseñadas para maximizar el rendimiento y la disponibilidad.

Esta infraestructura se compone principalmente de los siguientes elementos:

Componentes esenciales: nodos y direccionamiento IP. Los nodos representan los puntos de conexión de una red en los que residen dispositivos capaces de procesar información (tales como estaciones de trabajo, conmutadores o periféricos). Para que la infraestructura funcione de forma integrada, cada nodo se identifica mediante una dirección IP, la cual constituye un parámetro numérico único que define al dispositivo, su red de origen y su ubicación dentro de la jerarquía de direccionamiento. Este esquema es fundamental en los procesos de comunicación, ya que cada paquete de datos transmitido incorpora las direcciones IP de origen y destino, sirviendo de guía para que los enrutadores determinen la ruta óptima hacia el receptor final.

Equipos de conectividad: enrutadores y conmutadores. Los enrutadores (*routers*) y conmutadores (*switches*) constituyen el núcleo del transporte y conmutación de datos. Un

enrutador se especializa en la interconexión entre redes independientes: analiza los paquetes de información y, mediante tablas y algoritmos de enrutamiento, calcula la ruta más eficiente para transferirlos. En contraste, el conmutador gestiona la conectividad dentro de la red local (LAN); interconecta los dispositivos internos y conmuta los flujos de datos directamente entre los puertos correspondientes, garantizando que el tráfico llegue a su destino específico sin saturar los demás dominios de colisión.

2.5 Servicios de una red WISP

El despliegue de una infraestructura inalámbrica por parte de un proveedor WISP tiene como objetivo primordial la entrega de servicios digitales convergentes y optimizados para satisfacer la demanda de conectividad actual. Al no depender de las limitaciones físicas del cableado en la última milla, estas redes poseen la flexibilidad de empaquetar soluciones adaptadas tanto a las dinámicas de consumo residencial como a los estrictos acuerdos de nivel de servicio corporativos, destacando las siguientes prestaciones principales:

Internet de banda ancha. Este servicio representa la oferta principal de conectividad inalámbrica, diseñado para suministrar tasas de transferencia (velocidades de descarga y carga de datos) adaptadas a las necesidades específicas de cada perfil de cliente. En el entorno residencial, se configuran perfiles de tráfico asimétricos con factores de reúso o agregación orientados al consumo masivo de contenidos multimedia y navegación general. En contraste, para el sector empresarial o corporativo se despliegan enlaces dedicados y simétricos, los cuales aseguran una tasa de transferencia de datos garantizada (CIR, *Committed Information Rate*) y una alta disponibilidad, optimizando el rendimiento de aplicaciones críticas.

Garantía de calidad de servicio (QoS). La calidad de servicio abarca el conjunto de políticas y mecanismos gestionados en la red para garantizar la administración eficiente de los recursos del sistema y la priorización del tráfico. Su implementación resulta indispensable para mitigar la latencia, el tiempo de variación del retardo (*jitter*) y la pérdida de paquetes en servicios en tiempo real, tales como videollamadas, emisiones en directo y telefonía IP (VoIP). Operativamente, su aplicación requiere la clasificación y el marcado previo de los

paquetes en las cabeceras (como el campo DSCP en IPv4/IPv6), junto con la estructuración de árboles de colas jerárquicas (HTB) y algoritmos de ecualización de tráfico (como PCQ) dentro de los enrutadores centrales [18].

2.6 Estándares

2.6.1 *Estándar IEEE 802.11*

La importancia de la familia de estándares IEEE 802.11 radica en su capacidad para regular el uso eficiente del espectro radioeléctrico en las redes de área local inalámbricas (WLAN). Más allá de sus especificaciones a nivel de capa física y de enlace de datos, la adopción de este esquema ha permitido a los fabricantes y proveedores de servicios estandarizar parámetros de interoperabilidad, coberturas y tasas de transferencia.

A continuación, se detalla la evolución cronológica del estándar IEEE 802.11 [19]:

IEEE 802.11. Fue el protocolo pionero de las redes inalámbricas. Operaba exclusivamente en la banda ISM de 2.4 GHz y ofrecía una tasa de transferencia máxima de 2 Mbps, rendimiento limitado para las demandas de los servicios convergentes actuales.

IEEE 802.11a. Migró hacia la banda de frecuencias de 5 GHz con el fin de evadir la saturación de la banda de 2.4 GHz. Introdujo la modulación por división de frecuencias ortogonales (OFDM) para alcanzar velocidades de hasta 54 Mbps. Debido a las propiedades de propagación de los 5 GHz en el espacio libre, poseía un alcance de cobertura más reducido y requería costos de equipamiento más elevados.

IEEE 802.11b. Desarrollado en paralelo a la versión 802.11a, retornó a la banda de 2.4 GHz empleando la técnica de modulación por espectro ensanchado por secuencia directa (DSSS). Suministraba una velocidad máxima de 11 Mbps y, debido a la disparidad de frecuencias y esquemas de modulación, presentaba una incompatibilidad física absoluta con el estándar 802.11a.

IEEE 802.11g. Combinó los beneficios de las dos normas predecesoras al implementar la modulación OFDM dentro de la banda de 2.4 GHz, logrando elevar las tasas de transmi-

sión hasta los 54 Mbps y manteniendo la retrocompatibilidad con la infraestructura basada en 802.11b.

IEEE 802.11n. Marcó un hito en la ingeniería de radioenlaces al introducir la tecnología MIMO (*Multiple-Input Multiple-Output*), la cual permite la transmisión de múltiples flujos espaciales de datos en paralelo. Fue el primer estándar con capacidad de operación en banda dual simultánea (2.4 GHz y 5 GHz), alcanzando anchos de banda teóricos de hasta 600 Mbps y expandiendo significativamente el radio de cobertura.

IEEE 802.11ac. Optimizó la arquitectura inalámbrica mediante la implementación de canales de mayor ancho de banda (hasta 160 MHz) en la banda de 5 GHz y la incorporación de la tecnología DL MU-MIMO (*Downlink Multi-User MIMO*). Esto permitió a los puntos de acceso transmitir tramas de datos a múltiples estaciones receptoras de manera concurrente, optimizando el rendimiento global del espectro.

IEEE 802.11ax. Diseñado para entornos de alta densidad de clientes. Reorganizó la gestión del canal mediante el acceso múltiple por división de frecuencias ortogonales (OFDMA) y la tecnología MU-MIMO bidireccional, incrementando la eficiencia espectral y reduciendo la latencia en las bandas de 2.4 GHz y 5 GHz. Su extensión, Wi-Fi 6E, habilita el acceso a la banda de 6 GHz, agregando espectro adicional completamente libre de interferencias para enlaces de ultra alta velocidad.

IEEE 802.11i (Seguridad en redes inalámbricas). Diseñado específicamente para mitigar las vulnerabilidades de seguridad en el medio inalámbrico, este estándar surgió como una mejora directa sobre el protocolo WPA original. El estándar IEEE 802.11i fundamenta su arquitectura de seguridad en el algoritmo criptográfico de bloque AES (*Advanced Encryption Standard*) y la arquitectura RSN (*Robust Security Network*), garantizando la confidencialidad, autenticidad e integridad de la información en la capa de acceso [20].

2.6.2 IEEE 802.1Q

Este estándar resulta fundamental en la arquitectura de redes locales, ya que permite segmentar una infraestructura física en múltiples redes lógicas e independientes denominadas VLAN. Esta segmentación no solo facilita una administración equitativa y controlada del ancho de banda para cada perfil de usuario, sino que incrementa significativamente la seguridad perimetral al aislar el tráfico entre diferentes departamentos o servicios. Asimismo, el estándar IEEE 802.1Q permite aprovechar un único enlace o puerto troncal para canalizar el tráfico de múltiples redes virtuales, garantizando la integridad y el correcto encaminamiento de las tramas mediante la inserción de una etiqueta de 4 bytes en la cabecera Ethernet.

2.6.3 ANSI/TIA-568

Cableado estructurado para redes modernas. El estándar ANSI/TIA-568 establece las especificaciones de rendimiento y los métodos de instalación para el cableado estructurado en telecomunicaciones, redes empresariales y centros de datos. La relevancia de este conjunto de normas radica en su capacidad para viabilizar la interoperabilidad multifabricante, estandarizar los niveles de eficiencia en las vías de comunicación y salvaguardar la confiabilidad a largo plazo de la infraestructura tecnológica.

Estructura de la familia TIA-568. La familia de estándares TIA-568 se segmenta en normativas específicas para garantizar una cobertura integral del cableado estructurado [21]:

- **ANSI/TIA-568.0-E:** Define los requisitos de arquitectura genérica, rutas, espacios y procedimientos de prueba.
- **ANSI/TIA-568.1-E:** Rige las especificaciones operativas para el cableado dentro de edificios comerciales y enlaces troncales.
- **ANSI/TIA-568.2-E:** Especifica las métricas de rendimiento y transmisión para cables de cobre de par trenzado (Cat 5e, 6 y 6A).
- **ANSI/TIA-568.3-E:** Regula las pautas de diseño y componentes para sistemas de fibra óptica monomodo y multimodo.
- **ANSI/TIA-568.7:** Determina los esquemas de polaridad esenciales para transmisiones dú-

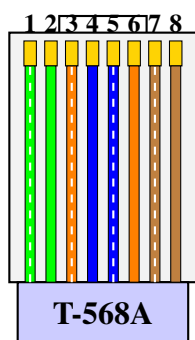
plex y tecnologías de conectores MPO.

Distancias máximas. El estándar TIA-568 especifica distancias máximas de canal para garantizar un rendimiento predecible en el enlace. Para el cableado de cobre de categoría 6A, la distancia máxima permitida en el canal horizontal es de 100 metros (comprendidos por 90 metros de cableado permanente y 10 metros en cables de parcheo o *patch cords*).

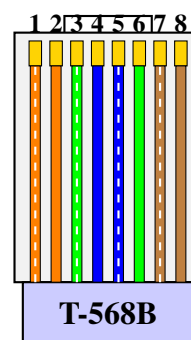
Código de colores. La norma establece códigos de colores estandarizados para facilitar la identificación y ponchado de los conductores en conectores RJ-45, dividiéndose en dos esquemas de patillaje principal:

Figura 6

Distribución de pines y códigos de colores normalizados para conectores RJ-45.



(a) Esquema de conexión T-568A.



(b) Esquema de conexión T-568B.

Nota. Representación gráfica de la distribución interna de los conductores en conectores RJ-45 para cable de par trenzado balanceado. Adaptado de [22].

- **Estándar T-568A:** Utilizado preferentemente en infraestructuras gubernamentales y proyectos específicos de automatización. El orden normalizado de los conductores es el siguiente:

1. Blanco / Verde
2. Verde
3. Blanco / Naranja
4. Azul
5. Blanco / Azul

6. Naranja
7. Blanco / Marrón
8. Marrón

- **Estándar T-568B:** Constituye el esquema de terminación más difundido y adoptado en redes comerciales y corporativas para el cableado estructurado horizontal. El orden normalizado de los conductores es el siguiente:

1. Blanco / Naranja
2. Naranja
3. Blanco / Verde
4. Azul
5. Blanco / Azul
6. Verde
7. Blanco / Marrón
8. Marrón

2.6.4 RFC 1918

El estándar RFC 1918 define las directrices fundamentales para la asignación y gestión del direccionamiento IP privado en redes locales. Con el propósito de mitigar el agotamiento de direcciones IPv4 y evitar colisiones de enrutamiento global, esta normativa reserva de forma estricta los siguientes segmentos de red, los cuales son descartados explícitamente por los enrutadores de la red internet pública [23]:

- **Clase A:** 10.0.0.0 a 10.255.255.255 (bloque 10.0.0.0/8).
- **Clase B:** 172.16.0.0 a 172.31.255.255 (bloque 172.16.0.0/12).
- **Clase C:** 192.168.0.0 a 192.168.255.255 (bloque 192.168.0.0/16).

En consecuencia, estos rangos pueden ser reutilizados de manera independiente en distintas infraestructuras privadas, garantizando la exclusividad de cada dirección únicamente dentro de su propio dominio de difusión. Dado que carecen de alcanzabilidad global en la red WAN, los dispositivos configurados dentro de estos segmentos requieren mecanismos de traducción de direcciones de red (NAT) o servidores intermediarios para establecer flujos de

comunicación con sistemas externos.

2.7 Protocolos

2.7.1 IP (*Internet Protocol*)

Es el protocolo fundamental de la capa de red encargado del direccionamiento lógico y del enrutamiento de los paquetes de datos. En una arquitectura de red de proveedor de servicios de internet inalámbrico (WISP), permite estructurar y segmentar las subredes locales mediante IPv4 o IPv6, asegurando que cada nodo desde los enrutadores principales hasta las estaciones base y los equipos del cliente (CPE) posea una identidad única para el transporte de tráfico [24].

2.7.2 TCP (*Transmission Control Protocol*)

El protocolo de control de transmisión es un estándar de la capa de transporte orientado a conexión, diseñado para garantizar la entrega confiable y ordenada de datos entre aplicaciones a través de redes IP. Incorpora mecanismos de control de flujo, control de congestión y retransmisión de paquetes perdidos mediante confirmaciones de recepción, garantizando la integridad de la información transferida [25].

2.7.3 UDP (*User Datagram Protocol*)

A diferencia de TCP, UDP es un protocolo de la capa de transporte no orientado a conexión ni con control de flujo, lo cual reduce significativamente el encabezado de la trama y la latencia. Resulta óptimo para la transmisión de tráfico en tiempo real o sujeto a limitaciones temporales, tales como transmisiones de video en línea, telefonía IP (VoIP) y consultas DNS. Aunque acelera las comunicaciones, no garantiza la entrega ni el orden de los paquetes, trasladando la gestión de pérdidas a la capa de aplicación [26].

2.7.4 DNS (*Domain Name System*)

El sistema de nombres de dominio es un servicio de la capa de aplicación responsable de la resolución jerárquica de nombres, traduciendo dominios alfanuméricos comprensibles

para el usuario en direcciones IP numéricas requeridas por los dispositivos de red para establecer flujos de comunicación [27].

2.7.5 DHCP (*Dynamic Host Configuration Protocol*)

Este protocolo de la capa de aplicación automatiza la asignación dinámica de parámetros de configuración de red a los dispositivos cliente o hosts que solicitan acceso a la infraestructura. Además de proveer direcciones IP únicas dentro del segmento, DHCP gestiona la entrega de componentes genéricos indispensables para la conectividad, tales como máscaras de subred, puertas de enlace predeterminadas y servidores DNS, facilitando tanto la comunicación local como el enrutamiento hacia la red WAN [28].

2.7.6 RSTP (*Rapid Spanning Tree Protocol*)

Protocolo de la capa de enlace de datos (IEEE 802.1w) desarrollado como una evolución directa del protocolo Spanning Tree (STP) para mitigar sus tiempos de convergencia. A diferencia de STP, que requiere entre 30 y 50 segundos para reestructurar la topología, RSTP introduce roles de puerto alternativos y de respaldo, así como estados de puerto simplificados que permiten reconfigurar la red en milisegundos ante el fallo de un enlace principal [29]. Esta rápida convergencia es crítica en infraestructuras WISP para mantener la redundancia en los anillos de distribución inalámbricos y evitar bucles de conmutación.

2.7.7 Protocolo PPPoE (*Point-to-Point Protocol over Ethernet*)

PPPoE es un protocolo de encapsulamiento utilizado por los proveedores de servicios de internet (ISP/WISP) para gestionar el control de acceso, la autenticación de usuarios mediante credenciales y la asignación dinámica de parámetros de red y perfiles de ancho de banda [30]. Al migrar la arquitectura de acceso hacia un servidor PPPoE, se elimina la vulnerabilidad asociada a los entornos DHCP abiertos y se optimiza el rendimiento del enrutador central en escenarios de alta densidad de clientes.

2.7.8 SSH (*Secure Shell*)

SSH es un protocolo de capa de aplicación que proporciona un canal de comunicación cifrado y seguro para la administración remota de dispositivos de red a través de redes no seguras [31]. En el contexto operativo de un WISP, SSH cifra el tráfico de gestión —incluyendo credenciales de acceso y comandos de la interfaz de línea de comandos (CLI), protegiendo la administración de los enrutadores y puntos de acceso contra interceptaciones no autorizadas en los enlaces de radio.

2.8 Tecnologías

2.8.1 *airMAX*

airMAX es una tecnología propietaria desarrollada por Ubiquiti Networks para la optimización de enlaces inalámbricos de banda ancha. A diferencia del protocolo estándar Wi-Fi (IEEE 802.11) basado en contención de medio (CSMA/CA), airMAX implementa un esquema de acceso al medio por multiplexación por división de tiempo (TDMA). Mediante este mecanismo, el punto de acceso (AP) actúa como un controlador centralizado que asigna intervalos de tiempo dinámicos e individuales a cada estación cliente (CPE) para la transmisión y recepción de tramas.

Esta asignación programada elimina las colisiones por nodo oculto, reduce sustancialmente el retraso en la red y optimiza la eficiencia del espectro radioeléctrico. Como resultado, airMAX mantiene un alto rendimiento (*throughput*) y una baja latencia, incluso en escenarios de alta densidad de clientes o entornos con elevado ruido radioeléctrico.

2.8.2 *RouterOS*

RouterOS es el sistema operativo propietario desarrollado por MikroTik, diseñado para transformar hardware dedicado (RouterBOARD) o arquitecturas basadas en x86 en enrutadores de red de alto rendimiento. Ofrece versatilidad operacional al permitir la gestión del sistema tanto a través de una interfaz de línea de comandos (CLI) para la ejecución de automatizaciones mediante scripts, como mediante una interfaz gráfica dedicada denominada

WinBox.

En el contexto de las arquitecturas WISP, RouterOS provee un conjunto integral de herramientas y protocolos de red, entre los que destacan:

- **Seguridad y tunelización:** Soporte nativo para IPsec, WireGuard y servicios VPN para la interconexión de nodos.
- **Segmentación de tráfico:** Configuración avanzada de redes de área local virtuales (VLANs) para el aislamiento de tramas de clientes y gestión.
- **Gestión de direccionamiento y perimetral:** Implementación de traducción de direcciones de red (NAT), enmascaramiento (*masquerade*) y filtrado mediante un motor de *firewall* de inspección de estado.
- **Gestión remota:** Integración del servicio MikroTik Cloud (IP Cloud y DDNS), habilitando la administración remota de los nodos de la red sin requerir una dirección IP pública estática dedicada en la interfaz de gestión.

2.9 Mecanismos de control de tráfico y calidad de servicio

2.9.1 Clasificación, diferenciación y marcado de tráfico (*Firewall Mangle*)

El marcado de paquetes mediante la herramienta *Mangle* es una función especializada del motor de *firewall* de MikroTik RouterOS que opera en las etapas iniciales del flujo de procesamiento de tramas. Su propósito principal es interceptar el tráfico, evaluar las propiedades presentes en las cabeceras de red o transporte y asociarles marcas lógicas internas. Estas marcas son transparentes para el usuario final y resultan indispensables para que otros subsistemas del router tales como las tablas de enrutamiento o el árbol de colas de prioridad apliquen políticas de gestión de ancho de banda y priorización [32].

De acuerdo con la documentación oficial de RouterOS, el procesamiento en la herramienta *Mangle* se rige por un conjunto de cadenas de flujo, acciones operativas y parámetros de optimización clave.

Cadenas de procesamiento (*Chains*). El tráfico que atraviesa el enrutador se evalúa en distintas etapas del flujo de paquetes mediante cadenas predefinidas, siendo las más rele-

vantes para la ingeniería de tráfico:

- **Prerouting:** Es la primera cadena que procesa el tráfico entrante. Evalúa los paquetes inmediatamente después de ser recibidos en la interfaz física o virtual, antes de que el procesador tome cualquier decisión de enrutamiento (*routing decision*). Constituye el punto óptimo para realizar marcados de conexión basados en subredes de origen o puertos de entrada.
- **Forward:** Procesa exclusivamente el tráfico de tránsito que atraviesa el enrutador desde una interfaz hacia otra (por ejemplo, desde los segmentos de clientes hacia la interfaz WAN de salida), sin que los paquetes estén destinados al propio sistema operativo local.
- **Postrouting:** Es la última cadena de evaluación por la que transita el tráfico saliente, justo antes de ser transmitido físicamente por la interfaz de red correspondiente.

Acciones operativas críticas. El comportamiento del filtro *Mangle* depende de la acción asignada a las reglas cuyos criterios de coincidencia (*matchers*) resultan positivos:

- **mark-connection (Marcado de conexión):** Asigna una etiqueta de seguimiento a la totalidad del flujo de comunicación bidireccional. Esta acción optimiza sustancialmente el uso del procesamiento, ya que permite identificar sesiones completas analizando únicamente el paquete inicial de establecimiento de conexión.
- **mark-packet (Marcado de paquete):** Asigna una marca de tráfico a paquetes de datos individuales. A diferencia de las marcas de conexión, las marcas de paquete son los únicos identificadores que el motor de colas jerárquicas (HTB) puede interpretar para aplicar limitadores de velocidad y colas de prioridad.
- **passthrough (Tránsito continuo):** Es un parámetro booleano esencial para la eficiencia lógica de la tabla de reglas:
 - Si se configura en *yes*, el paquete recibe la marca actual y continúa descendiendo en la lista para ser evaluado por las reglas subsiguientes.
 - Si se establece en *no*, el procesamiento dentro de esa cadena finaliza inmediatamente para el paquete evaluado, evitando que reglas posteriores sobrescriban la marca asignada y reduciendo la carga de CPU en la plataforma.

2.9.2 Algoritmos de distribución equitativa del canal (*Per Connection Queueing - PCQ*)

El algoritmo *Per Connection Queueing* (PCQ) es un tipo de encolamiento avanzado desarrollado por MikroTik, diseñado específicamente para simplificar la administración de ancho de banda en redes con una gran cantidad de usuarios activos para entornos de ISP. Su objetivo principal es automatizar la asignación de recursos sin requerir la creación manual de colas individuales para cada abonado [33].

De acuerdo con la documentación oficial de RouterOS, el algoritmo funciona tomando el flujo de tráfico global de una cola principal y subdividiéndolo de manera dinámica en múltiples sub-colas o sub-flujos (*sub-streams*) basados en clasificadores específicos.

Parámetros de configuración y control de PCQ. La optimización y el comportamiento del algoritmo PCQ dentro de RouterOS se definen mediante los siguientes parámetros clave:

- **PCQ Classifiers (Clasificadores):** Determinan cómo se agrupa el tráfico para generar las sub-colas dinámicas, el enrutador analiza las cabeceras de los paquetes utilizando los siguientes criterios principales:
 - *src-address* (Dirección de origen): Agrupa los paquetes por la IP del emisor y es utilizado típicamente para controlar el tráfico de subida (*upload*), donde cada cliente genera su propio sub-flujo de salida.
 - *dst-address* (Dirección de destino): Agrupa los paquetes por la IP del receptor y permite controlar el tráfico de descarga (*download*), garantizando que cada usuario reciba su parte correspondiente de datos.
 - *src-port* y *dst-port*: Permiten una subdivisión aún más granular, creando sub-colas individuales para cada puerto de origen o destino (aplicaciones específicas).
- **PCQ Rate (Tasa de velocidad):** Define la velocidad máxima asignada a cada sub-cola individual.
 - Si se configura con un valor específico (por ejemplo, *pcq-rate=10M*), cada sub-flujo activo tendrá un límite estricto de velocidad de 10 Mbps.
 - Si se configura en cero (*pcq-rate=0*), el algoritmo PCQ dividirá el ancho de banda total

disponible de la cola padre de manera completamente equitativa entre todas las sub-colas que demanden tráfico en ese instante.

- **PCQ Limit (Límite por sub-cola):** Especifica la cantidad máxima de datos que una sub-cola dinámica de usuario puede retener en memoria antes de comenzar a descartar paquetes (*tail drop*).
- **PCQ Total Limit (Límite global):** Define la capacidad máxima de almacenamiento acumulada de todas las sub-colas PCQ combinadas. Es un mecanismo de seguridad para evitar que el motor de colas sature la memoria RAM del enrutador bajo condiciones extremas de congestión.

Dinámica de asignación y comportamiento del tráfico. Cuando se activa el clasificador (por ejemplo, por *dst-address* para descarga), el algoritmo rastrea activamente qué direcciones IP están transmitiendo datos. Si un solo usuario está activo, este puede consumir la totalidad del canal disponible, siempre que el *pcq-rate* esté en 0 o sea lo suficientemente alto.

En el momento en que se detectan nuevos flujos provenientes de diferentes direcciones IP, el algoritmo reasigna los recursos en tiempo real, dividiendo el canal de forma matemática y justa. Esto previene eficazmente que un único usuario consuma de manera egoísta todo el canal disponible con aplicaciones de descarga masiva, garantizando la equidad de acceso a nivel de capa de red.

2.9.3 Asignación jerárquica de recursos (*Hierarchical Token Bucket - HTB*)

El algoritmo *Hierarchical Token Bucket* (HTB) es el método de encolamiento y modelado de tráfico por defecto en MikroTik RouterOS para la gestión de estructuras complejas. Su propósito principal es segmentar y distribuir el ancho de banda global de manera jerárquica a través de una estructura de árbol, permitiendo a su vez el reuso eficiente del canal físico de transmisión. [34]

De acuerdo con las especificaciones de diseño de RouterOS, el árbol HTB clasifica los elementos de su estructura en dos tipos de nodos o colas:

- **Hojas (Leaf Queues):** Son los nodos terminales del árbol que no poseen colas hijas. Estas

son las únicas que almacenan físicamente los paquetes en buffers de memoria y aplican directamente los algoritmos de encolamiento seleccionados.

- **Nodos internos o padres (Inner Queues):** Son aquellos nodos intermedios que tienen al menos una cola hija asociada. No almacenan paquetes directamente en buffers; su única función dentro de la arquitectura es la distribución lógica de tokens de ancho de banda y la gestión de los préstamos de recursos entre sus respectivas colas hijas.

El sistema de límites duales (CIR y MIR). La asignación de recursos dentro del esquema HTB de RouterOS se rige estrictamente por dos parámetros de velocidad configurados de forma individual en cada nodo:

1. **Limit-at (Committed Information Rate - CIR):** Representa el ancho de banda mínimo garantizado que el enrutador reserva y asegura para una cola específica, incluso bajo el peor escenario de congestión generalizada en la red.
2. **Max-limit (Maximum Information Rate - MIR):** Establece el techo máximo de velocidad que la cola puede alcanzar, es decir un flujo de datos jamás superará este límite, aun cuando exista ancho de banda excedente y libre en la red de acceso.

El algoritmo de decisión de tres estados (Semáforo HTB). Para calcular dinámicamente cómo distribuir el ancho de banda en tiempo real, el motor HTB de MikroTik evalúa de forma continua el estado operativo de cada cola basándose en un sistema de tres colores o estados lógicos, los cuales determinan la acción del planificador sobre el flujo de paquetes:

- **Estado Verde (Satisfecho):** Se presenta cuando el tráfico actual de la cola es menor o igual a su parámetro *limit-at*. Las colas en estado verde se procesan con la máxima prioridad de despacho. No requieren préstamo de recursos del nodo padre y su entrega de ancho de banda está 100 % asegurada.
- **Estado Amarillo (Préstamo):** Se activa en el momento en que el tráfico de la cola supera su valor de *limit-at*, pero se mantiene por debajo de su *max-limit*. En este escenario, la cola consume tokens adicionales solicitando un préstamo de ancho de banda a su cola padre, sujeto a la disponibilidad del canal común.
- **Estado Rojo (Limitado):** Ocurre cuando la cola ha alcanzado su límite *max-limit*. El al-

goritmo HTB bloquea el despacho de paquetes adicionales para este flujo, procediendo a descartar los paquetes o retenerlos en el búfer físico hasta que existan nuevos tokens de transmisión disponibles.

Los parámetros de prioridad van de 1 a 8, donde 1 representa la prioridad máxima y 8, la prioridad mínima. Mientras las colas se mantengan en estado verde, el enrutador entregará el tráfico de forma equitativa, independientemente del nivel de prioridad asignado, gracias al cumplimiento garantizado del CIR de cada abonado.

2.10 Mecanismos de seguridad y mitigación de vulnerabilidades

2.10.1 NAT (*Network Address Translation*)

NAT es una técnica que utilizan los proveedores de servicio de internet y organizaciones para permitir que múltiples dispositivos compartan una sola dirección IP pública. Al usar NAT, los dispositivos en una red privada pueden comunicarse con dispositivos en una red pública sin la necesidad de que cada dispositivo tenga su propia dirección IP única. [35]

¿Cómo funciona NAT?.

NAT se ejecuta en el enrutador de borde, el cual se encarga de conectar dos redes, la local y la global. La función principal de esta técnica es interceptar el tráfico saliente de la red local y sustituir la IP privada, como 192.168.0.23, por una pública, como 203.0.113.45, para enviarla a su destino. Una vez procesada la petición, al momento de ingresar de nuevo a la red local, el enrutador vuelve a cambiar la IP pública por una IP interna, para que los datos lleguen al dispositivo correcto.

¿Por qué es importante el NAT?.

La traducción de direcciones de red es el pilar fundamental de toda red en telecomunicaciones. A continuación, se presentan algunas ventajas mencionadas por [35]:

- **Preservación de direcciones IP:** Resuelve el problema del agotamiento de IPv4 al permitir que múltiples dispositivos dentro de una red local compartan una única dirección IP pública para comunicarse con el exterior.
- **Seguridad:** Funciona como una barrera defensiva, al ocultar las direcciones IP privadas

de los equipos internos frente a internet, lo que dificulta que atacantes externos localicen o accedan directamente a los equipos de la red.

- **Flexibilidad de diseño:** Permite modificar la estructura de la red interna, con cambio de IPs o nuevos dispositivos sin alterar la forma en que la red se muestra a internet.
- **Redundancia y alta disponibilidad:** Facilita la conexión simultánea a varios proveedores de internet: en caso de que una línea de internet se caiga, el tráfico se redirige de forma automática por la otra línea, garantizando que nunca se pierda la conexión.
- **Reducción de costos:** Evita que las empresas tengan que pagar tarifas elevadas a sus proveedores de internet por el alquiler de múltiples direcciones IP públicas.
- **Gestión simplificada:** Al disminuir la cantidad de direcciones IP públicas que se deben configurar y monitorear, la administración de la red se vuelve mucho más ágil y eficiente para los equipos de TI.

La seguridad en las redes de acceso del WISP está diseñada aplicando políticas de control de tráfico dirigidas tanto al propio enrutador como a los paquetes que transitan a través de la red.

2.10.2 Filtrado de paquetes y mitigación de amenazas (*Firewall Filter*)

El filtrado de paquetes en MikroTik RouterOS se ejecuta a través de la herramienta *Firewall Filter*, la cual inspecciona el flujo de datos y aplica reglas de seguridad para permitir o denegar el paso de paquetes. Este opera bajo un modelo de inspección de estado de conexiones (*Stateful Firewall*), procesando los paquetes de manera secuencial de arriba hacia abajo dentro de cadenas predefinidas. [36]

Cadenas de flujo estándar (Default Chains). El motor de filtrado organiza el tráfico en tres cadenas principales según el destino y origen del paquete en relación con el propio enrutador:

- **input:** Se aplica a los paquetes que entran al enrutador a través de una de sus interfaces y cuyo destino final es el propio sistema operativo del dispositivo, por ejemplo, peticiones de gestión como Winbox, SSH o servicios locales de infraestructura como DNS y DHCP.
- **forward:** Procesa los paquetes que transitan a través del enrutador, es decir, que ingresan

por una interfaz física o lógica y salen por otra con destino a un host externo, como el tráfico de navegación de los usuarios de las VLANs hacia la WAN.

- **output:** Evalúa los paquetes que son originados directamente por el propio enrutador y que son enviados hacia el exterior a través de cualquiera de sus interfaces de red.

Mecanismo de inspección de estado (Connection Tracking). El firewall de Mikro-Tik es altamente eficiente debido a que no analiza cada paquete como un elemento aislado, sino como parte de un flujo lógico mediante el seguimiento de conexiones (*connection tracking*). Esto clasifica los paquetes en cuatro estados de conexión fundamentales:

- **established (Establecida):** Paquetes que pertenecen a una conexión existente y bidireccional que ya ha sido aprobada previamente por el firewall.
- **related (Relacionada):** Paquetes que, aunque abren una nueva sesión de comunicación, están directamente asociados a una conexión establecida previamente; por ejemplo, flujos auxiliares de protocolos de transferencia o señalización.
- **new (Nueva):** Paquetes que intentan iniciar una conexión de comunicación inédita que no ha sido registrada por el sistema de seguimiento.
- **invalid (Inválida):** Paquetes que no pertenecen a ninguna conexión conocida, que carecen de una estructura válida o que no siguen la secuencia correcta del protocolo de comunicación.

Acciones operativas del firewall. Cuando un paquete de datos coincide con los criterios definidos en una regla, el enrutador interrumpe la lectura de la lista y ejecuta de forma inmediata una de las siguientes acciones configuradas:

- **accept:** El paquete es aprobado y se le permite continuar su tránsito a través de la cadena sin ser evaluado por las reglas inferiores.
- **drop:** El paquete es descartado de forma silenciosa por el enrutador. No se envía ningún mensaje de notificación de error al host de origen, lo cual es altamente recomendado en redes públicas para mitigar el escaneo de puertos.
- **reject:** El paquete es descartado inmediatamente, pero el enrutador envía un paquete ICMP de notificación de error (como *destination-unreachable*) de vuelta al emisor, informándole

que la conexión ha sido rechazada explícitamente.

2.10.3 Aislamiento lógico e inter-VLAN de abonados

El aislamiento de abonados en una red de acceso WISP requiere una segmentación estricta desde el nivel de acceso físico hasta la capa de enrutamiento lógico. De acuerdo con la documentación de MikroTik RouterOS, esto se logra mediante la implementación de la función *Bridge VLAN Filtering*, una característica que permite al enrutador comportarse como un conmutador de Capa 2 compatible con el estándar IEEE 802.1Q, controlando de manera rigurosa el tránsito de tramas etiquetadas y no etiquetadas [37].

Mecanismo de operación en Capa 2 (*Bridge VLAN Filtering*). Por defecto, un puente lógico (*bridge*) en RouterOS permite que todos los dispositivos conectados se comuniquen libremente dentro de un mismo dominio de difusión. Al activar el parámetro `vlan-filtering=yes`, el enrutador habilita la inspección estricta dentro de la tabla de VLANs del *bridge*, aplicando las siguientes reglas de conmutación:

- **Puertos de acceso (*Access Ports / Untagged*):** Asocian interfaces físicas a un identificador de VLAN nativo (*PVID / Port VLAN ID*). Al ingresar una trama sin etiqueta a un puerto de acceso, el *bridge* le asigna internamente el PVID correspondiente; del mismo modo, al transmitir la trama hacia el dispositivo final, la etiqueta IEEE 802.1Q se remueve automáticamente.
- **Puertos troncales (*Trunk Ports / Tagged*):** Permiten transportar tráfico perteneciente a múltiples VLANs a través de un único enlace físico. El *bridge* inspecciona el identificador de VLAN (*VLAN ID*) de cada trama entrante y descarta cualquier paquete cuya etiqueta no esté explícitamente permitida en la tabla de VLANs del puerto.

Principio de aislamiento y enrutamiento inter-VLAN. El aislamiento lógico de abonados se fundamenta en que las tramas de datos no pueden conmutarse entre distintas VLANs en Capa 2. Por ejemplo, si un host perteneciente a la subred *VLAN 30-EMP* intenta comunicarse con un host de la *VLAN 50-STD*, los conmutadores y puntos de acceso bloquearán el tráfico en el dominio de conmutación al carecer de un identificador común.

Para que dicha comunicación sea posible, el tráfico debe ser elevado a la Capa 3 (enrutamiento inter-VLAN). Esto permite al enrutador central evaluar las políticas de seguridad mediante reglas de *firewall*, aplicando un filtrado perimetral estricto que restringe el tráfico entre abonados antes de autorizar cualquier flujo de datos.

2.10.4 Robustecimiento del plano de control

El plano de control de un enrutador es responsable de la toma de decisiones de enrutamiento y de la administración del sistema. Su exposición degrada la seguridad del nodo y compromete la disponibilidad del servicio ante ataques de denegación de servicio (DoS) o accesos no autorizados. De acuerdo con MikroTik RouterOS, el robustecimiento de este plano se ejecuta de manera rigurosa mediante la administración del módulo de servicios IP. [38]

Este mecanismo de defensa reduce los ataques del sistema mediante tres directivas de seguridad fundamentales:

Desactivación de sistemas inseguros. Por defecto, RouterOS mantiene activos múltiples servicios de administración y transferencia. En una arquitectura robusta, se aplica el principio de mínimo privilegio, donde se busca desactivar de forma inmediata los protocolos que transmiten credenciales en texto plano o que no son requeridos para la operación del WISP:

- **Telnet y FTP (Puertos 23 y 21):** Deshabilitados debido a la ausencia de cifrado en el canal de comunicación, lo que expone las credenciales de administración a técnicas de escucha activa (*sniffing*).
- **API y API-SSL (Puertos 8728 y 8729):** Desactivados a menos que se integren sistemas externos de aprovisionamiento automático de usuarios, como un software de facturación o CRM automatizado.
- **HTTP / www (Puerto 80):** Deshabilitado en favor de accesos cifrados, mitigando la interceptación de la interfaz gráfica web.

Restricción por direccionamiento de origen. La medida de seguridad más efectiva del motor de servicios de RouterOS es el parámetro `address`. Este atributo permite definir una lista de control de acceso en segundo plano.

Incluso si un atacante conoce el puerto y las credenciales de administración, el enrutador descartará la conexión en la capa de transporte si el paquete no se origina desde un prefijo IP estrictamente autorizado, por ejemplo, la subred exclusiva de la VLAN de administración 10.10.10.0/24.

Ofuscación de puertos de enlace. Consiste en modificar los puertos estandarizados por defecto para los servicios que permanecen activos, como el puerto 22 utilizado por SSH, hacia un puerto alto aleatorio.

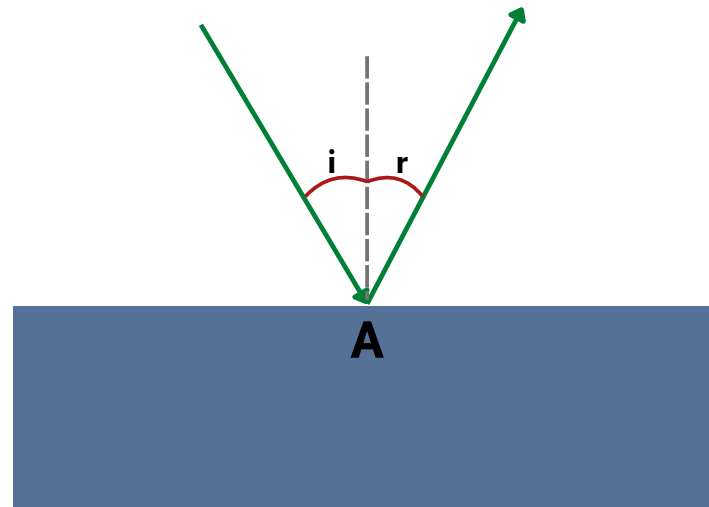
2.11 Fenómenos físicos de la propagación de onda

En una red WISP, la propagación de la onda de radio es de suma importancia para garantizar la calidad de servicio y una seguridad robusta. Al propagarse, esta atraviesa diferentes medios que degradan la señal; a este fenómeno se le llama atenuación de onda, la cual puede ser provocada por:

2.11.1 Reflexión

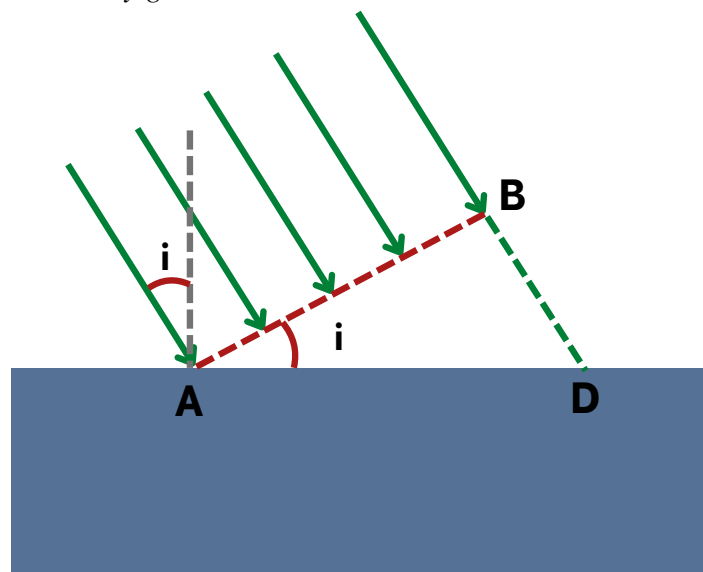
La reflexión es el fenómeno por el cual una onda, al incidir sobre el límite de separación de dos medios con propiedades diferentes, cambia su dirección de propagación sin cambiar de medio.

Figura 7
Frente de onda plano incidente



Consideremos un frente de onda plano que incide sobre una superficie reflectante lisa, como se ilustra en la Figura 7, su dirección de propagación es perpendicular a estas. El ángulo i representa el ángulo de incidencia, medido entre la dirección de propagación y la normal a la superficie en el punto de incidencia.

Figura 8
Reflexión del frente de onda y generación de ondas secundarias

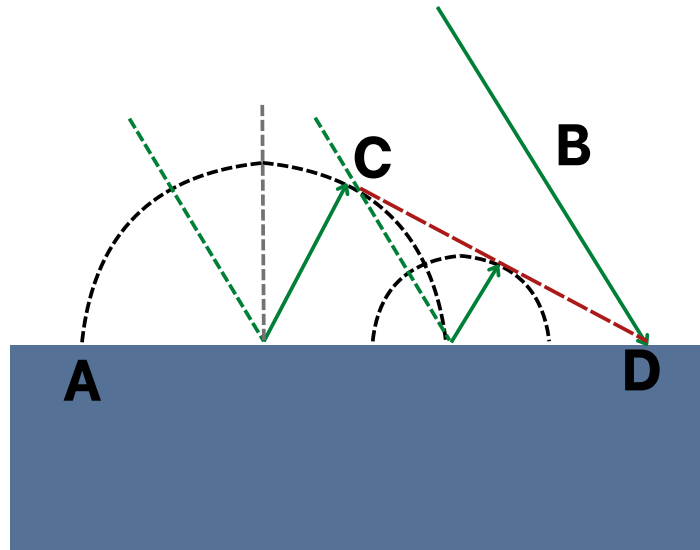


Según el principio de Huygens, cada punto de un frente de onda actúa como una fuente de ondas. Al llegar el frente de onda al punto A de la superficie, este punto se convierte en

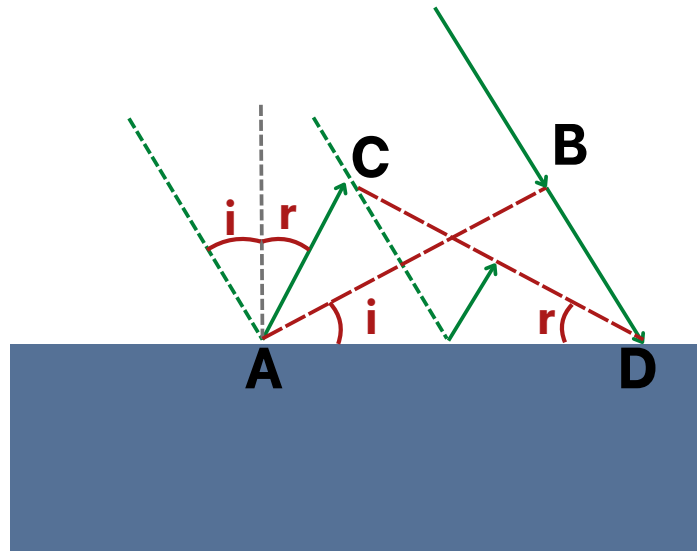
un nuevo centro de emisión. Mientras la parte del frente de onda en **A** ya está generando una onda reflejada, la parte del frente de onda en **B** aún no ha alcanzado la superficie.

Figura 9

Formación del frente de onda reflejado



Para el instante de tiempo t que tarda el punto **B** en alcanzar la superficie en **D**, el punto **A** ha emitido una onda reflejada que se ha propagado una distancia **AC** en el mismo tiempo t . La nueva posición del frente de onda reflejado será la envolvente de todas las ondículas secundarias emitidas por los puntos de la superficie. Como se observa en la Figura 9, la distancia recorrida por la onda incidente de **B** a **D** es $\mathbf{BD} = \mathbf{v} \cdot \mathbf{t}$, donde $\mathbf{v}$ es la velocidad de propagación de la onda en el medio. Del mismo modo, la distancia **AC** de la ondícula reflejada desde **A** es $\mathbf{AC} = \mathbf{v} \cdot \mathbf{t}$.

Figura 10*Geometría para la deducción de la ley de reflexión*

A partir de la geometría de los triángulos rectángulos $\triangle ABD$ y $\triangle ACD$ de la figura 10, y considerando que $BD = AC = vt$, ya que la velocidad de la onda es la misma en el mismo medio, podemos establecer las siguientes relaciones trigonométricas:

$$\sin i = \frac{\text{cateto opuesto}}{\text{hipotenusa}} = \frac{BD}{AD} = \frac{vt}{AD}$$

$$\sin r = \frac{\text{cateto opuesto}}{\text{hipotenusa}} = \frac{AC}{AD} = \frac{vt}{AD}$$

Dado que las expresiones para $\sin i$ y $\sin r$ son idénticas, se deduce que:

$$\sin i = \sin r$$

$$i = r$$

Esta relación fundamental se conoce como la **ley de reflexión**, y establece que el ángulo de incidencia es igual al ángulo de reflexión. Además, los rayos incidente, reflejado y la normal a la superficie en el punto de incidencia se encuentran en el mismo plano.

La reflexión no es siempre sinónimo de pérdida de señal, por el contrario, existen técnicas que aprovechan la reflexión de una señal, por ejemplo, cuando existe un obstáculo de

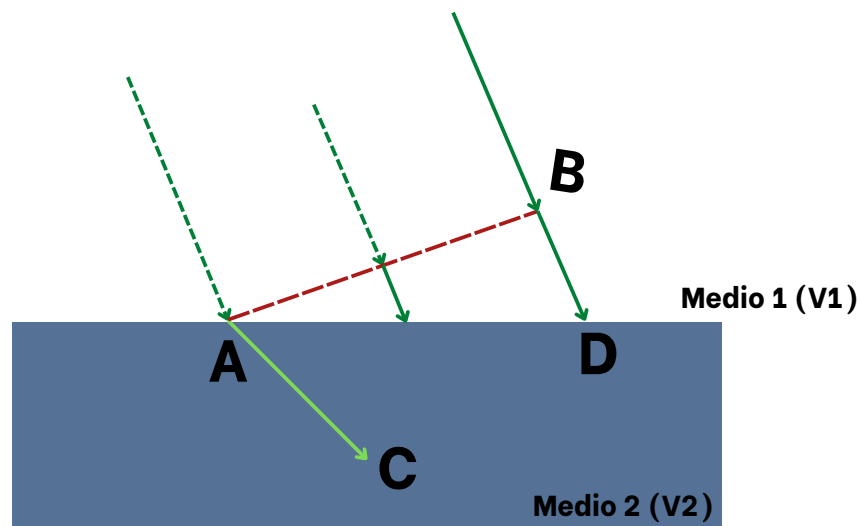
gran tamaño entre un punto A y un punto B, y no hay línea de vista directa, es posible utilizar una reflexión controlada sobre una superficie adecuada como lo es una pared, una montaña o una estructura metálica para redirigir la señal hacia el receptor.

2.11.2 Refracción

La refracción es el fenómeno de cambio de dirección que experimenta una onda al pasar de un medio a otro con diferente índice de refracción, lo que implica un cambio en su velocidad de propagación. Como se observa en la figura 11

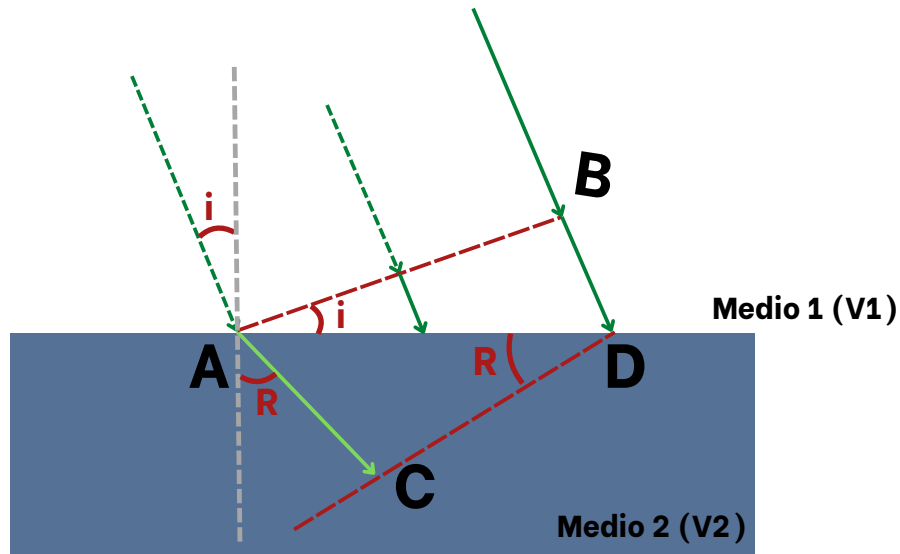
Figura 11

Geometría para la deducción de la ley de la refracción



En la figura 12 se observa el frente de onda plano que incide oblicuamente sobre la superficie de separación entre dos medios transparentes con velocidades de propagación de onda diferentes, v_1 en el primer medio y v_2 en el segundo medio. El ángulo i es el ángulo de incidencia, medido respecto a la normal a la superficie.

Figura 13
Ley de refracción



Observando la geometría que se forma por los puntos **A**, **B**, **D** y **C** (donde **AD** es la hipotenusa común a los triángulos rectángulos formados por el rayo incidente y el rayo refractado), podemos establecer las siguientes relaciones trigonométricas:

$$\sin i = \frac{\text{cateto opuesto}}{\text{hipotenusa}} = \frac{BD}{AD} = \frac{v_1 t}{AD}$$

$$\sin r = \frac{\text{cateto opuesto}}{\text{hipotenusa}} = \frac{AC}{AD} = \frac{v_2 t}{AD}$$

Despejando **AD** de ambas ecuaciones, obtenemos:

$$AD = \frac{v_1 t}{\sin i}$$

$$AD = \frac{v_2 t}{\sin r}$$

Igualando las expresiones para **AD**:

$$\frac{v_1 t}{\sin i} = \frac{v_2 t}{\sin r}$$

Simplificando t y reorganizando, llegamos a la ley de Snell o ley de refracción:

$$\frac{\sin i}{\sin r} = \frac{v_1}{v_2}$$

Esta relación también puede expresarse en términos de los índices de refracción n , definidos como $n = c/v$, donde c es la velocidad de la luz en el vacío. Así, $v_1 = c/n_1$ y $v_2 = c/n_2$:

$$\frac{\sin i}{\sin r} = \frac{c/n_1}{c/n_2} = \frac{n_2}{n_1}$$

Finalmente, la forma más común de la ley de Snell es:

$$n_1 \sin i = n_2 \sin r$$

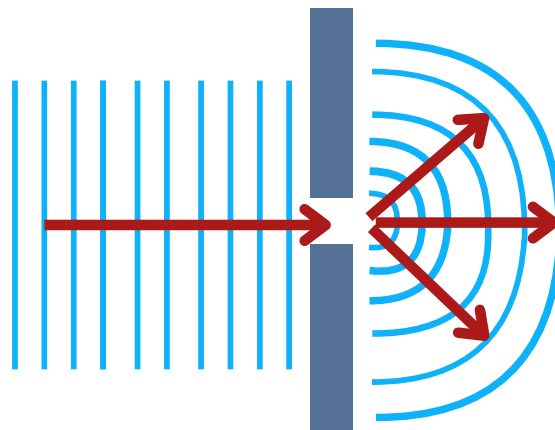
Esta ley describe cómo el ángulo de refracción depende del ángulo de incidencia y de las propiedades de los dos medios.

2.11.3 Difracción

La difracción es un fenómeno ondulatorio en el que las ondas de radio se curvan alrededor de los obstáculos o se propagan a través de aberturas. En lugar de ser completamente bloqueadas por un objeto, una parte de la energía de la onda se desvía de su trayectoria original como se observa en la figura 14.

Figura 14

Difracción



¿Qué causa la difracción?. Ocurre cuando una onda encuentra un borde afilado, una esquina o una abertura cuyo tamaño es comparable a su longitud de onda. En estas condiciones, el obstáculo actúa como una nueva fuente puntual de ondas, permitiendo que la señal se propague hacia áreas que estarían bloqueadas por la línea de vista directa.

- Bloqueo parcial de frente de onda. - El obstáculo interrumpe el frente de onda incidente
- Generación de ondas secundarias. - Los puntos del frente de onda no son bloqueados por el obstáculo, actuando como fuentes secundarias.
- Propagación en la zona de sombra. - Las ondas secundarias generadas en los bordes del obstáculo se extienden y se superponen en regiones conocidas como zona de sombra.

Difracción de Fresnel y Fraunhofer. La difracción de Fresnel o campo cercano ocurre cuando la fuente o el punto de observación están cerca del obstáculo, y por motivos del punto de emisión, el frente de onda no es plano.

La difracción de Fraunhofer se da cuando la fuente y el punto de observación están lo suficientemente lejos del obstáculo como para considerar que los frentes de onda son planos, simplificando así su cálculo.

Donde, para una rendija simple de un ancho a , la intensidad de la onda difractada en un ángulo θ se describe con la siguiente ecuación:

$$I(\theta) = I_0 \left(\frac{\sin(\beta)}{\beta} \right)^2$$

siendo

- $I(\theta)$, intensidad en el ángulo θ
- I_0 , intensidad máxima central
- $\beta = \frac{\pi a \sin(\theta)}{\lambda}$
- a , ancho de la rendija
- λ , longitud de onda

2.11.4 *Dispersión*

La dispersión se refiere al fenómeno en el que la velocidad de fase de una onda depende de su frecuencia. Esto ocasiona que la señal llegue en instantes de tiempo diferentes, ya que el índice de refracción del medio no es el mismo para todas las frecuencias. Es decir que las ondas de radio con diferentes frecuencias se retrasan de manera distinta al pasar por cualquier medio, como el aire. La dispersión en una onda de radio puede ocasionar un ensanchamiento del pulso, interferencias entre símbolos, distorsión de la señal, y límites en el ancho de banda y en la distancia.

2.11.5 *Interferencias*

Las interferencias son cualquier perturbación o señal no deseada que se interpone o se mezcla con la señal que se desea transmitir o recibir, dificultando su interpretación. Entra en acción lo que conocemos como principio de superposición.

El principio de superposición ocurre cuando dos o más ondas se combinan, dando como resultado una suma algebraica de las ondas individuales.

Ecuación general de una onda

$$y = A \sin[\omega t + \theta]$$

Donde:

- A amplitud
- $\omega = 2\pi n$
- t tiempo
- θ desfase

Tipos de interferencia

Interferencia constructiva. ocurre cuando las crestas de una onda coinciden con las crestas de la otra, resultando en una amplitud resultante mayor. Esto sucede cuando la diferen-

cia de fase es un múltiplo par de π radianes:

$$\Delta\theta = \theta_1 - \theta_2 = 2n\pi \quad (\text{donde } n = 0, \pm 1, \pm 2, \dots)$$

En este caso, $\cos\left(\frac{\Delta\theta}{2}\right) = \cos(n\pi)$. Para que sea completamente constructiva, necesitamos que n sea un número par, lo que hace $\cos(n\pi) = 1$.

Ejemplo: Desfase de 0° o 0 radianes. Si $\theta_1 = \theta_2$, entonces $\Delta\theta = 0$.

$$y_R = \left[2A \cos\left(\frac{0}{2}\right) \right] \sin\left(\omega t + \frac{\theta_1 + \theta_1}{2}\right)$$

$$y_R = [2A \cdot 1] \sin(\omega t + \theta_1)$$

$$y_R = 2A \sin(\omega t + \theta_1)$$

La amplitud resultante es $2A$, el doble de la amplitud original.

Interferencia destructiva. ocurre cuando las crestas de una onda coinciden con los valles de la otra, resultando en una amplitud resultante menor, incluso cero si las amplitudes son iguales. Esto sucede cuando la diferencia de fase es un múltiplo impar de π radianes:

$$\Delta\theta = \theta_1 - \theta_2 = (2n + 1)\pi \quad (\text{donde } n = 0, \pm 1, \pm 2, \dots)$$

En este caso, $\cos\left(\frac{\Delta\theta}{2}\right) = \cos\left(\frac{(2n+1)\pi}{2}\right) = 0$.

Ejemplo: Desfase de 180° o π radianes. Si $\Delta\theta = \pi$, por ejemplo, si $\theta_1 = \pi$ y $\theta_2 = 0$:

$$y_R = \left[2A \cos\left(\frac{\pi}{2}\right) \right] \sin\left(\omega t + \frac{\theta_1 + \theta_2}{2}\right)$$

$$y_R = [2A \cdot 0] \sin\left(\frac{\theta_1 + \theta_2}{2}\right)$$

$$y_R = 0$$

Las ondas se cancelan completamente, resultando en una amplitud de cero.

2.11.6 Absorción

La absorción es un proceso físico fundamental en la propagación de ondas electromagnéticas, caracterizado por la disipación de la energía de una onda de radio a medida que esta interactúa con un medio material. A diferencia de otros fenómenos, como la reflexión o la difracción, donde la energía cambia de dirección, en la absorción la energía de la onda se convierte en otras formas de energía, principalmente calor, lo que resulta en una atenuación directa de la señal.

Causas principales de la absorción:.

- **Resonancia molecular atmosférica:** Ocurre cuando las frecuencias de las ondas de radio coinciden con las frecuencias de resonancia vibracional o rotacional de las moléculas presentes en la atmósfera y al coincidir estas frecuencias, las moléculas absorben energía de la onda, pasando a estados de energía superiores, la cual es posteriormente disipada en forma de calor. Los gases más comunes y significativos que causan este tipo de absorción son:
 - **Vapor de agua (H_2O):** Es un absorbente principal, con picos de absorción notables alrededor de los 22 GHz y 183 GHz. Su impacto aumenta con la humedad y la longitud del trayecto.
 - **Oxígeno (O_2):** Otro absorbente importante, con un pico de absorción significativo alrededor de los 60 GHz y otro cerca de los 118 GHz.
 - **Dióxido de carbono (CO_2):** También contribuye a la absorción, aunque en menor medida que el vapor de agua y el oxígeno.
- **Precipitación y partículas en suspensión:** Fenómenos meteorológicos como la lluvia, nieve, niebla y nubes son causas significativas de absorción, especialmente para frecuencias elevadas (superiores a 10 GHz). Las gotas de agua o cristales de hielo en suspensión absorben la energía de la onda, convirtiéndola en calor. La atenuación aumenta con la densidad de la precipitación y la frecuencia de la señal.
- **Interacción con materiales sólidos (terreno y obstáculos):** Cuando las ondas de radio inciden sobre materiales como edificios, vegetación (árboles, follaje), el suelo o montañas, parte de su energía es absorbida. La cantidad de absorción depende de las propiedades die-

léctricas y la conductividad del material, así como de la frecuencia de la onda y el espesor del obstáculo.

- **Absorción ionosférica:** En las capas ionizadas de la atmósfera (capas D, E, F), especialmente en la capa D durante el día, los electrones libres pueden absorber energía de las ondas de radio, particularmente en las frecuencias bajas (HF - alta frecuencia). Esta energía se disipa a través de colisiones con otras partículas.

Medición de la absorción:. La absorción no se mide de forma aislada directamente con un solo valor, sino que se infiere como parte de la pérdida total de propagación que experimenta una onda de radio. La forma más básica de cuantificar la atenuación total desde el transmisor hasta el receptor es midiendo la diferencia entre la potencia transmitida y la potencia recibida:

$$\text{Pérdida Total de Trayectoria (dB)} = P_{TX}(\text{dBm}) - P_{RX}(\text{dBm})$$

Donde:

- $P_{TX}(\text{dBm})$: Es la potencia de la señal transmitida, expresada en decibelios por milivatios.
- $P_{RX}(\text{dBm})$: Es la potencia de la señal recibida en el punto de interés, también en decibelios por milivatios.

Esta ecuación proporciona la pérdida total que sufrió la onda de radio desde el punto de transmisión hasta el receptor. Es importante destacar que esta pérdida total incluye la contribución de la absorción, pero también de otros fenómenos como la atenuación por espacio libre, la reflexión, la difracción y la dispersión.

2.11.7 Atenuación

Como hemos visto, la propagación de ondas de radio es parte fundamental para las redes WISP; sin embargo, los diversos fenómenos físicos vistos hasta ahora, conocidos generalmente como atenuación, debilitan la señal a medida que esta se propaga por un medio no guiado. Esta disminución de la señal tiene un impacto en la calidad de servicio de la red, afectando cada parámetro crítico, como el jitter, la latencia y la pérdida de paquetes.

La atenuación se hace presente a través de:

- Reflexión. - Como sabemos, en la reflexión las ondas rebotan en grandes superficies, ocasionando que la señal se divida y siga caminos diferentes; por lo tanto, parte de la señal no llega a su destino, lo que provoca pérdidas de paquetes. Por otro lado, si estas señales llegan a su destino pero en fases diferentes, esto provoca un retardo o latencia.
- Difracción. - Aunque se pueda usar a nuestro favor la difracción para realizar una comunicación sin una línea de vista clara, debido a que las ondas se curvan al rozar con los obstáculos, esta provoca que la señal sea significativamente más débil siendo más susceptible a las pérdidas de paquetes.
- Dispersión. - Las ondas, al chocar con objetos, se dispersan en distintas direcciones, lo que reduce la potencia de la señal y afecta la recepción.
- Interferencias. - Las señales de otras redes inalámbricas pueden superponerse en la señal transmitida provocando que la relación señal-ruido sea menor, afectando directamente la latencia y por consiguiente las pérdidas de paquetes.
- Absorción. - Las ondas son absorbidas por materiales como el concreto, los árboles o el aire. Este fenómeno actúa con mayor fuerza mientras más alta es la frecuencia de operación, debido a su longitud de onda más pequeña. La absorción afecta a la potencia de señal recibida, disminuyendo el ancho de banda disponible y, por lo tanto, la fiabilidad del enlace.
- Refracción. - Afecta a la estabilidad del enlace, ya que modifica la línea de vista aparente debido a un cambio de dirección de la onda al atravesar diferentes materiales con distintas densidades.

En resumen, una mala planificación afecta directamente a la calidad del servicio que se puede entregar, generando los siguientes problemas:

- Reducción del alcance y cobertura: A una mayor atenuación, menor es la distancia que una señal puede cubrir desde una estación base. Por lo tanto, se necesitará la implementación de más puntos de acceso o, directamente, la instalación de equipos con mejores características que permitan solventar esta deficiencia en la cobertura.
- Disminución del rendimiento: De la misma forma que el punto anterior, la atenuación causa que las señales se vuelvan débiles y, por lo tanto, más susceptibles a las interferencias

y al ruido, lo que conlleva una retransmisión de los paquetes, provocando así que aumente la latencia o retardo de la señal, crucial para transmisiones en vivo como videollamadas o streaming.

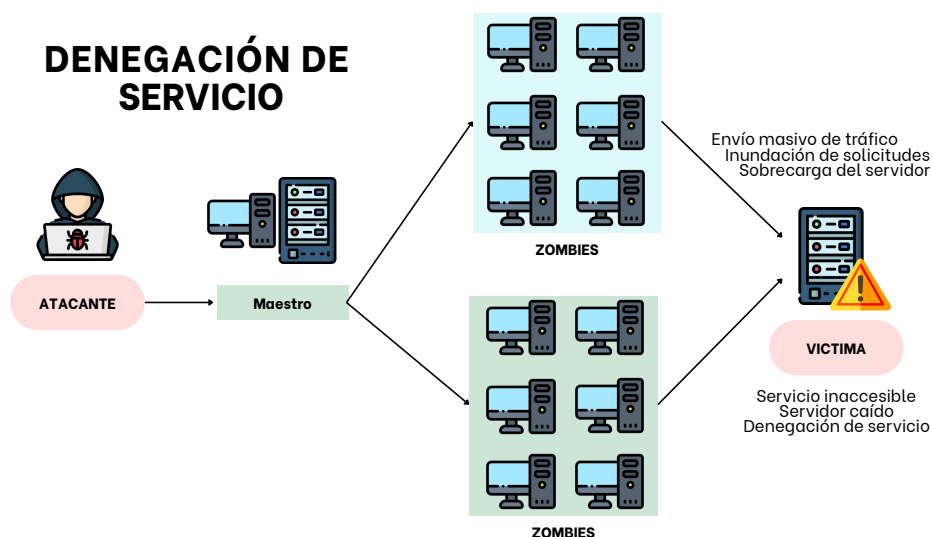
- **Fiabilidad de la conexión:** Una señal con una alta atenuación ocasiona que estas sean inestables y propensas a desconexiones, lo que reduce la fiabilidad del servicio para el abonado.

2.12 Ataques cibernéticos en redes inalámbricas

Hoy en día las redes inalámbricas forman parte de nuestra vida, debido a que es una forma más sencilla de acceder a una conexión a internet, en vez de una conexión por cable de cobre o fibra, pero no todo son ventajas. La desventaja más clara es su seguridad, debido a que transmitir a través de un medio no guiado como lo es el aire, conlleva que los atacantes puedan interceptar nuestra señal y por lo tanto ejecutar ataques que pongan en riesgo los datos.

2.12.1 Denegación de servicio

Figura 15
Denegación de servicio

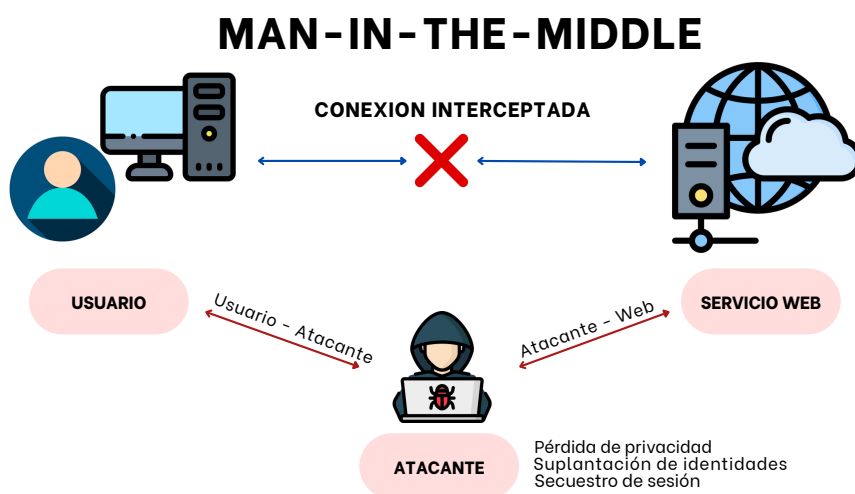


Existen varias formas de denegar el servicio a los usuarios finales. Uno de los métodos más usados por los atacantes es el ataque DoS, que consiste en generar una gran cantidad de peticiones al servidor con el fin de que los equipos encargados de administrarlas agoten todo el procesamiento del CPU. Al sobrecargarse, el sistema comienza a ralentizar sus procesos,

impidiendo que los usuarios legítimos puedan acceder al servicio y provocando pérdida parcial de paquetes, lentitud e incluso la pérdida total de la conexión. [39]

2.12.2 Hombre en el medio

Figura 16
MitM

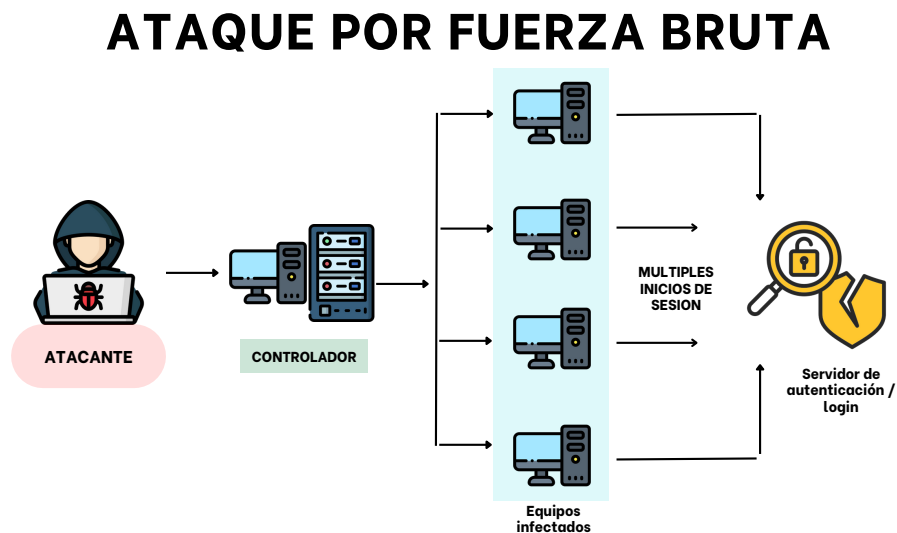


Comúnmente conocido por sus siglas en inglés, MitM es un tipo de ataque en el que un equipo actúa como intermediario entre el cliente y el servidor. Esto se logra mediante el uso de equipos especializados en duplicar una red; entre las más utilizadas están las redes públicas, ya que no cuentan con contraseña para poder ingresar. El objetivo de estos ataques es interceptar datos sin cifrar, identificando usuarios y contraseñas personales o datos financieros, ya sea para el robo de dinero bancario o para la suplantación de identidad con fines de fraude. En internet existe software de código abierto con la etiqueta de “White Hat Hacking” para este tipo de ataques MitM, tales como Ettercap, una potente herramienta de código abierto diseñada para funcionalidades MitM que incluye rastreo de conexiones en vivo, filtrado de contenido sobre la marcha y la disección activa o pasiva de numerosos protocolos. [40]

2.12.3 Ataques por fuerza bruta

Figura 17

Ataques por fuerza bruta



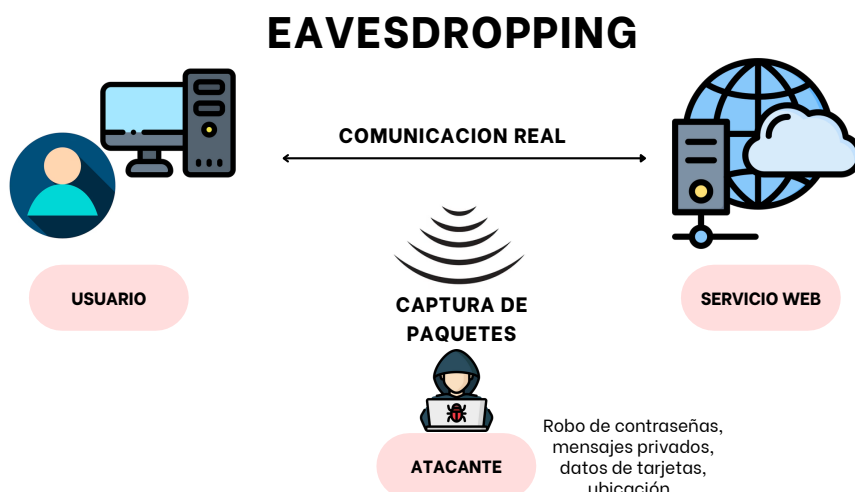
“Los ataques de fuerza bruta son un método de ensayo y error para adivinar la información de inicio de sesión, las claves de cifrado o encontrar una página web oculta” [41].

Estos ataques tienen como objetivo principal el robo de datos personales, la difusión de malware y el secuestro de sistemas para actividades fraudulentas. Hay dos tipos de ataques por fuerza bruta, los cuales son:

- **Ataques simples:** Ataques donde los atacantes intentan adivinar las credenciales, sin ayuda de herramientas externas, suelen usar contraseñas y PIN extremadamente sencillas.
- **Ataques de diccionario:** Los atacantes eligen un objetivo y validan las credenciales posibles con un nombre de usuario elegido.

2.12.4 Espionaje

Figura 18
Eavesdropping

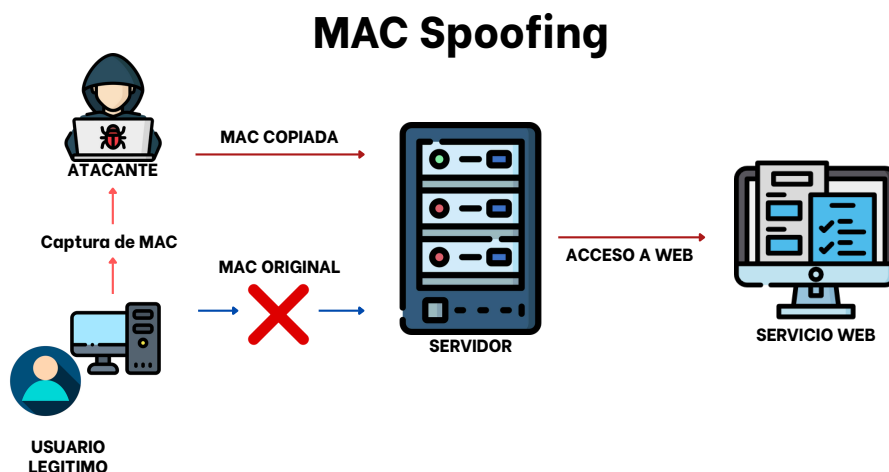


El espionaje digital o Eavesdropping tiene como función principal obtener información confidencial de usuarios, usando técnicas y herramientas para obtener acceso. Este tipo de ataques es difícil de detectar porque no provoca efecto alguno en la calidad y velocidad de internet. El espionaje varía según la técnica utilizada, entre las cuales están:

- **Wi-Fi no seguras:** Los atacantes acceden a redes Wi-Fi sin contraseñas para capturar el tráfico con softwares de rastreo, por ejemplo Wireshark.
- **Redes Wi-Fi falsas:** Crean redes falsas usando el mismo nombre de la red original, para que usuarios conectados a ellas queden vulnerables.
- **Equipos externos:** El uso de antenas de gran alcance permite amplificar la recepción de señales débiles para la captura de tráfico de forma pasiva mediante la transferencia inalámbrica de datos.

2.12.5 Suplantación de MAC

Figura 19
MAC Spoofing



Conocida también como MAC Spoofing, consiste en el cambio o duplicado de una dirección de control de acceso al medio o mejor conocido como dirección MAC de un equipo víctima. Consiste en tres fases: la primera es el análisis previo de la red, con el objetivo de detectar la MAC objetivo; la segunda consiste en usar un software especializado para cambiar la MAC real de la propia tarjeta de red e imitar la dirección del objetivo; y la tercera, finalmente, es la conexión a la red con la dirección MAC falsa, evadiendo los controles de seguridad basados en direcciones MAC.

3 CAPÍTULO 3: PROPUESTA DEL PROYECTO

3.1 Arquitectura y diseño lógico de la red

Para garantizar la operabilidad, estabilidad y escalabilidad de la red de acceso WISP, se diseñó una infraestructura fundamentada en el modelo de referencia jerárquico de tres capas: núcleo (*core*), distribución y acceso (última milla). Esta estructuración lógica permite canalizar eficientemente los flujos de datos desde el proveedor de servicios de internet (ISP) principal hasta los equipos en las instalaciones del cliente (CPE).

Asimismo, la segmentación modular por capas optimiza la administración del tráfico, garantiza una alta disponibilidad de los servicios y mitiga la degradación del rendimiento en los nodos activos, al liberar a los dispositivos de conmutación y enrutamiento de cargas de procesamiento innecesarias.

3.2 Topología lógica y flujo de datos

La arquitectura lógica de la red se estructuró bajo un enfoque jerárquico de segmentación por servicios mediante la implementación del estándar IEEE 802.1Q para redes de área local virtuales (VLAN). Este modelo permite que una misma infraestructura física transporte múltiples flujos de datos independientes, optimizando el uso de los recursos de hardware e incrementando la seguridad perimetral mediante el aislamiento estricto del tráfico de gestión respecto del de los usuarios finales.

Con el fin de sistematizar el análisis técnico de la infraestructura, la topología y el flujo de datos asociado se organizan en tres capas funcionales:

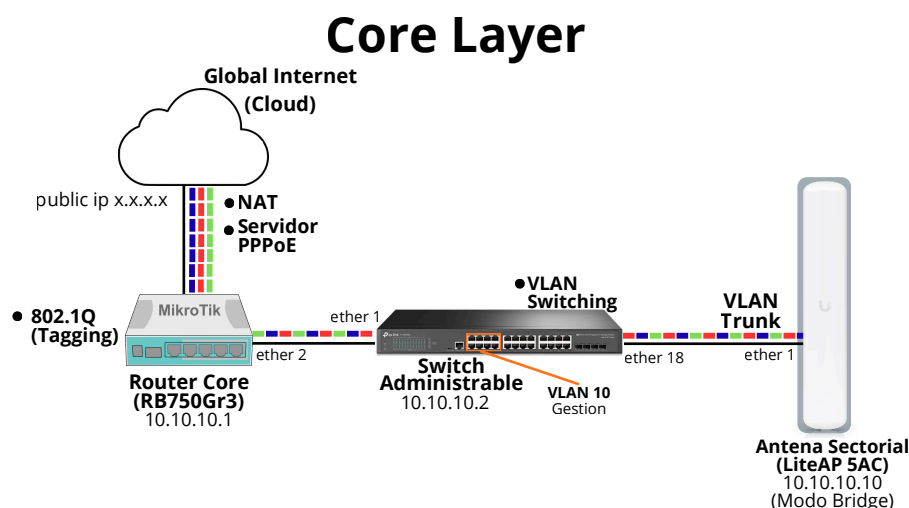
- **Capa de núcleo (*Core*):** Encargada del enrutamiento de alta velocidad, la interconexión con el proveedor WAN, la gestión del direccionamiento lógico y la autenticación centralizada de sesiones mediante el servidor PPPoE.
- **Capa de distribución:** Responsable de la agregación de enlaces, la conmutación de tráfico en Capa 2/Capa 3 hacia las estaciones base, y la aplicación de políticas de marcado y calidad de servicio (QoS).
- **Capa de acceso:** Conformada por los puntos de acceso sectoriales (AP) y los equipos en

las instalaciones del cliente (CPE), los cuales concretan el enlace inalámbrico de última milla y la entrega del servicio al usuario final.

3.2.1 Núcleo (Core Layer)

Figura 20

Topología de la capa de núcleo (Core Layer).



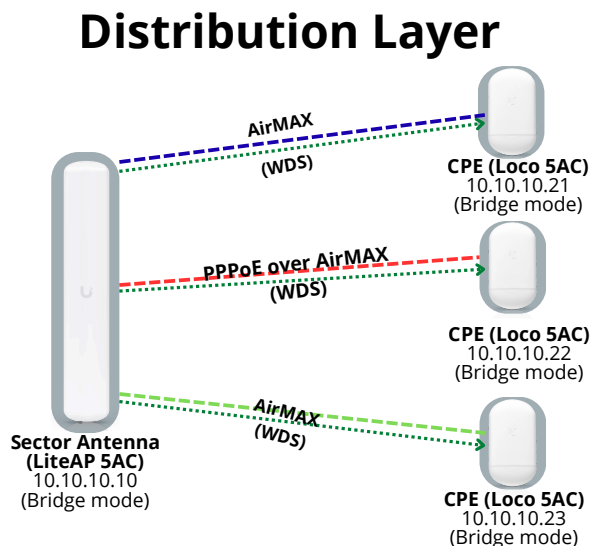
La capa de núcleo es el centro encargado del procesamiento, enrutamiento y de la red inalámbrica. Los datos inician con la conexión hacia el internet global a través de la interfaz ether1 del enrutador central MikroTik RB750Gr3, donde se aplica traducción de direcciones de red (NAT). Este dispositivo actúa como el cerebro de la red, ejecutando funciones críticas como el servidor PPPoE para la autenticación de usuarios y políticas de calidad de servicio (QoS).

Posteriormente se procedió a crear las diferentes VLANs y marcado para enviar el tráfico con etiquetado 802.1Q hacia el Switch Administrable de Capa 2, el cual realiza la conmutación de VLANs. Posteriormente, el tráfico unificado se propaga mediante un enlace troncal (VLAN Trunk) desde el puerto ether18 del switch hacia la interfaz cableada de la estación base sectorial. La estructura lógica de este segmento se ilustra en la Figura 20.

3.2.2 Capa de distribución (Distribution Layer)

Figura 21

Topología e interconexión de la capa de distribución.



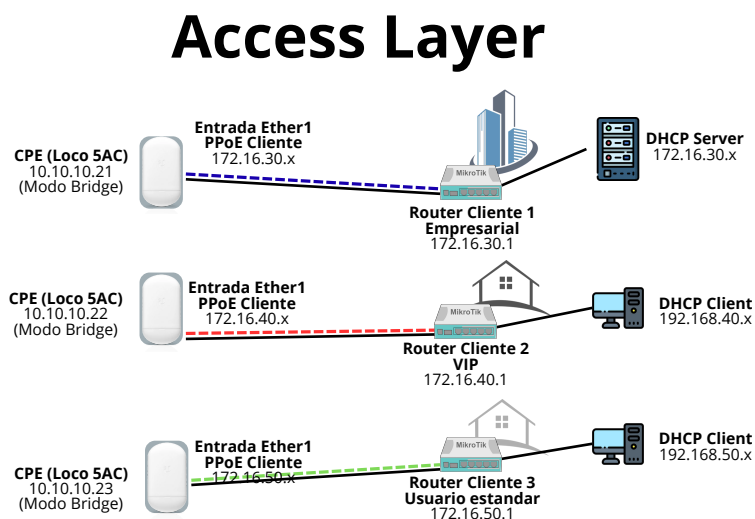
La capa de distribución gestiona el transporte inalámbrico masivo de datos desde el nodo central hacia los terminales remotos. El dispositivo emisor principal es la Antena Sectorial LiteAP 5AC, que está configurada en modo Bridge. Esta estación base establece la cobertura y distribuye el ancho de banda utilizando el protocolo propietario AirMAX AC en modo WDS (Wireless Distribution System).

La ventaja operativa de activar WDS radica en que los enlaces inalámbricos operan de manera transparente en Capa 2, permitiendo el paso de las tramas etiquetadas 802.1Q sin modificación alguna del etiquetado además de las sesiones de túneles PPPoE. Los datos viajan por el espectro radioeléctrico divididos en intervalos de tiempo (TDMA), dirigiéndose de forma segmentada hacia cada uno de los terminales CPE NanoStation Loco 5AC de los abonados, los cuales actúan también en modo puente de red y están configurados con la VLAN correspondiente al cliente. El flujo inalámbrico de distribución se detalla en la Figura 21.

3.2.3 Capa de acceso (Access Layer)

Figura 22

Topología y direccionamiento de la capa de acceso.



La capa de acceso es la última milla de la red, es la que se encarga de la entrega final del servicio y la asignación de direccionamiento IP a los usuarios finales. Cada terminal CPE entrega el tráfico de forma cableada a través de su puerto Ethernet hacia el Router residencial del cliente. En este punto, la interfaz ether1 de cada router doméstico actúa como un cliente PPPoE, encargándose de levantar la sesión cifrada directamente con el enrutador central de la red. La organización lógica de los abonados finales se presenta en la Figura 22.

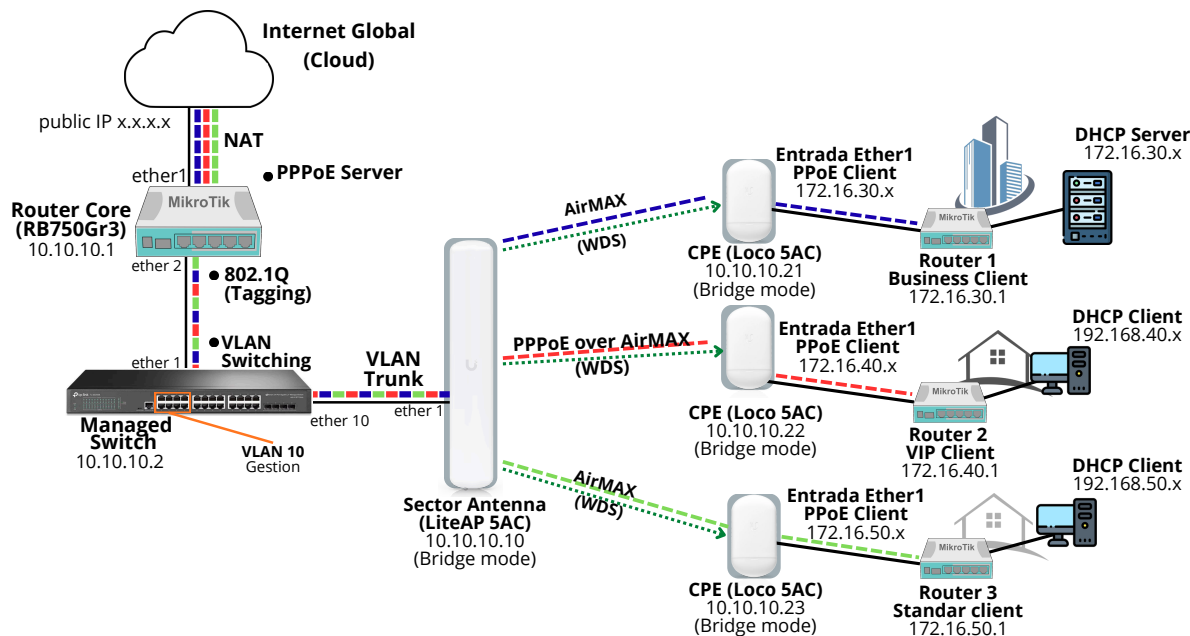
Dependiendo del perfil configurado, se realiza una asignación dinámica de dirección IP.

- **Cliente 1 (Empresarial):** El enrutador del cliente levanta el túnel PPPoE en el segmento 172.16.30.x.
- **Cliente 2 (VIP):** Establece su enlace PPPoE dentro del segmento 172.16.40.x y provee direcciones IP automáticas a los dispositivos finales mediante un cliente DHCP en la LAN.
- **Cliente 3 (Usuario estándar):** Inicia la sesión de datos en el segmento 172.16.50.x, distribuyendo direcciones IP locales en el rango de 192.168.50.x.

3.2.4 Integración de la red completa

Figura 23

Topología lógica integral y flujo de datos extremo a extremo de la red WISP.



Una vez delimitadas las especificaciones operativas y funcionales de cada segmento, se agrupa la arquitectura global e integrada de la red de acceso inalámbrica WISP. Como se ilustra en la figura 23, la topología lógica unifica el flujo de datos desde el núcleo de la red hasta el destino final, evidenciando la interacción entre el enrutamiento central, la segmentación mediante etiquetas de VLAN, el transporte inalámbrico optimizado bajo el protocolo airMAX y la terminación de los túneles de autenticación PPPoE asignados a cada perfil de abonado. Esta sinergia asegura un control granular del tráfico, mitigando la degradación de rendimiento y garantizando el aislamiento criptográfico y operativo del sistema.

3.2.5 Segmentación de red mediante redes locales virtuales (VLANs)

Se han definido cuatro redes virtuales (VLANs) para organizar el tráfico desde el Core MikroTik hasta los puntos de acceso. La configuración de los puertos entre el Router y el Switch se establecerá en modo *Trunk* (Etiquetado), mientras que la entrega hacia los equipos de radio se realizará de forma específica según el servicio como se observa en la tabla 2.

Tabla 2
Segmentación de red mediante VLANs

Nombre de VLAN	ID (Tag)	Descripción del Tráfico
VLAN_GESTION	10	Tráfico exclusivo para administración de radios y switches.
VLAN_EMPRESARIAL	30	Clientes empresariales con prioridad de ancho de banda.
VLAN_VIP	40	Clientes con ancho de banda media.
VLAN_RESIDENCIAL	50	Clientes estándar bajo túneles PPPoE

3.2.6 Esquema de direccionamiento IP (IPv4)

Para evitar conflictos de red y facilitar el monitoreo, se implementará un esquema de direccionamiento privado basado en la normativa RFC 1918. El diseño jerárquico se detalla a continuación:

Tabla 3
Dispositivos y direccionamiento IP de la topología lógica

Dispositivo	Dirección IP
Internet global (Nube)	IP Pública: x.x.x.x
MikroTik Core (RB750Gr3)	Gestión: 10.10.10.1
Switch administrable	Gestión: 10.10.10.2
Antena sectorial (LiteAP 5AC)	Gestión: 10.10.10.10
CPE cliente 1 (Loco 5AC)	Gestión: 10.10.10.21
Router cliente 1 (Empresarial)	Gateway: 172.16.30.1
CPE cliente 2 (Loco 5AC)	Gestión: 10.10.10.22
Router cliente 2 (VIP)	Gateway: 172.16.40.1
CPE cliente 3 (Loco 5AC)	Gestión: 10.10.10.23
Router cliente 3 (Estándar)	Gateway: 172.16.50.1

- **Red de gestión:** Segmento 10.10.10.0/24. Se utiliza para la administración centralizada de la infraestructura. El Router Core asume la IP 10.10.10.1, el Switch administrable la 10.10.10.2, la Antena sectorial la 10.10.10.10 y las antenas CPE el rango 10.10.10.21 - 10.10.10.254.
- **Segmento empresarial (Cliente 1):** Red 172.16.30.x/24. Destinado a usuarios corporativos que requieren una infraestructura de red robusta.
- **Segmento VIP (Cliente 2):** Red 172.16.40.0/24. Segmento con prioridad de tráfico para usuarios residenciales de alto consumo.
- **Segmento estándar (Cliente 3):** Red 172.16.50.0/24. Red base para usuarios residenciales convencionales.

3.2.7 Transición del modelo de red: Migración de DHCP a PPPoE

Tabla 4

Comparativa técnica en la transición del modelo de red: DHCP vs. PPPoE

Modelo DHCP (Limitaciones)	Modelo PPPoE (Ventajas técnicas)
Configuración rápida y asignación automática de parámetros, pero deficiente a largo plazo.	Entorno de red privado, optimizado y escalable para la gestión de abonados.
Generación de tráfico de broadcast constante que satura el espectro inalámbrico.	Eliminación completa del tráfico de broadcast innecesario en los enlaces de radio.
Ruido en el medio que degrada de forma progresiva la velocidad del servicio.	Maximización de la eficiencia del ancho de banda y estabilidad en la transmisión.
Frecuentes conflictos por direcciones IP duplicadas que interrumpen la conexión.	Asignación unívoca y controlada de direcciones IP por cada sesión activa.
Vulnerabilidad ante accesos no autorizados y alta exposición al robo de servicio.	Autenticación obligatoria mediante credenciales únicas de inicio para cada cliente.

- **Limitaciones del modelo DHCP** Aunque el modelo DHCP ofrece ventajas iniciales como una configuración rápida de la red y facilidad para nuevos abonados de forma automática, a largo plazo conlleva riesgos de seguridad y problemas de optimización. Esto se debe a que genera un tráfico de broadcast constante que produce un ruido innecesario en el espectro inalámbrico, saturando las antenas y degradando la velocidad. Además, la falta de un control estricto bajo este sistema provoca conflictos por direcciones IP duplicadas que dejan a los usuarios sin recepción de internet, abriendo también la puerta a vulnerabilidades como el acceso no autorizado a la infraestructura y el robo de servicio.
- **Ventajas técnicas y justificación del protocolo PPPoE** Para solucionar los problemas del modelo DHCP, se migró a PPPoE, ya que transforma la red en un entorno privado y optimizado. Esto se debe a que exige credenciales de inicio para cada abonado, eliminando por completo el tráfico de broadcast y los conflictos de IP duplicadas.

3.3 Especificaciones y requerimientos técnicos de hardware

Para la implementación de la red de acceso inalámbrico, la aplicación de políticas de calidad de servicio (QoS) y la evaluación de los protocolos de red, se seleccionó equipamiento que garantiza un rendimiento óptimo bajo escenarios reales de operación. A continuación, se detallan las especificaciones técnicas y la función operativa de los dispositivos principales que conforman la topología propuesta.

3.3.1 Estación base: Transmisión y recepción centralizada

En el nodo central de distribución, se determinó el despliegue de un punto de acceso con antena sectorial integrado, encargado de concentrar el tráfico radioeléctrico proveniente de las estaciones de abonado. Para cumplir este rol, se seleccionó el equipo LiteAP AC (LAP-120) de Ubiquiti Networks.

Este dispositivo opera en la banda de frecuencia de 5 GHz, lo cual mitiga el impacto del ruido electromagnético e interferencias asociadas a redes inalámbricas locales que transmiten en el espectro saturado de 2.4 GHz. Asimismo, incorpora compatibilidad nativa con la tecnología airMAX AC (TDMA), garantizando un rendimiento elevado (*throughput*) y una baja latencia en entornos multipunto (PtMP).

Tabla 5*Especificaciones técnicas de la estación base LiteAP GPS (LAP-GPS)*

Parámetro	Especificación LiteAP GPS
Modelo	LAP-GPS
Frecuencia de operación	5 GHz (U-NII-1, U-NII-2A, U-NII-2C, U-NII-3)
Ganancia de antena	17 dBi
Apertura (Beamwidth)	90° (Azimuth)
Sincronización	GPS incorporado
Procesador	Atheros MIPS 74Kc
Memoria	64 MB DDR2
Interfaz de red	(1) 10/100/1000 Ethernet Port
Rendimiento (Throughput)	450+ Mbps
Fuente de alimentación	24V, 0.5A Gigabit PoE Adapter (Incluido)
Protocolo de red	airMAX AC (MIMO TDMA)

Nota. Datos extraídos del manual de especificaciones de Ubiquiti Networks para la serie LiteAP ac.

La transmisión se ejecuta mediante el protocolo propietario *airMAX ac* de Ubiquiti Networks, fundamentado en la tecnología de acceso múltiple por división de tiempo. Este mecanismo asigna intervalos de tiempo programados a cada estación de abonado (CPE), lo que elimina las colisiones por contención de paquetes en el medio inalámbrico y optimiza la eficiencia espectral en arquitecturas punto a multipunto (PtMP). Las especificaciones técnicas detalladas de este dispositivo se presentan en la Tabla 5.

3.3.2 Terminal de usuario / Estación de abonado

En el lado del usuario o abonado, se requiere un dispositivo CPE (*Customer Premises Equipment*) compacto, pero con alta eficiencia directiva para entornos de corto y medio alcance. La opción seleccionada es la NanoStation Loco 5AC.

Este equipo actúa como terminal receptor e integra una antena de 13 dBi que asegura la estabilidad del enlace inalámbrico hacia la estación base. Además, incorpora un puerto Gigabit Ethernet que previene los cuellos de botella en la interfaz física, garantizando una adecuada tasa de transferencia del enlace de radio. Los parámetros técnicos se describen en la Tabla 6.

Tabla 6*Especificaciones técnicas del terminal de abonado Loco NanoStation 5AC*

Parámetro	Especificación NanoStation AC loco
Modelo	Loco5AC
Frecuencia de operación	5 GHz (U-NII-1, U-NII-2A, U-NII-2C, U-NII-3)
Ganancia de antena	13 dBi
Procesador	Atheros MIPS 74Kc
Memoria	64 MB DDR2
Interfaz de red	(1) 10/100/1000 Ethernet Port
Rendimiento (Throughput)	450+ Mbps
Potencia de salida	25 dBm
Consumo máximo de energía	8.5W
Método de alimentación	24V Passive PoE (Paquetes de 1 no incluyen PoE)
Protocolo de red	airMAX AC (MIMO TDMA)

Nota. Datos obtenidos del datasheet oficial de Ubiquiti Networks para la serie NanoStation AC.

3.3.3 Enrutador central / Administrador de red

El enrutador actúa como el núcleo principal de la infraestructura, asumiendo el rol de administrador central de la red de acceso. Para cumplir con la función de enrutamiento y control de tráfico entre los abonados e internet, se seleccionó el equipo MikroTik hEX (RB750Gr3).

Este dispositivo fue elegido por su arquitectura de procesamiento de doble núcleo, cualidad esencial para implementar políticas estrictas de calidad de servicio (QoS) destinadas a priorizar tráfico sensible a la latencia y al retardo, tales como transmisiones en tiempo real. Asimismo, el equipo opera con el sistema operativo RouterOS, el cual ofrece la robustez necesaria para mitigar la pérdida de paquetes y mantener una latencia mínima bajo escenarios de alta carga en un entorno WISP. Sus especificaciones técnicas se muestran en la Tabla 7.

En la tabla 8 se detallan de forma resumida los componentes principales que conforman la topología propuesta.

Tabla 7*Especificaciones técnicas del router principal MikroTik hEX (RB750Gr3)*

Parámetro	Especificación MikroTik RB750Gr3
Arquitectura	MMIPS
CPU	MT7621A (2 núcleos, 4 hilos)
Frecuencia nominal de CPU	880 MHz
Memoria RAM	256 MB
Almacenamiento	16 MB Flash
Puertos Ethernet	5x 10/100/1000 Mbps
Aceleración de Hardware IPsec	Sí
Ranura de expansión	1x MicroSD / 1x USB tipo A
Sistema operativo	RouterOS (Licencia Nivel 4)

Nota. Datos técnicos obtenidos del fabricante MikroTik para la revisión de hardware hEX v3.

3.3.4 Especificaciones de medio de transmisión

- **Cableado estructural:** Se empleará cable FTP Categoría 6 para exteriores con blindaje de aluminio para mitigar y proteger la integridad de los datos frente a las descargas electrostáticas.
- **Conectores:** Se utilizarán conectores RJ-45 blindados para asegurar la continuidad de toma tierra desde la antena hasta los inyectores PoE, con el fin de prevenir futuros daños en los puertos Ethernet.
- **Suministro de energía:** El sistema utilizará fuentes de alimentación PoE pasivas de 24V.

3.4 Configuración de calidad de servicio (QoS)

La gestión del ancho de banda es un componente crítico para garantizar los niveles de servicio (SLA) y la estabilidad de la red. Para ello, se implementará un sistema de QoS basado en la jerarquía de prioridades de MikroTik, estructurado en el marcado de tráfico y la ejecución de colas jerárquicas.

Tabla 8*Especificaciones técnicas del hardware seleccionado para la red WISP*

Componente	Modelo	Función Principal	Justificación Técnica
Router Core	MikroTik RB750Gr3	Enrutamiento central y servidor PPPoE.	Procesador Dual Core 880MHz con soporte de cifrado por hardware para gestión de colas (QoS).
Switch	TP-Link TL-SG3452	Gestión de VLANs y segmentación.	Soporte nativo de estándar IEEE 802.1Q para el aislamiento de tráfico en Capa 2.
Punto de Acceso	Ubiquiti LiteAP 5AC	Emisión sectorial (PMP).	Tecnología airMAX AC con apertura de 120° para optimización de ancho de banda inalámbrico.
CPE / Cliente	Ubiquiti NanoStation Loco 5AC	Recepción de señal en abonado.	Ganancia de 13 dBi y diseño compacto para enlaces de última milla con alta inmunidad al ruido.

3.4.1 Clasificación y marcado de tráfico (*Mangle*)

Antes de aplicar restricciones de velocidad, el router debe identificar el origen y destino de los paquetes. Se utilizará el módulo *Mangle* del Firewall para inspeccionar el tráfico de las interfaces PPPoE y asignar marcas de paquete (*packet marks*) según el segmento correspondiente:

- **MARK_EMPRESARIAL:** Tráfico asociado al segmento 172.16.30.0/24.
- **MARK_VIP:** Tráfico asociado al segmento 172.16.40.0/24.
- **MARK_ESTANDAR:** Tráfico asociado al segmento 172.16.50.0/24.

3.4.2 Jerarquía de prioridades (*Queue Tree*)

A diferencia de las colas simples, el Queue Tree permite definir una estructura de nodos “Padre e Hijo” que optimiza el uso del ancho de banda total. Se establece una escala de prioridad, donde el valor 1 representa la mayor prioridad de salida, como se detalla en la Ta-

bla 9.

Tabla 9

Jerarquía de prioridades y garantía de ancho de banda

Categoría de Cliente	Prioridad	Garantía de Tráfico (CIR)
Empresarial (Cliente 1)	1	50 % del plan contratado en hora pico.
VIP (Cliente 2)	3	30 % del plan contratado en hora pico.
Estándar (Cliente 3)	8	Mejor esfuerzo (<i>Best Effort</i>).

3.4.3 Implementación de subcolas para el sector empresarial

Para optimizar la experiencia de navegación de los usuarios del segmento empresarial, se diseñó un árbol de colas (HTB) en el enrutador central. Este mecanismo trasciende la simple limitación de velocidad máxima, permitiendo analizar activamente el tráfico para otorgar preferencia a los servicios críticos y sensibles a la latencia.

La priorización se estructuró clasificando los flujos de datos mediante las siguientes subcolas:

- **Tráfico de alta prioridad (Protocolos interactivos y UDP):** Se asignó la máxima prioridad a estos flujos debido a que sostienen servicios en tiempo real como voz sobre IP (VoIP), videoconferencias y transmisiones de video en vivo. Al procesar estos paquetes en primera instancia, se previenen la fluctuación de retardo (*jitter*) y los cortes en la comunicación cuando la red experimenta niveles de congestión.
- **Tráfico de prioridad media (Navegación web y servicios empresariales):** Engloba protocolos basados en TCP que toleran ligeras variaciones de tiempo, correspondiente a la carga de sitios web, correo electrónico, redes sociales y mensajería instantánea.
- **Tráfico de baja prioridad (Descargas masivas y transferencias en segundo plano):** Corresponde a transferencias de archivos de gran volumen y actualizaciones automáticas de sistemas operativos. Estos flujos se procesan únicamente con el ancho de banda remanente, evitando que la descarga masiva de datos comprometa la calidad de servicio de los demás

usuarios.

3.5 Protocolos de seguridad e integridad de datos

La infraestructura implementa múltiples capas de seguridad para mitigar riesgos de intrusión, suplantación de identidad y ataques de denegación de servicios (DoS), asegurando la continuidad operativa del WISP.

3.5.1 *Aislamiento de clientes y capa inalámbrica*

Para prevenir que los abonados dentro de un mismo segmento inalámbrico interactúen entre sí, se habilitará la función de Client Isolation en el apartado de reglas de firewall del router administrador. Esto garantiza que el tráfico sea procesado por el Core, donde se aplican las políticas de seguridad. Asimismo, el cifrado de los enlaces se realizará bajo el estándar WPA2-AES, desactivando el protocolo WPS para mitigar vulnerabilidades de acceso.

3.5.2 *Filtrado de tráfico y seguridad en el core*

Para garantizar la estabilidad de la red WISP y proteger el nodo central, se diseñó e implementó una estrategia de seguridad basada en el principio de bloquear todo por defecto y permitir únicamente el tráfico estrictamente necesario. Esto evita que el procesador del router se sature con peticiones maliciosas y asegura que los recursos de hardware se dediquen exclusivamente a enrutar el tráfico de internet de los abonados de forma fluida.

Las configuraciones clave aplicadas en el router se dividen en tres áreas fundamentales:

1. **Aseguramiento de accesos al router (Hardening):** Se cerraron las posibles puertas de entrada vulnerables desactivando por completo los servicios de fábrica que viajan sin cifrar y que no son necesarios para la operación, tales como Telnet, FTP y HTTP. Para los accesos administrativos esenciales, Winbox y SSH, se cambiaron los números de puerto por defecto por puertos personalizados ocultos. Adicionalmente, se apagaron los protocolos de descubrimiento de equipos en las interfaces que conectan a los clientes, evitando que cualquier usuario pueda escanear la red o conocer el modelo y la dirección MAC del router

principal.

2. **Políticas del firewall:** En el cortafuegos del sistema se establecieron reglas dinámicas para mitigar amenazas comunes y aislar de forma correcta el tráfico de la siguiente manera:

- **Aislamiento de tráfico:** Se restringió el acceso directo hacia el router, permitiendo que solo las IPs del administrador puedan gestionarlo. Del mismo modo, se bloqueó la comunicación entre los propios usuarios, asegurando que el tráfico de un cliente viaje directamente hacia internet sin posibilidad de interactuar o invadir la privacidad de los demás vecinos conectados.
- **Control de acceso administrativo:** Se bloquearon todos los intentos de conexión externa hacia el router, permitiendo la gestión del equipo únicamente desde direcciones IP locales específicas y autorizadas.
- **Mitigación de ataques automatizados:** Se crearon reglas dinámicas asociadas a listas de bloqueo para detectar y banear automáticamente por 24 horas a cualquier dirección que intente realizar ataques de fuerza bruta para adivinar contraseñas.
- **Aislamiento de usuarios:** Se configuraron reglas de filtrado que impiden la comunicación directa entre las diferentes cuentas de clientes, esto garantiza que el tráfico de cada hogar o empresa viaje de forma aislada hacia internet, impidiendo que usuarios maliciosos intenten escanear o invadir los equipos de sus vecinos dentro de la misma red inalámbrica.

3. **Control de navegación seguro (NAT):** Para otorgar la salida a internet, se configuró el enmascaramiento de red de forma restrictiva, amarrándolo exclusivamente al rango de direcciones asignado al pool de clientes PPPoE. De esta manera, si un equipo intenta navegar utilizando una dirección IP estática o no autorizada, el router descarta sus paquetes inmediatamente, neutralizando el robo de servicio.

3.6 Procedimiento de implementación técnica

La ejecución del proyecto se estructurará en fases consecutivas, garantizando un despliegue ordenado de los servicios de red.

3.6.1 Fase 1: Configuración del enrutador central (Core MikroTik)

En esta etapa se establecerán los cimientos lógicos del sistema, incluyendo el endurecimiento de la seguridad del dispositivo, la segmentación de tráfico en la Capa 2 mediante el estándar IEEE 802.1Q, la habilitación de los servidores de autenticación PPPoE y el despliegue del mecanismo de gestión de tráfico. El procedimiento detallado abarca las siguientes acciones:

- **Configuración inicial y seguridad:** Se procederá con la actualización del *firmware* y del sistema operativo RouterOS a la versión estable v7.19.6. Seguidamente, se desactivarán los servicios de administración vulnerables o innecesarios (tales como FTP, Telnet y SSH si no se requiere), restringiendo el acceso mediante WinBox únicamente al segmento de administración interna y asignando una identidad única al nodo (*identity*) para mitigar vectores de ataque perimetrales.
- **Configuración de interfaces y VLANs (IEEE 802.1Q):** En lugar de asociar subinterfaces directamente a puertos físicos, se creará un puente lógico (*Bridge*) principal con la función de filtrado de etiquetas activa (*vlan-filtering=yes*). Sobre esta entidad virtual se estructurarán los segmentos lógicos: *VLAN 10* (Administración), *VLAN 30* (Empresarial), *VLAN 40* (VIP) y *VLAN 50* (Estándar), vinculando los puertos físicos en modo troncal (*Tagged*) o modo acceso (*Untagged*) según la topología. A cada interfaz virtual de VLAN se le asignará su respectiva dirección IP para operar como puerta de enlace predeterminada (*default gateway*) de su segmento. El bloque de comandos CLI correspondiente se detalla en el Anexo 4.10.
- **Implementación del servidor PPPoE:** La gestión y aprovisionamiento del acceso a internet para los abonados se estructurará bajo los siguientes criterios:
 1. Se definirán los rangos de direccionamiento IP dinámico específicos para cada clase de abonado (Empresarial, VIP y Estándar).
 2. Se estructurarán los perfiles de servicio, en los cuales se configurarán los servidores DNS y la optimización del tamaño máximo de segmento TCP (*TCP MSS Adjustment*) para prevenir problemas de fragmentación sobre los enlaces inalámbricos, delegando el

control de ancho de banda de forma centralizada al árbol de colas jerárquico.

3. Se instanciarán los servidores PPPoE sobre sus respectivas interfaces VLAN de datos, permitiendo el levantamiento de túneles lógicos seguros para la conectividad punto a punto de los abonados. Las instrucciones de consola integrales se detallan en el Anexo 4.10.

- **Gestión de calidad de servicio (QoS) y árbol de colas:** Para garantizar la calidad de servicio y optimizar el rendimiento del ancho de banda total disponible, se implementará una estructura centralizada de QoS basada en marcas de paquetes generadas en el *Firewall Mangle* y un árbol de colas jerárquico combinado con colas por conexión (*PCQ - Per Connection Queue*):

1. **Clasificación y priorización de clientes:** Se establecerá una jerarquía de prioridades sobre la raíz del WISP mapeando tres categorías principales de usuarios:
 - *Sector empresarial (Prioridad 2):* Ancho de banda garantizado (*Limit At*) de 5 Mbps y un límite máximo (*Max Limit*) de 60 Mbps.
 - *Clientes VIP (Prioridad 4):* Límite máximo asignado de hasta 30 Mbps.
 - *Clientes estándar (Prioridad 7):* Límite máximo asignado de hasta 15 Mbps.
2. **Subcolas de tráfico para el sector empresarial:** Con el fin de mitigar la latencia en las operaciones corporativas críticas, el ancho de banda del segmento empresarial se subdividirá dinámicamente en tres subcolas jerárquicas:
 - *Tráfico de tiempo real y voz/video (Prioridad 1):* Máxima prioridad dedicada exclusivamente a plataformas de videoconferencia e interacciones sensibles a la latencia (por ejemplo, Zoom o VoIP).
 - *Tráfico web general (Prioridad 3):* Prioridad intermedia asignada a la navegación web sobre puertos HTTP y HTTPS (puertos TCP 80 y 443).
 - *Tráfico residual y descargas (Prioridad 7):* Menor prioridad destinada a transferencias en segundo plano, descargas pesadas y tráfico no clasificado.
3. **Ecualización de ancho de banda:** Se configurarán tipos de cola (*Queue Types*) con el algoritmo PCQ basados en la dirección de origen (*src-address*) para la subida y en la dirección de destino (*dst-address*) para la descarga. Esto asegura una distribución

equitativa del canal entre los usuarios concurrentes de cada segmento, evitando que un solo abonado monopolice la capacidad total de la cola. Las instrucciones completas de consola pueden consultarse en el Anexo 4.10.

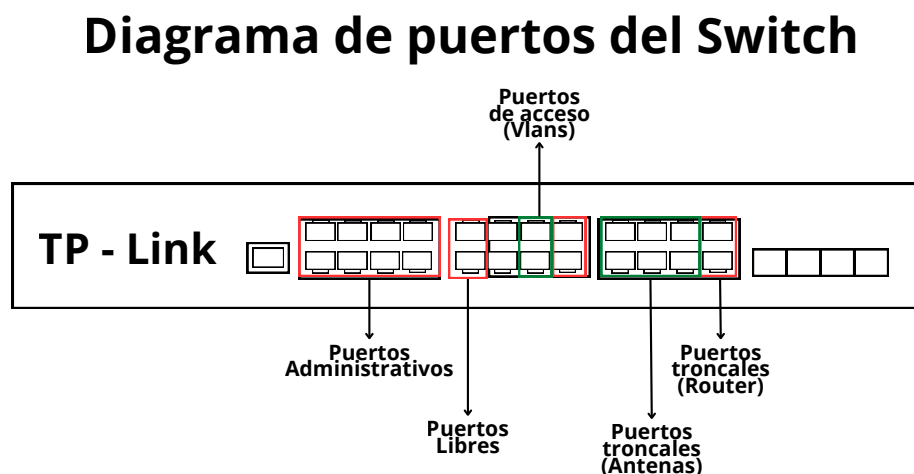
3.6.2 Fase 2: Configuración del switch y distribución

Se procederá a la configuración del Switch TP-Link para el manejo de puertos Trunk y Access. Esta fase asegura que las tramas de datos sean dirigidas correctamente hacia la antena sectorial sin pérdida de etiquetas de VLAN, siguiendo el estándar IEEE 802.1Q. La configuración de puertos se observa en la tabla 10.

Tabla 10
Asignación de puertos y etiquetado VLAN en el Switch.

Puerto Físico	Tipo de Enlace	VLAN Asociadas	Función / Destino
Port 1	Acceso (<i>Untagged</i>)	1	Puerto auxiliar (Administración)
Port 2 - 8	Acceso (<i>Untagged</i>)	10	Servidor Local (Administración)
Port 9 - 10	Shutdown	-	Puertos libres
Port 11 - 12	Acceso (<i>Untagged</i>)	30	Enlace Empresarial para pruebas
Port 13 - 14	Acceso (<i>Untagged</i>)	40	Enlace VIP para pruebas
Port 15 - 16	Acceso (<i>Untagged</i>)	50	Enlace STD para pruebas
Port 17 - 23	Troncal (<i>Tagged</i>)	10, 30, 40, 50	Enlace hacia Antena AP Sectoriales
Port 24	Troncal (<i>Tagged</i>)	10, 30, 40, 50	Interconexión con Core Router (ether2)

El etiquetado de tramas bajo el estándar IEEE 802.1Q en el conmutador garantiza que los paquetes viajen multiplexados a través de los enlaces troncales hacia las antenas del sector de distribución, manteniendo de extremo a extremo el aislamiento de tráfico configurado originalmente en el enrutador central.

Figura 24*Diagrama de puertos del switch*

- **Configuración del puerto Trunk:** El puerto conectado al Router Core se configurará en modo Trunk, donde se etiquetarán todas las VLANs definidas (10, 30, 40 y 50), permitiendo que el switch identifique y distribuya los diferentes flujos de servicios provenientes del MikroTik.
- **Configuración de puertos de acceso:** El puerto destinado a la antena sectorial se configurará para transportar la VLAN 10 (Gestión) y las VLANs de datos, dependiendo del diseño, este puerto puede actuar como un segundo Trunk hacia el AP o como un puerto de acceso específico si la antena solo gestiona un segmento.
- **Seguridad de puerto:** Como medida preventiva, se desactivarán los puertos que no estén en uso y se habilitará el aislamiento de puertos (Port Isolation) para evitar el tráfico innecesario de Capa 2 entre diferentes equipos de distribución.
- **Interfaz de gestión:** Se asignará una dirección IP estática al switch dentro del rango de la VLAN 10 (10.0.0.2), permitiendo el monitoreo remoto y la administración de la tabla de direcciones MAC.

3.6.3 Fase 3: Configuración de antenas (Enlaces inalámbricos)

Esta etapa comprende la configuración de los Puntos de Acceso (AP) ubicados en la torre principal y de los equipos receptores (CPE) instalados en las dependencias de los clien-

tes. Debido a que los parámetros de radiofrecuencia y la selección de canales mediante el análisis de espectro se gestionan dinámicamente, la parametrización se realiza a través de la interfaz gráfica de usuario (*GUI*) del fabricante Ubiquiti, aplicando los criterios técnicos que se resumen en la Tabla 11.

Tabla 11

Matriz de parámetros de radiofrecuencia para AP y CPE.

Parámetro Técnico	Configuración en punto de acceso (AP)	Configuración en cliente (CPE)
Modo de operación	<i>Access Point PtMP</i> (punto a multi-punto)	<i>Station PtMP</i> (Estación)
Banda de frecuencia	5 GHz (Línea de vista requerida)	5 GHz (Línea de vista requerida)
Ancho de canal (<i>Channel Width</i>)	20 MHz / 40 MHz (Según densidad de ruido)	Automático (Heredado del AP)
Seguridad inalámbrica	WPA2-PSK (Encriptación AES)	WPA2-PSK (Encriptación AES)
Configuración de red	Puente transparente (<i>Bridge Mode</i>)	Puente transparente (<i>Bridge Mode</i>)

Se configurará la antena LiteAP 5AC en modo *Access Point PtMP airMAX AC*, activando la tecnología propietaria de multiplexación por división de tiempo (TDMA). Posteriormente, se vincularán las estaciones de abonado (CPE), optimizando los parámetros de frecuencia y ancho de canal para minimizar la interferencia electromagnética. El procedimiento técnico contempla los siguientes ajustes:

- **Selección de frecuencia y ancho de canal:** Se realizará un escaneo de espectro mediante la herramienta *airView* para identificar canales con menor nivel de ruido en la banda de 5 GHz, donde se seleccionará un ancho de canal de 20 MHz o 40 MHz, buscando un equilibrio entre capacidad de transporte (throughput) e inmunidad a la interferencia.
- **Configuración de modo inalámbrico:** La estación base se establecerá en modo *Access Point PtMP airMAX AC*, activando la función de TDD Framing (Flexible o New Fixed) para optimizar el tiempo de transmisión de los datos hacia los múltiples CPEs conectados.
- **Alineación y ganancia:** En el lado del abonado (CPE), se utilizará la herramienta de ali-

neación visual del sistema operativo *airOS* para obtener un nivel de señal (RSSI) óptimo, apuntando a un rango entre -40 dBm y -50 dBm, con una ganancia de -4 dBm.

- **Seguridad de enlace:** Se implementará el cifrado WPA2-PSK (AES) con una clave compartida de alta complejidad, asegurando que solo los CPEs autorizados con el SSID de la red puedan asociarse al punto de acceso.

3.6.4 Fase 4: Configuración de MikroTik (Cliente)

Se procede a la configuración del MikroTik instalado en el abonado, el cual cumplirá el rol de puerta de enlace. El procedimiento técnico se detalla a continuación.

1. **Configuración del cliente PPPoE:** Se habilitará un cliente PPPoE sobre la interfaz física conectada al CPE. Se ingresarán las credenciales (usuario y contraseña) asignadas previamente en el Core, permitiendo la obtención de una dirección IP dinámica dentro del segmento de gestión y estableciendo el túnel de datos.
2. **Configuración de la red local (LAN):** Se definirá una interfaz Bridge que agrupe los puertos restantes y la interfaz WLAN. A este bridge se le asignará la dirección IP correspondiente al segmento del cliente (ej. 192.168.40.1/24 para usuarios estándar), funcionando como el Default Gateway de la red interna.
3. **Servidor DHCP y NAT:** Se configurará un servidor DHCP para la asignación automática de direcciones IP a los dispositivos del abonado, asimismo, se implementará una regla de enmascaramiento en el Firewall NAT para permitir que el tráfico de la LAN salga a través del túnel PPPoE hacia el internet global.
4. **Seguridad básica:** Se establecerá un usuario y contraseña al router del cliente asegurando la integridad del acceso local.

3.6.5 Fase 5: Pruebas de validación y QoS

Finalmente, se realizarán pruebas de estrés sobre la red para verificar el correcto funcionamiento del Queue Tree. Se validará que, ante la saturación del segmento residencial, el tráfico del segmento empresarial mantenga los parámetros de latencia y ancho de banda estipulados.

4 CAPÍTULO 4: RESULTADOS

4.1 Identificación de elementos de la red

Gracias a la topología detallada en el Capítulo 3 (Figura 23) y a la estructura presentada en las Tablas 2 y 3, en las que se indica la segmentación de VLAN y el direccionamiento IP de los diferentes equipos, se logró implementar de forma exitosa la red de acceso inalámbrico con la totalidad de sus funcionalidades y parámetros configurados.

4.2 Implementación bajo normativas y estándares

Los equipos utilizados en la red, detallados en las Tablas 5 y 6, aseguran el cumplimiento de la normativa de ARCOTEL, la cual establece que las redes WISP deben operar dentro de bandas de frecuencia del espectro libre. Por consiguiente, las antenas LiteAP 5AC y NanoStation Loco 5AC del fabricante Ubiquiti se encuentran configuradas para operar en la banda de 5 GHz. Asimismo, estos dispositivos cumplen con el estándar internacional IEEE 802.11ac mediante el protocolo propietario *airMAX ac*, fundamentado en la tecnología de acceso múltiple por división de tiempo (*Time Division Multiple Access* - TDMA).

Por otra parte, en lo que respecta a la infraestructura de cableado estructurado, la interconexión entre los dispositivos cumple con el estándar ANSI/TIA-568. Dicha norma especifica que los cables utilizados para el enlace hacia las antenas mediante alimentación a través de ethernet deben corresponder a la categoría 5e o 6 con blindaje para exteriores (*Outdoor STP/FTP*). De igual forma, en la terminación de los conectores RJ-45 se aplicó el esquema de cableado T568B, garantizando la correcta disposición de los pares de conductores durante el conectorizado.

4.3 Pruebas de rendimiento

4.3.1 Pruebas internas de la red con *iPerf3*

Para evaluar el rendimiento de la infraestructura, se realizaron pruebas de estrés mediante la herramienta de código abierto *iPerf3*, la cual permite determinar la capacidad de

transferencia de los enlaces inalámbricos y verificar el comportamiento del esquema de colas de prioridad aplicadas a los abonados. Durante estas mediciones, se monitorearon los parámetros de tasa de bits (*bitrate*) y el porcentaje de pérdida de paquetes (*packet loss*).

Con este propósito, se instanciaron tres servicios en modo de escucha (*listener*) dentro del segmento de administración (10.10.10.0/24), asociados a los puertos TCP/UDP 5201, 5202 y 5203. Por parte de los terminales de usuario, se ejecutaron clientes *iPerf3* configurados para la generación de tráfico sobre el protocolo UDP dirigido a los servidores mencionados. En estas pruebas se respetaron los perfiles de ancho de banda contratados por cada categoría de abonado: 60 Mbps para el sector Empresarial, 30 Mbps para clientes VIP y 15 Mbps para el segmento Estándar.

4.3.2 Prueba de red sin priorización de tráfico

El objetivo de esta prueba es comprobar el rendimiento inicial de la red, previo a la aplicación de algoritmos para priorizar el tráfico de los clientes dependiendo de la VLAN asignada, con una velocidad total de 375 Mbps en dos escenarios: uno con red no saturada y otro con red saturada.

Prueba con red no saturada. Se realizó una prueba de rendimiento enviando tráfico desde los abonados, de forma individual obteniendo los siguientes resultados.

- **Abonado Empresa:** Obtuvo un *bitrate* promedio de 94.9 Mbps con pérdidas de paquetes de 0.03 %.
- **Abonado VIP:** Logró un *bitrate* de 98.2 Mbps y una tasa de error del 1.4 %.
- **Abonado Estándar:** Registró un *bitrate* de 77.8 Mbps y una tasa de pérdidas del 2.60 %.

Prueba con red saturada. Se procedió a una nueva prueba de rendimiento pero con una red saturada, observando los siguientes resultados.

- **Abonado Empresa:** Obtuvo un *bitrate* promedio de 41.5 Mbps con pérdidas de paquetes de 72.0 %.
- **Abonado VIP:** Logró un *bitrate* de 39.9 Mbps y una tasa de error del 60.0 %.
- **Abonado Estándar:** Registró un *bitrate* de 38.7 Mbps y una tasa de pérdidas del 51.0 %.

4.3.3 *Prueba red no saturada con priorización de tráfico*

Esta prueba busca verificar el comportamiento de cada cliente transmitiendo de forma individual y sin interferencias, una vez aplicadas las colas de prioridad. Esto nos permite verificar que la tasa de transferencia sea la correcta para cada abonado.

- **Abonado Empresa:** Alcanzó un bitrate promedio de 58.9 Mbps con un jitter bajo de 0.870ms y pérdidas de paquetes de 1.8 %.
- **Abonado VIP:** Logró un bitrate de 29.5 Mbps prácticamente saturando su canal asignado, un jitter de 0.456ms y una tasa de error del 1.8 %.
- **Abonado Estándar:** Registró un bitrate de 14.6 Mbits/sec, un jitter de 1.855ms y una tasa de pérdidas del 2.3 %.

Este primer test nos permite identificar que la red se encuentra alineada y en funcionamiento, logrando condiciones óptimas para los clientes VIP y Estándar, encontrándose cerca del 100 % de sus canales asignados.

4.3.4 *Prueba con red saturada con priorización de tráfico*

En esta prueba el objetivo es identificar el comportamiento de la red saturada por la gran cantidad de tráfico enviado por los clientes.

- **Abonado empresa:** La tasa de transferencia llegó a 55.4 Mbps con una tasa de pérdida del 7 %.
- **Abonado VIP:** El bitrate llegó a 29.5 Mbps, sufriendo una tasa de pérdida del 1.7 %.
- **Abonado Estándar:** La tasa de transmisión se mantuvo en 14.7 Mbps, reportando una pérdida del 1.7 %.

Durante esta prueba, con la red operando a su máxima capacidad, los enlaces inalámbricos funcionan con normalidad, evidenciando el QoS configurado.

4.4 **Pruebas de rendimiento usando nperf**

En esta sección se presentarán los resultados obtenidos mediante la herramienta nperf, donde se verificará el comportamiento de las velocidades de descarga y subida, así como la

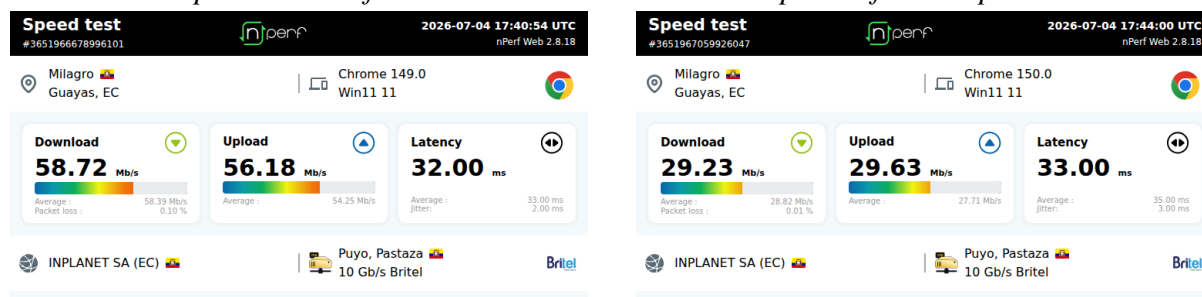
latencia que presenta la red para los distintos usuarios: empresa, VIP y estándar.

Para evaluar el rendimiento de la infraestructura bajo diferentes escenarios, se realizaron dos pruebas: la primera con una red no saturada, simulando un poco de tráfico de usuarios, y la segunda con una red saturada, simulando una hora pico con una alta cantidad de tráfico.

4.4.1 Prueba 1: Red no saturada

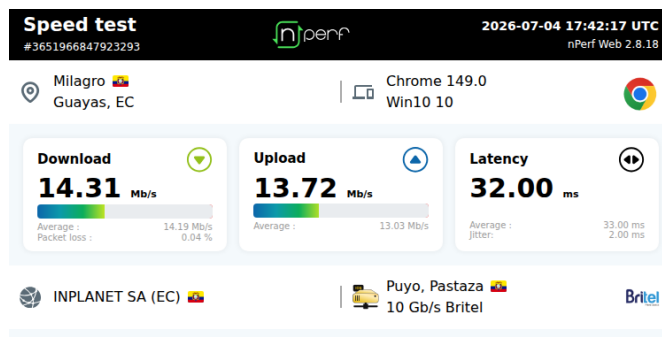
Figura 25

Resultados de pruebas nPerf en escenario de uso individual para diferentes planes de cliente.



(a) Cliente Empresa

(b) Cliente VIP



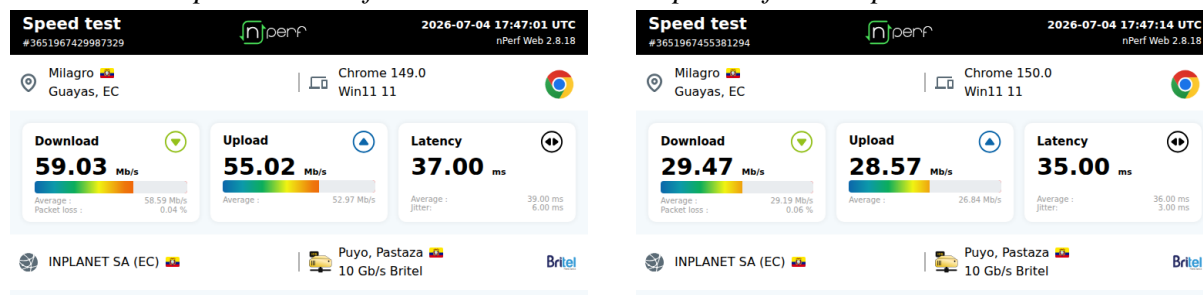
(c) Cliente Estándar

Durante esta prueba, el cliente empresa obtuvo 58.72 Mbps de Download y 56.18 Mbps de Upload con latencia de 32 ms, como se observa en la figura 25a, mientras que en la figura 25b el usuario VIP presentó 29.23 Mbps de Download y 29.63 Mbps de Upload con latencia de 33 ms. Por último, el usuario estándar obtuvo un resultado de 14.31 Mbps / 13.72 Mbps de Download y Upload correspondiente, además de una latencia de 32 ms, como se observa en la figura 25c.

4.4.2 Prueba 2: Red saturada

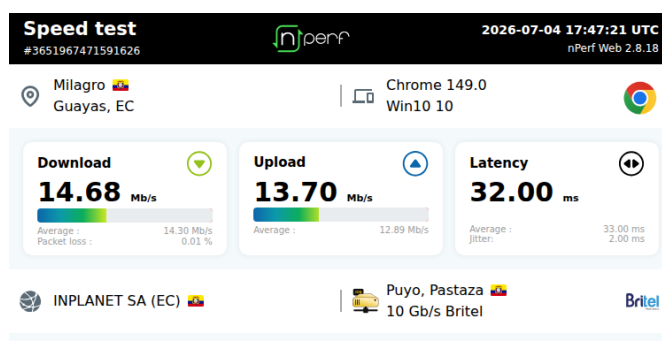
Figura 26

Resultados de pruebas nPerf en escenario saturado para diferentes planes de cliente.



(a) *Cliente Empresa*

(b) *Cliente VIP*



(c) *Cliente Estándar*

Por otro lado, al momento de las pruebas con la red saturada se observa que en la figura 26a, el cliente Empresa obtuvo una velocidad de descarga de 59.03 Mbps y 55.02 Mbps de subida y bajada, manteniendo una latencia de 37 ms. En el caso del usuario VIP, que se muestra en la figura 26b, obtuvo 29.47 Mbps de descarga y 28.57 Mbps de subida con una latencia de 35 ms. Por último, el usuario Estándar (figura 26c) mantuvo una velocidad de 14.68 Mbps de descarga y 13.70 Mbps de subida con 32 ms de latencia.

4.5 Análisis de resultados y discusión en QoS

En la siguiente sección se analizarán las pruebas de rendimiento ya mencionadas en el apartado anterior.

4.5.1 Análisis de resultados Iperf previo a la aplicación de QoS

Tabla 12

Rendimiento en red sin QoS ni priorización por VLANs (Iperf)

Perfil de Abonado	Test 1 (Red no saturada)		Test 2 (Red saturada)	
	Bitrate	% Pérd.	Bitrate	% Pérd.
Empresa (60M)	94.9 Mbps	0.03 %	41.5 Mbps	72.0 %
VIP (30M)	98.2 Mbps	1.40 %	39.9 Mbps	60.0 %
Estándar (15M)	77.8 Mbps	2.60 %	38.7 Mbps	51.0 %

En la tabla 12 se evidencia la falta de políticas de priorización de tráfico de los clientes, donde en condiciones de red no saturada los abonados superan deliberadamente los límites de sus planes contratados. Esto ocurre debido a la ausencia de mecanismos de control de ancho de banda, permitiendo que el perfil VIP (30M) y Estándar (15M) alcancen tasas de transferencia de 98.2 Mbps y 77.8 Mbps respectivamente, consumiendo recursos que comprometen la estabilidad general del enlace.

Por otro lado, al inducir un escenario de red saturada, la carencia de segmentación por VLANs y de algoritmos de calidad de servicio (QoS) provoca una degradación crítica en el rendimiento. Sin una cola de prioridad asignada, el abonado de perfil Empresa (60M) sufre una pérdida de paquetes extrema del 72.0 % y una caída de su bitrate a 41.5 Mbps. Un comportamiento similar se observa en los servicios VIP y Estándar, cuyas pérdidas superan el 50 %, demostrando que bajo situaciones de estrés el tráfico se distribuye de manera caótica e injusta, afectando severamente a los clientes que requieren mayor disponibilidad.

4.5.2 Análisis de resultados Iperf posterior a la aplicación de QoS

Tabla 13

Comparativa de rendimiento UDP mediante iPerf3

Perfil de Abonado	Test 1 (Red no saturada)		Test 2 (Red saturada)	
	Bitrate	% Pérd.	Bitrate	% Pérd.
Empresa (60 Mbps)	58.9 Mbps	1.8 %	55.4 Mbps	7.0 %
VIP (30 Mbps)	29.5 Mbps	1.8 %	29.5 Mbps	1.7 %
Estándar (15 Mbps)	15.6 Mbps	1.8 %	14.7 Mbps	1.7 %

En el escenario de la Prueba 1 con una red no saturada, los resultados tienen un comportamiento cercano al 100 % de eficiencia para los perfiles de cliente Empresa, VIP y Estándar. Las tasas de transferencia registradas se aproximan a las velocidades previamente configuradas en el router, lo que demuestra que, ante un tráfico de red bajo o controlado, la infraestructura entrega el rendimiento teórico esperado para cada abonado.

Por otro lado, durante la Prueba 2 con una red saturada, al someter la infraestructura a su máxima exigencia mediante el consumo simultáneo del ancho de banda de todos los abonados, se evidenció que los perfiles mantuvieron su tasa de transferencia dentro del rango de las velocidades asignadas. Esto confirma la efectividad de las políticas de control de tráfico implementadas, impidiendo el colapso de un canal sobre otro en horas pico.

Por consiguiente, se determina que el comportamiento de la red se adecúa de manera óptima a los requerimientos de diseño estipulados en capítulos anteriores. Este comportamiento se observa cuantitativamente por los valores mostrados en la tabla 13.

4.5.3 Análisis de resultados nPerf

Tabla 14

Comparativa de rendimiento de red mediante nPerf

Perfil de Abonado	Red no saturada			Red saturada		
	Descarga	Subida	Latencia	Descarga	Subida	Latencia
Empresa (60 Mbps)	58.72 Mbps	56.18 Mbps	32 ms	59.03 Mbps	55.02 Mbps	37 ms
VIP (30 Mbps)	29.23 Mbps	29.63 Mbps	33 ms	29.47 Mbps	28.57 Mbps	35 ms
Estándar (15 Mbps)	14.31 Mbps	13.72 Mbps	32 ms	14.68 Mbps	13.70 Mbps	32 ms

Con base en los resultados obtenidos de las pruebas con nPerf, se procede a medir la calidad de experiencia del usuario final, usando parámetros de descarga, subida y latencia, como se muestra en la tabla 14, con el fin de evaluar el comportamiento de la red en última milla.

4.5.4 Análisis del canal de descarga (Download)

Tabla 15

Porcentajes de eficiencia y degradación en la tasa de descarga (Download)

Perfil de abonado	Red no saturada		Red saturada	
	Eficiencia	Degradación	Eficiencia	Degradación
Empresa (60 Mbps)	97.9 %	2.1 %	98.4 %	1.6 %
VIP (30 Mbps)	97.4 %	2.6 %	98.2 %	1.8 %
Estándar (15 Mbps)	95.4 %	4.6 %	97.9 %	2.1 %

Nota. Porcentajes calculados tomando como referencia únicamente el canal de descarga (*Download throughput*).

De acuerdo con la tabla 15, el canal de descarga mostró una estabilidad casi perfecta en ambos escenarios de prueba. En condiciones normales, red no saturada, los tres perfiles obtuvieron un rendimiento excelente, con eficiencias que van desde el 95.4 % en el plan Estándar hasta el 97.9 % en el plan Empresa. Lo más destacable ocurre al saturar la red: al exigir el máximo ancho de banda de forma simultánea, las velocidades de descarga no sufrieron caí-

das. Al contrario, se mantuvieron estables con eficiencias superiores al 97.9 % en todos los casos y niveles de degradación mínimos, entre el 1.6 % y el 2.1 %. Esto demuestra que el sistema protege con éxito el tráfico de bajada de los usuarios, asegurando que reciban la velocidad contratada incluso en las horas de mayor consumo.

4.5.5 Análisis del canal de subida (Upload)

Tabla 16

Porcentajes de eficiencia y degradación en la tasa de subida (Upload)

Perfil de abonado	Red no saturada		Red saturada	
	Eficiencia	Degradación	Eficiencia	Degradación
Empresa (60 Mbps)	93.6 %	6.4 %	91.7 %	8.3 %
VIP (30 Mbps)	98.8 %	1.2 %	95.2 %	4.8 %
Estándar (15 Mbps)	91.5 %	8.5 %	91.3 %	8.7 %

Nota. Porcentajes calculados tomando como referencia únicamente el canal de subida (*Upload throughput*).

Al observar los porcentajes de la Tabla 16, se evidencia que el canal de subida experimenta variaciones notables al cambiar las condiciones de tráfico. Cuando la red opera sin saturación, el rendimiento es óptimo: el cliente VIP obtiene la mejor eficiencia, con un 98.8 % y apenas 1.2 % de degradación, mientras que los planes Empresa y Estándar registran pérdidas más bajas, del 6.4 % y 8.5 % respectivamente.

Al pasar a un escenario con red saturada, el impacto del consumo simultáneo se hace visible en este canal, provocando un aumento general en los niveles de degradación. El plan Empresa eleva su pérdida al 8.3 % y el plan Estándar alcanza el 8.7 %. En el caso del cliente VIP, la degradación es mayor, pasando del 1.2 % al 4.8 % debido al estrés de la red en hora pico. A pesar de este incremento en las pérdidas, el canal de subida demuestra una sólida estabilidad, ya que todos los abonados logran mantener una eficiencia superior al 91 %, evitando caídas drásticas en el servicio.

4.6 Verificación del comportamiento de las colas de prioridad

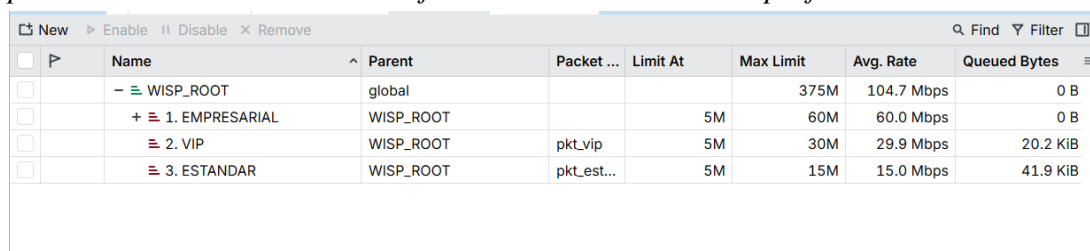
En esta sección se analiza visualmente el comportamiento de las reglas de control de tráfico configuradas en el Queue Tree del enrutador central. A través de capturas en tiempo real de la herramienta WinBox, se observa cómo el sistema distribuye, prioriza y limita el ancho de banda bajo diferentes escenarios de estrés.

4.6.1 Verificación de tráfico constante de todos los abonados

Para evaluar la equidad en la distribución del ancho de banda, se inyectó a la red una carga constante donde todos los clientes principales exigen su velocidad máxima contratada. El comportamiento del router se evidencia en la figura 27.

Figura 27

Comportamiento de las colas con tráfico constante en todos los perfiles.



	Name	Parent	Packet ...	Limit At	Max Limit	Avg. Rate	Queued Bytes
	WISP_ROOT	global			375M	104.7 Mbps	0 B
	1. EMPRESARIAL	WISP_ROOT		5M	60M	60.0 Mbps	0 B
	2. VIP	WISP_ROOT	pkt_vip	5M	30M	29.9 Mbps	20.2 KiB
	3. ESTANDAR	WISP_ROOT	pkt_est...	5M	15M	15.0 Mbps	41.9 KiB

Como se observa en dicha captura, las tasas promedio o *Avg. Rate* se estabilizan de manera exacta en los valores de diseño asignados en el *Max Limit* de cada clase, el cliente Empresa alcanza los 60.0 Mbps, el cliente VIP llega a 29.9 Mbps y el cliente Estándar se mantiene en 15.0 Mbps. El consumo total del árbol de colas (*WISP_ROOT*) marca un tráfico global de 104.7 Mbps. Además se observa que la coloración roja en las colas de los clientes evidencia que están operando al límite de su capacidad permitida, confirmando que las políticas de control impiden que un perfil absorba los recursos asignados a los demás abonados.

4.6.2 Verificación de subcolas del área empresarial

Con el fin de validar la priorización interna dentro de un mismo perfil de abonado, se verificó el comportamiento de las subcolas del área empresarial utilizando la figura 28.

Figura 28

Distribución de tráfico interno en las subcolas del perfil Empresa.

	Name	Parent	Packet ...	Limit At	Max Limit	Avg. Rate	Queued Bytes
	WISP_ROOT	global			375M	105.3 Mbps	0 B
	1. EMPRESARIAL	WISP_ROOT		5M	60M	60.2 Mbps	0 B
	1.1 Video_Emp	1. EMPRESARIAL	pkt_em...	5M	60M	880 bps	0 B
	1.2 Web_Emp	1. EMPRESARIAL	pkt_em...	5M	60M	3.1 kbps	0 B
	1.3 Resto_Emp	1. EMPRESARIAL	pkt_em...	5M	60M	59.9 Mbps	14.5 KiB
	2. VIP	WISP_ROOT	pkt_vip	5M	30M	29.9 Mbps	13.0 KiB
	3. ESTANDAR	WISP_ROOT	pkt_est...	5M	15M	14.9 Mbps	21.7 KiB

Al momento de desglosar la cola padre **1. EMPRESARIAL**, el sistema segmenta el tráfico según el tipo de servicio. En este escenario, la subcola **1.3 Resto_Emp** registra 59.9 Mbps de tráfico activo y la subcola **1.2 Web_Emp** se sitúa en 3.1 kbps, debido a que en este escenario se realizó una descarga de un archivo pesado, evidenciando el correcto marcado de paquetes en las subcolas de prioridad.

4.6.3 Inyección de tráfico UDP con descarga

El último escenario consistió en inyectar un flujo masivo de paquetes UDP junto con una descarga, con el fin de evidenciar las prioridades de tráfico según el protocolo de transmisión. Este escenario se registró a través de la Figura 29.

Figura 29

Comportamiento del Queue Tree ante la inyección de tráfico UDP con descarga activa.

	Name	Parent	Packet ...	Limit At	Max Limit	Avg. Rate	Queued Bytes
	WISP_ROOT	global			375M	86.5 Mbps	0 B
	1. EMPRESARIAL	WISP_ROOT		5M	60M	59.8 Mbps	0 B
	1.1 Video_Emp	1. EMPRESARIAL	pkt_em...	5M	60M	52.5 Mbps	33.2 KiB
	1.2 Web_Emp	1. EMPRESARIAL	pkt_em...	5M	60M	43.2 kbps	0 B
	1.3 Resto_Emp	1. EMPRESARIAL	pkt_em...	5M	60M	7.4 Mbps	40.2 KiB
	2. VIP	WISP_ROOT	pkt_vip	5M	30M	11.7 Mbps	0 B
	3. ESTANDAR	WISP_ROOT	pkt_est...	5M	15M	14.9 Mbps	31.9 KiB

Durante esta prueba, el tráfico UDP fue marcado correctamente pasando por la subcola de prioridad **1.1 Video_Emp** donde se evidencia que el tráfico UDP absorbe 52.5 Mbps, dejando a las otras subcolas en prioridad baja, tal como se muestra en la subcola **1.3 Resto_Emp**, donde pasó de 59.9 Mbps a 7.4 Mbps, mostrando un total de 59.8 Mbps usados por el cliente empresa.

Esto demuestra que las colas descartan adecuadamente el tráfico excedente en la interfaz, evitando la degradación del servicio de los demás abonados.

4.7 Verificación de seguridad de clientes

Para evaluar la efectividad de las medidas de seguridad estructuradas en el modelo por capas, se llevaron a cabo pruebas funcionales en cada una de las fases de control definidas en la arquitectura de red.

4.7.1 Etapa 1: Control de acceso y autenticación mediante servidor PPPoE

La validación del control de acceso se ejecutó simulando un intento de conexión no autorizada. Para ello, se conectó un router cliente sin credenciales válidas a un CPE previamente enlazado a una VLAN de la red.

Tabla 17

Resultados de la prueba de control de acceso y autenticación PPPoE.

Parámetro / Escenario	Detalle / Resultado Observado
Dispositivo de prueba	Router cliente sin credenciales válidas
Punto de acceso	CPE enlazado a VLAN de la red
Mecanismo de validación	Servidor PPPoE en RouterBoard
Negociación del túnel	Denegada
Asignación de IP	Nula (Sin direccionamiento dinámico)
Gestión de ancho de banda	Sin asignación en colas de procesamiento (<i>Queues</i>)
Resultado de seguridad	Uso no autorizado prevenido de forma efectiva

En la tabla 17, se validó que al no suministrar un usuario y contraseña registrado en la base de datos del *RouterBoard*, el servidor PPPoE denegó la negociación del túnel. Como consecuencia, el dispositivo no obtuvo un direccionamiento IP dinámico ni fue asignado a las colas de procesamiento de ancho de banda, previniendo de forma efectiva el uso no autorizado de la infraestructura.

4.7.2 Etapa 2: Aislamiento e interceptación de tráfico inter-VLAN

Tabla 18

Evaluación de conectividad PING entre la VLAN 10 (Gestión) y los diferentes segmentos de clientes antes y después de aplicar reglas de firewall.

(a) Conectividad bidireccional entre VLAN 10 y segmento Empresa

Parámetro / Métrica	VLAN 10 → Empresa		Empresa → VLAN 10	
	Sin reglas	Con reglas	Sin reglas	Con reglas
Origen	VLAN 10	VLAN 10	Empresa	Empresa
IP Destino	172.16.30.254	172.16.30.254	10.10.10.223	10.10.10.223
Protocolo	ICMP	ICMP	ICMP	ICMP
Enviados / Recibidos	4 / 4	4 / 4	4 / 4	4 / 0
Porcentaje de pérdida	0 %	0 %	0 %	100 %
RTT Promedio	12 ms	12 ms	12 ms	N/A
Estado del tráfico	Permitido	Permitido	Permitido	Bloqueado

(b) Conectividad bidireccional entre VLAN 10 y segmento VIP

Parámetro / Métrica	VLAN 10 → VIP		VIP → VLAN 10	
	Sin reglas	Con reglas	Sin reglas	Con reglas
Origen	VLAN 10	VLAN 10	VIP	VIP
IP Destino	172.16.40.254	172.16.40.254	10.10.10.223	10.10.10.223
Protocolo	ICMP	ICMP	ICMP	ICMP
Enviados / Recibidos	4 / 4	4 / 4	4 / 4	4 / 0
Porcentaje de pérdida	0 %	0 %	0 %	100 %
RTT Promedio	12 ms	12 ms	12 ms	N/A
Estado del tráfico	Permitido	Permitido	Permitido	Bloqueado

(c) Conectividad bidireccional entre VLAN 10 y segmento Estándar

Parámetro / Métrica	VLAN 10 → Estándar		Estándar → VLAN 10	
	Sin reglas	Con reglas	Sin reglas	Con reglas
Origen	VLAN 10	VLAN 10	Estándar	Estándar
IP Destino	172.16.50.254	172.16.50.254	10.10.10.223	10.10.10.223
Protocolo	ICMP	ICMP	ICMP	ICMP
Enviados / Recibidos	4 / 4	4 / 4	4 / 4	4 / 0
Porcentaje de pérdida	0 %	0 %	0 %	100 %
RTT Promedio	12 ms	12 ms	12 ms	N/A
Estado del tráfico	Permitido	Permitido	Permitido	Bloqueado

La efectividad de las reglas de *Firewall* se evaluó en dos escenarios, mediante ping, verificando el aislamiento entre los clientes y el área de administración, manteniendo como única excepción la VLAN 10, cuya regla de precedencia le permite administrar las subredes de abonados para labores de mantenimiento y monitoreo, tal como se muestra en la tabla 18.

4.7.3 Etapa 3: Auditoría de hardening e inactivación de servicios

Finalmente, el robustecimiento de la infraestructura se validó mediante un escaneo activo de puertos utilizando la herramienta *Nmap*, ejecutado desde la estación de trabajo de un cliente hacia la dirección IP del router de administración.

Tabla 19

Resultados de hardening e inactivación de servicios de gestión.

Servicio / Protocolo	Puerto	Estado Observado	Observación / Protocolo Seguro
Telnet	23	Filtered	Inactivo (bloqueado)
FTP	21	Filtered	Inactivo (bloqueado)
HTTP	80	Filtered	Inactivo (bloqueado)
SSH	22	Open / Encrypted	Canal seguro para gestión CLI
Winbox	–	Open / Encrypted	Acceso seguro restringido por IP/VLAN

Los resultados de la tabla 19 confirmaron que los puertos para ataques comunes y protocolos no cifrados tales como Telnet (puerto 23), HTTP (puerto 80) y FTP (puerto 21) se encuentran en estado **Filtered**. De esta manera, se garantiza que la gestión de red se realice exclusivamente a través de canales seguros y cifrados (SSH y Winbox), elevando la seguridad del sistema.

4.8 Análisis de resultados y discusión en seguridad

A modo de síntesis, en la Tabla 20 se verifica la evaluación del modelo de seguridad por capas implementado en la red, detallando los mecanismos, las pruebas ejecutadas, los resultados cuantitativos obtenidos y el estado de cumplimiento final de cada etapa.

Tabla 20

Matriz de verificación y validación de la estrategia de seguridad en la red

Etapas de Seguridad	Mecanismo	Prueba Realizada	Resultado Obtenido	Estado
Etapas 1: Acceso	Servidor PPPoE	Solicitud de acceso con y sin credenciales únicas.	100 % de autenticaciones válidas; 0 accesos no autorizados.	Cumplido
Etapas 2: Aislamiento	Regla Inter-VLAN	Ping entre VLANs de distintos abonados.	0 % de conectividad inter-VLAN (100 % de paquetes descartados).	Cumplido
	Excepción VLAN 10	Ping desde VLAN administrativa hacia abonados.	100 % de conectividad (0 % de pérdidas)	Cumplido
Etapas 3: Hardening	Puertos Inseguros	Escaneo Nmap a la IP del router (Telnet, FTP, HTTP).	Servidores y puertos inseguros deshabilitados (0 puertos abiertos).	Cumplido
	Gestión Segura	Intento de gestión remota mediante Winbox y SSH.	Conexiones cifradas y autenticadas correctamente.	Cumplido

4.9 Recomendaciones

- **Dejar un puerto de emergencia en el switch:** Configurar un puerto específico en una VLAN de administración y sin bloqueos de seguridad. Para evitar una pérdida de conexión completa con el switch, este puerto sirve como puerta trasera o como puerto de recuperación en caso de una mala configuración.
- **Respaldos al terminar y usar Modo Seguro:** Realizar una copia de seguridad (*backup*) de la configuración apenas todo quede funcionando correctamente. Además, activar siempre el *Safe Mode* (Modo Seguro) del router antes de realizar algún cambio, de modo que, en caso de quedar desconectado, el equipo revierta el cambio automáticamente y se evite tener que formatearlo por pérdida de la conexión.
- **Cuidar los niveles de señal en las antenas:** Al alinear los equipos, controlar la potencia de transmisión para que el nivel de señal (*RSSI*) quede en un punto intermedio, entre -50 dBm y -65 dBm. Si la señal queda más fuerte que -40 dBm, la antena se saturará y el enlace estará inestable a causa del ruido.
- **Etiquetar cables en ambos extremos:** Poner etiquetas claras en cada punta de los cables indicando de dónde viene, a dónde va y qué servicio lleva, esto permite ahorrar horas de búsqueda de fallas en el rack y evita desconexiones accidentales del cable equivocado.
- **Respetar la norma T568B al ponchar:** Usar siempre la norma T568B en todos los conectores RJ-45 para que todo el cableado sea uniforme. Después de ponchar, es obligatorio pasar el *tester* para asegurar que no queden hilos sueltos, cruzados o con falso contacto.
- **Revisar el estado físico del cableado:** Realizar inspecciones visuales para verificar que los cables no estén aplastados, demasiado doblados o deteriorados por la exposición al sol y al agua si se encuentran a la intemperie. Un cable dañado afecta el rendimiento y puede causar cortocircuitos.
- **Verificar la compatibilidad de los puertos PoE pasivos y activos:** Revisar qué tipo de alimentación requiere cada equipo antes de conectarlo. Suministrar PoE pasivo de 24V a un puerto que no lo soporta quemará la tarjeta de red del equipo de forma instantánea.

4.10 Conclusiones

A partir del diseño, implementación y evaluación experimental de la infraestructura de red de acceso para el proveedor de servicios de internet inalámbrico o WISP, se establecen las siguientes conclusiones, correspondientes con los objetivos planteados:

- **Identificación y rol de los elementos del WISP:** Se identificaron los componentes esenciales para la infraestructura del WISP, determinando que una red de acceso inalámbrica eficiente requiere la integración de tres pilares fundamentales: equipos de enrutamiento, conmutadores y enlaces inalámbricos de transporte. Esta base física y lógica demostró ser indispensable para garantizar la escalabilidad de la red, una distribución ordenada de los segmentos y un control granular del tráfico de datos.
- **Implementación de infraestructura bajo estándares y normativas:** El despliegue de la infraestructura de red se ejecutó bajo normativas y estándares internacionales de telecomunicaciones, tales como la especificación de cableado estructurado ANSI/TIA-568, el estándar de etiquetado de redes virtuales IEEE 802.1Q y el estándar de direccionamiento privado RFC 1918. La adopción de este marco normativo permitió establecer un esquema de direccionamiento IP jerárquico, garantizando el aislamiento lógico del tráfico entre clientes y blindando la seguridad y privacidad de sus datos.
- **Diagnóstico mediante pruebas de rendimiento preliminares:** Las pruebas de rendimiento ejecutadas sobre la configuración base e inicial de la red fueron críticas para el éxito del proyecto, ya que permitieron diagnosticar de forma cuantitativa problemas de diseño, tales como la ineficiencia en las políticas de seguridad del firewall, la total ausencia de colas de prioridad y un consumo excesivo de los recursos de hardware del enrutador central bajo condiciones de estrés.
- **Optimización de protocolos para eficiencia y estabilidad:** Como respuesta directa a los cuellos de botella identificados en la fase de diagnóstico, se aplicaron mecanismos avanzados de optimización de ancho de banda. Esto se logró mediante el diseño de una estructura jerárquica de árbol de colas basada en el algoritmo HTB Hierarchical Token Bucket, acoplada con el marcado de conexiones y paquetes en el motor de *Mangle* y la distribución

equitativa de flujos a través del algoritmo de encolamiento PCQ.

- **Evaluación de impacto de las políticas de QoS y seguridad:** La evaluación comparativa tras la implementación final de las políticas de calidad de servicio (*QoS*) y las reglas de seguridad en el firewall (*Filter*) demostró un impacto altamente positivo, evidenciando una reducción drástica de la carga de procesamiento en el enrutador, un correcto etiquetado y filtrado de tramas de Capa 2, y por consiguiente, una priorización precisa del tráfico que garantizó los parámetros de ancho de banda comprometidos para cada perfil de abonado.

ANEXOS

Script completo de configuración del core router

A continuación, se presenta la totalidad de las instrucciones de la interfaz de línea de comandos (CLI) implementadas en el dispositivo de enrutamiento principal (MikroTik RB750Gr3) bajo RouterOS v7.19.6. El script engloba la segmentación de red por Capa 2 (VLANs), la autenticación de abonados PPPoE, el marcado de paquetes por Firewall Mangle y el árbol de colas jerárquico para el control de calidad de servicio (QoS).

```

1  # 2026-05-25 08:55:22 by RouterOS 7.19.6
2  # software id = 1UU7-E239
3  #
4  # model = RB750Gr3
5  # serial number = HKF0AY60EAV
6
7  #-----
8  # Configuración de Capa 2 (Bridge y VLANs)
9  #-----
10 /interface bridge
11 add name=bridge-wisp vlan-filtering=yes
12
13 /interface ethernet
14 set [ find default-name=ether2 ] comment="salida de internet" name=\
15 "Lan puerto troncal"
16 set [ find default-name=ether1 ] comment="Entrada de internet" name=Wan1
17
18 /interface vlan
19 add interface=bridge-wisp name=VLAN10-ADM vlan-id=10
20 add interface=bridge-wisp name=VLAN30-EMP vlan-id=30
21 add interface=bridge-wisp name=VLAN40-VIP vlan-id=40
22 add interface=bridge-wisp name=VLAN50-STD vlan-id=50
23
24 /interface list
25 add name=LISTA_ADMIN
26
27 #-----
28 # Segmentación de Direccionamiento (Pools e Interfaces)
29 #-----
30 /ip pool
31 add name=pool-adm ranges=10.10.10.21-10.10.10.254
32 add name=pool-emp ranges=172.16.30.10-172.16.30.254
33 add name=pool-vip ranges=172.16.40.10-172.16.40.254
34 add name=pool-std ranges=172.16.50.10-172.16.50.254
35
36 /ip dhcp-server

```

```

37 add address-pool=pool-adm interface=VLAN10-ADM name=server-adm
38
39 #-----
40 # Perfiles de Servicio de Capa 3 (PPP Profiles)
41 #-----
42 /ppp profile
43 add change-tcp-mss=yes comment="Perfil Comercial Empresa" dns-server=\
44 1.1.1.1,8.8.8.8 local-address=172.16.30.1 name=perfil-empresa \
45 remote-address=pool-emp
46 add change-tcp-mss=yes comment="Perfil Comercial VIP" dns-server=\
47 1.1.1.1,8.8.8.8 local-address=172.16.40.1 name=perfil-vip remote-address=\
48 pool-vip
49 add change-tcp-mss=yes comment="Perfil Comercial Estandar" dns-server=\
50 1.1.1.1,8.8.8.8 local-address=172.16.50.1 name=perfil-estandar \
51 remote-address=pool-std
52
53 #-----
54 # Estructura del Arbol de Colas Jerarquico (Queue Tree y QoS)
55 #-----
56 /queue tree
57 add max-limit=375M name=WISP_ROOT parent=global
58
59 /queue type
60 add kind=pcq name=PCQ_Descarga_WISP pcq-classifier=dst-address
61 add kind=pcq name=PCQ_Subida_WISP pcq-classifier=src-address
62
63 /queue tree
64 add limit-at=110M max-limit=150M name="1. EMPRESARIAL" packet-mark=no-mark \
65 parent=WISP_ROOT priority=2 queue=PCQ_Descarga_WISP
66 add limit-at=30M max-limit=100M name="2. VIP" packet-mark=pkt_vip parent=\
67 WISP_ROOT priority=4 queue=PCQ_Descarga_WISP
68 add limit-at=10M max-limit=80M name="3. ESTANDAR" packet-mark=pkt_estandar \
69 parent=WISP_ROOT priority=7 queue=PCQ_Descarga_WISP
70 add limit-at=40M max-limit=150M name="1.1 Video_Emp" packet-mark=\
71 pkt_emp_video parent="1. EMPRESARIAL" priority=1 queue=PCQ_Descarga_WISP
72 add limit-at=60M max-limit=150M name="1.2 Web_Emp" packet-mark=pkt_emp_web \
73 parent="1. EMPRESARIAL" priority=3 queue=PCQ_Descarga_WISP
74 add limit-at=10M max-limit=150M name="1.3 Resto_Emp" packet-mark=\
75 pkt_emp_resto parent="1. EMPRESARIAL" priority=7 queue=PCQ_Descarga_WISP
76
77 #-----
78 # Asignacion de Puertos Fisicos y Logicos al Bridge
79 #-----
80 /interface bridge port
81 add bridge=bridge-wisp comment="Puerto Trunk" interface="Lan puerto troncal"
82 add bridge=bridge-wisp comment="Puerto Acceso Admin" interface=ether3 pvid=10
83
84 /ip neighbor discovery-settings
85 set discover-interface-list=LISTA_ADMIN
86
87 /interface bridge vlan

```

```

88 add bridge=bridge-wisp tagged="bridge-wisp,Lan puerto troncal" vlan-ids=\
89 10,30,40,50
90
91 /interface list member
92 add interface=VLAN10-ADM list=LISTA_ADMIN
93
94 #-----
95 # Habilitacion de Servidor PPPoE
96 #-----
97 /interface pppoe-server server
98 add default-profile=perfil-empresa disabled=no interface=VLAN30-EMP \
99 one-session-per-host=yes service-name=srv-pppoe-emp
100 add default-profile=perfil-vip disabled=no interface=VLAN40-VIP \
101 one-session-per-host=yes service-name=srv-pppoe-vip
102 add default-profile=perfil-estandar disabled=no interface=VLAN50-STD \
103 one-session-per-host=yes service-name=srv-pppoe-std
104
105 #-----
106 # Asignacion de Direcciones IP Estaticas a Interfaces
107 #-----
108 /ip address
109 add address=10.10.10.1/24 interface=VLAN10-ADM network=10.10.10.0
110 add address=172.16.30.1/24 interface=VLAN30-EMP network=172.16.30.0
111 add address=172.16.40.1/24 interface=VLAN40-VIP network=172.16.40.0
112 add address=172.16.50.1/24 interface=VLAN50-STD network=172.16.50.0
113
114 /ip cloud
115 set ddns-enabled=yes
116
117 #-----
118 # Interfaz de Entrada WAN (Cliente DHCP)
119 #-----
120 /ip dhcp-client
121 add comment="Entrada de Internet" interface=Wan1
122
123 /ip dhcp-server network
124 add address=10.10.10.0/24 dns-server=8.8.8.8 gateway=10.10.10.1
125 add address=172.16.30.0/24 dns-server=8.8.8.8 gateway=172.16.30.1
126 add address=172.16.40.0/24 dns-server=8.8.8.8 gateway=172.16.40.1
127 add address=172.16.50.0/24 dns-server=8.8.8.8 gateway=172.16.50.1
128
129 /ip dns
130 set servers=1.1.1.1
131
132 #-----
133 # Segmentacion y Listas de Direcciones IP (Firewall Address List)
134 #-----
135 /ip firewall address-list
136 add address=172.16.30.0/24 list=REDES_USUARIOS
137 add address=172.16.40.0/24 list=REDES_USUARIOS
138 add address=172.16.50.0/24 list=REDES_USUARIOS

```

```

139 add address=172.16.30.0/24 list="red lan"
140
141 #-----
142 # Filtros de Seguridad de Red (Firewall Filter)
143 #-----
144 /ip firewall filter
145 add action=accept chain=forward connection-state=established,related
146 add action=accept chain=forward comment="Admin accede a todo" in-interface=\
147 VLAN10-ADM
148 add action=drop chain=forward comment="Bloqueo Inter-VLAN Clientes" \
149 dst-address-list=REDES_USUARIOS src-address-list=REDES_USUARIOS
150 add action=drop chain=forward comment="Clientes no ven Infraestructura" \
151 dst-address=10.10.10.0/24 src-address-list=REDES_USUARIOS
152 add action=accept chain=input comment="Permitir solo DNS y DHCP al Router" \
153 dst-port=53,67 protocol=udp src-address-list=REDES_USUARIOS
154 add action=drop chain=input comment=\
155 "Bloqueo total Clientes a la Config del Router" src-address-list=\
156 REDES_USUARIOS
157
158 #-----
159 # Marcado de Trafico para Clasificacion QoS (Firewall Mangle)
160 #-----
161 /ip firewall mangle
162 add action=mark-connection chain=prerouting comment="QoS Empresa Prerouting" \
163 new-connection-mark=con_empresa src-address=172.16.30.0/24
164 add action=mark-packet chain=forward connection-mark=con_vip new-packet-mark=\
165 pkt_vip passthrough=no
166 add action=mark-connection chain=prerouting comment="QoS VIP Prerouting" \
167 new-connection-mark=con_vip src-address=172.16.40.0/24
168 add action=mark-packet chain=forward connection-mark=con_estandar \
169 new-packet-mark=pkt_estandar passthrough=no
170 add action=mark-connection chain=prerouting comment="QoS Estandar Prerouting"
171 \
172 new-connection-mark=con_estandar src-address=172.16.50.0/24
173 add action=mark-packet chain=forward comment=Zoom_Priority connection-mark=\
174 con_empresa dst-port=3478,3479,8801-8810 new-packet-mark=pkt_emp_video \
175 passthrough=no protocol=udp
176 add action=mark-packet chain=forward comment=YouTube_QUIC connection-mark=\
177 con_empresa dst-port=443 new-packet-mark=pkt_emp_video passthrough=no \
178 protocol=udp
179 add action=mark-packet chain=forward comment="2. Prioridad Web" \
180 connection-mark=con_empresa dst-port=80,443 new-packet-mark=pkt_emp_web \
181 passthrough=no protocol=tcp
182 add action=mark-packet chain=forward comment="3. Prioridad Resto" \
183 connection-mark=con_empresa new-packet-mark=pkt_emp_resto passthrough=no
184
185 #-----
186 # Enmascaramiento de Interfaz hacia Internet (NAT Masquerade)
187 #-----
188 /ip firewall nat
189 add action=masquerade chain=srcnat out-interface=Wan1

```

```

189 #-----
190 # Enrutamiento Estatico Predeterminado (Gateway)
191 #-----
192
193 /ip route
194 add check-gateway=ping comment="Ruta por defecto hacia ISP" disabled=no
195 distance=1 \
196 dst-address=0.0.0.0/0 gateway=Wan1 routing-table=main scope=30 \
197 suppress-hw-offload=no target-scope=11
198
199 #-----
200 # Hardening de Seguridad de Servicios locales
201 #-----
202
203 /ip service
204 set ftp disabled=yes
205 set ssh disabled=yes
206 set telnet disabled=yes
207 set www-ssl disabled=no
208 set winbox address=10.10.10.0/24
209 set api disabled=yes
210 set api-ssl disabled=yes
211
212 #-----
213 # Credenciales del Servidor Base de Usuarios (PPP Secrets)
214 #-----
215
216 /ppp secret
217 add comment="Cliente Empresa - VLAN 30" name=user_emp profile=perfil-empresa \
218 service=pppoe
219 add comment="Cliente VIP - VLAN 40" name=user_vip profile=perfil-vip service=\
220 pppoe
221 add comment="Cliente Estandar - VLAN 50" name=user_std profile=\
222 perfil-estandar service=pppoe
223
224 #-----
225 # Configuraciones del Sistema Local
226 #-----
227
228 /system clock
229 set time-zone-name=America/Guayaquil
230
231 /system identity
232 set name=RouterCore
233
234 /tool mac-server
235 set allowed-interface-list=LISTA_ADMIN

```

Listing 1: Script de configuración integral del enrutador MikroTik RB750Gr3.

Consideraciones de seguridad en usuarios (PPP Secrets)

Es importante señalar que al momento de extraer la configuración de respaldo del Router, por motivos de seguridad este omite las cadenas de texto de las contraseñas correspondientes a los usuarios.

Sin embargo, para una implementación real desde la línea de comandos del Router, la sintaxis completa requiere del argumento "password".

```
1  #-----
2  # Base de Datos de Usuarios Completa
3  #-----
4  /ppp secret
5  add comment="Cliente Empresa - VLAN 30" name=user_emp password=
6  contraseña_segura_emp profile=perfil-empresa service=pppoe
7  add comment="Cliente VIP - VLAN 40" name=user_vip password=
8  contraseña_segura_vip profile=perfil-vip service=pppoe
9  add comment="Cliente Estandar - VLAN 50" name=user_std password=
10 contraseña_segura_std profile=perfil-estandar service=pppoe
```

Listing 2: Sintaxis completa para el registro de credenciales en PPP Secrets.

Configuración de la infraestructura de red

En este apartado se presentan las capturas de pantalla correspondientes al despliegue técnico del conmutador de distribución y del sistema de transmisión inalámbrica sectorial.

Configuración del switch de distribución

A continuación, se detallan los respaldos visuales de la programación de los puertos de acceso, la multiplexación de enlaces troncales IEEE 802.1Q y el direccionamiento IP de gestión:

Figura 30

VLANs habilitadas en el dispositivo.

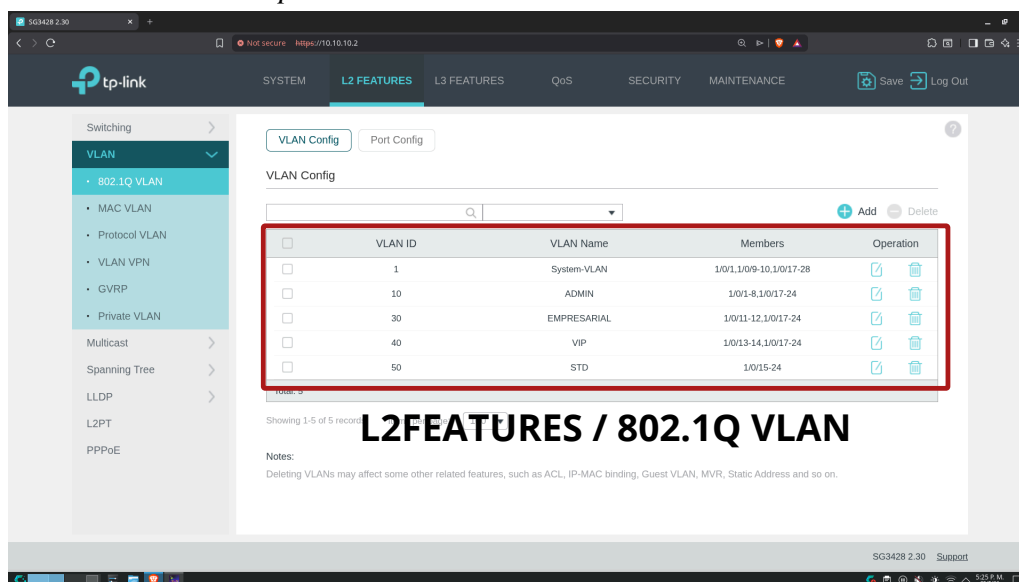
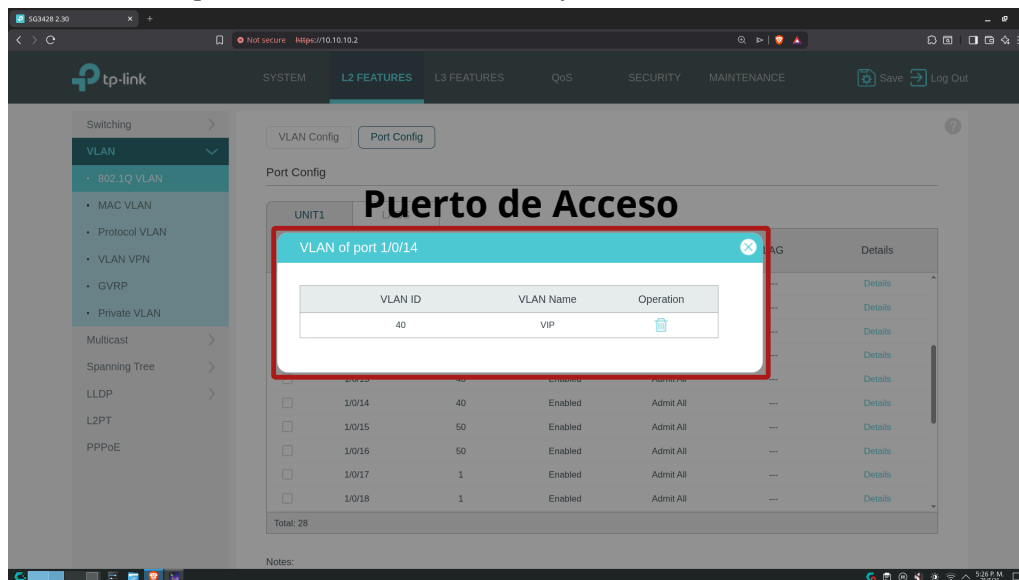


Figura 31

Configuración de los puertos de acceso en la interfaz del conmutador.

**Figura 32**

Asignación y etiquetado de los puertos troncales (VLAN Trunk).

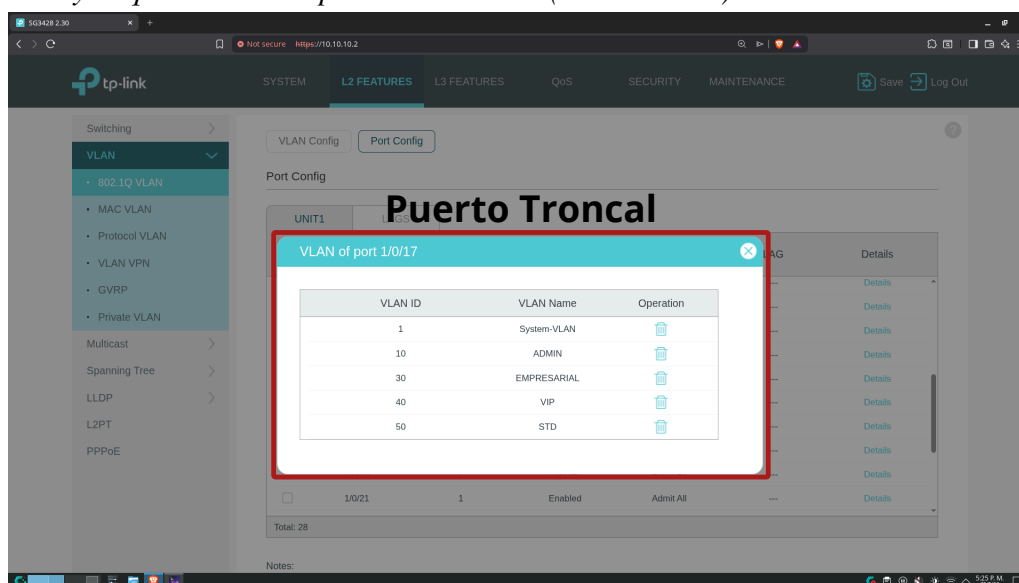
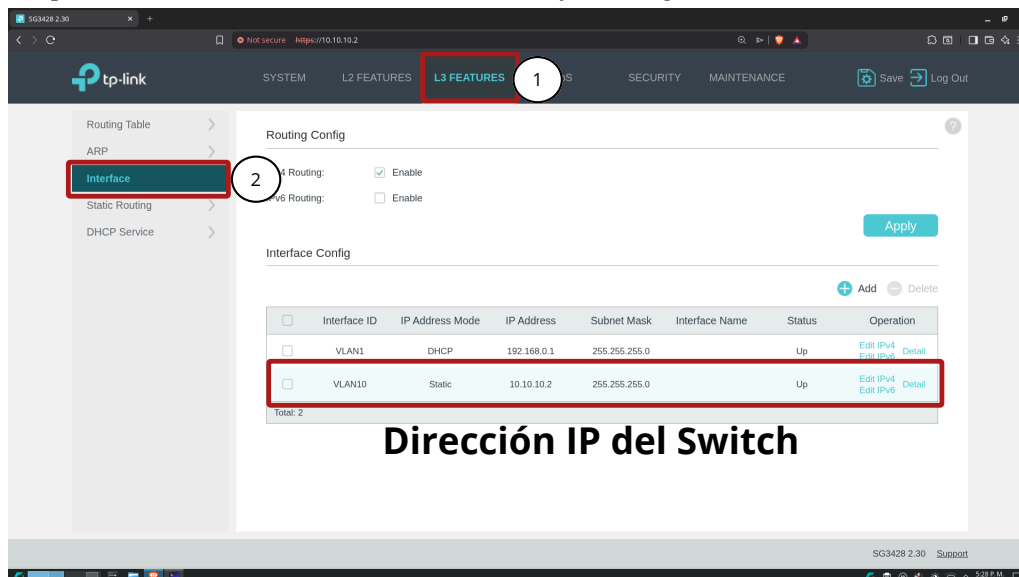
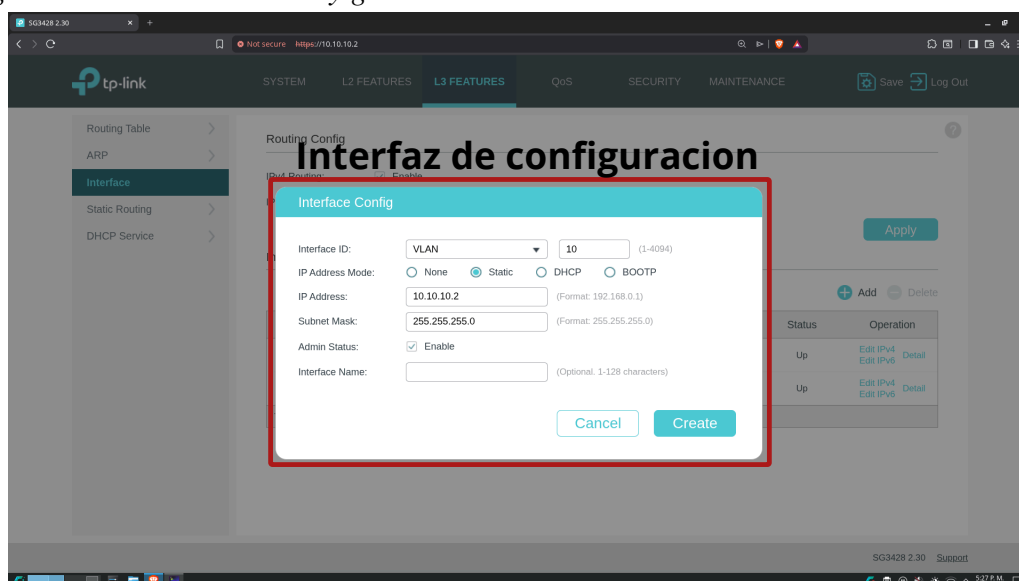


Figura 33

Segmento primario de direccionamiento IP e interfaces lógicas.

**Figura 34**

Configuración de enrutamiento y gestión IP del switch.



Configuración del sistema inalámbrico (Antenas)

A continuación, se presentan las capturas de la interfaz gráfica de administración web correspondientes a la calibración de radiofrecuencia, enlaces y servicios inalámbricos:

Figura 35

Parámetros inalámbricos de operación en modo punto de acceso (AP).

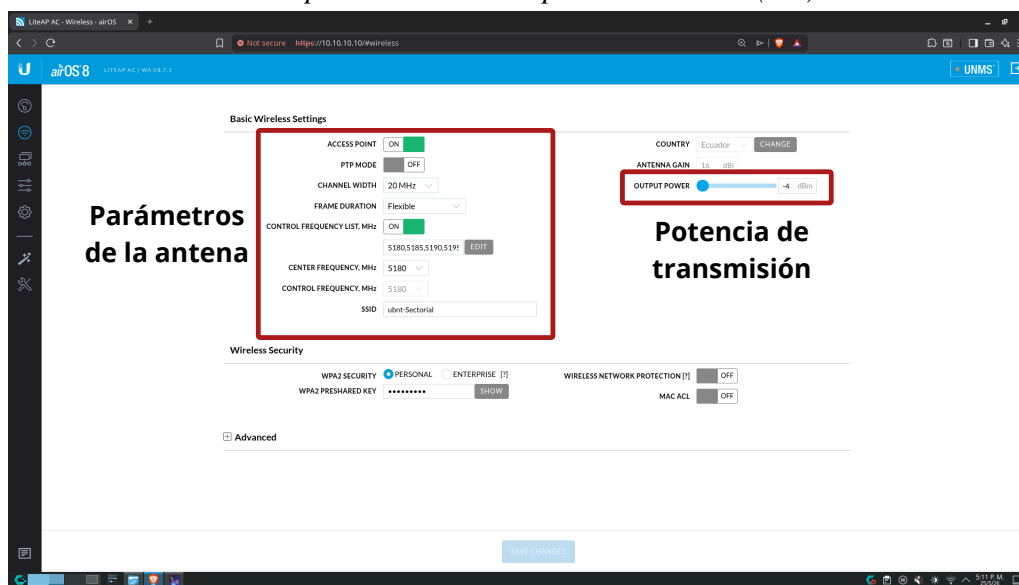


Figura 36

Configuración de las interfaces de red y enrutamiento del sistema inalámbrico.

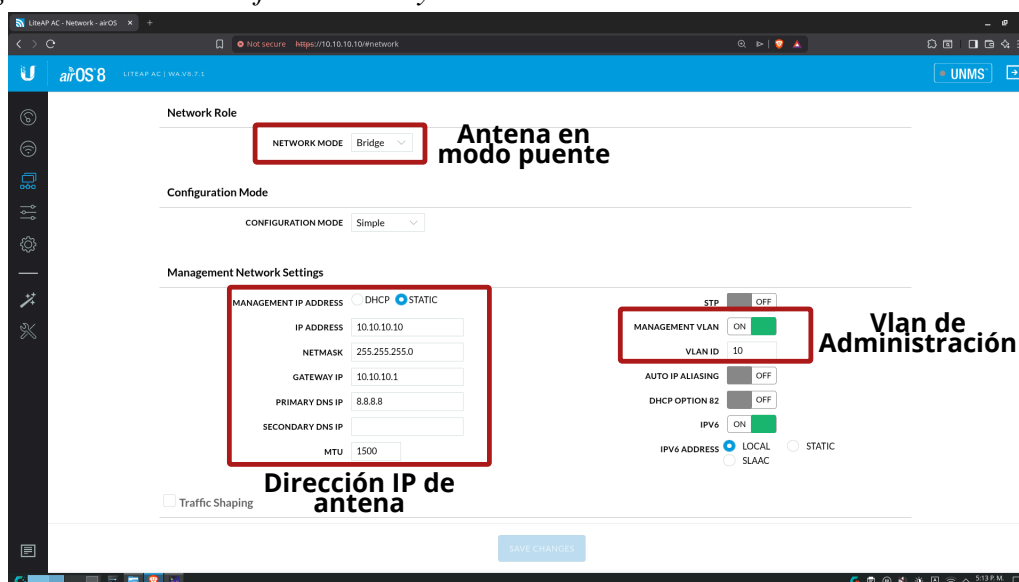
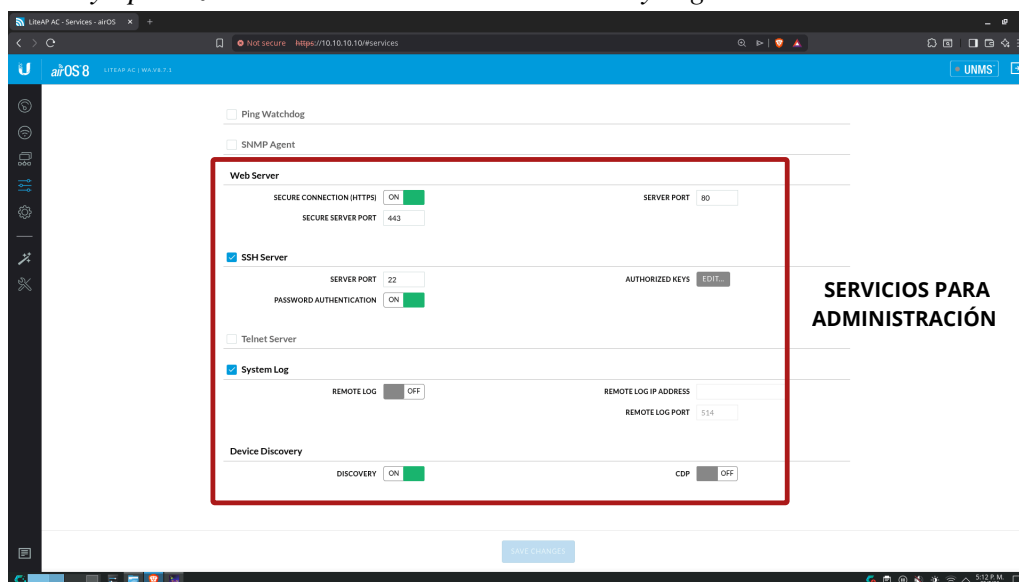


Figura 37

Habilitación y optimización de servicios de transmisión y seguridad.



**SERVICIOS PARA
ADMINISTRACIÓN**

Anexos: Evidencias de instalación

Figura 38

Conectorización, guiado y organización de cordones de parcheo en el conmutador de distribución.



Figura 39

Instalación y energización del enrutador residencial del abonado en el panel de distribución.



Figura 40

Fijación mecánica, montaje y alineación azimutal de la estación base sectorial.



Figura 41

Instalación y orientación del equipo transceptor inalámbrico (CPE) en el nodo terminal del cliente.



Figura 42

Implementación física de la infraestructura central y distribución del prototipo WISP.



Referencias

- [1] Asetel. *Panorama de las Telecomunicaciones en Ecuador*. 2025. URL: <https://asetel.org.ec/panorama-de-las-telecomunicaciones-en-ecuador/>.
- [2] National Geographics. *¿Quién inventó el wifi y cuándo surgió esta tecnología?* 2024. URL: <https://www.nationalgeographicla.com/historia/2024/11/quien-invento-el-wifi-y-cuando-surgio-esta-tecnologia>.
- [3] aireEC. *¿Qué es un WISP?* 2024. URL: <https://aire.ec/equipos-isp-wisp-mikrotik-mimosanetworks-ubiquiti/>.
- [4] Aspiazu Juan Parraga Andres. *Análisis, diseño e implementación de módulo WISP como herramienta práctica y demostrativa del manejo de redes inalámbricas para uso en el laboratorio de telecomunicaciones de la Universidad Politécnica Salesiana*. 2021. URL: <https://dspace.ups.edu.ec/bitstream/123456789/20805/1/UPS-GT003348.pdf>.
- [5] Ricardo Rendon Roy Aguilar Melissa Guerrero. «Diseño de un proveedor de servicios de Internet inalámbrico usando la tecnología de Spread Spectrum para la ciudad de Machala». Trabajo de titulación. Escuela Superior Politecnica del Litoral, 2004. URL: <https://www.dspace.espol.edu.ec/bitstream/123456789/42646/1/D-84157.pdf>.
- [6] Carlos Suarez. «Estudio para la implementación de redes comunitarias (WISP) para la Comuna Bellavista del Cerro». Trabajo de Titulación. Universidad Estatal Peninsula de Santa Elena, 2021. URL: <https://repositorio.upse.edu.ec/items/b44da169-5f1a-41c9-832e-eb1e7629f2ff>.
- [7] SIGET. *Boletín sobre Radiación no Ionizante*. 2024.
- [8] Javier Luque. «Título completo del artículo». En: *Espectro electromagnético y espectro radioeléctrico* (2026). URL: https://www.acta.es/medios/articulos/ciencias_y_tecnologia/062017.pdf (visitado 08-07-2026).

- [9] Comisión Interamericana de Telecomunicaciones (CITEL). *El espectro Radioeléctrico*. Boletín electrónico N° 52. Publicado por la Organización de los Estados Americanos (OEA). Oct. de 2008. URL: https://www.oas.org/en/citel/infocitel/2008/octubre/espectro_e.asp (visitado 08-07-2026).
- [10] Bruno D'Angelo. *Zonas de Fresnel en radioenlaces: Definición y Fórmulas*. 2025. URL: <https://todotelco.com/zonas-de-fresnel/>.
- [11] IBM. *¿Qué es la Topología de red?* es. IBM, oct. de 2024. URL: <https://www.ibm.com/mx-es/think/topics/network-topology> (visitado 09-07-2026).
- [12] FGN64. *Clasificación de las Redes*. <https://fgn64.wordpress.com/clasificacion-de-las-redes/>. Accedido el 9 de julio de 2026. 2012. URL: <https://fgn64.wordpress.com/clasificacion-de-las-redes/>.
- [13] Gadae Netweb. *Tipos de redes informáticas según su alcance*. <https://www.gadae.com/blog/tipos-de-redes-informaticas-segun-su-alcance/>. Accedido el 9 de julio de 2026. 2022. URL: <https://www.gadae.com/blog/tipos-de-redes-informaticas-segun-su-alcance/>.
- [14] Javier Jiménez. *WISP: qué es y por qué tiene tanta importancia en las conexiones*. 2025. URL: <https://www.redeszone.net/tutoriales/redes-cable/wisp-conexiones-internet/>.
- [15] abc xperts. *¿Cuál es el significado de CPE y WISP?* 2025. URL: <https://abcxperts.com/docs/cual-es-el-significado-de-cpe-y-wisp/>.
- [16] ARCOTEL. *Espectro Radioeléctrico*. 2025. URL: <https://www.arcotel.gob.ec/espectro-radioelectrico-2/>.
- [17] IBM. *¿Qué es la infraestructura de red?* Accedido el 10 de julio de 2026. 2024. URL: <https://www.ibm.com/es-es/think/topics/network-infrastructure>.
- [18] Fortinet. *What Is Quality Of Service (QoS) In Networking?* 2025. URL: <https://www.fortinet.com/resources/cyberglossary/qos-quality-of-service>.

- [19] Tesswave. *¿Cuáles son los estándares IEEE 802.11?* Accedido el 10 de julio de 2026. 2024. URL: <https://www.tesswave.com/es/what-are-the-ieee-802-11-standards/>.
- [20] Miguel García, J. Melero y A. Santos. «Evolución de la Seguridad en Redes Inalámbricas: Del WEP al 802.11i». En: *Boletín de la RedIRIS* 73 (2005). Accedido el 10 de julio de 2026, págs. 15-22. URL: <https://www.rediris.es/difusion/publicaciones/boletin/73/ENFOQUE1.pdf>.
- [21] Holight Optic. *Requisitos de cableado estructurado según las normas TIA-568*. Accedido: 10 de julio de 2026. 2026. URL: <https://www.holightoptic.com/es/Requisitos-de-cableado-estructurado-segun-las-normas-TIA-568/>.
- [22] FS Community. *T568A vs. T568B: ¿Cuál es la diferencia entre el cable directo y el cable cruzado?* <https://www.fs.com/es/blog/t568a-vs-t568b-difference-between-straight-through-and-crossover-cable-4762.html>. Accedido: 10 de julio de 2026. 2026.
- [23] CyberHoot. *RFC 1918*. <https://cyberhoot.com/es/cybrario/rfc-1918/>. Accedido: 10 de julio de 2026. 2026.
- [24] Cloudflare. *¿Qué es el protocolo de internet (IP)?* <https://www.cloudflare.com/es-es/learning/network-layer/internet-protocol/>. Accedido: 10 de julio de 2026. 2026.
- [25] Fortinet. *¿Qué es el modelo TCP/IP?* <https://www.fortinet.com/lat/resources/cyberglossary/tcp-ip>. Accedido: 10 de julio de 2026. 2026.
- [26] Cloudflare. *¿Qué es el protocolo de datagramas de usuario (UDP)?* <https://www.cloudflare.com/es-es/learning/ddos/glossary/user-datagram-protocol-udp/>. Accedido: 10 de julio de 2026. 2026.
- [27] IBM. *¿Qué es el Sistema de Nombres de Dominio (DNS)?* <https://www.ibm.com/mx-es/think/topics/dns>. Accedido: 10 de julio de 2026. 2026.

- [28] Fortinet. *¿Qué es el protocolo de configuración dinámica de host (DHCP)?* <https://www.fortinet.com/lat/resources/cyberglossary/dynamic-host-configuration-protocol-dhcp>. Accedido: 10 de julio de 2026. 2026.
- [29] QSFPTK. *¿Cuál es la diferencia entre STP, RSTP y MSTP?* <https://www.qsfptek.com/es/qt-news/what-is-the-difference-between-stp-rstp-and-mstp.html>. Accedido: 10 de julio de 2026. Mar. de 2026.
- [30] VAS Experts. *Configuración de PPPoE: características, ventajas y diferencias con otros protocolos de conexión.* <https://vasexperts.com/es/blog/telecom/pppoe-setting-features-advantages-and-differences-from-other-connection-protocols/>. Accedido: 10 de julio de 2026. Mar. de 2026.
- [31] Cloudflare. *¿Qué es SSH? | Secure Shell.* <https://www.cloudflare.com/es-es/learning/access-management/what-is-ssh/>. Accedido: 10 de julio de 2026. 2026.
- [32] MikroTik. *Manual:IP/Firewall/Mangle.* Documentación oficial sobre el motor de marcado de paquetes en RouterOS v7. MikroTik Support y Documentation. 2024. URL: <https://help.mikrotik.com/docs/spaces/ROS/pages/48660587/Mangle> (visitado 15-07-2026).
- [33] MikroTik. *Manual:Queues - Per Connection Queueing (PCQ).* Documentación oficial sobre gestión de colas en RouterOS v7. MikroTik Support y Documentation. 2024. URL: <https://help.mikrotik.com/docs/spaces/ROS/pages/328088/Queues#Queues-PCQ> (visitado 15-07-2026).
- [34] MikroTik. *HTB - Hierarchical Token Bucket.* Manual de documentación oficial de RouterOS. MikroTik Support y Documentation. 2024. URL: <https://help.mikrotik.com/docs/spaces/ROS/pages/137986076/HTB+Hierarchical+Token+Bucket> (visitado 15-07-2026).
- [35] Fortinet. *¿Qué es la traducción de direcciones de red (NAT)?* <https://www.fortinet.com/lat/resources/cyberglossary/network-address-translation>. Accedido: 10 de julio de 2026. 2026.

- [36] MikroTik. *Manual:IP/Firewall/Filter*. Documentación oficial sobre el filtrado de paquetes y firewall en RouterOS v7. MikroTik Support y Documentation. 2024. URL: <https://help.mikrotik.com/docs/spaces/ROS/pages/48660574/Filter> (visitado 15-07-2026).
- [37] MikroTik. *Manual:Interface/VLAN*. Documentación oficial sobre segmentación de redes virtuales y Bridge VLAN Filtering en RouterOS v7. MikroTik Support y Documentation. 2024. URL: <https://help.mikrotik.com/docs/spaces/ROS/pages/88014957/VLAN> (visitado 15-07-2026).
- [38] MikroTik. *Manual:IP/Services*. Documentación oficial sobre el control de acceso y aseguramiento de servicios de administración en RouterOS v7. MikroTik Support y Documentation. 2024. URL: <https://help.mikrotik.com/docs/spaces/ROS/pages/103841820/Services> (visitado 15-07-2026).
- [39] Cludflare. *¿Qué es un ataque de denegación de servicio (DoS)?* 2025. URL: <https://www.cloudflare.com/es-es/learning/ddos/glossary/denial-of-service/>.
- [40] Ettercap. *Welcome to the Ettercap Project*. 2025. URL: <https://www.ettercap-project.org>.
- [41] Kaspersky. *Ataque de fuerza bruta*. 2025. URL: <https://www.kaspersky.es/resource-center/definitions/brute-force-attack>.