REDES Y COMUNICACIÓN DE DATOS

FUNDAMENTOS, DISEÑO Y GESTIÓN

Paucar Córdova, Rosman José
Prado Ortega, Mauricio Xavier
Calero Romero, Luis Alberto
Añazco Lalangui, Karen Anabelle

EDITORIAL
edulearn
Academy SAS

Redes y Comunicación de Datos: fundamentos, diseño y gestión

EDITORIAL
edulearn
Academy SAS

Redes y Comunicación de Datos: fundamentos, diseño y gestión

Paucar Córdova, Rosman José
Prado Ortega, Mauricio Xavier
Calero Romero, Luis Alberto
Añazco Lalangui, Karen Anabelle

Editorial EduLearn Academy S.A.S.

Website: https://editorial.edulearn.ec/

Email: editorial@edulearn.ec

Telf. (+593) 992663228

Machala, Ecuador

Primera edición, 2025

ISBN: 978-9942-7393-3-9

DOI: https://doi.org/10.64973/edu.2025.2515

Distribución online

EDITORIAL
edulearn
Academy SAS

Rosman José Paucar Córdova
https://orcid.org/0000-0001-5254-4921

Docente universitario con más de nueve años de trayectoria al servicio de la formación profesional de futuros docentes y profesionales ecuatorianos, con una sólida instrucción formal como Ingeniero en Sistemas, Máster en Tecnología Educativa y Competencias Digitales, Magíster en Interconectividad de Redes de Computadoras y Doctor en Educación. Posee amplias competencias en pedagogía, didáctica e investigación, así como en tecnología educativa, redes de computadoras, programación, inteligencia artificial y análisis de datos. Ha desempeñado cargos en instituciones públicas y privadas, ejerciendo la docencia en los niveles de educación secundaria, pregrado y posgrado, además de participar activamente en la asesoría y publicación de artículos científicos, tesis, libros y ponencias en eventos académicos nacionales e internacionales.

Mauricio Xavier Prado Ortega
https://orcid.org/0000-0003-0809-9693

Docente universitaria con más de veinte años de trayectoria dedicada a la formación de futuros docentes y profesionales ecuatorianos. Ingeniera en Sistemas e Ingeniera Comercial, Magíster en Educación Superior, Magíster en Gerencia de Salud para el Desarrollo Local y Máster Universitario en Tecnología Educativa y Competencias Digitales. Ha desempeñado cargos en instituciones públicas y privadas, ejerciendo la docencia a nivel de pregrado, además de participar activamente en la publicación de artículos científicos, libros y ponencias presentadas en eventos nacionales e internacionales. Ha recibido reconocimiento al mérito científico por su destacada producción académica, contribuyendo a la proyección y visibilidad nacional e internacional de la Universidad Nacional de Loja.

Luis Alberto Calero Romero
https://orcid.org/0009-0009-5462-7611

Profesional apasionado por la educación y la tecnología, con una trayectoria de más de nueve años combinando la labor docente y el liderazgo estratégico. Ha ejercido la docencia en la Unidad Educativa José Anselmo García Cajamarca y en la Unidad Educativa Arenillas, complementando su experiencia con funciones de gestión como Analista Distrital de Tecnologías en la Dirección Distrital 07D05 (Arenillas–Huaquillas–Las Lajas), donde se consolidó como un actor clave en la transformación digital del distrito. Su labor ha estado orientada a la integración de herramientas tecnológicas innovadoras y al diseño y comunicación de estrategias para su adopción efectiva, articulando acciones entre directivos, docentes y personal administrativo para fortalecer la innovación educativa y la gestión institucional.

Karen Anabelle Añazco Lalangui
https://orcid.org/0009-0009-8190-504X

Licenciada en Pedagogía de la Informática, egresada de la Universidad Técnica de Machala, con 23 años de edad. Se caracteriza por su compromiso con la enseñanza y por el uso de las tecnologías como herramientas para optimizar los procesos educativos. Posee una sólida formación pedagógica y tecnológica, y una marcada motivación por continuar aprendiendo e implementando estrategias innovadoras que fortalezcan la calidad del aprendizaje en el ámbito educativo.

Sinopsis

Este libro constituye una guía práctica y progresiva que introduce, con un lenguaje cercano, los fundamentos de las redes y la comunicación de datos, inicia con los modelos OSI y TCP/IP y continúa con el direccionamiento IPv4 e IPv6 usando VLSM, para explicar de forma sencilla cómo viajan los datos y cómo se codifican en la red, integra prácticas que se pueden repetir y verificar, de modo que el lector consolide lo aprendido con ejercicios reales.

La obra desarrolla la seguridad aplicada desde los principios de confidencialidad, integridad y disponibilidad, junto con autenticación, autorización y auditoría, e incorpora funciones hash, uso de TLS, manejo de certificados, listas de control de acceso y firma electrónica. Propone el diseño de redes de área amplia con enrutamiento estático y dinámico, incluyendo OSPF y RIPv2, además de traducción de direcciones con NAT y PAT y la protección de comunicaciones mediante IPsec. Profundiza en la interconexión y segmentación a través de conmutación, tabla MAC, VLAN, etiquetado 802.1Q y enrutamiento entre VLANs, la gestión y el monitoreo se abordan con SNMP, MIB y NMS, usando indicadores clave como latencia, fluctuación, pérdida y rendimiento, junto con estudios de sitio con NetSpot, conceptos de calidad de servicio, gestión de incidentes y mejora continua.

Cada capítulo combina explicaciones claras con laboratorios en Packet Tracer y Wireshark, además de anexos, plantillas en formato APA séptima edición y rúbricas que permiten dejar evidencia y asegurar trazabilidad. El recorrido culmina en un proyecto integrador que exige justificar decisiones con métricas y documentación técnica, preparando a estudiantes, docentes y profesionales para diseñar, implementar, medir y sostener redes seguras, escalables y auditables.

Palabras Claves: *Redes de computadoras, comunicación de datos y arquitectura OSI/TCP-IP, direccionamiento IP, enrutamiento y redes WAN, seguridad de redes.*

Synopsis

This book serves as a practical and progressive guide that introduces, in accessible language, the fundamentals of networks and data communication. It begins with the OSI and TCP/IP models and continues with IPv4 and IPv6 addressing using VLSM, explaining in simple terms how data travels and is encoded across the network. It integrates hands-on exercises that can be repeated and verified, allowing readers to consolidate their learning through real-world practice.

The work develops applied security based on the principles of confidentiality, integrity, and availability, along with authentication, authorization, and auditing. It incorporates hash functions, TLS usage, certificate management, access control lists, and digital signatures. It proposes the design of wide area networks (WAN) with static and dynamic routing, including OSPF and RIPv2, as well as address translation using NAT and PAT, and communication protection through IPsec. It delves into interconnection and segmentation through switching, MAC tables, VLANs, 802.1Q tagging, and inter-VLAN routing. Management and monitoring are addressed using SNMP, MIB, and NMS, applying key performance indicators such as latency, jitter, packet loss, and throughput, alongside site surveys with NetSpot, quality of service concepts, incident management, and continuous improvement.

Each chapter combines clear explanations with labs in Packet Tracer and Wireshark, along with appendices, APA 7th edition templates, and rubrics that enable evidence tracking and ensure traceability. The journey culminates in an integrative project that requires justifying decisions through metrics and technical documentation, preparing students, teachers, and professionals to design, implement, measure, and maintain secure, scalable, and auditable networks.

Keywords: *Computer networks, data communication and OSI/TCP-IP architecture, IP addressing, routing and WAN networks, network security.*

ÍNDICE GENERAL

CAPÍTULO 1. FUNDAMENTOS Y ARQUITECTURA DE REDES 14

Introducción 14

1.1 Modelos de referencia OSI y TCP IP 15

1.2 Direccionamiento IPv4 e IPv6 y subredes VLSM básico 17

1.3. Dispositivos de red switches, routers y puntos de acceso 20

1.4. Topologías físicas y lógicas 22

1.5. Captura básica con Wireshark 25

CAPÍTULO 2: TRANSMISIÓN Y CODIFICACIÓN DE DATOS ... 30

Introducción 30

2.1. Señales digitales y analógicas 32

2.2. Codificación de línea NRZ, Manchester y 4B/5B 36

2.3. Detección y corrección de errores: paridad, CRC y Hamming ... 39

2.4. Medios de transmisión UTP, fibra y radio 42

2.5. Simulación con Falstad Circuit Simulator 45

2.6. Medición de tasa de error de bit y rendimiento efectivo 48

CAPÍTULO 3: SEGURIDAD DE DATOS APLICADA 55

Introducción 55

3.1. Principios CIA y AAA y políticas básicas 57

3.2. Hash y codificación con CyberChef 59

3.3. TLS, PKI y certificados X punto 509 en Wireshark 63

3.4. Control de acceso con listas en emulador TP Link..... 67

3.5. Buenas prácticas y cumplimiento..... 70

CAPÍTULO 4: EVALUACIÓN CON ENFOQUE DE INCLUSIÓN Y EQUIDAD..... 75

Introducción..... 75

4.1. Topologías de área amplia..... 76

4.2. Enrutamiento estático y enrutamiento dinámico 79

4.3. OSPF y RIPv2 principios 82

4.4. Traducción de direcciones NAT y PAT..... 85

4.5. Red privada virtual básica concepto IPsec 91

4.6. Verificación y resolución de problemas..... 95

CAPITULO 5: INTERCONEXIÓN Y SEGMENTACIÓN 101

Introducción..... 101

5.1. Conmutación y tabla MAC..... 102

5.2. Redes virtuales de área local y etiquetado 802.1Q 106

5.3. Transporte etiquetado entre equipos..... 109

5.4. Enrutamiento inter VLAN..... 112

5.5. Práctica en emulador Packet Tracer..... 115

CAPITULO 6: GESTIÓN Y MONITOREO..... 122

Introducción..... 122

6.1. SNMP, MIB y NMS 123

6.2. KPIs de red: latencia, fluctuación, pérdida y rendimiento 128

6.3. Site Survey con NetSpot 132

6.4. Calidad de servicio (QoS) 136

6.5. Gestión de incidencias y bitácoras 140

6.6. Mejora continua 144

CAPITULO 7: GESTIÓN Y MONITOREO 150

Introducción 150

7.1. Requerimientos y alcance 151

7.2. Diseño lógico y físico 155

7.3. Implementación en simulación y emuladores 157

7.4. Seguridad y cumplimiento 160

7.5. Entrega y defensa 163

Referencias Bibliográficas: 170

CAPÍTULO 1. FUNDAMENTOS Y ARQUITECTURA DE REDES

«La ventaja de los estándares es que tienes tantos entre los cuales elegir.»

Andrew S. Tanenbaum.

Introducción

Las redes de comunicación de datos sostienen gran parte de la vida moderna y del quehacer académico, dado que permiten que mensajes, clases, transacciones y servicios digitales circulen con oportunidad y confiabilidad. Comprender sus fundamentos evita tratar a la red como una caja negra y mejora las decisiones técnicas, este capítulo inicia con una mirada clara y accesible que conecta conceptos esenciales con prácticas reales, la ruta va desde la arquitectura general hasta la verificación de conectividad con evidencias.

El punto de partida es entender cómo se organiza una red en capas y funciones, los modelos OSI y TCP IP ofrecen un lenguaje común para describir servicios, protocolos y unidades de datos, al reconocer qué sucede en cada capa podemos ubicar dispositivos y responsabilidades con precisión, esta perspectiva ayuda a interpretar el flujo extremo a extremo y a anticipar efectos de diseño, veremos cómo clasificar protocolos y relacionarlos con tareas y equipos concretos.

Luego pasamos al direccionamiento que da identidad y alcance a los participantes de la red trabajaremos con conceptos básicos de IPv4 e

IPv6 y con cálculo inicial de subredes, el objetivo es asignar prefijos y rangos válidos sin solapamientos y con documentación clara, estas habilidades permiten segmentar una red para mejorar organización, seguridad y desempeño, también preparan el terreno para configuraciones y pruebas posteriores.

Finalmente abordaremos dispositivos y topologías que materializan las decisiones de arquitectura, identificaremos funciones típicas de switches, routers y puntos de acceso y compararemos topologías físicas y lógicas. Cerraremos con verificación práctica mediante capturas en Wireshark para observar tramas y paquetes, la intención es construir una primera red local funcional y respaldar cada paso con evidencia, con esta base el estudiante podrá avanzar con seguridad hacia diseños más complejos

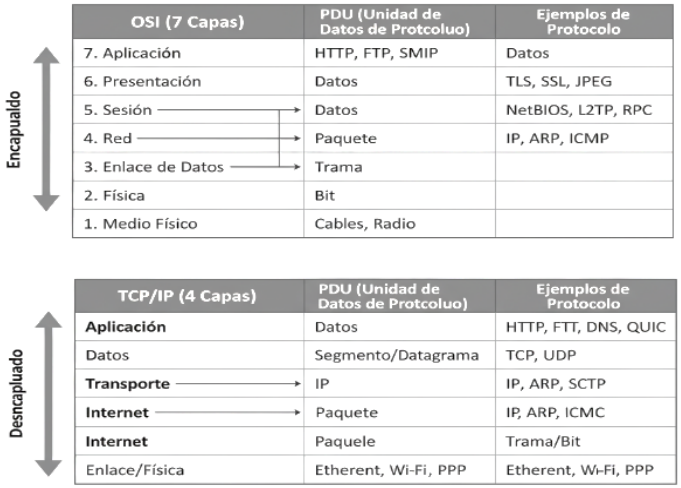
1.1 Modelos de referencia OSI y TCP IP

Los modelos OSI y TCP IP organizan la comunicación en capas con responsabilidades claramente definidas, su propósito es describir cómo cada capa ofrece servicios a la superior mediante interfaces estables (ISO/IEC, 1994), la unidad de datos de protocolo o PDU encapsula información y encabezados específicos por capa, este enfoque permite asignar protocolos y dispositivos a funciones precisas dentro de la arquitectura, así se favorece el razonamiento sistemático y la interoperabilidad entre equipos heterogéneos.

OSI propone siete capas, mientras TCP IP agrupa funciones en menos niveles prácticos. Protocolos como Ethernet, IP, TCP y QUIC se ubican según el servicio que brindan (Eddy, 2022; Iyengar & Thomson, 2021). Switches implementan funciones de enlace y aprendizaje, mientras los routers ejecutan decisiones de red y enrutamiento, la comunicación de tipo extremo a extremo resulta de encapsular y desencapsular PDU a través de cada capa, cada entidad de igual nivel interpreta su encabezado y entrega datos al nivel superior.

Figura 1

Esquema comparativo de OSI vs TCP/IP



Nota. Imagen comparativa entre los modelos OSI (7 capas) y TCP/IP (4 capas), detallando sus niveles, tipos de datos, procesos de

encapsulado y ejemplos de protocolos en cada capa. Fuente. Elaboración propia.

Un equipo A envía un eco hacia B usando la utilidad de diagnóstico ping en una LAN, la aplicación solicita el envío y el sistema genera un mensaje ICMP tipo eco de red, la capa de red encapsula el mensaje dentro de un datagrama IP con direcciones válidas. La capa de enlace agrega direcciones físicas y control de errores para atravesar el primer salto, el estándar de ICMP establece estos mensajes de control y diagnóstico fundamentales para la red (Postel, 1981).

Durante el recorrido la aplicación valida coherencia de la solicitud y la respuesta recibida, el transporte confirma puertos de origen y destino y puede verificar confiabilidad o control de flujo, la red examina direcciones y rutas factibles, mientras enlace arbitra el acceso y detecta errores, y por último la capa física transmite señales con temporización adecuada y niveles acordes al medio utilizado, con esta base pasaremos al direccionamiento y a la planificación de subredes necesarias para el diseño.

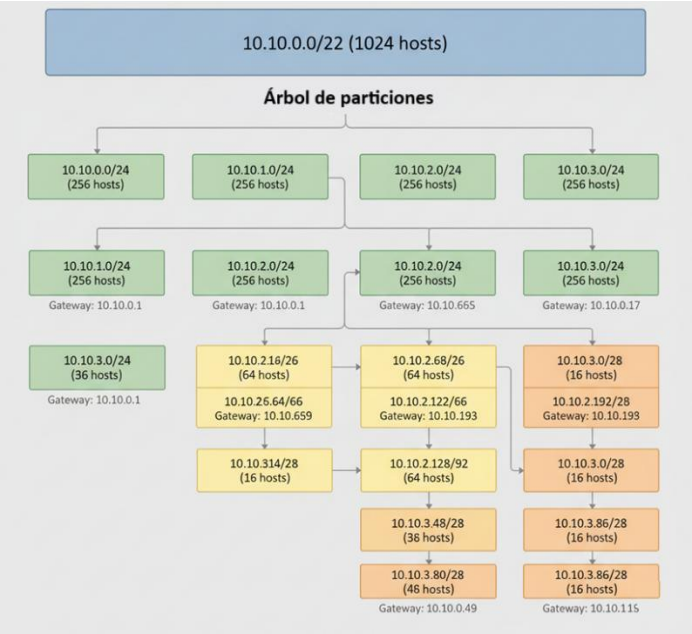
1.2 Direccionamiento IPv4 e IPv6 y subredes VLSM básico

Un plan de direcciones bien diseñado sostiene la escalabilidad y evita solapamientos en entornos crecientes, partimos de un bloque 10.10.0.0/22 para tres áreas con demandas diferentes, el laboratorio necesita alrededor de doscientos hosts, ingeniería cerca de sesenta y

administración unos catorce, VLSM permite asignar un /24, un /26 y un /28 aprovechando mejor el espacio, esta planificación ordenada protege el crecimiento y facilita futuras agregaciones sin reestructurar.

Figura 2

Diagrama VLSM: 10.10.0.0/22



Nota. árbol de particiones de red que divide el bloque 10.10.0.0/22 en subredes jerárquicas más pequeñas, indicando la cantidad de hosts y las direcciones **gateway** correspondientes a cada subred. Fuente. Elaboracion propia

La validación inicia confirmando que cada rango excluya direcciones de red y difusión en IPv4 se define una puerta de enlace coherente por subred y se documenta el prefijo asignado, luego se prueba eco hacia la puerta de enlace y rastreo de saltos hacia destinos externos. La coherencia se confirma observando resolución de direcciones, tablas de vecinos y rutas resultantes, estas verificaciones brindan evidencia reproducible y fortalecen el control de cambios.

En IPv6 la planificación emplea prefijos globales agregables y subredes típicamente de tamaño /64 por enlace, la autoconfiguración sin estado genera identificadores de interfaz y el descubrimiento de vecinos valida alcance inmediato, la especificación de IPv6 establece estos principios y formatos de direccionamiento estables para redes modernas (Deering & Hinden, 2017), las extensiones de direcciones temporales mejoran la privacidad del usuario en escenarios públicos y corporativos (Gont, Krishnan, & Narten, 2021).

La lógica práctica de VLSM asigna primero los bloques mayores y fragmenta progresivamente el prefijo padre, así el caso anterior preserva espacio utilizable y evita intersecciones entre subredes en producción, CIDR formaliza la agregación y la asignación eficiente en dominios heterogéneos de gran escala (Fuller & Li, 2006), un plan documentado vincula direccionamiento con políticas, seguridad y pruebas operativas verificables, con esta base pasaremos a

seleccionar dispositivos de red acordes con capas y direccionamiento requerido.

1.3. Dispositivos de red switches, routers y puntos de acceso

Los conmutadores resuelven la segmentación de dominios de difusión y el reenvío eficiente dentro de una red local, los enrutadores conectan redes diferentes aplicando decisiones de capa de red y políticas de alcance coherentes. Los puntos de acceso extienden la conectividad inalámbrica y gestionan el acceso compartido al medio radioeléctrico, los Switches dominan principalmente el plano de datos, routers combinan planos de control y datos, y los puntos de acceso integran gestión del medio y autenticación, en sintonía con las capas de los modelos de referencia (Song et al., 2022).

Para un entorno académico o de pequeña empresa conviene equilibrar rendimiento sostenido, número de puertos y capacidades de administración centralizada, un conmutador con enlaces de mayor velocidad y suficientes interfaces cubre aulas y laboratorios con holgura razonable, un enrutador con soporte de listas de control y traducción de direcciones posibilita segmentación y salida controlada a Internet. Un punto de acceso con administración en la nube y alimentación por cable ofrece despliegue ágil y visibilidad operativa inmediata, estas decisiones mejoran la observabilidad si el equipo expone telemetría estandarizada desde los planos pertinentes (Song et al., 2022).

El conmutador aprende direcciones físicas y construye una tabla que orienta el envío selectivo de tramas, este comportamiento reduce tráfico innecesario y mantiene baja la latencia interna habilitando redes virtuales para aislar grupos, en la arquitectura por capas, su función se alinea con enlace de datos y, en equipos avanzados, con enrutamiento interno limitado.

El enrutador mantiene tablas de rutas y ejecuta selección de siguiente salto con base en prefijos, puede aplicar políticas de calidad de servicio, listas de control y traducción de direcciones para proteger recursos, al operar en la capa de red, conecta subredes heterogéneas y define fronteras administrativas claras.

El punto de acceso coordina estaciones inalámbricas y optimiza el uso del espectro en entornos densos, estándares recientes como Wifi seis introducen técnicas que mejoran capacidad y eficiencia del canal compartido, estos avances favorecen aulas concurridas y pasillos con tráfico elevado donde múltiples dispositivos compiten, la elección del estándar adecuado asegura mayor rendimiento por área y experiencia más estable (IEEE, 2021).

En conjunto estos dispositivos definen funciones complementarias que sostienen redes confiables, observables y escalables, su correcta selección y configuración responden a necesidades de capa políticas

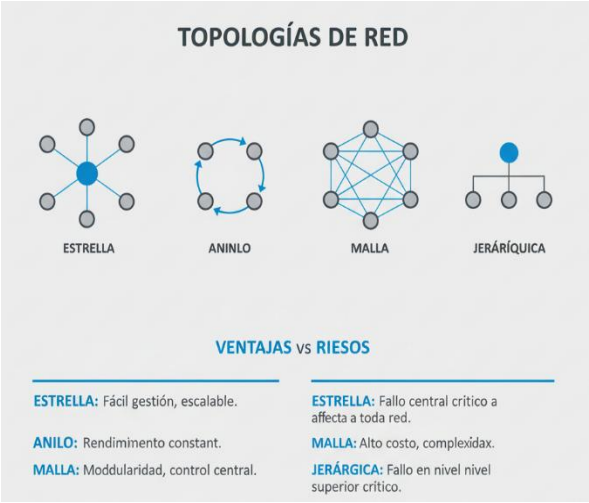
y direccionamiento coherente, con esta base avanzaremos al análisis de topologías físicas y lógicas para materializar el diseño.

1.4. Topologías físicas y lógicas

Las topologías físicas describen cómo se conectan los equipos y las lógicas indican cómo fluye el tráfico, en estrella, un conmutador central simplifica la gestión, pero concentra el dominio de fallo; en anillo, el tráfico circula ordenadamente con mecanismos de protección; en malla, varios caminos reducen interrupciones con mayor costo; y el diseño jerárquico separa acceso, distribución y núcleo para acotar dominios de difusión y facilitar crecimiento. Estas elecciones impactan directamente en la expansión futura, el aislamiento de broadcast y la estabilidad operativa del campus.

Figura 3

Topologías de Red



Nota. La imagen presenta las principales topologías junto con sus ventajas y riesgos en términos de gestión, rendimiento, costo y criticidad del fallo. Fuente. Elaboración propia.

Para documentar un diagrama mínimo conviene representar capas, enlaces y prefijos con nombres consistentes y legibles, deben identificarse vínculos ascendentes, rutas de respaldo y puertas de enlace por segmento, resaltando umbrales de capacidad y posibles puntos únicos de fallo, tal documentación permite prever congestión, planificar redundancias y comunicar decisiones técnicas con claridad a equipos académicos o de pequeña empresa.

En entornos pequeños la estrella física resulta fácil de implementar y entender, con monitoreo directo desde el conmutador central. Sin embargo, su centro exige alta disponibilidad eléctrica y de hardware, pues un fallo desconecta múltiples áreas simultáneamente, el tamaño del dominio de difusión debe manejarse con segmentación para contener tormentas y reducir tráfico innecesario.

El anillo ofrece trayectos previsibles y protección rápida frente a cortes si se emplean protocolos de conmutación de respaldo en redes de capa dos, la conmutación de protección en anillo especificada por G.8032 brinda resiliencia operativa con tiempos de recuperación acotados en la práctica, su utilidad aparece en troncales de edificios y corredores donde la continuidad resulta prioritaria.

La malla y el diseño jerárquico aumentan resiliencia distribuyendo tráfico y límites de fallo entre capas claramente definidas, en campus modernos se privilegia el modelo jerárquico con funciones de acceso, distribución y núcleo, o un núcleo colapsado cuando la escala es menor, por su modularidad y crecimiento ordenado, estas arquitecturas facilitan políticas consistentes y simplifican operaciones y solución de problemas cotidianos.

Las topologías lógicas complementan a las físicas mediante segmentación en redes virtuales y enrutamiento consistente entre dominios, estándares de puenteo y etiquetado como IEEE 802.1Q

sustentan VLAN, redundancia controlada y caminos determinísticos en redes conmutadas actuales (IEEE, 2022), la validación de decisiones se apoya en capturas básicas que confirmen alcance, etiquetado y rutas, por ejemplo, con un analizador como Wireshark antes de avanzar.

1.5. Captura básica con Wireshark

La captura introductoria busca observar solicitudes de resolución y mensajes de eco para validar conectividad, un filtro de visualización sencillo como “arp” or “icmp” or “icmpv6” or “dns” aísla rápidamente tráfico relevante sin distracciones (Wireshark Foundation, 2025).

La evidencia debe exportarse como archivo pcapng o resumen CSV, preservando marcas temporales y longitudes originales. Para anonimizar direcciones, sustituye identificadores sensibles y considera direcciones temporales IPv6 para privacidad, verificando coherencia con direccionamiento y topología definidos (Gont et al., 2021).

Figura 4

Guía rápida de captura con WireShark

Nota. Guía rápida haciendo uso de WireShark. Fuente. Elaboración propia.

Inicia la captura en la interfaz adecuada y provoca tráfico controlado mediante un eco hacia la puerta de enlace, la secuencia esperada incluye resolución inicial y el intercambio de eco, cuya temporalidad permite confirmar alcance local y salida correcta.

Observa campos clave como tiempo de vida, identificadores de conversación y tamaño, verificando consistencia entre cabeceras y capas observadas, si empleas segmentación lógica, confirma etiquetas VLAN visibles y pertenencia de tramas según el diseño documentado del dominio respectivo (IEEE, 2022).

En redes IPv6, confirma el intercambio de descubrimiento de vecinos y la correcta generación de identificadores temporales cuando corresponda, las tramas deben mostrar prefijos asignados y alcance coherente, con mensajes de eco funcionando entre segmentos autorizados conforme a políticas planificadas. Genera un breve resumen con estadísticas de captura incluyendo cuentas de protocolos, tiempos relativos y direcciones participantes principales, ese sumario complementa las evidencias exportadas y facilita la trazabilidad de pruebas frente a cambios de configuración planificados.

Con la conectividad validada y la evidencia anonimizada, archiva las pruebas junto con el plan de direccionamiento aprobado, en el siguiente capítulo profundizaremos en transmisión y codificación de datos para interpretar las señales que sustentan estas tramas observadas.

Cierre del capitulo

Este capítulo ofreció una visión clara del funcionamiento esencial de las redes modernas actuales, se aprendió que los modelos OSI y TCP IP ordenan funciones por capas colaborativas interdependientes. Cada capa entrega servicios a la siguiente mediante interfaces definidas y comportamientos medibles claros, la unidad de datos o PDU encapsula cabeceras que guían el recorrido extremo completo,

con estos conceptos la red deja de ser caja negra y resulta comprensible técnicamente.

El plan de direccionamiento sostiene el crecimiento y previene solapamientos entre segmentos presentes futuros, con IPv4 e IPv6 asignamos prefijos coherentes, rangos válidos y puertas de enlace estables, la técnica VLSM permite dar tamaños adecuados según necesidades reales de cada área funcional, documentamos decisiones con nombres consistentes y tablas simples que conectan topología y direcciones asignadas, gracias a ello, las pruebas posteriores tienen un referente confiable y repetible siempre documentado.

Los conmutadores mueven tramas con eficiencia y limitan dominios de difusión dentro de segmentos, los enrutadores conectan subredes, aplican políticas y deciden rutas según prefijos definidos y métricas. Los puntos de acceso coordinan estaciones inalámbricas y administran el uso del espectro disponible, seleccionarlos exige equilibrar rendimiento, cantidad de puertos y capacidades de administración centralizada segura escalable, una elección adecuada mejora experiencia diaria, reduce fallos y simplifica operaciones cotidianas de red.

La topología física define cables y enlaces, mientras la lógica organiza rutas y límites, la topología estrella simplifica instalación, aunque concentra riesgo en el punto central de conmutación

principal, el anillo proporciona protección rápida ante cortes usando mecanismos de conmutación específicos bien configurados, la malla distribuye carga y ofrece rutas alternativas con mayor costo administrativo y operativo, el diseño jerárquico acota dominios, separa funciones y facilita crecimiento ordenado del campus institucional.

Validamos nuestras decisiones observando capturas con un analizador de protocolos confiable como Wireshark actualizado, vemos resoluciones de direcciones, mensajes de eco y etiquetas coherentes con el diseño documentado, la evidencia obtenida permite comparar tiempos, rutas y políticas con parámetros esperados para validación. Al archivar pruebas, la red deja de ser misteriosa y se vuelve medible objetivamente, con esta base avanzaremos hacia transmisión y codificación, entendiendo señales que sostienen paquetes confiables.

CAPÍTULO 2: TRANSMISIÓN Y CODIFICACIÓN DE DATOS

«La capacidad C de un canal ruidoso debe ser la tasa máxima posible de transmisión.»

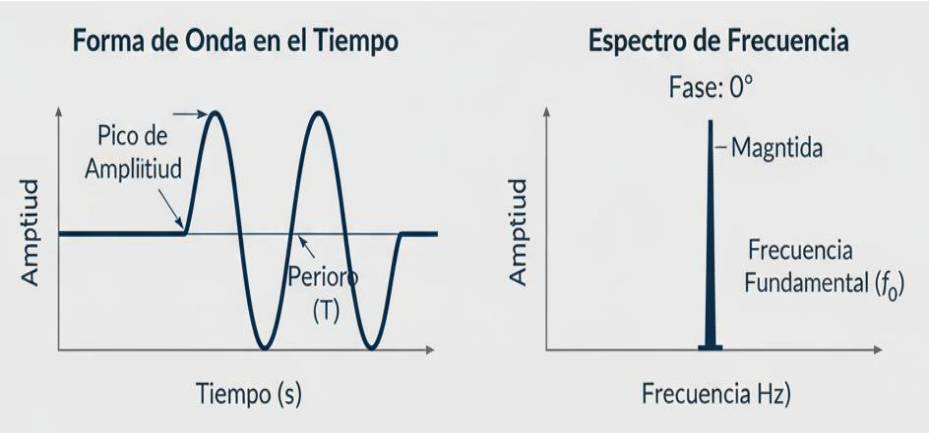
Claude E. Shannon.

Introducción

Las redes existen porque una señal puede transportar información de un punto a otro con confiabilidad suficiente, en este capítulo exploraremos cómo la forma de esa señal, el ruido presente y el ancho de banda disponible determinan lo que realmente llega al destino, comprender transmisión y codificación evita suposiciones peligrosas y permite decisiones técnicas más acertadas, conectaremos estos elementos con la arquitectura por capas vista antes, traduciendo conceptos físicos en efectos prácticos sobre protocolos y servicios.

Figura 5

Formas de onda



Nota. Formación de ondas de acuerdo a amplitud, tiempo y frecuencia. Fuente. Elaboración propia.

Comenzaremos diferenciando señales analógicas y digitales, atendiendo a sus parámetros básicos de amplitud, frecuencia y fase, veremos cómo la digitalización introduce tolerancia al ruido, pero exige sincronización precisa entre emisor y receptor. La codificación de línea ordena los bits en formas de onda interpretables y estables para los equipos, este encuadre nos permitirá leer con criterio temporizaciones, niveles y transiciones observadas en instrumentos o simuladores.

Analizaremos esquemas de codificación representativos como NRZ, Manchester y 4B 5B, relacionando sus ventajas con contextos concretos, discutiremos cómo influyen en la detección de reloj, la densidad de transiciones y la tasa de error. Integraremos mecanismos

de integridad como paridad, CRC y códigos de Hamming para reducir fallas observables, también compararemos medios de transmisión como cableado UTP, fibra óptica y radio, según distancia, capacidad y costo.

Finalmente practicaremos con un simulador para visualizar formas de onda y efectos de la codificación bajo condiciones controladas, mediremos tasas de error de bit, rendimiento efectivo y sensibilidad frente a ruido añadido de manera intencional, documentaremos evidencias con capturas y conclusiones que justifiquen elecciones de diseño específicas, con esta base, avanzaremos al estudio detallado de señales digitales y analógicas para cimentar el razonamiento técnico del resto del capítulo.

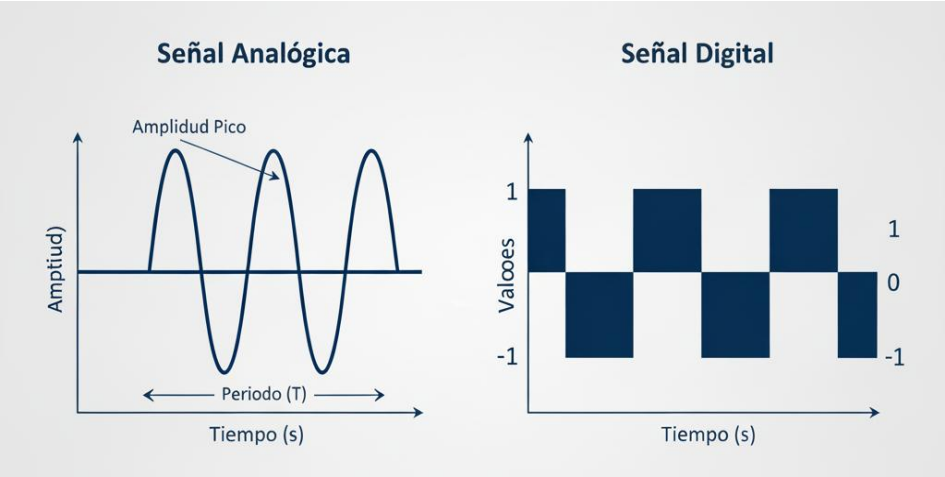
2.1. Señales digitales y analógicas

Comparar señales analógicas y digitales permite decidir cómo transportar información con confiabilidad en redes actuales, la distinción impacta la selección de medios, la sincronización, la tolerancia al ruido y los métodos de diagnóstico. Entender estas diferencias reduce ensayos fallidos y orienta pruebas que confirmen desempeño real en laboratorio y producción, este marco conceptual también enlaza con decisiones de direccionamiento, segmentación y políticas que se verifican mediante evidencia reproducible.

La amplitud describe el nivel de la señal y condiciona márgenes frente al ruido del entorno, la frecuencia expresa cuántos ciclos por segundo ocurren y delimita el ancho de banda útil disponible para transmisión confiable, la fase indica el desplazamiento temporal relativo entre señales y afecta la coherencia de recepción y la interpretación correcta, juntas determinan la capacidad de transporte, la sensibilidad a interferencias y la interpretabilidad de las formas de onda observadas.

Figura 6

Forma de onda analógica vs digital



Nota. Comparación de las formas de las ondas analógicas y digitales. Fuente. Elaboración propia.

El muestreo toma valores discretos en el tiempo y la cuantificación asigna niveles posibles a cada muestra, si la tasa de muestreo resulta insuficiente, aparece “aliasing” que confunde frecuencias altas con bajas durante la reconstrucción, un ejemplo claro es digitalizar voz con frecuencia inadecuada y escuchar tonos distorsionados por componentes mal representados, la elección de frecuencia y filtros adecuados controla ese error y mantiene fidelidad aceptable para el servicio previsto (Mudge, 2023).

El ruido aparece por diafonía entre cables, fuentes conmutadas, motores, radiofrecuencia ambiental y acoplos (adaptaciones) inesperados dentro del recinto, sus efectos incluyen errores de bit, fluctuación temporal, y degradación de formas de onda observables mediante instrumentos de laboratorio. Investigaciones recientes describen acoplamientos indeseados desde sistemas cercanos hacia cableados sensibles y enlaces expuestos en campo (Cruciani et al., 2022; Panholzer et al., 2021), estas condiciones exigen diseño físico cuidadoso y validaciones de compatibilidad electromagnética antes de desplegar producción estable.

En cobre trenzado conviene controlar longitudes, rutas y cercanía a fuentes ruidosas, aplicando blindaje cuando la interferencia resulte severa, en fibra óptica se eliminan corrientes parásitas y se gana inmunidad frente a campos electromagnéticos intensos habituales, las pruebas incluyen mediciones de errores, latencia y estabilidad bajo carga comparadas contra objetivos definidos en el plan de diseño, documentar resultados con marcas temporales confiables facilita reproducibilidad, auditoría y decisiones de corrección antes del despliegue definitivo.

Reconocer degradación implica observar caídas de amplitud, desplazamientos de fase y contaminación espectral persistente durante pruebas controladas, cuando las condiciones físicas están claras, la codificación de línea convierte bits en formas de onda

robustas y sincronizables. En el siguiente tema estudiaremos cómo esquemas como NRZ, Manchester y cuatro B cinco B mejoran sincronía y confiabilidad del enlace, estas decisiones se conectan directamente con la tasa de error y el rendimiento efectivo que experimentarán aplicaciones y usuarios reales.

2.2. Codificación de línea NRZ, Manchester y 4B/5B

La codificación de línea convierte bits en formas de onda que preservan datos y reloj durante el trayecto, un esquema con suficientes transiciones facilita la recuperación de temporización en el receptor y mejora la inmunidad frente a desplazamientos de continua. Esta auto sincronía sostiene enlaces baseband (enlace de banda base) y se refleja en normas modernas de capa física y en diseños de códigos con restricciones bien definidas (Immink, 2022; IEEE, 2022).

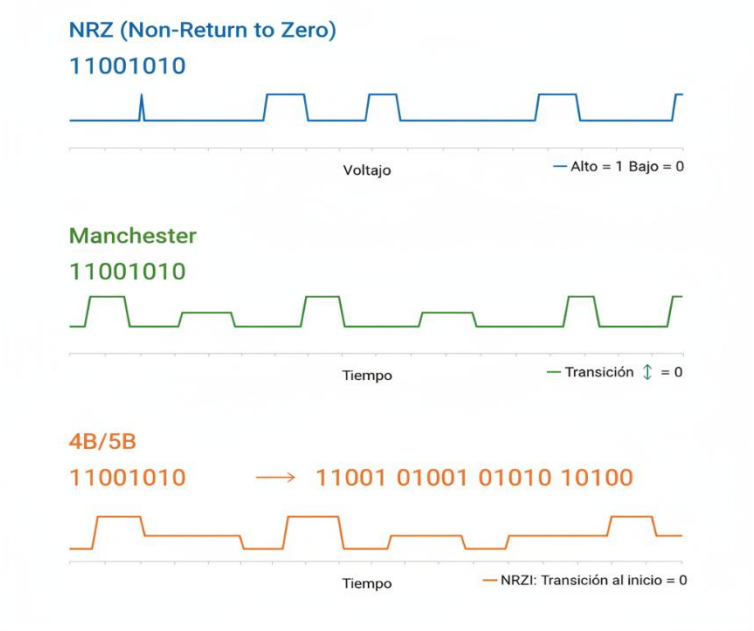
NRZ resulta simple y eficiente en ancho de banda pero puede acumular componente de continua y provocar corrimiento de la línea base, las corridas largas sin transiciones dificultan la recuperación del reloj y elevan sensibilidad a ruido de baja frecuencia. Por ello muchos sistemas combinan NRZ con escramble (codificación de datos), y ecualización para limitar corridas y estabilizar la referencia temporal del receptor, manteniendo eficiencia espectral aceptable en medios controlados (IEEE, 2022).

Manchester asegura al menos una transición por periodo, integrando el reloj en la propia señal y mejorando tolerancia a desalineación, su fortaleza en sincronía se paga con el doble de tasa de símbolos respecto a NRZ y una demanda mayor de ancho de banda efectivo, implementaciones recientes muestran decodificación confiable bajo jitter y ruido realista, especialmente en enlaces de sensórica (detectar y medir fenómenos físicos), y luz visible con trayectos cortos y entornos ruidosos (Ricci et al., 2025).

4B/5B introduce expansión controlada mapeando cuatro bits en cinco símbolos válidos que garantizan transiciones frecuentes, el diccionario evita corridas largas de ceros y facilita la recuperación de reloj cuando se combina con la señalización apropiada, esta estrategia sostiene sincronía en enlaces de cien megabits por segundo ampliamente desplegados en campus y pequeñas empresas con cableado de par trenzado normalizado (IEEE, 2022).

Figura 7

Codificación de línea NRZ, Manchester y 4B/5B



Nota. Figura comparativa de la codificación de línea NRZ, Manchester y 4B/5B. Fuente. Elaboración propia.

La elección depende del medio, la distancia y la tolerancia a errores prevista por el servicio, un laboratorio puede preferir Manchester para telemetría corta y ruidosa, mientras un enlace de acceso a cien megabits adopta 4B 5B por su equilibrio entre sincronía y eficiencia, en backplanes (placas de circuitos) bien acoplados y distancias mínimas, NRZ con escramble ofrece simplicidad y aprovechamiento

del espectro, manteniendo una tasa de error adecuada para la aplicación objetivo (Immink, 2022; IEEE, 2022; Ricci et al., 2025).

La codificación seleccionada determina densidad de transiciones, recuperación de reloj y sensibilidad a desplazamientos de continua, influyendo directamente en la tasa de error observada, en el siguiente tema integraremos estos esquemas con detección y corrección de errores mediante paridad, CRC y códigos de Hamming, cerrando el ciclo de integridad extremo a extremo con criterios medibles y reproducibles.

2.3. Detección y corrección de errores: paridad, CRC y Hamming

Incluso con una codificación de línea adecuada, los enlaces reales introducen atenuación, interferencias y jitter que alteran bits durante el transporte, por esta razón se requieren verificaciones de integridad adicionales que detecten daños accidentales antes de aceptar una unidad de datos en el receptor, estos controles operan cerca del medio o en capas superiores y complementan la sincronía del enlace, los estándares de enlace modernos incorporan mecanismos explícitos de verificación para reducir fallas silenciosas en operación continua (IEEE, 2021; IEEE, 2022).

La paridad agrega un bit que fuerza un conteo par o impar de unos dentro de la palabra, este mecanismo permite detectar alteraciones simples en un único bit con costo casi nulo. Sin embargo, dos errores

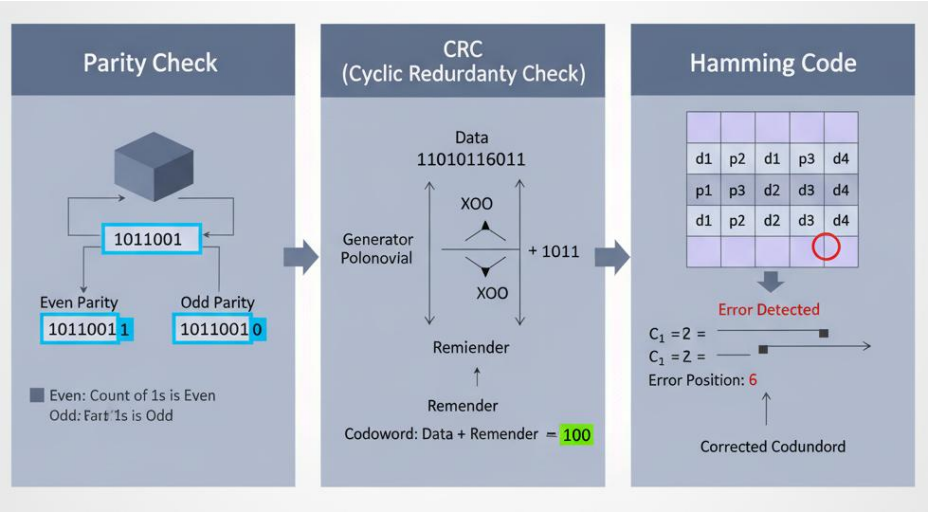
simultáneos pueden neutralizarse y pasar inadvertidos para el verificador de paridad, en redes actuales se reserva para canales cortos o ejercicios didácticos donde la simplicidad resulta prioritaria frente a la cobertura de fallas amplia (IEEE, 2022).

Los códigos de redundancia cíclica usan polinomios generadores sobre campos finitos para producir un residuo representativo de la trama, en recepción se recalcula el residuo y se compara con el campo de verificación, rechazando tramas con discrepancias observables, protocolos masivos como Ethernet y Wi-Fi implementan variantes de CRC que ofrecen alta probabilidad de detección frente a errores en ráfaga, implementaciones recientes documentan CRC treinta y dos compatibles con normas vigentes y hardware accesible (Dewanty & Wardijono, 2022; IEEE, 2021; IEEE, 2022).

Los códigos de Hamming introducen redundancias posicionadas que establecen una distancia mínima capaz de localizar un error, el cálculo del síndrome revela el patrón y permite corregir un bit y detectar dos, con complejidad moderada. Investigaciones recientes confirman su conveniencia en sistemas embebidos y sensado cuando el presupuesto computacional es acotado, este equilibrio favorece aplicaciones de borde donde la latencia y el consumo resultan determinantes (Ali et al.,2024)

Figura 8

Detección y corrección de errores



Nota. Imagen de detección y corrección de errores. Fuente. Elaboración propia.

En la verificación práctica se interpretan campos de control en capturas y contadores de errores del equipo, según la interfaz empleada, la captura puede exponer el campo de verificación o delegar la comprobación al adaptador registrando fallas en el conmutador, la coherencia entre la comprobación, el prefijo asignado y la topología prevista respalda conclusiones reproducibles, ante una discrepancia consistente corresponde documentar el rechazo y revisar el tramo sospechoso con evidencia.

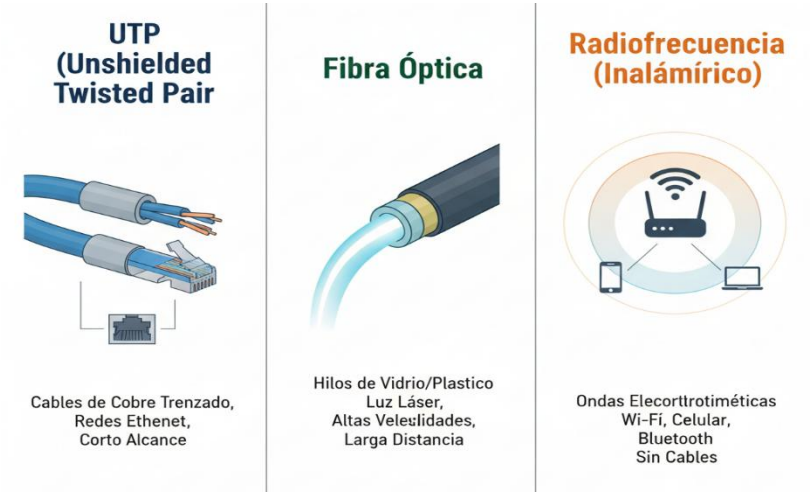
En síntesis, la paridad conviene para canales muy simples, el CRC protege tramas completas con alta capacidad de detección, y Hamming equilibra detección y corrección con costo contenido, la elección depende del medio, la distancia, el ruido esperado y los objetivos de disponibilidad definidos para el servicio. En el siguiente tema conectaremos estos mecanismos con la selección de medios de transmisión y su impacto directo sobre la tasa de error y la confiabilidad observada.

2.4. Medios de transmisión UTP, fibra y radio

La elección del medio condiciona capacidad disponible, alcance máximo, sensibilidad a interferencias y esfuerzo de mantenimiento operativo, un medio adecuado reduce errores, facilita ampliaciones futuras y sostiene las políticas de calidad del servicio planificadas, en redes de campus o empresas medianas, la decisión impacta costos inmediatos y el costo total de propiedad durante todo el ciclo de vida.

Figura 9

Medios de transmisión



Nota. UTP, Fibra óptica y radiofrecuencia como medios de transmisión. Fuente. Elaboración propia.

El par trenzado sin blindaje resulta económico y flexible para interiores bien administrados, aunque exige cuidado en tendido y cercanía a fuentes ruidosas, las categorías superiores mejoran atenuación y control de diafonía, pero requieren certificación de canal y respeto de radios de curvatura, para velocidades altas y alimentación sobre Ethernet conviene validar parámetros eléctricos de enlace según los perfiles de la norma Ethernet vigente (IEEE, 2022).

La fibra óptica ofrece inmunidad a campos electromagnéticos y márgenes amplios para distancias crecientes, el multimodo favorece enlaces de edificio con ópticas económicas, mientras la monomodo habilita troncales de campus y crecimiento sostenido, las ventanas ópticas alrededor de 1310 y 1550 nanómetros equilibran atenuación y dispersión según el presupuesto de potencia disponible y el escenario de uso previsto (Keiser, 2021).

La radio aporta movilidad y rapidez de despliegue, pero su desempeño depende fuertemente del entorno, las bandas de 2.4, 5 y 6 gigahercios presentan comportamientos distintos frente a muros, humedad y redes vecinas, estándares recientes mejoran eficiencia por área y coordinación entre generaciones, aunque requieren planificación de canales, potencias y densidad de celdas basada en estudios de cobertura reales (IEEE, 2021).

Un campus mediano puede usar cobre categoría alta en pisos interiores con tramos cortos y alimentación sobre Ethernet controlada, para unir edificios separados varios cientos de metros, la fibra monomodo ofrece robustez y margen futuro, en patios o zonas temporales, una solución radio planificada con encuestas de sitio brinda movilidad y costos contenidos, integrándose al resto de la arquitectura sin fricciones operativas.

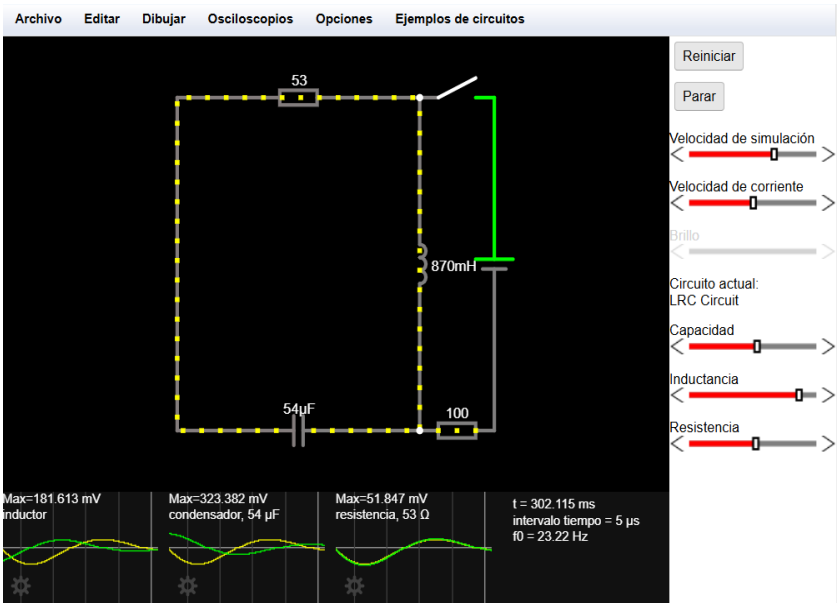
La combinación correcta de medio, distancia y mitigación de interferencias reduce errores y estabiliza el rendimiento observable en producción, estas decisiones condicionan las formas de onda que veremos en simulación y la codificación de línea que mejor conserva reloj y datos. En el siguiente tema conectaremos cada medio con la visualización de señales y la evaluación comparativa de esquemas de codificación para justificar elecciones medibles.

2.5. Simulación con Falstad Circuit Simulator

Una simulación breve en Falstad permite observar cómo los bits se transforman en formas de onda interpretables y estables, al mirar niveles lógicos, tiempos entre transiciones y posibles desplazamientos de línea base se construye intuición operacional, la intuición facilita comprender por qué ciertos esquemas mantienen mejor la sincronía que otros bajo perturbaciones, ver la señal en movimiento ayuda a relacionar teoría con decisiones de diseño concretas y reproducibles en laboratorio (Immink, 2022).

Figura 10

Circuito en simulador Falstad



Nota. Simulación de un circuito en Falstad. Fuente: https://www.falstad.com/circuit/

Para preparar el escenario mínimo configura lo siguiente:

- Configura una fuente binaria temporizada por un reloj estable conectada a un canal ideal, observa en el dominio temporal la alineación entre reloj y datos, y en frecuencia la distribución de energía espectral, cambia gradualmente la frecuencia del reloj y la amplitud para delinear márgenes operativos del enlace virtual, esta preparación sienta bases comparables para

evaluar distintos esquemas de codificación con criterios consistentes (IEEE, 2022).

- Con NRZ reproduce secuencias que incluyan corridas largas de ceros o unos, manteniendo igual periodo de bit, notarás pérdidas de sincronía cuando falten transiciones suficientes y, en acoplos en alterna, corrimiento de la línea base, la señal se vuelve más sensible a ruido de baja frecuencia y a pequeñas desalineaciones temporales, este comportamiento explica el uso de técnicas complementarias como scrambling y ecualización en muchos PHY modernos (IEEE, 2022).
- Cambia el transmisor a Manchester y repite exactamente la misma secuencia de datos y reloj, la transición garantizada por periodo integra el reloj en la propia señal, mejorando tolerancia a desalineación y jitter, observarás trayectorias más regulares y un espectro más extendido que demanda mayor ancho de banda efectivo, la decodificación resulta más confiable en trayectos cortos y entornos ruidosos, como demuestran implementaciones recientes en luz visible (Ricci et al., 2025).
- Introduce después un bloque 4B 5B que mapea cuatro bits en cinco símbolos válidos con transiciones aseguradas, al enviar tramas con corridas prolongadas verás cruces por umbral más regulares, sin introducir componente continua neta con

señalización apropiada, este compromiso mejora la auto sincronía manteniendo eficiencia razonable para enlaces baseband ampliamente estandarizados en campus, el enfoque refleja la lógica de diseño documentada para Ethernet de cien megabits y tecnologías afines (IEEE, 2022; Immink, 2022).

En conjunto, la simulación muestra cómo la densidad de transiciones gobierna la recuperación de reloj y la robustez frente a perturbaciones, estos hallazgos preparan el terreno para medir tasa de error de bit y rendimiento efectivo bajo tráfico controlado, relacionaremos los errores observados con decisiones de codificación y temporización, cerrando el puente entre forma de onda y desempeño medible. Así se consolidará un criterio técnico que conecte teoría, instrumentación y resultados reproducibles en práctica (Immink, 2022; Ricci et al., 2025; IEEE, 2022).

2.6. Medición de tasa de error de bit y rendimiento efectivo

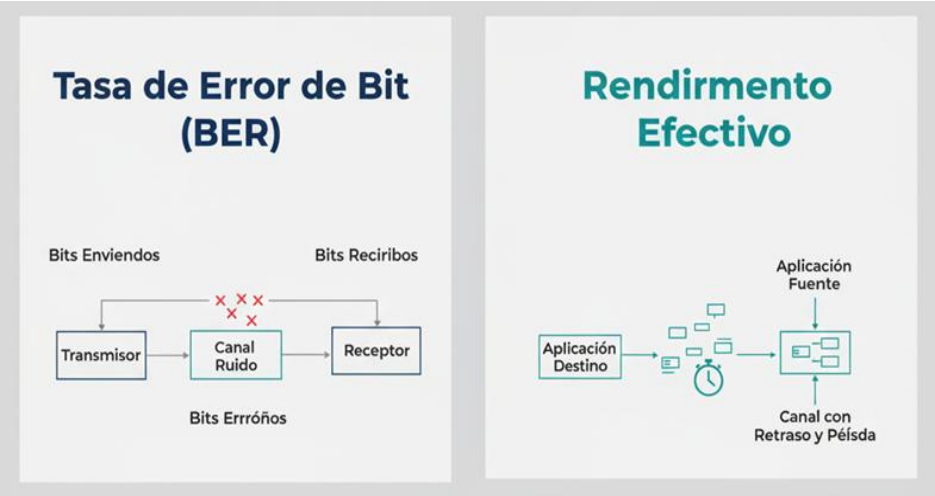
Medir la tasa de error de bit y el rendimiento efectivo orienta decisiones de diseño porque vincula teoría con comportamiento observable, estas métricas permiten estimar márgenes operativos reales y priorizar correcciones donde más impacto producen, un enlace aparentemente estable puede esconder pérdidas pequeñas que, acumuladas, degradan aplicaciones sensibles, cuantificar esos efectos convierte las percepciones en evidencia y evita ajustes basados únicamente en intuiciones o anécdotas.

La tasa de error de bit se define como el cociente entre los bits erróneos detectados y el total de bits recibidos durante una ventana de observación, esta razón ofrece una medida directa de la confiabilidad del canal bajo una combinación concreta de medio, codificación y condiciones ambientales, en óptica y cobre se interpreta junto con presupuesto de potencia, atenuación y dispersión para ubicar la causa probable, su comparación entre configuraciones alternativas guía la selección de parámetros más robustos para el servicio objetivo (Keiser, 2021).

El rendimiento efectivo se distingue de la capacidad nominal porque descuenta cabeceras, control, rellenos y retransmisiones. Dos enlaces con la misma tasa física pueden entregar volúmenes de datos útiles muy distintos ante pérdidas o timeouts, protocolos modernos optimizan confirmaciones y recuperación para elevar el goodput (tamaño de archivos dividido entre el tiempo de transmisión) bajo error y latencia variables, aunque siempre existe sobrecarga inevitable, medir esa diferencia permite dimensionar reservas y entender cuánta capacidad usable perciben realmente las aplicaciones (IEEE, 2022; Iyengar & Thomson, 2021).

Figura 11

Métricas clave de comunicación digital



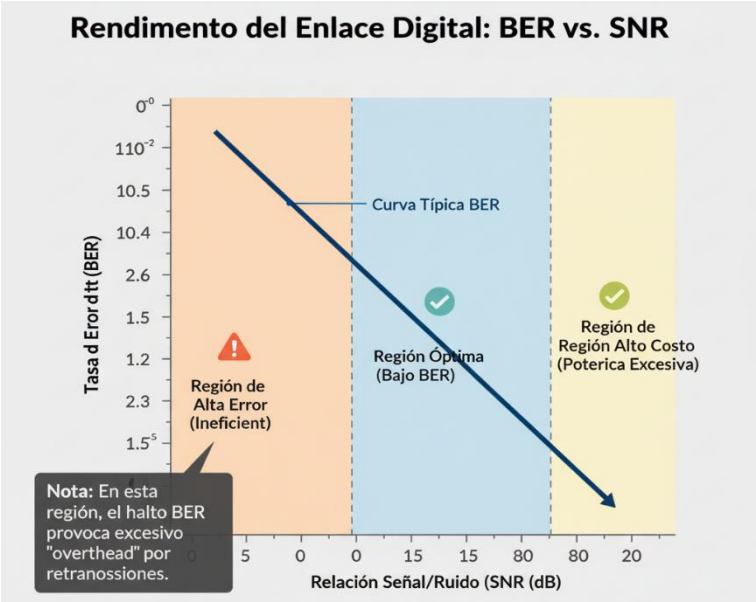
Nota. Métricas clave de comunicación digital y la comparación entre la taza de Bit y el rendimiento efectivo. Fuente. Elaboración propia.

Un procedimiento simple y reproducible consiste en generar tráfico de prueba con tamaño y patrón conocidos durante ventanas temporales claras, se registra el total de bits transmitidos, los bits útiles recibidos y los errores detectados por el verificador correspondiente, la sincronización de relojes y el control del reloj del generador evitan sesgos por discrepancias temporales, repetir con al menos dos cargas distintas permite observar tendencias y descartar resultados atípicos por calentamiento o interferencias puntuales.

El análisis relaciona resultados con la codificación empleada, el medio físico y el ruido ambiental medido o estimado, una BER elevada con NRZ y acoplo en alterna puede mejorar al introducir scrambling o adoptar Manchester en tramos ruidosos, si el rendimiento efectivo cae con pérdidas intermitentes, conviene revisar colas, retransmisiones y control de congestión del protocolo, protocolos recientes modelan explícitamente pérdida y latencia, lo que ayuda a inferir cuellos de botella dominantes (Iyengar & Thomson, 2021; Iyengar & Swett, 2021).

Figura 12

Rendimiento del BER vs SNR



Nota. Grafica del rendimiento del enlace digital VER y SNR
Fuente. Elaboración propia.

En conjunto, BER y rendimiento efectivo concentrarán el seguimiento del desempeño a medida que integremos seguridad y cifrado, el encapsulado adicional y los intercambios de establecimiento introducen sobrecarga que debe considerarse en enlaces ajustados, evaluaremos cómo los mecanismos de integridad y confidencialidad interactúan con pérdidas, latencia y recuperación para sostener experiencias aceptables, ese puente permitirá elegir parámetros de cifrado y control apropiado sin comprometer la confiabilidad alcanzada (IEEE, 2022; Iyengar & Thomson, 2021)

Cierre del capitulo

Este capítulo te llevó desde la naturaleza de las señales hasta su impacto directo en el desempeño de la red, comprendiste cómo la forma de onda, el ruido y el ancho de banda condicionan lo que realmente llega a destino, viste que la sincronía entre emisor y receptor depende de transiciones suficientes y temporización estable, aprendiste además que observar la señal en el tiempo y la frecuencia cambia hipótesis vagas por criterios medibles.

Diferenciaste señales analógicas y digitales usando amplitud, frecuencia y fase como guías para interpretar fenómenos cotidianos, entendiste que el muestreo y la cuantificación imponen límites

prácticos que exigen frecuencias adecuadas y filtrado pertinente, reconociste el aliasing como un riesgo real cuando se muestrean contenidos sin respetar esos límites, construiste intuición técnica con simulaciones que mostraron márgenes, deformaciones y desplazamientos de línea base con claridad suficiente.

Contrastaste esquemas de codificación y observaste cómo influyen en sincronía, densidad de transiciones y ocupación espectral, NRZ ofreció eficiencia, aunque sensible a corridas largas y desplazamientos de continua en acoplos específicos, Manchester mejoró la recuperación de reloj con costo de mayor ancho de banda y robustez apreciable en entornos ruidosos, cuatro B cinco B equilibró auto sincronía y eficiencia mediante una expansión controlada adecuada para enlaces ampliamente desplegados.

Relacionaste integridad lógica con medios y entorno al aplicar paridad, CRC y Hamming según objetivos y presupuesto, mediste tasa de error de bit y rendimiento efectivo para convertir percepciones en evidencia reproducible y comparable, viste que cabeceras, retransmisiones y control de congestión separan capacidad nominal de datos útiles realmente entregados, documentaste resultados con ventanas temporales claras y aprendiste a justificar aceptaciones o rechazos apoyándote en campos de verificación.

Con estas bases puedes diseñar enlaces realistas, justificar decisiones y prever efectos de cambios físicos sobre capas superiores, en el próximo capítulo integrarás seguridad aplicando confidencialidad, integridad y disponibilidad sobre los canales ya caracterizados, analizarás cómo el cifrado, los certificados y los intercambios iniciales conviven con pérdidas, latencia y variaciones del medio, llevarás la evidencia de tus mediciones para elegir parámetros seguros sin sacrificar la experiencia de usuarios y aplicaciones..

CAPÍTULO 3: SEGURIDAD DE DATOS APLICADA

«El único sistema verdaderamente seguro es aquel que está apagado»

Eugene H. Spafford

Introducción

La seguridad de datos aplicada convierte principios en decisiones verificables que protegen información y servicios en entornos reales, este capítulo parte de una idea simple y poderosa: no basta con que la transmisión funcione, también debe ser confiable, auténtica y disponible. Usaremos el marco de confidencialidad, integridad y disponibilidad junto con autenticación, autorización y contabilización para ordenar controles, de esta manera conectaremos los riesgos cotidianos con respuestas técnicas que pueden medirse y auditarse, la meta es que puedas justificar cada medida con evidencia y no solo con intuición.

Nos enfocaremos en herramientas concretas que fortalecen la integridad y la confianza en el intercambio, generaremos y verificaremos huellas digitales con funciones de resumen como SHA doscientos cincuenta y seis y practicaremos codificación Base sesenta y cuatro cuando el transporte lo requiera, observaremos el inicio de una sesión segura con el protocolo de seguridad de la capa de transporte en un analizador de protocolos, identificaremos certificados X punto quinientos nueve, validaremos su cadena de

confianza y reconoceremos parámetros de cifrado activo, cada verificación quedará respaldada con capturas claras y reproducibles.

La protección de acceso se llevará al plano operativo con listas de control en un emulador de práctica, aplicaremos el principio de mínimo privilegio para decidir qué tráfico pasa y qué tráfico se bloquea según origen, destino y puerto, relacionaremos estas políticas con la segmentación existente y con los objetivos de direccionamiento definidos en capítulos anteriores, comprobaremos el efecto de las reglas utilizando pruebas controladas y registraremos resultados para facilitar la solución de problemas, la intención es que cada regla tenga un propósito explícito y una evidencia que certifique su eficacia.

Cerraremos integrando la seguridad con la gestión documental que exige trazabilidad y aceptación formal, configuraremos un flujo de firma electrónica para actas y entregables, cuidando privacidad y resguardo de datos personales, organizaremos un repositorio con procedimientos, capturas y resúmenes para responder a auditorías internas o externas. Finalmente, consolidaremos buenas prácticas y cumplimiento mínimo con un enfoque realista que priorice impacto y sostenibilidad, con esta base estarás preparado para defender decisiones técnicas y para continuar hacia redes de área amplia y enrutamiento con controles coherentes.

3.1. Principios CIA y AAA y políticas básicas

Los principios de confidencialidad, integridad y disponibilidad, junto con autenticación, autorización y contabilización, sostienen decisiones de seguridad en redes educativas y empresariales porque traducen riesgos en controles observables, definir su alcance evita políticas genéricas que no protegen lo que realmente importa y desperdician esfuerzo valioso, documentar políticas claras crea un lenguaje común para docentes, estudiantes y personal técnico, y permite auditorías con criterios repetibles alineados con marcos reconocidos. Este enfoque encaja con lineamientos actuales de control organizacional y de arquitectura de confianza mínima publicados por organismos de referencia (National Institute of Standards and Technology, 2020; Rose et al., 2020).

La confidencialidad protege contra divulgación no autorizada y se mide con cifrado correcto en tránsito y en reposo, además de controles de acceso revisables, la integridad asegura que los datos no cambien sin detección, apoyándose en firmas, hashes verificables y registros inmutables asociados a flujos de aprobación, la disponibilidad mantiene servicios accesibles dentro de objetivos de continuidad definidos, respaldados por capacidad, redundancia y respuesta ante incidentes, cada principio se vuelve tangible cuando existe evidencia de configuración, pruebas periódicas y responsables

identificados para sostener su operación (National Institute of Standards and Technology, 2020).

Autenticación verifica identidades de usuarios y sistemas, autorización decide qué acciones se permiten bajo condiciones explícitas, y contabilización registra quién hizo qué y cuándo, este ciclo continuo reduce privilegios excesivos, facilita investigación forense y respalda cumplimiento ante terceros. En prácticas modernas, credenciales fuertes se combinan con tokens y atestación del cliente para reforzar decisiones de acceso y trazabilidad asociada, estos patrones aparecen formalizados en perfiles recientes para emisión de tokens y en mecanismos de autenticación mutua de transporte (Campbell, Bradley, Sakimura, & Jones, 2020; Richer, 2021).

Una política mínima coherente define requisitos de contraseñas y segundos factores, segmenta la red según riesgo y establece uso aceptable de recursos, tales reglas se vinculan a amenazas probables, como suplantación, fuga de información y denegación, y se actualizan con base en hallazgos operativos, la alineación con marcos de control consolida prácticas repetibles sin depender de memorias individuales ni de interpretaciones cambiantes. Además, la desactivación de protocolos obsoletos y la negociación segura de transporte refuerzan la postura de protección en servicios expuestos a Internet (Sheffer & Farrell, 2021).

La evidencia de cumplimiento proviene de registros de autenticación, decisiones de autorización, cambios de configuración y eventos de seguridad con marcas de tiempo confiables, capturas de intercambio inicial, comprobaciones de certificados y bitácoras firmadas digitalmente fortalecen la trazabilidad y la defensa ante auditorías técnicas o académicas, consolidar esa evidencia en expedientes versionados permite seguimiento de hallazgos, medidas correctivas y verificación posterior sin ambigüedades, el resultado es una cadena completa de custodia documental que conecta política, control, prueba y decisión.

En síntesis, se actualizan políticas cuando cambian amenazas, tecnologías o requisitos legales, priorizando controles con mayor impacto y menor complejidad operativa, el siguiente paso profundiza en hashing y codificación con una herramienta de laboratorio para reforzar integridad y transporte seguro, verificar huellas y procedimientos repetibles reducirá ambigüedades y alineará controles con los objetivos de disponibilidad y confiabilidad establecidos, así se cierra el puente entre principios, políticas y evidencias medibles que sostienen la seguridad cotidiana de la red.

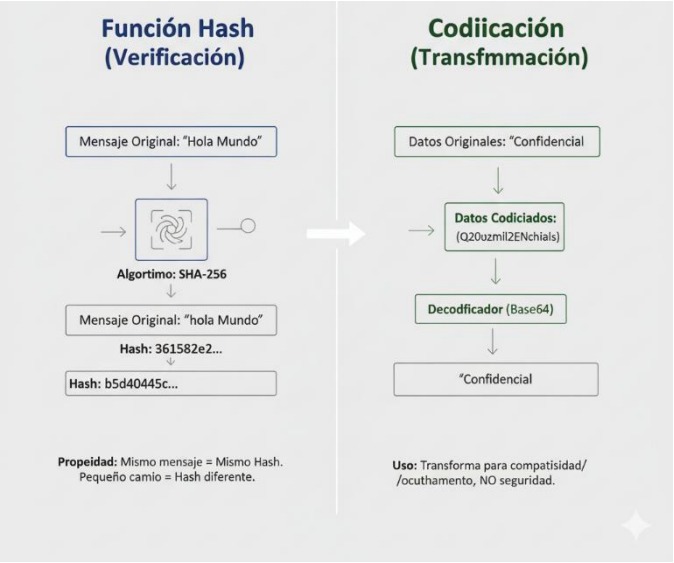
3.2. Hash y codificación con CyberChef

Los hashes resuelven un problema concreto: detectar si un artefacto cambió por error o por manipulación intencional durante el tránsito o el almacenamiento, una codificación segura facilita mover datos por

canales que solo aceptan texto y, a diferencia de un hash, no pretende brindar integridad por sí misma, en la práctica se combinan ambos: el dato viaja codificado y su huella se verifica para confirmar que nadie alteró el contenido, el uso de funciones robustas responde a evidencia reciente sobre debilidades en algoritmos obsoletos y a guías actuales para servicios seguros en tránsito (Leurent & Peyrin, 2020; Sheffer et al., 2022).

Figura 13

Representación de Hash y codificación de datos

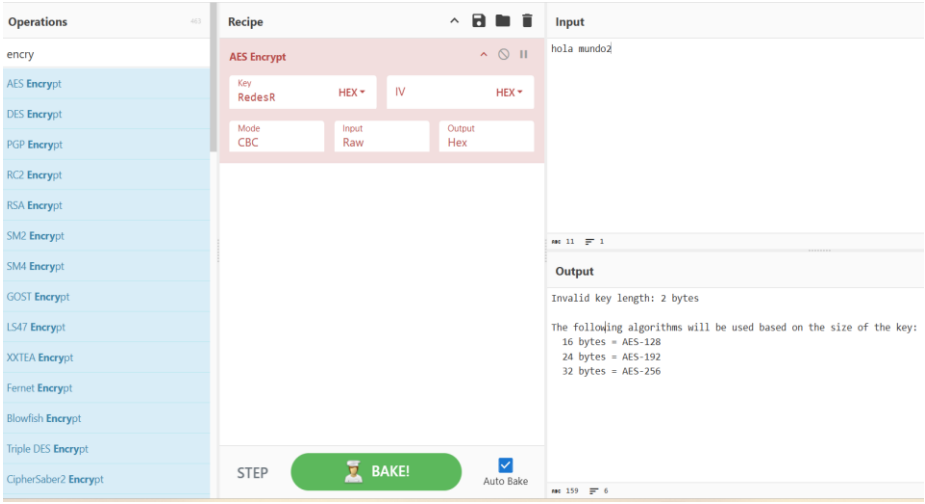


Nota. Imagen de representación de Hash y codificación de datos. Fuente. Elaboración propia.

Un hash útil para seguridad ofrece resistencia a colisiones, unidireccionalidad y alta sensibilidad ante cambios mínimos, hoy se recomiendan familias SHA-2 o SHA-3 para integridad general, y funciones de derivación resistentes a hardware paralelo como Argon2 para proteger contraseñas y secretos, estas elecciones desalientan ataques por colisión o preimagen y reducen riesgos frente a fuerza bruta masiva, la evidencia técnica y normativa reciente respalda abandonar algoritmos débiles y adoptar parámetros modernos verificables (Biryukov et al., 2021; Sheffer et al., 2022; Sheffer et al., 2020).

Figura 14

Representación de encriptado en CyberChef



Nota. Imagen capturada en representación de encriptado en CyberChef Fuente: https://gchq.github.io/CyberChef/

En un taller con CyberChef, carga un archivo de prueba y aplica una receta de hash como SHA-256 dejando trazado reproducible de cada paso, observa el digest en hexadecimal y si necesitas transportar la huella por un canal restringido, codifícala en Base64url sin perder fidelidad. Conserva la receta y el artefacto para que otra persona pueda repetir el cálculo y obtener exactamente el mismo resultado, identificar claramente entrada, operación y salida evita ambigüedades al compartir evidencias entre equipos técnicos y docentes (GCHQ, 2025; Sheffer et al., 2020).

La validación de integridad compara el hash esperado con el calculado sobre el artefacto recibido bajo las mismas transformaciones y codificaciones declaradas, si las huellas coinciden carácter por carácter, se acepta el archivo como íntegro para el contexto definido; si difieren, se rechaza y se investiga el punto de alteración. Al documentar el procedimiento, especifica claramente algoritmo, formato de salida y, si aplica, normalización previa, este rigor elimina dudas y alinea la comprobación con prácticas recomendadas para intercambios protegidos (Sheffer et al., 2022).

Para el reporte, captura pantallas que muestren entrada, receta aplicada y digest final, anotando versión de CyberChef, fecha y

parámetros relevantes, incluye el archivo de receta exportado y un resumen breve que permita a un tercero replicar el cálculo sin asistencia adicional, al citar la herramienta en APA 7, utiliza autor corporativo, año y formato de software con URL, por ejemplo: GCHQ. (2025). CyberChef desde su url: https://gchq.github.io/CyberChef/. Este nivel de trazabilidad agiliza revisiones docentes y auditorías de pares.

En síntesis, usa hash cuando debas verificar integridad o vincular evidencias a un artefacto concreto, y usa codificación cuando solo necesites representación segura para transporte, en los siguientes temas uniremos estas prácticas con certificados y con el intercambio seguro de claves, observando el establecimiento y la validación en un analizador de protocolos. Así conectarás la evidencia de integridad con políticas de sesión, cifrado y autenticaciones contemporáneas en redes reales (Sheffer et al., 2022; Sheffer et al., 2020; Biryukov et al., 2021).

3.3. TLS, PKI y certificados X punto 509 en Wireshark

El cifrado en tránsito protege credenciales y datos frente a observadores y manipulaciones en redes compartidas, públicas o internas, un protocolo seguro como TLS negocia claves efímeras y establece confidencialidad e integridad verificables sobre el canal esa negociación se apoya en una infraestructura de clave pública que permite autenticar identidades mediante certificados válidos y firmas

confiables. Las guías actuales recomiendan configuraciones modernas y la desactivación de versiones antiguas que ya no ofrecen protección adecuada (Sheffer et al., 2022; Sheffer et al., 2021; Rescorla, 2022).

Un certificado X punto 509 contiene el sujeto, la clave pública, el emisor, el periodo de validez, los usos permitidos y el nombre alternativo del sujeto, la confianza surge del encadenamiento correcto hacia una entidad certificadora reconocida por el sistema que valida la firma del emisor inmediato, la validez temporal delimita el periodo durante el cual la identidad puede considerarse vigente y comprobable. El control de fechas protege contra certificados caducados o prematuros y apoya decisiones de revocación registradas por la autoridad correspondiente (Sheffer et al., 2022).

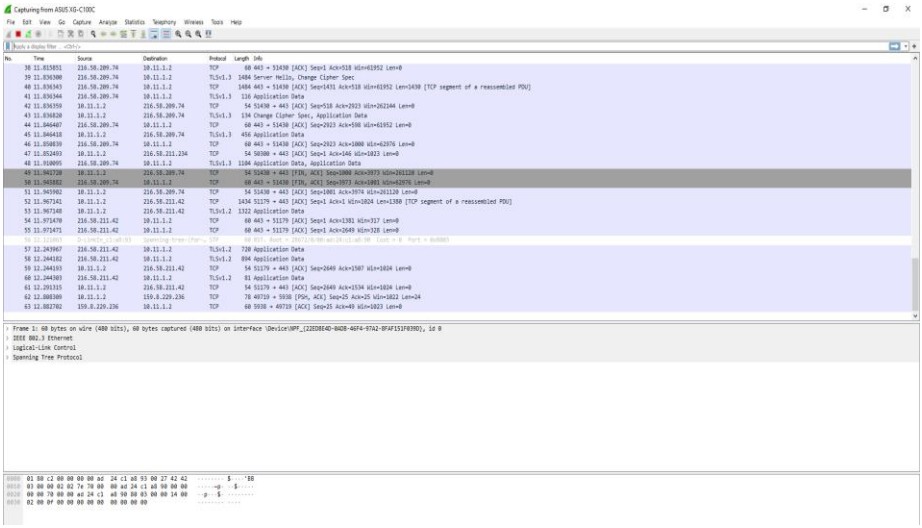
En Wireshark puedes aislar el inicio de un intercambio con un filtro por puerto o por protocolo y centrarte en los mensajes de establecimiento, observa el saludo del cliente, el nombre del servidor indicado por la extensión correspondiente, el conjunto de suites y el intercambio de claves propuesto. Revisa el saludo del servidor y la respuesta con parámetros aceptados, junto con el mensaje de certificado y la indicación del protocolo de aplicación negociado, en TLS moderno parte del intercambio se cifra tempranamente, pero la identificación del servidor y el encadenamiento siguen siendo visibles para análisis (Sheffer et al., 2022; Rescorla, 2022).

Las validaciones mínimas incluyen verificar que el nombre presentado en el certificado coincida con el servicio solicitado y que el periodo de validez resulte apropiado, también deben confirmarse la firma y la cadena hasta una entidad certificadora confiable para el sistema donde se verifica, alertas por nombre no coincidente, emisor desconocido o certificado expirado deben impedir continuar con la conexión hasta corregir la causa, estas comprobaciones reducen riesgos de suplantación y alinean el análisis con prácticas recomendadas para servicios expuestos a Internet (Sheffer et al., 2022; Sheffer et al., 2021).

Para generar evidencia replicable exporta únicamente los paquetes relevantes en un archivo dedicado y registra los filtros y la versión de la herramienta utilizada, incluye capturas que muestren la vista del certificado, los parámetros negociados y los detalles de la cadena de confianza, referencia cada archivo en el informe con nombre, fecha, hora y una huella criptográfica calculada con un algoritmo moderno de resumen, esa trazabilidad permite a otra persona reproducir hallazgos y confirmar que no hubo alteraciones posteriores al levantamiento.

Figura 15

Representación de datos y captura en Wireshark



Nota. Imagen capturada en representación de datos en Wireshark

Fuente: Trafico en Whireshark.

En conjunto, la observación del intercambio y la validación del certificado producen una cadena de evidencia que conecta política, control y prueba, con estos fundamentos podrás aplicar decisiones coherentes en el borde de la red mediante listas de control que restrinjan accesos según identidad y necesidad, este puente fortalece la postura de seguridad porque une autenticación confiable, cifrado efectivo y autorización verificable en escenarios operativos, en los siguientes ejercicios integraremos estas verificaciones con controles

de acceso para sostener decisiones consistentes y auditables en campus y pequeñas empresas

3.4. Control de acceso con listas en emulador TP Link

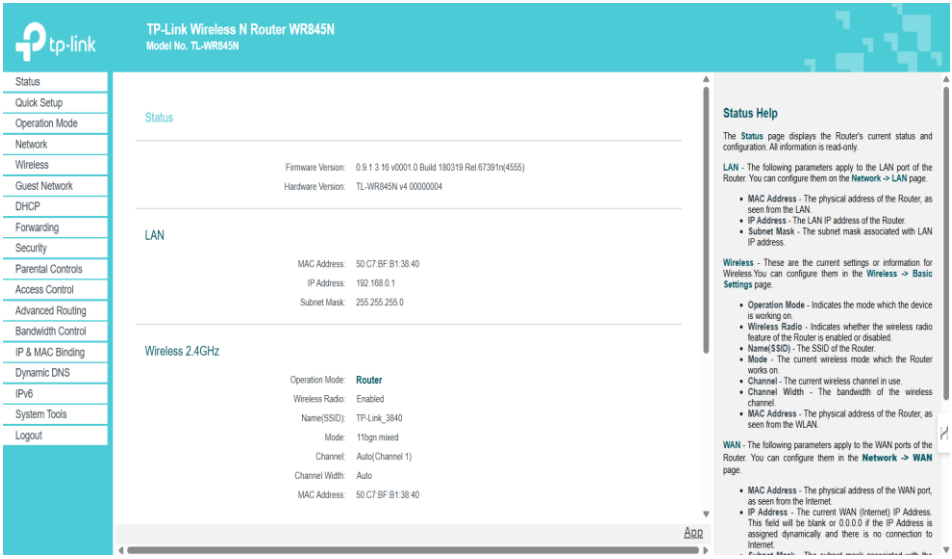
Las listas de control de acceso limitan el tráfico por origen, destino y servicio antes de que alcance recursos sensibles por lo que son un pilar de defensa en profundidad, en un laboratorio con conmutadores administrables y un equipo de borde, el alcance incluye segmentación entre áreas, exposición controlada de servicios y generación de evidencia auditable, este enfoque se alinea con arquitecturas de confianza mínima y con controles organizacionales que exigen decisiones explícitas y verificables sobre cada flujo observado en la red (National Institute of Standards and Technology, 2020a; National Institute of Standards and Technology, 2020b).

Las reglas deben derivarse de requisitos de negocio y de riesgo, como permitir administración desde una subred autorizada y negar accesos no justificados a sistemas académicos, el orden de evaluación es determinante porque los motores de listas suelen aplicar la primera coincidencia, por lo que las condiciones específicas deben anteceder a las genéricas para evitar resultados inesperados, documentar la intención de cada regla con su justificación y alcance reduce permisos excesivos y facilita revisiones de cumplimiento basadas en evidencia (National Institute of Standards and Technology, 2020b).

En el emulador de TP Link la implementación consiste en crear reglas, asociarlas a interfaces de entrada o salida y aplicarlas a puertos o VLAN según el diseño, conviene capturar pantallas que muestren la regla, la interfaz asociada y el estado final adoptando una convención de nombres que incluya propósito, ámbito y fecha. Esta trazabilidad se refuerza cuando la configuración sigue modelos estructurados y exportables coherentes con marcos modernos de automatización y gestión declarativa (Wu, Boucadair, López, Xie, & Geng, 2021).

Figura 16

Emulador en TP Link



Nota. Imagen de Emulador en TP Link. Fuente: https://emulator.tp-link.com/Emulator_TL-WR845NV4(UN)/index.htm

La verificación combina eco hacia puertas de enlace definidas, resolución de nombres y pruebas de servicios puntuales autorizados y denegados deben conservarse evidencias de conectividad esperada, rechazos justificados y marcas temporales coherentes con el plan de pruebas y la topología, los registros de autenticación y autorización, junto con contadores de coincidencias por regla completan la cadena de custodia que sustenta conclusiones reproducibles y auditables por terceros competentes (National Institute of Standards and Technology, 2020b).

Los errores más frecuentes incluyen falsos positivos por reglas demasiado amplias ubicadas antes que excepciones legítimas y falsos negativos por omisiones o prioridades incorrectas, para aislar conflictos conviene revisar el orden, observar contadores de impacto por regla y probar desde fuentes y destinos representativos, la gestión centralizada de identidades y políticas apoyada en modelos estandarizados facilita mantener la coherencia entre entornos y reduce desviaciones operativas durante cambios controlados (Wu et al., 2021; National Institute of Standards and Technology, 2020a).

El mantenimiento periódico exige revisar reglas ante cambios de servicios, segmentación o riesgos, confirmando que la evidencia aún sostenga la intención original, una vez estabilizadas las listas en el equipo de borde, el paso siguiente es formalizar entregables con firma electrónica que asegure integridad y trazabilidad de acuerdos y

resultados, este puente conecta control de acceso, documentación verificable y aceptación formal, reforzando la gobernanza de la seguridad en el curso y en la operación cotidiana (National Institute of Standards and Technology, 2020b).

3.5. Buenas prácticas y cumplimiento

En redes educativas y pymes destacan riesgos como credenciales débiles, configuraciones expuestas, ransomware y suplantación mediante correos persuasivos, que provocan interrupciones, fuga de datos y costos operativos imprevistos, adoptar un enfoque de higiene y cumplimiento transforma esos riesgos en controles medibles, priorizando lo que más afecta la continuidad del servicio y la docencia, utilizar marcos reconocidos aporta un vocabulario común y una lista base de salvaguardas para seleccionar, justificar y auditar sin ambigüedades (National Institute of Standards and Technology, 2020; Marshall et al., 2024).

Los mínimos de higiene incluyen actualización oportuna del software, copias de seguridad verificadas y gestión sólida de contraseñas con autenticación multifactor cuando sea posible, la adherencia se mide con indicadores simples como latencia de parches críticos, tasa de éxito de restauraciones y cobertura de factores adicionales en cuentas privilegiadas, estas métricas convierten políticas abstractas en compromisos operativos rastreables y comparables entre periodos, facilitando decisiones de inversión

sostenidas por evidencia (National Institute of Standards and Technology, 2020).

La protección de datos exige minimizar recolección, definir retenciones razonables y anonimizar evidencia cuando se compartan capturas o bitácoras, en prácticas de laboratorio conviene ocultar nombres y direcciones internas y considerar direcciones temporales en IPv6 que rotan identificadores para disminuir correlaciones indeseadas, las decisiones deben equilibrar utilidad analítica y riesgo de reidentificación, dejando documentados supuestos, transformaciones y límites del anonimizado aplicado (Gont et al, 2021; Gadotti et al., 2024).

Las guías breves, los entrenamientos periódicos y los simulacros estructurados refuerzan conductas seguras y reducen variaciones entre equipos con responsabilidades distintas, la eficacia puede evaluarse con indicadores de proceso y resultado, por ejemplo, reducción de clics en campañas de prueba o mejora en reportes oportunos de incidentes. La literatura reciente muestra beneficios y límites de la capacitación, por lo que la evidencia local debe guiar ajustes iterativos en contenido y frecuencia (Hillman et al., 2023; Marshall et al., 2024).

Un ciclo de revisión con listas de verificación, métricas básicas y acciones priorizadas por impacto y coste fomenta mejora continua sin

sobrecarga, verificar criptografía y transporte seguro, retirar versiones obsoletas y alinear accesos con principios de confianza mínima reduce superficie de ataque y facilita conformidad, integrar estas comprobaciones con políticas de red y registros firmados sostiene decisiones coherentes y trazables ante auditorías internas o externas (Sheffer et al., 2022; Rose, Borchert et al., 2020).

La combinación de higiene técnica, privacidad responsable, procedimientos claros y verificación periódica construye una cultura de seguridad que resiste la rotación de personal y los cambios tecnológicos, estas prácticas no sustituyen el juicio experto, pero establecen un piso común y auditable para operar con confianza en aulas, laboratorios y oficinas. Cerrar el capítulo conlleva institucionalizar hábitos, asignar responsables y asegurar continuidad de controles, integrándolos con transporte cifrado y autenticación robusta para sostener una seguridad práctica, medible y sostenible.

Cierre del capitulo

Este capítulo convirtió la seguridad en un conjunto de decisiones verificables que acompañan al diseño y la operación diaria, pasaste de los principios de confidencialidad, integridad y disponibilidad a controles medibles que se sostienen con autenticación, autorización y contabilización. Entendiste que una red segura no depende de intuiciones aisladas, sino de políticas claras y evidencias repetibles,

la meta fue que cada medida tenga propósito explícito, responsable definido y una prueba que confirme su efectividad.

Consolidaste políticas mínimas que reducen riesgos frecuentes y ordenan el acceso a recursos según necesidad comprobada, viste cómo la documentación y la trazabilidad alinean a estudiantes, docentes y personal técnico alrededor de criterios comunes. Aprendiste a registrar decisiones con bitácoras, capturas y marcas temporales que resisten auditorías internas y externas, esa disciplina convierte la seguridad en un proceso continuo y no en una acción puntual difícil de mantener.

Llevaste la integridad al laboratorio calculando huellas con herramientas accesibles y codificando cuando el transporte lo requiere, observaste en un analizador de protocolos el inicio de sesiones seguras, validando certificados, nombres, periodos de validez y cadenas de confianza. Relacionaste esas verificaciones con configuraciones modernas del protocolo para proteger credenciales y contenidos en tránsito, quedó claro que la evidencia técnica debe acompañar siempre la política declarada y el servicio ofrecido.

Trasladaste el control de acceso a un emulador gráfico, derivando reglas desde requisitos y ordenándolas con prioridades correctas, probaste permisos y rechazos con tráfico controlado, registrando resultados y corrigiendo falsos positivos o falsos negativos cuando

aparecieron, formalizaste la aceptación de entregables mediante firma electrónica para reforzar la cadena de custodia documental. Así uniste control técnico, gobernanza y aceptación formal en un mismo flujo coherente y auditable.

Finalmente integraste higiene técnica, privacidad responsable y mejora continua usando indicadores sencillos que orientan inversiones y esfuerzo, con esta base puedes planificar cambios con menor incertidumbre y defender decisiones frente a evaluaciones académicas o revisiones profesionales. En el próximo capítulo abordarás redes de área amplia y enrutamiento, conectando estas garantías con topologías distribuidas, políticas entre dominios y conectividad extremo a extremo, llevarás contigo el mismo enfoque basado en evidencia para que cada salto y cada ruta mantengan confidencialidad, integridad y disponibilidad sin comprometer el desempeño esperado.

CAPÍTULO 4: EVALUACIÓN CON ENFOQUE DE INCLUSIÓN Y EQUIDAD

«No se introduce un paquete nuevo en la red hasta que otro haya salido.»

Van Jacobson

Introducción

Las redes de área amplia conectan sedes, aulas remotas, laboratorios y servicios en la nube con objetivos de continuidad y eficiencia, este capítulo aborda cómo transformar requerimientos de negocio y académicos en decisiones concretas de arquitectura entre dominios, verás que el diseño de área amplia no solo une puntos distantes, también establece márgenes de disponibilidad, capacidad y crecimiento ordenado, el propósito es que puedas justificar una topología coherente con riesgos, presupuesto y metas de servicio medibles.

Comenzaremos comparando alternativas de interconexión y sus implicaciones sobre resiliencia, latencia y operación cotidiana, analizaremos cuándo conviene una topología simple y cuándo resulta preferible distribuir funciones en un diseño jerárquico con enlaces redundantes. Revisaremos criterios de selección de enlaces y equipos, considerando rutas primarias, rutas de respaldo y límites de fallo razonables, la idea central es que el diagrama físico y lógico refleje objetivos claros y verificables.

Luego entraremos al enrutamiento como mecanismo que hace efectiva la arquitectura planificada. Practicarás rutas estáticas para entornos pequeños y protocolos dinámicos cuando cambian rutas, costos o prefijos con frecuencia, exploraremos principios de RIPv2 y OSPF para comprender métricas, convergencia y políticas de preferencia entre múltiples caminos, también integraremos traducción de direcciones mediante NAT y PAT para publicar servicios y controlar salidas hacia Internet con registros reproducibles.

Finalmente incorporaremos el concepto de red privada virtual con una mirada operativa a IPsec y su flujo básico, puedes observar cómo combinar cifrado con rutas coherentes para sostener confidencialidad sin romper la conectividad extremo a extremo, cerraremos con un enfoque sistemático de verificación y resolución de problemas, apoyado en pruebas y evidencias que confirmen cada decisión, con esta base quedas listo para diseñar, configurar y validar una red de área amplia que soporte cambios sin perder estabilidad.

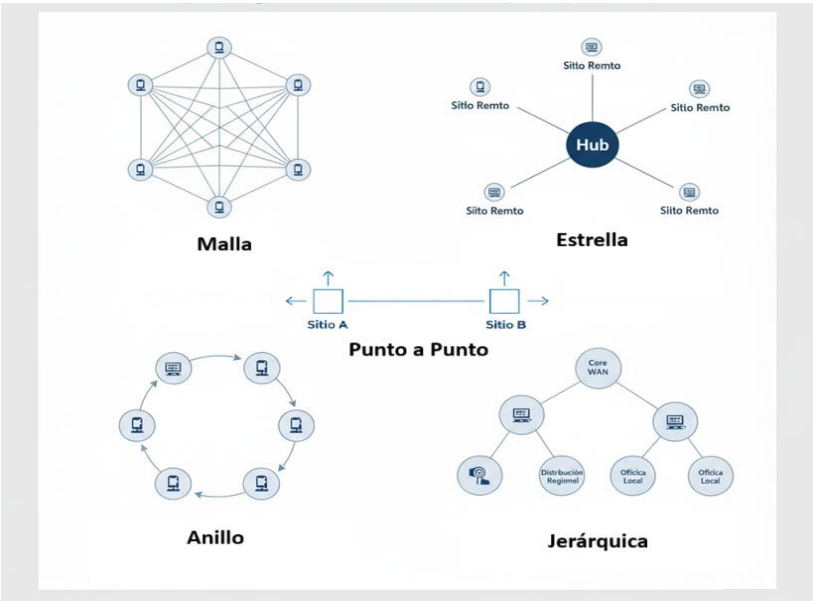
4.1. Topologías de área amplia

Las redes de área amplia conectan sedes, aulas remotas, centros de datos y servicios en la nube para sostener actividades esenciales, el alcance de este tema abarca criterios de selección basados en capacidad, latencia, cobertura geográfica, resiliencia operativa y costo total, evaluar cada opción con métricas comparables evita

decisiones reactivas y permite justificar la arquitectura frente a riesgos y presupuestos realistas.

Figura 17

Topologías de redes de áreas amplia (wan)



Nota. Topologías de redes de áreas amplia y su representación den 5 tipos. Fuente. Elaboración propia.

Las tecnologías y medios disponibles incluyen circuitos dedicados sobre fibra, servicios conmutados de operador, enlaces de acceso de banda ancha y soluciones inalámbricas de macro o microonda, la última milla condiciona latencia y disponibilidad, mientras los acuerdos de nivel de servicio definen umbrales de continuidad y

tiempos de respuesta. En escenarios híbridos, capas de aplicación modernas pueden mejorar rendimiento sobre Internet pública mediante técnicas de recuperación y control de congestión eficientes (Iyengar & Thomson, 2021).

El diseño lógico organiza segmentos y define rutas preferentes entre sedes, además de enlaces de respaldo con políticas de activación claras, un diagrama legible debe mostrar flujos de datos, control y gestión, junto con dependencias entre servicios críticos. Esta representación guía la operación diaria y orienta pruebas de conmutación y capacidad antes de cambios de producción.

La resiliencia se logra introduciendo diversidad física y lógica, por ejemplo, proveedores distintos y trayectos separados hasta el edificio, la conmutación por falla debe ser rápida y verificable, con pruebas periódicas que confirmen que el tráfico retoma el servicio sin intervención manual, el costo adicional se justifica cuando la continuidad evita pérdidas académicas o económicas superiores al gasto recurrente de la redundancia.

La seguridad y la operación requieren segmentación entre dominios, monitoreo continuo y registros confiables que respalden auditorías técnicas, la automatización y los modelos de gestión facilitan aplicar políticas consistentes y medir cumplimiento frente a objetivos de desempeño, un enfoque de confianza mínima reduce privilegios

innecesarios y acota efectos de incidentes a segmentos controlados (Rose et al., 2020; Wu et al., 2021).

En síntesis, seleccionar una arquitectura de área amplia implica balancear capacidad, alcance, resiliencia y costo bajo supuestos explícitos y medibles. El siguiente paso decide entre enrutamiento estático para escenarios estables y enrutamiento dinámico cuando la escala y los cambios exigen convergencia y adaptación confiables, manteniendo la trazabilidad de cada elección con evidencia operativa (Iyengar & Thomson, 2021; Rose et al., 2020).

4.2. Enrutamiento estático y enrutamiento dinámico

El enrutamiento determina el siguiente salto hacia un destino y define cómo fluye el tráfico entre dominios, por lo que su elección impacta convergencia, mantenimiento y riesgo operativo, un plan adecuado evita bucles, reduce tiempos de recuperación y simplifica la operación diaria a medida que cambian prefijos y caminos. La decisión entre rutas fijas o aprendizaje distribuido debe considerar escala, variabilidad de la red y necesidades de visibilidad y control, un marco organizacional claro ayuda a alinear estos criterios con objetivos de continuidad y seguridad definidos para el servicio (Rose et al., 2020).

Las rutas estáticas ofrecen simplicidad, control estricto y ausencia de tráfico de control, lo que resulta útil en enlaces pequeños y estables,

su principal fragilidad aparece cuando cambian prefijos o fallan enlaces, ya que la adaptación depende de intervención humana o de mecanismos externos, el error de tipeo, la falta de documentación o un orden incorrecto de rutas por defecto pueden causar pérdidas de alcance difíciles de diagnosticar. Por ello conviene reservarlas para escenarios muy previsibles, documentarlas con precisión y acompañarlas de verificación periódica reproducible.

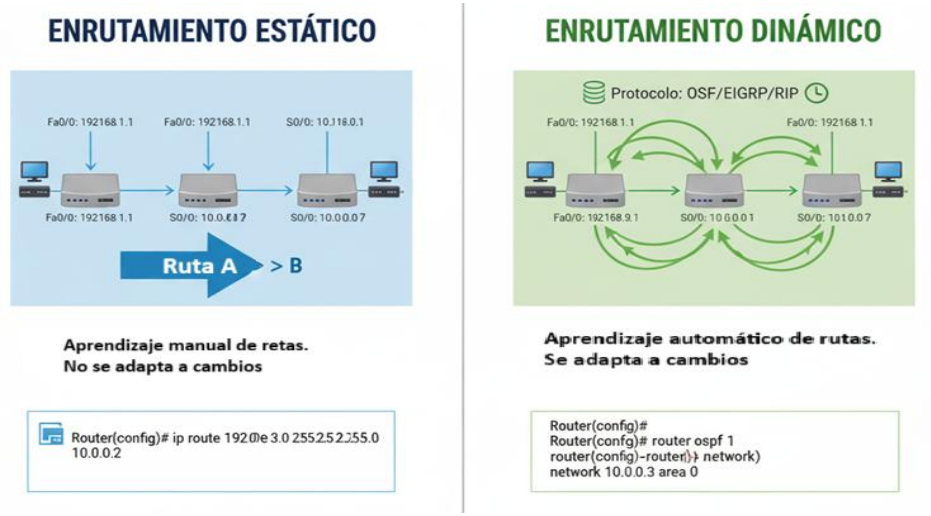
Los protocolos dinámicos descubren caminos, intercambian métricas y ajustan tablas ante fallas o variaciones de costo sin intervención manual, esta adaptación continua acelera la convergencia y reduce tareas operativas en topologías con múltiples enlaces y prefijos variables. La tabla de enrutamiento resultante refleja estados compartidos por los nodos, alimentados por mensajes periódicos o desencadenados por eventos, la estandarización y la automatización facilitan operar estos protocolos en redes heterogéneas con modelos declarativos consistentes (Wu et al., 2021; Chroboczek, 2020).

Para decidir conviene estimar cuántos prefijos existen, cuán a menudo cambian y cuánta capacidad operativa está disponible, en un pequeño caso de dos sedes con un solo enlace estable, una ruta estática por sede puede ser suficiente y fácil de auditar, si añadimos un segundo enlace con costos distintos y crecimiento de subredes, la gestión manual se vuelve frágil y propensa a errores, en ese punto un

protocolo dinámico reduce tiempo de ajuste, expone métricas útiles y mejora la resiliencia frente a cortes parciales (Rose et al., 2020).

Figura 18

Ruteo estático vs dinámico



Nota. Imagen representativa del enrutamiento estático y el enrutamiento dinámico. Fuente. Elaboración propia.

La verificación exige confirmar que las tablas reflejen la intención y que los caminos efectivos coincidan con el diseño, resulta útil comparar salidas de comandos de enrutamiento con pruebas de conectividad y, cuando aplique, revisar intercambios de mensajes en un analizador como Wireshark. Los contadores de prefijos, las rutas preferidas y los eventos de cambio documentados forman parte de la evidencia reproducible, esta trazabilidad respalda la confiabilidad del

diseño y permite corregir desalineaciones entre política esperada y comportamiento observado (Wu et al., 2021).

En síntesis, las rutas estáticas brindan control y previsibilidad con bajo costo operativo inicial, mientras los protocolos dinámicos ofrecen adaptación y convergencia rápida en entornos cambiantes, la elección depende de escala, variación de topología y recursos de operación disponibles, y prepara el terreno para analizar OSPF y RIPv2 con mayor detalle. En el siguiente tema estudiaremos cómo sus métricas, estados y temporizadores gobiernan selección de rutas y tiempos de recuperación bajo condiciones reales (Chroboczek, 2020; Rose et al., 2020).

4.3. OSPF y RIPv2 principios

Los protocolos interiores siguen dos enfoques clásicos: estado de enlace y vector distancia. En estado de enlace cada router difunde su visión del grafo y todos calculan rutas con algoritmos de costo mínimo, logrando convergencia más rápida y buena escalabilidad, en vector distancia cada router anuncia alcances resumidos hacia destinos y ajusta por saltos, con mayor sencillez y convergencia más lenta en topologías complejas, esta diferencia condiciona recuperación ante fallas, carga de control y límites de crecimiento del dominio operativo (Psenak et al., 2023; Kabir et al., 2021).

En OSPF, la red se organiza en áreas con una columna vertebral, y los routers intercambian anuncios de estado de enlace que alimentan una base de datos común para calcular árboles de rutas mínimas por costo, diseños habituales emplean un área interna y otra de borde para aislar cambios, mientras extensiones recientes permiten atributos específicos por aplicación sin modificar los principios fundamentales del protocolo, estas extensiones refinan la señalización de costos y capacidades de enlace, mejorando control y escalabilidad en dominios amplios (Psenak et al., 2023; Talaulikar & Psenak, 2023).

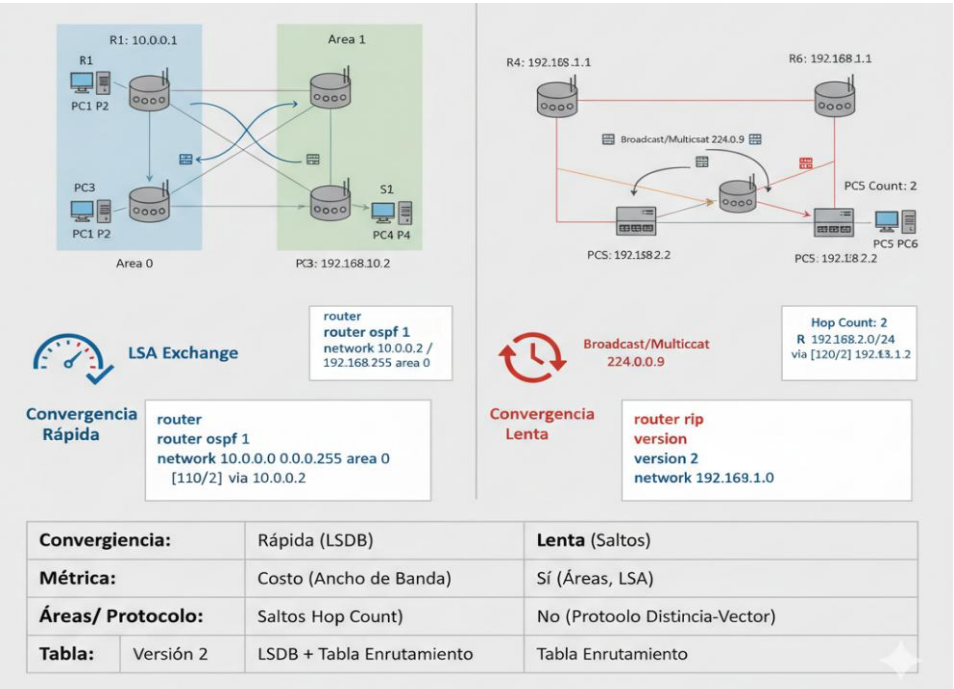
En RIPv2, la métrica principal es el número de saltos, y el comportamiento se rige por temporizadores de actualización, invalidación y retención, el soporte para prefijos sin clase habilita VLSM, aunque persisten límites de tamaño y estabilidad por el techo de saltos y la convergencia, la gestión y automatización contemporáneas disponen de modelos YANG que describen configuración y estado de RIPv2, lo que facilita control y auditoría con herramientas modernas (Liu et al., 2020).

OSPF suele ser preferible cuando existen múltiples enlaces, crecimiento de prefijos y objetivos estrictos de recuperación, porque converge rápido y ofrece granularidad de políticas, donde hay pocas rutas, cambios escasos y personal limitado, RIPv2 continúa siendo suficiente y transparente para operación diaria. Por ejemplo, dos sedes con un único vínculo estable y rutas previsibles funcionan bien

con RIPv2, mientras un campus con enlaces redundantes y políticas diferenciadas obtiene mejores resultados con OSPF (Kabir et al., 2021).

Figura 19

Ruteo protocolos OSPF vs RIP



Nota. Imagen del Ruteo protocolos OSPF vs RIP. Fuente. Elaboración propia.

La validación compara vecindades establecidas, bases de datos o tablas de rutas resultantes con el diseño y las políticas definidas,

conviene revisar costos preferidos o saltos efectivos y observar anuncios o respuestas durante cambios controlados, acompañando con capturas cuando corresponda. Estas evidencias reproducibles respaldan ajustes de métricas, límites de área o temporizadores según el comportamiento observado y facilitan auditoría técnica sostenida en el tiempo (Talaulikar & Psenak, 2023; Psenak et al., 2023).

En síntesis, OSPF aporta convergencia rápida, jerarquía y control de costos, mientras RIPv2 maximiza simplicidad a costa de escalabilidad limitada, la elección práctica depende de escala, variación prevista y recursos de operación disponibles y prepara el terreno para profundizar en métricas, áreas y temporizadores específicos. A continuación, conectaremos estas decisiones con la traducción de direcciones para publicar servicios internos manteniendo políticas coherentes y evidencia operativa (Psenak et al., 2023; Liu et al., 2020)

4.4. Traducción de direcciones NAT y PAT

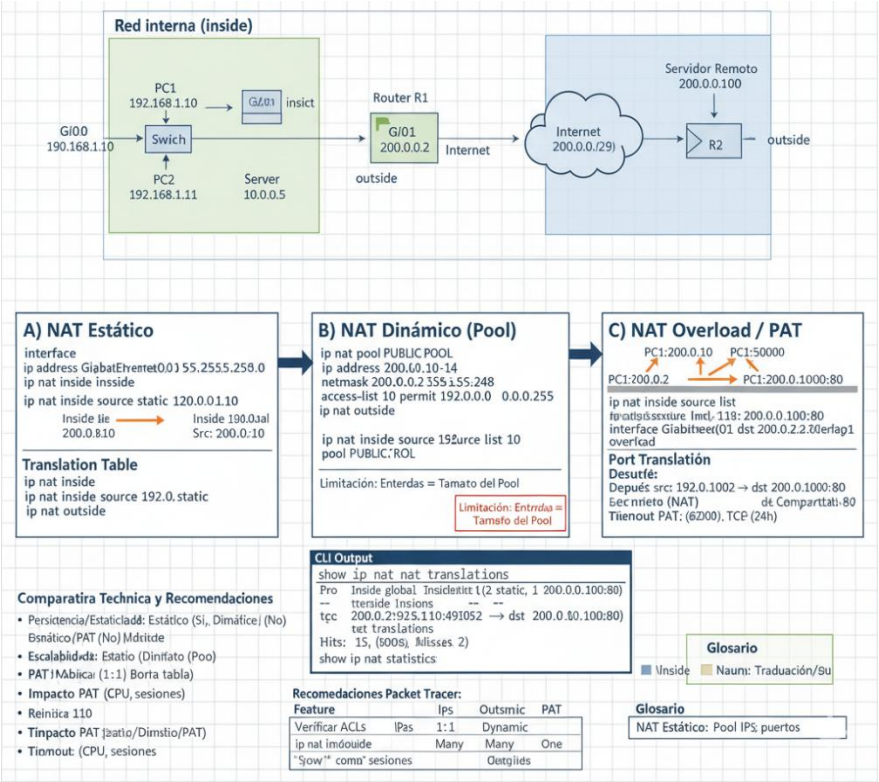
La traducción de direcciones resuelve la presión por escasez de direcciones públicas y permite controlar qué servicios internos se exponen realmente a Internet, un esquema de traducción bien diseñado también aporta privacidad operativa porque oculta espacios internos y facilita el registro centralizado de salidas y publicaciones, en redes educativas y empresariales, estas decisiones sostienen continuidad y trazabilidad mientras se avanza gradualmente hacia

despliegues con soporte nativo de la versión más reciente del protocolo de Internet y mecanismos de interconexión entre pilas. Este enfoque convive con técnicas de interoperabilidad modernas que preservan conectividad cuando existen dominios con versiones distintas del protocolo de red (Colitti & Linkova, 2020).

Existen dos familias prácticas de traducción para entornos de campus y pymes, la traducción uno a uno asigna una dirección pública dedicada a un sistema interno específico, lo que simplifica publicaciones y auditoría a cambio de mayor consumo de direcciones, la sobrecarga por puertos agrega multiplexación sobre una sola dirección pública y permite escalar salidas de muchos clientes, aunque introduce ambigüedad de origen que debe resolverse con registros precisos y puede afectar aplicaciones con expectativas estrictas de extremo a extremo. La elección combina requisitos de exposición, cantidad de clientes simultáneos y sensibilidad de las aplicaciones a particularidades de traducción (Petit et al., 2020).

Figura 20

Traducciones de direcciones NAT



Nota. Traducciones de direcciones NAT en red interna. Fuente. Elaboración propia.

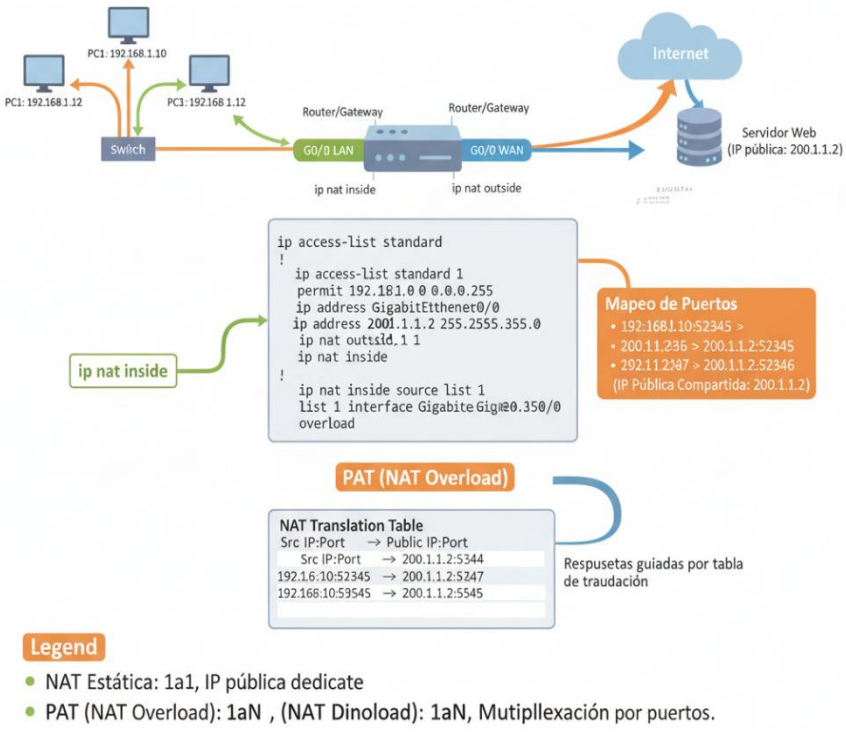
El diseño comienza con la selección explícita de rangos internos y el mapeo entre segmentos, declarando reglas de salida, publicaciones específicas y excepciones bien justificadas, cuando un servicio interno debe ser accesible desde Internet, conviene reservar

traducciones estáticas, documentar puertos, nombres y certificados, y anclar dependencias de resolución y balanceo, en dominios con coexistencia de versiones de protocolo, la interconexión basada en traducción entre pilas debe declararse para que las rutas de publicación y de retorno mantengan consistencia y registrabilidad o inscripción/registro de actividades (Colitti & Linkova, 2020).

En un emulador de práctica, las reglas se configuran en el módulo de traducción del equipo de borde y se asocian a interfaces de salida o zonas definidas, resulta útil adoptar una convención de nombres que codifique propósito, alcance y fecha, y capturar pantallas del mapeo, contadores y estados, mantener un expediente con versión del firmware y exportes de configuración facilita auditorías, comparaciones y restauraciones controladas sin ambigüedades operativas.

Figura 21

Traducciones de direcciones PAT



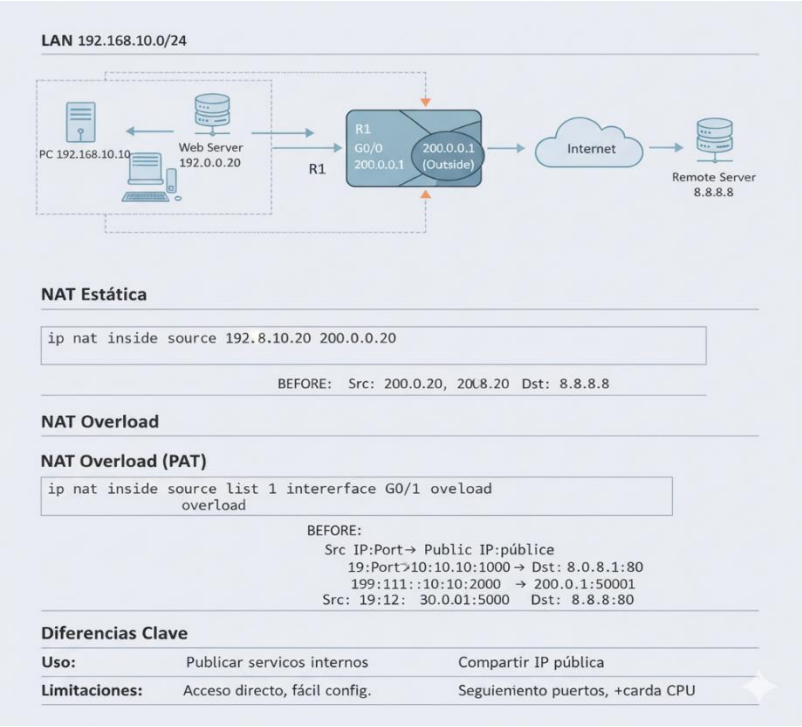
Nota. Imagen de las traducciones de direcciones PAT Fuente. Elaboración propia.

La verificación combina comprobaciones de conectividad hacia Internet y validación de publicaciones desde redes externas controladas, observando que el servicio responda con la dirección prevista, para diagnosticar efectos colaterales puede añadirse una

prueba de descubrimiento y atravesamiento con un servidor adecuado, verificando que la traducción de puertos no rompa flujos sensibles y que las listas de control acompañen la intención de salida y, de entrada. Protocolos contemporáneos muestran tolerancia mayor a traductores cuando usan mensajes de sondeo, descubrimiento y cifrado de establecimiento sobre datagramas con control de pérdidas eficiente (Petit et al., 2020; Iyengar & Thomson, 2021).

Figura 22

Traducciones de direcciones NAT y PAT



Nota. Traducciones de direcciones NAT y PAT, y las diferencias clave. Fuente. Elaboración propia.

En síntesis, la traducción estática simplifica publicaciones específicas y la sobrecarga por puertos escala salidas con menor consumo de direcciones, aunque ambas requieren registro cuidadoso y pruebas periódicas, decidir implica ponderar capacidad disponible, sensibilidad de aplicaciones, auditoría requerida y costos de operación. En el siguiente tema abordarás el establecimiento de una red privada virtual para transportar tráfico cifrado sobre los mismos enlaces, manteniendo coherencia entre rutas, traducción y políticas de seguridad (Iyengar & Thomson, 2021).

4.5. Red privada virtual básica concepto IPsec

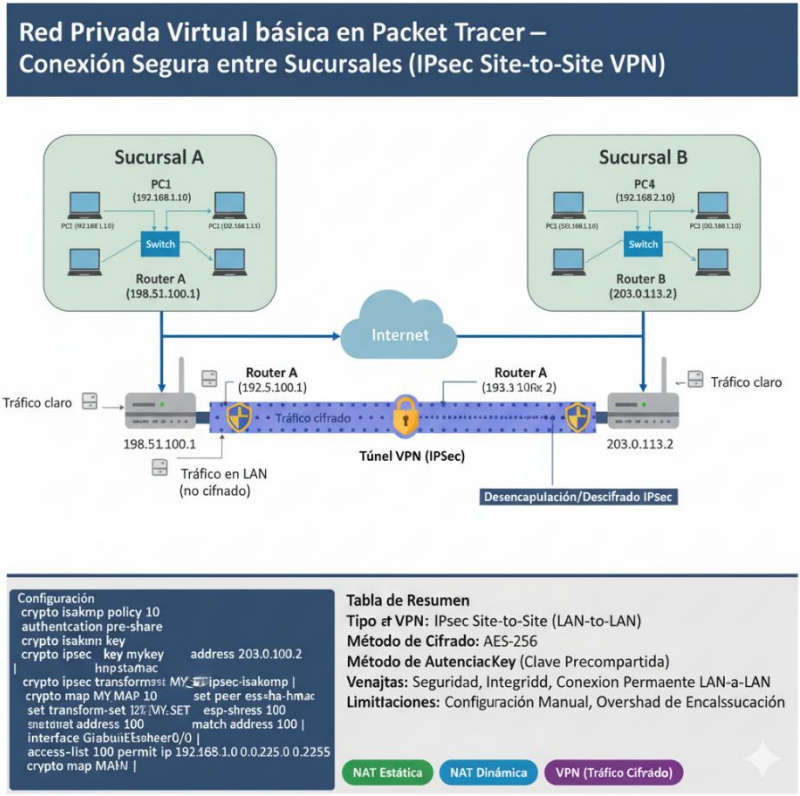
Una red privada virtual con IPsec resuelve la necesidad de transportar información entre sedes y usuarios remotos a través de redes no confiables manteniendo confidencialidad, integridad y autenticación, el establecimiento de asociaciones de seguridad con IKE versión dos crea llaves compartidas y parámetros criptográficos antes de proteger el tráfico real con el protocolo de encapsulamiento seguro, este enfoque también favorece la trazabilidad, porque cada intercambio y cada política quedan registradas y pueden auditarse con capturas y bitácoras. En entornos educativos y empresariales, la meta es habilitar acceso seguro y predecible sin perder visibilidad operativa

ni romper el direccionamiento existente (National Institute of Standards and Technology, 2020).

Los modos de protección se centran en transporte y túnel, y se aplican tanto a conexiones sitio a sitio como a acceso remoto, con preferencia actual por algoritmos autenticados que integran cifrado e integridad, recomendaciones contemporáneas definen conjuntos consistentes basados en AES en modo Galois con autenticación integrada y funciones de resumen robustas para negociación y autenticación, lo que simplifica la interoperabilidad y mejora la resistencia frente a errores de configuración. La pila moderna contempla además descubrimiento de encapsulación adecuada cuando existen dispositivos de traducción, e incluso la posibilidad de encapsular el protocolo seguro dentro de una conexión confiable cuando los intermedios bloquean datagramas. (Corcoran & Jenkins, 2022; Pauly & Smyslov, 2022).

Figura 23

Representación de una VPN



Nota. Representación de una VPN con ejemplo en sucursal A y B. Fuente. Elaboración propia.

El diseño parte de una política clara que define qué tráfico debe protegerse, qué pares establecen túneles y qué subredes se anuncian a través del canal cifrado, es necesario decidir identidades, método

de autenticación, tiempos de vida, grupos de intercambio y si se requiere separación de dominios mediante múltiples asociaciones de seguridad, resulta conveniente planificar el impacto de agregados de encabezados en el tamaño efectivo de unidad máxima de transmisión y prever ajustes de tamaño de segmento para evitar fragmentaciones inesperadas. En escenarios con requisitos elevados, pueden adoptarse perfiles que fijan suites y parámetros seguros de manera uniforme para toda la infraestructura (National Institute of Standards and Technology, 2020; Corcoran & Jenkins, 2022).

La implementación práctica exige configurar los extremos con políticas y pares coincidentes y después verificar el establecimiento del intercambio inicial y la creación de asociaciones hijas, cuando la red intermedia bloquea datagramas o altera encabezados el encapsulamiento del intercambio y del tráfico protegido sobre una conexión confiable permite atravesar dichos filtros manteniendo la semántica del protocolo seguro, en laboratorios y pruebas de aceptación conviene capturar el saludo inicial y observar los parámetros negociados, además de registrar versiones y convenciones de nombres para reproducibilidad (Pauly & Smyslov, 2022; National Institute of Standards and Technology, 2020).

La verificación combina pruebas de conectividad extremo a extremo con observación del flujo cifrado y evaluación de desempeño bajo pérdidas o latencia adicional, es útil confirmar que el tráfico previsto

efectivamente viaja dentro de cargas cifradas y que los contadores de paquetes y bytes crecen de manera coherente con la carga generada, en dispositivos restringidos o escenarios con recursos limitados, implementaciones mínimas del encapsulamiento seguro mantienen interoperabilidad mientras reducen complejidad, aunque deben evaluarse cuidadosamente frente a los objetivos de resiliencia y auditoría (Migault & Guggemos, 2023).

En síntesis, una red privada virtual con IPsec aporta un canal cifrado consistente que preserva políticas de segmentación y registro sin exponer estructuras internas, la elección de modos, algoritmos y encapsulamientos debe alinear seguridad, desempeño y operabilidad, considerando además extensiones recientes que facilitan escalabilidad y preparación criptográfica futura, en el siguiente tema conectarás este túnel seguro con un plan de pruebas de verificación y resolución de problemas, integrando métricas de tiempo de convergencia, disponibilidad percibida y evidencias replicables. (Smyslov, 2022; National Institute of Standards and Technology, 2020)

4.6. Verificación y resolución de problemas

Un método de diagnóstico eficaz avanza por capas desde el medio físico hasta la aplicación, con pruebas simples y registros claros que permitan aislar causas, comienza verificando señales básicas y termina correlacionando resultados con políticas, rutas y servicios

específicos, el objetivo es reducir hipótesis, confirmar restauración del servicio y dejar una cadena de evidencia que pueda auditarse y repetirse sin ambigüedad.

En la capa física y de enlace revisa energía, conectores, tipos de cable y parámetros de negociación, validando velocidades, dúplex y Auto Negociación, observa contadores de errores, especialmente tramas con verificación fallida, desalineaciones y pérdidas que indican problemas de medio o desacuerdo de parámetros, cuando exista segmentación por etiquetas, confirma consistencia de identificadores y pertenencia correcta para evitar tráfico descartado silenciosamente (IEEE, 2022a; IEEE, 2022b).

En la capa de red comprueba prefijos, puertas de enlace y tablas de enrutamiento, asegurando que existan rutas específicas o por defecto coherentes con el diseño, confirma caminos efectivos comparando salidas de comandos con pruebas dirigidas entre segmentos y sedes verificando que la selección de siguiente salto coincida con la intención, registra cambios de estado, anuncios y convergencia para relacionar eventos con ventanas de intervención planificadas y con la disponibilidad percibida por los usuarios.

En políticas y traducción revisa listas de control y reglas de NAT o PAT, buscando bloqueos inesperados por orden, prioridades o mapeos expirados, si existen dispositivos intermedios, considera rebindings

y cambios de puerto que afectan flujos sensibles, y valida que las excepciones de publicación estén activas, los protocolos modernos contemplan pérdidas y variaciones de ruta, lo que debe reflejarse en métricas y diagnósticos de extremo a extremo (Iyengar & Thomson, 2021).

Como evidencia utiliza mensajes de eco hacia puertas de enlace y destinos autorizados, seguimiento de ruta para observar saltos y capturas selectivas en puntos clave, anota filtros, interfaces, marcas temporales y conserva pantallas de tablas, contadores relevantes que demuestren el antes y el después. Consolidar datos en un expediente con hash del archivo de captura y versión de herramienta facilita la revisión por pares y la repetibilidad técnica.

Para el informe final integra resultados de eco, seguimiento y captura con registros de configuración y bitácoras del equipo, explica por qué se descartaron hipótesis, qué cambio restauró el servicio y cómo se verificó que el comportamiento permanezca estable bajo carga. Incluye recomendaciones operativas que prevengan la recurrencia y definan umbrales de alerta alineados con objetivos de servicio y políticas vigentes.

Este procedimiento fortalece la capacidad de aislar fallas y validar la recuperación con evidencia suficiente y ordenada, en el siguiente capítulo profundizaremos en interconexión y segmentación, donde la

consistencia de etiquetas, transporte y enrutamiento inter VLAN depende de diagnósticos por capas igualmente rigurosos y de métricas que reflejen el comportamiento real de la red (IEEE, 2022b; Iyengar & Thomson, 2021).

Cierre del capitulo

Este capítulo te llevó desde los conceptos de área amplia hasta decisiones operativas que sostienen continuidad entre sedes y servicios en la nube, aprendiste a traducir requisitos de capacidad, alcance, resiliencia y costo en arquitecturas verificables que resisten cambios y fallas previsibles, descubriste cómo la última milla, los acuerdos de nivel de servicio y la diversidad de rutas condicionan latencia, disponibilidad y presupuestos reales. El resultado es un criterio sólido para justificar cada enlace y cada proveedor ante una rúbrica técnica exigente.

Construiste diagramas físicos y lógicos que muestran flujos, dependencias y límites de fallo, permitiendo pruebas de conmutación planificadas, diferenciaste cuándo mantener un diseño simple y cuándo introducir redundancia selectiva con trayectorias separadas y proveedores distintos. Comprendiste que la resiliencia no es gratuita y que el retorno de inversión depende de la criticidad del servicio. La documentación clara de rutas primarias, rutas de respaldo y umbrales de capacidad acelera diagnósticos y reduce tiempos fuera de servicio.

Analizaste la elección entre enrutamiento estático y enrutamiento dinámico considerando escala, frecuencia de cambios y recursos operativos disponibles. Reconociste que protocolos como OSPF ofrecen convergencia rápida y granularidad de políticas en entornos con múltiples enlaces, mientras RIPv2 aún puede resultar suficiente en dominios pequeños y estables. Aprendiste a validar tablas y caminos efectivos con comandos, pruebas dirigidas y capturas selectivas cuando corresponde, la trazabilidad de estos resultados permite corregir desalineaciones entre diseño esperado y comportamiento observado.

Integraste traducción de direcciones para publicar servicios y controlar salidas, equilibrando traducciones estáticas y sobrecarga por puertos con registros confiables, complementaste esa exposición controlada con túneles IPsec que preservan confidencialidad, integridad y autenticación sin romper la conectividad extremo a extremo. Consideraste tamaños efectivos de unidad máxima de transmisión, parámetros criptográficos recomendados y efectos sobre rendimiento percibido, cerraste el ciclo con un método de verificación y resolución por capas que deja evidencia reproducible y lista para auditorías.

Con esta base conceptual y práctica estás preparado para avanzar hacia la interconexión y la segmentación dentro del campus, en el siguiente capítulo trabajarás con redes virtuales, transporte

etiquetado, enrutamiento inter VLAN y conceptos de árbol de expansión. Llevarás contigo el mismo enfoque de diseño, verificación y documentación para que cada enlace troncal y cada segmento mantengan coherencia con las políticas y con los objetivos de servicio establecidos, así consolidarás una red que escala con orden, protege sus fronteras y entrega una experiencia consistente a usuarios y aplicaciones.

CAPITULO 5: INTERCONEXIÓN Y SEGMENTACIÓN

«En teoría de redes, el valor de un sistema crece aproximadamente con el cuadrado del número de usuarios.»

Robert Metcalfe

Introducción

La interconexión y la segmentación convierten una red de campus en un conjunto ordenado de dominios bien definidos, en este capítulo aprenderás a separar el tráfico por funciones, áreas y riesgos, de modo que cada segmento tenga políticas y alcances claros, verás por qué la segmentación reduce tormentas de difusión, facilita el control de acceso y mejora la experiencia de usuarios y aplicaciones. También comprenderás cómo los enlaces troncales transportan múltiples redes virtuales sin perder coherencia ni trazabilidad operativa.

Comenzaremos con los fundamentos de la conmutación y el aprendizaje de direcciones, porque allí nace el comportamiento de la red local, construiremos redes virtuales de área local y las haremos visibles en los enlaces adecuados mediante etiquetado consistente, revisaremos la diferencia entre puertos de acceso y troncales, y cómo su configuración impacta el alcance de cada política. Acompañaremos cada decisión con criterios prácticos para nombrar, documentar y verificar de forma reproducible.

Luego activaremos comunicación controlada entre segmentos mediante enrutamiento inter VLAN, ya sea con interfaces virtuales o

subinterfaces enrutadas, analizaremos qué políticas deben atravesar entre redes y cómo validar que se cumplan con pruebas simples y capturas selectivas. Revisaremos señales típicas de errores de configuración y su efecto en conectividad, desempeño y seguridad percibida, el objetivo es que puedas explicar cada flujo, justificar cada excepción y demostrarlo con evidencia.

Finalmente abordaremos los conceptos esenciales de árbol de expansión para evitar bucles y sostener convergencia estable, entenderás por qué la redundancia física necesita control lógico y qué ajustes básicos mejoran tiempos de recuperación, cerraremos con una práctica guiada en emulador para consolidar la configuración y recoger pantallas clave como parte del expediente técnico, con esta base estarás listo para diseñar, implementar y documentar una segmentación clara que escale sin perder orden ni visibilidad.

5.1. Conmutación y tabla MAC

La conmutación sostiene el desempeño de redes locales modernas al reenviar tramas solo por los puertos necesarios reduciendo tráfico innecesario y latencia, la tabla de direcciones o tabla MAC es el centro de esta eficiencia porque asocia cada dirección física con el puerto de llegada permitiendo entregas selectivas, cuando la tabla refleja fielmente la topología activa el conmutador evita inundaciones y aprovecha mejor el ancho de banda disponible, esta conducta se integra con los estándares de enlace y puenteo que

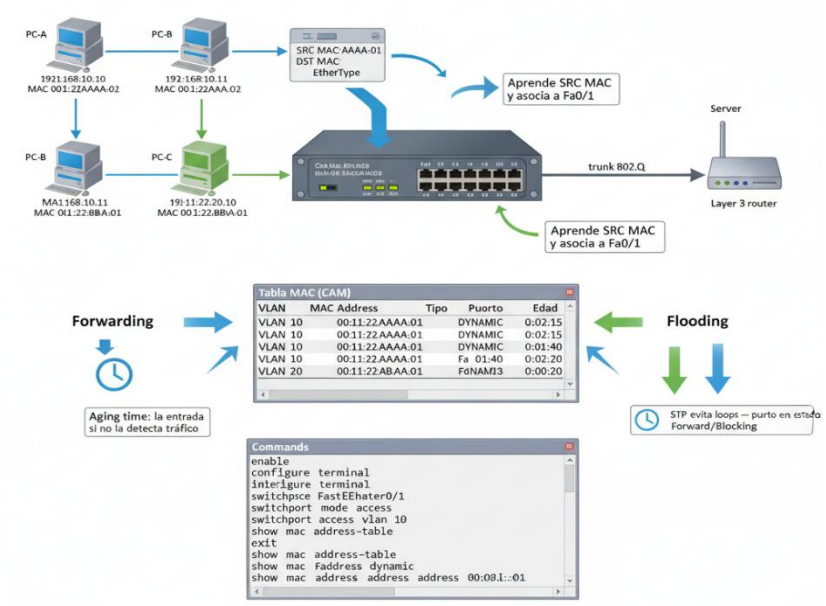
gobiernan el reenvío determinista en dominios locales (IEEE, 2022a; IEEE, 2022b).

El aprendizaje ocurre al leer la dirección origen de cada trama y registrar el puerto asociado, mientras que el envejecimiento retira entradas inactivas tras un intervalo definido, en tiempo de envejecimiento demasiado corto provoca reaprendizajes frecuentes e inundaciones transitorias que afectan aplicaciones sensibles, un tiempo demasiado largo mantiene asociaciones obsoletas y puede desviar tráfico por puertos inadecuados hasta que se actualicen. Ajustar estos parámetros al patrón real de movilidad y uso mejora estabilidad y reduce picos innecesarios de difusión.

El comportamiento varía según el tipo de tráfico: unicast conocido se reenvía únicamente por el puerto asociado en la tabla, unicast desconocido se inunda hasta aprender el destino, y la difusión se replica a todos los puertos del mismo dominio lógico. La multidifusión puede gestionarse de forma más eficiente cuando el equipo aplica snooping y limita el envío a interesados reduciendo carga en receptores ajenos, la presencia de dominios lógicos separados garantiza que estas decisiones respeten límites definidos por la arquitectura, la consistencia de la tabla MAC sostiene estos tratamientos diferenciados al minimizar incertidumbre en el camino de cada trama (IEEE, 2022b).

Figura 24

Comunicación de datos y tabla MAC



Nota. Representación gráfica de la comunicación de datos y tabla MAC. Fuente. Elaboración propia.

La conmutación reduce dominios de colisión al aislarlos por puerto y, en modo dúplex completo, elimina colisiones a nivel físico, superando limitaciones de topologías heredadas esta segmentación del acceso al medio libera recursos y mejora el rendimiento agregado sin cambios en las capas superiores, en entornos densos, múltiples enlaces ascendentes y colas adecuadas sostienen tráfico simultáneo con menor contención. El resultado práctico es una red más

predecible donde el cuello de botella se analiza por enlaces y no por choques generalizados (IEEE, 2022).

Para verificar el funcionamiento conviene observar la tabla MAC en un equipo de práctica y correlacionar entradas con dispositivos conectados, un analizador permite confirmar inundación inicial para destinos desconocidos y la posterior selectividad una vez aprendido el camino, capturas breves anotadas con hora, puerto e identificación del equipo, muestran transiciones desde difusión hacia unicast conocido, estos pasos producen evidencia reproducible que explica variaciones de tráfico y justifica ajustes de temporizadores o políticas.

Es así que, diagnosticar problemas de aprendizaje implica revisar entradas inestables, picos de inundación y asociaciones inconsistentes con el cableado o la topología activa, cuando los dominios lógicos crecen, resulta necesario segmentar mediante redes virtuales para contener la difusión y alinear políticas por función o riesgo. La transición natural es pasar del aprendizaje básico de direcciones al diseño de VLAN y etiquetado consistente, manteniendo la tabla MAC como base de reenvío eficiente y verificable (IEEE, 2022b).

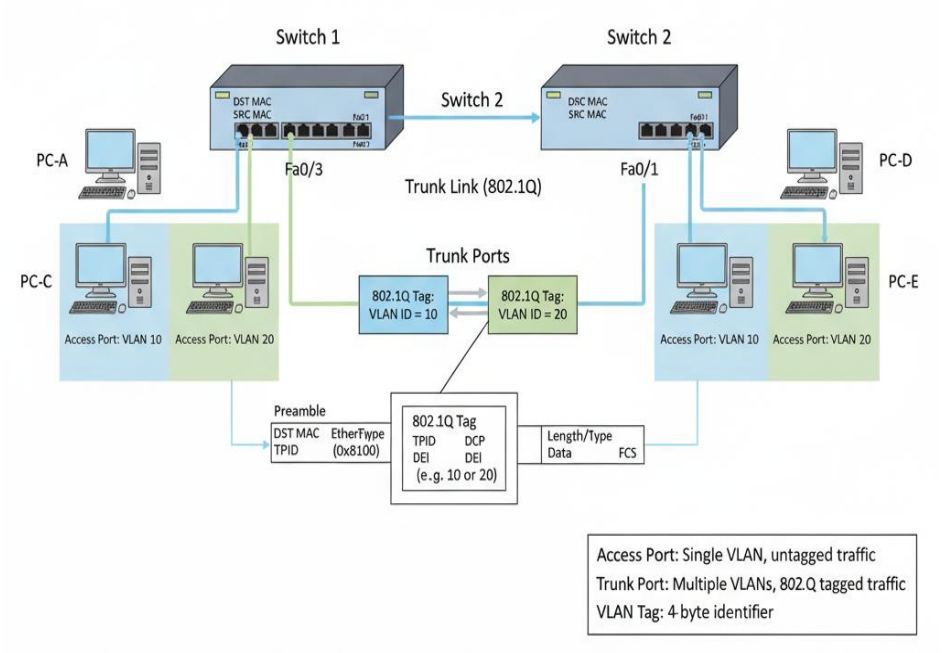
5.2. Redes virtuales de área local y etiquetado 802.1Q

Las redes virtuales se adoptan para aislar dominios de difusión, ordenar el tráfico por funciones y reducir la superficie de ataque sin reconfigurar el cableado físico en un campus o una pequeña empresa, separar administración, aulas, invitados y servicios disminuye tormentas innecesarias y facilita aplicar políticas diferenciadas. La segmentación también simplifica el diagnóstico porque limita el alcance de fallas y mejora la experiencia de usuarios y aplicaciones al mantener flujos previsibles y medibles (IEEE, 2022a).

Una red virtual es un dominio de difusión lógico definido en el plano de conmutación que no depende de la vecindad física inmediata, puede formarse por puerto, por dirección o por un criterio lógico asociado a identidad, siempre que el control mantenga consistencia entre equipos, quienes comparten una red virtual escuchan las difusiones del mismo dominio, mientras el resto permanece aislado, lo que favorece seguridad y orden operativo en topologías de campus.

Figura 25

Implementación de VLANs



Nota. Imagen de la implementación de VLANs y su conectividad. Fuente. Elaboración propia.

El etiquetado estandarizado inserta un campo con identificador de red virtual y bits de prioridad para tratamiento preferente preservando la separación a través de enlaces compartidos, ese encabezado permite que un enlace troncal transporte múltiples redes virtuales sin mezclar difusiones ni unicast conocidos, manteniendo coherencia extremo a

extremo. El identificador del dominio guía el reenvío y la prioridad influye en colas de salida cuando existen políticas de calidad de servicio documentadas y aplicadas de manera consistente (IEEE, 2022a; IEEE, 2022b).

Un plan de segmentación eficaz nombra cada red con una convención clara, asigna prefijos coherentes y define puertas de enlace por segmento para apoyar enrutamiento inter redes, conviene agrupar dispositivos con perfiles de riesgo similares y evitar mezclar huéspedes con sistemas internos críticos que requieran controles estrictos, la documentación debe reflejar función, alcance y dependencias, de modo que auditorías y pruebas puedan reproducirse con facilidad y sin ambigüedades interpretativas.

La evidencia práctica se obtiene creando redes virtuales en el emulador, asignando puertos de acceso y configurando troncales que transporten los identificadores definidos, luego se provoca tráfico entre equipos del mismo segmento y de segmentos distintos, observando con un analizador las tramas etiquetadas mediante un filtro adecuado. Las capturas deben mostrar el identificador correcto y, cuando proceda, los valores de prioridad, confirmando que la separación y el tratamiento preferente funcionan según el diseño acordado (IEEE, 2020; IEEE, 2022a).

En síntesis, la segmentación con etiquetado estandarizado organiza la red por dominios de difusión y conserva esa separación a través de troncales, mejorando seguridad, orden y desempeño, las decisiones clave son definir criterios claros de pertenencia, documentar nombres y prefijos y verificar etiquetas y prioridades en tránsito. El paso siguiente profundiza en el transporte simultáneo de múltiples redes virtuales por un mismo enlace, manteniendo continuidad operativa y trazabilidad de extremo a extremo en el campus (IEEE, 2022a; IEEE, 2022b).

5.3. Transporte etiquetado entre equipos

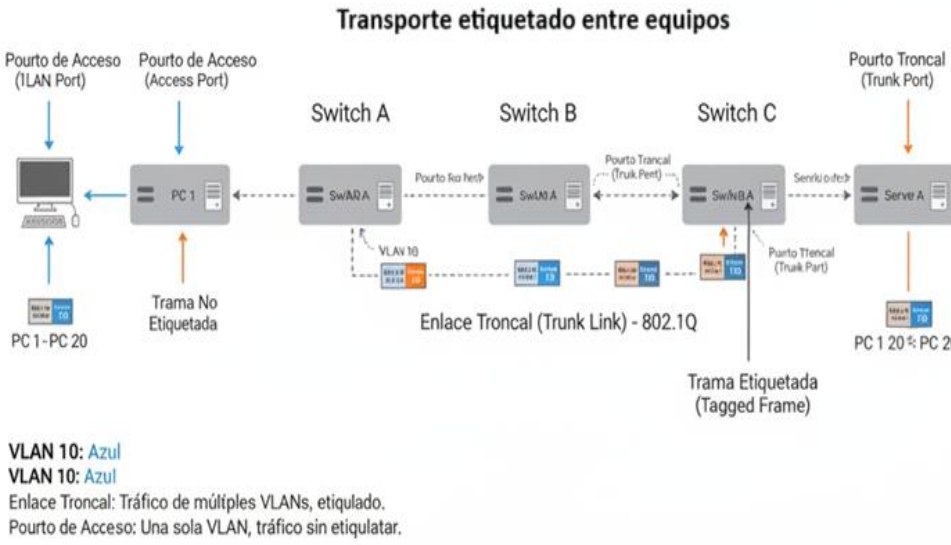
Las redes virtuales se adoptan para aislar dominios de difusión, ordenar áreas funcionales y reducir la superficie de ataque sin reconfigurar el cableado, en campus o pequeñas empresas, separar administración, aulas, invitados y servicios disminuye ruido, mejora la experiencia y facilita aplicar políticas diferenciadas, la clave es conservar la identidad de cada segmento cuando el tráfico cruza enlaces compartidos entre equipos conmutadores y enrutadores.

Una red virtual es un dominio de difusión lógico definido en el plano de conmutación que no depende de la vecindad física inmediata, la pertenencia puede derivarse por puerto, por dirección o por un criterio lógico asociado a identidad y postura siempre que el control mantenga consistencia entre equipos, este aislamiento lógico permite

que solo los miembros de un segmento reciban difusiones y servicios internos específicos.

Figura 26

Transporte de datos y etiquetado entre equipos



Nota. Imagen de transporte etiquetado entre equipos. Fuente. Elaboración propia.

El etiquetado estandarizado inserta en la trama un campo con identificador de red virtual y bits de prioridad para tratamiento preferente, ese encabezado permite transportar múltiples redes virtuales por un mismo enlace, evitando mezclar difusiones y unicast conocidos entre dominios distintos, la prioridad influye en colas de

salida cuando existen políticas de calidad de servicio coherentes con los objetivos de la organización (IEEE, 2022a; IEEE, 2022b).

El transporte etiquetado entre equipos requiere un plan que defina qué redes virtuales cruzarán cada troncal y cómo nombrarlas y direccionarlas, conviene asignar prefijos y puertas de enlace consistentes por segmento y documentar dependencias con servicios como autenticación o telefonía, una convención de nombres clara y un inventario de identificadores evitan solapamientos y simplifican auditorías futuras.

Para evidenciar el funcionamiento, configura redes virtuales y troncales en el emulador y provoca tráfico entre equipos del mismo y de distinto segmento, observa en el analizador tramas etiquetadas con un filtro específico y confirma que el identificador y la prioridad coinciden con el diseño, conserva capturas y pantallas con marcas temporales y versiones para sostener reproducibilidad y trazabilidad del experimento (IEEE, 2020; IEEE, 2022a).

En síntesis, el transporte etiquetado preserva separación y orden a través de enlaces compartidos, habilitando crecimiento con control y verificabilidad, las decisiones clave son criterios de pertenencia, nomenclatura, asignación de prefijos y validación de etiquetas y prioridades en tránsito. A continuación, avanzarás hacia el transporte simultáneo de múltiples redes virtuales por un enlace y su relación

directa con el enrutamiento inter VLAN y las políticas de acceso asociadas (IEEE, 2022a; IEEE, 2022b).

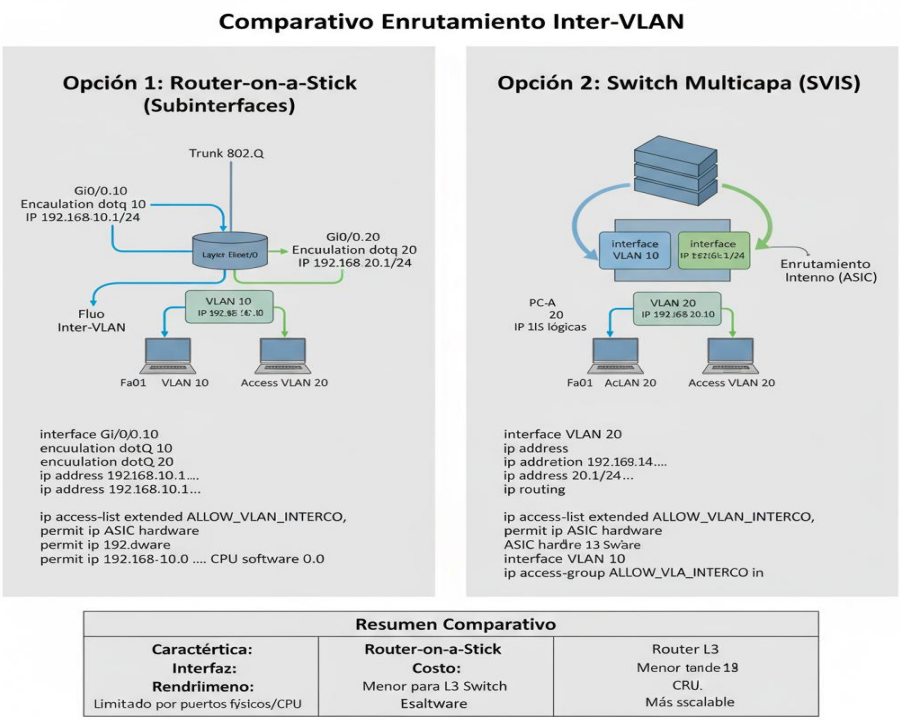
5.4. Enrutamiento inter VLAN

La comunicación entre redes virtuales requiere un punto de enrutamiento que permita el paso controlado del tráfico sin perder aislamiento, cada VLAN delimita un dominio de difusión distinto y, por diseño, no puede alcanzar otra VLAN sin una decisión explícita de capa tres, intervenir en ese límite con políticas verificables habilita flujos necesarios y bloquea los innecesarios, manteniendo orden y trazabilidad según objetivos del servicio y principios de mínima confianza (IEEE, 2022a; Rose et al., 2020).

Existen dos enfoques comunes para interconectar VLAN: interfaces virtuales conmutadas en un equipo de capa tres y subinterfaces etiquetadas en un equipo de borde, las interfaces virtuales conmutadas aprovechan hardware de reenvío para lograr latencias bajas y simplificar la operación en campus, aunque requieren conmutadores con licencia o capacidades de capa tres, las subinterfaces en un enrutador central permiten “router-on-a-stick” con un único troncal etiquetado, lo que reduce costos iniciales, pero concentra el tráfico y crea un punto único de fallo si no hay redundancia adecuada (IEEE, 2022a; IEEE, 2022b).

Figura 27

Comparativo en enrutamiento inter VLAN



Nota. Imagen comparativa en enrutamiento Inter-VLAN, Router on a Stivk y Swith Multicapa. Fuente. Elaboración propia.

El plan de direccionamiento define una puerta de enlace por VLAN, normalmente ubicada en la SVI o en la subinterfaz correspondiente, desde allí se anuncian rutas hacia redes adicionales, ya sea mediante rutas estáticas para dominios pequeños o protocolos dinámicos cuando crece la cantidad de prefijos, la coherencia entre prefijos,

máscaras y nombres facilita auditorías y reduce ambigüedades durante la resolución de problemas y las pruebas de aceptación (IEEE, 2022a).

Las políticas de acceso se aplican en el punto de enrutamiento para restringir flujos entre segmentos, preservando aislamiento y minimizando exposición lateral, reglas claras y documentadas permiten excepciones justificadas, siendo posible permitir DNS y servicios específicos desde una VLAN de aulas hacia una VLAN de servicios, manteniendo bloqueos por defecto para el resto, este control se alinea con enfoques de confianza mínima que exigen decisiones explícitas por aplicación y por segmento con registros que respalden auditorías posteriores (Rose et al., 2020).

La verificación combina eco hacia cada puerta de enlace, resolución de nombres y pruebas de acceso entre VLAN autorizadas, además de capturas en la SVI o en la subinterfaz, en el analizador conviene observar tramas etiquetadas en el troncal y paquetes enrutados en la interfaz de capa tres, confirmando que los contadores crezcan y que las políticas actúen según lo definido, conservar comandos, filtros, marcas temporales y archivos de captura con huella criptográfica produce evidencia replicable para revisión docente o de pares (IEEE, 2022a).

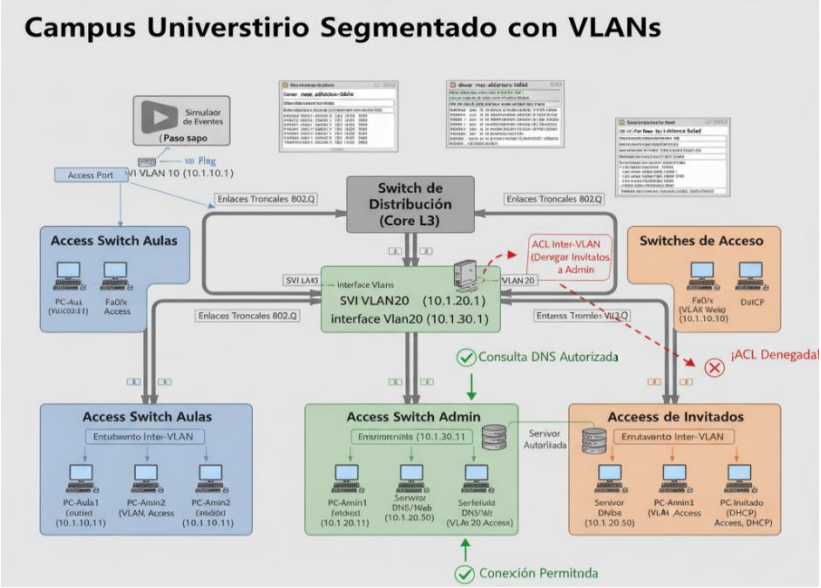
En conjunto, el enrutamiento inter VLAN habilita comunicación controlada entre segmentos con un diseño que une direccionamiento claro, políticas explícitas y verificación sistemática. La decisión entre SVI o subinterfaces dependerá de escala, presupuesto y requisitos de resiliencia, manteniendo siempre documentación y pruebas de respaldo, en el siguiente tema abordaremos la prevención de bucles y la convergencia del plano de enlace mediante árbol de expansión, pieza clave para sostener estabilidad cuando existen enlaces redundantes en la capa dos (IEEE, 2022a; IEEE, 2022b).

5.5. Práctica en emulador Packet Tracer

Imagina un campus pequeño con tres redes virtuales para aulas, administración e invitados y un equipo central que enruta entre ellas, el objetivo es lograr conectividad controlada extremo a extremo, manteniendo aislamiento de difusión y políticas diferenciadas por segmento. La práctica busca confirmar que cada estación alcance su puerta de enlace, resuelva nombres autorizados y acceda solo a los servicios permitidos entre redes, sin romper la segmentación establecida por el etiquetado, esta meta se alinea con el estándar de puenteo y etiquetas que preservan identidades lógicas sobre enlaces compartidos en el dominio conmutado (IEEE, 2022a; IEEE, 2022b).

Figura 28

Representación de campus universitario para prácticas en Packet Tracer equipos



Nota. Representación de la distribución de campus universitario para prácticas en Packet Tracer equipos. Fuente. Elaboración propia.

Configura tres redes virtuales con nombres y descriptores consistentes, asigna puertos de acceso a cada área, activa troncales con etiquetado y crea puertas de enlace por VLAN en interfaces virtuales o subinterfaces, define un esquema de direccionamiento claro que refleje pertenencia y alcance, por ejemplo, prefijos no solapados y nomenclatura de interfaz que incluya función y número de identificador. Verifica que los troncales transporten únicamente los

identificadores planeados y que las puertas de enlace respondan a eco dentro de su propia red, esta disciplina reduce ambigüedades y facilita el diagnóstico posterior cuando se habilite el enrutamiento inter VLAN (IEEE, 2022a).

Aplica listas en el punto de enrutamiento para restringir flujos entre segmentos, documentando excepciones justificadas como servicio de nombres o autenticación, valida con comprobaciones dirigidas que incluyan eco hacia puertas de enlace y resoluciones de nombres hacia servidores autorizados, asegurando que los rechazos aparezcan donde corresponde. Cuando la política sea más específica incorpora un caso de acceso permitido para confirmar coincidencias y un caso explícitamente denegado para evidenciar control efectivo, de este modo, la práctica reúne conectividad básica, control de exposición y trazabilidad operativa en un mismo escenario (Mwansa et al., 2024; IEEE, 2022a).

Recoge evidencia con capturas de pantalla del simulador mostrando tabla de direcciones, estado de troncales, interfaces de enrutamiento y resultados de pruebas, complementa con la vista de eventos o la simulación paso a paso para ilustrar entradas y salidas relevantes, identificando tiempo, equipo y puerto. Estructura el informe con apartados mínimos de diseño, configuración y validación, agregando un resumen breve de hallazgos y de decisiones de mejora, esta organización facilita revisión por pares y reproducibilidad del

ejercicio en cohortes futuras o entornos distintos (Allison, 2022; Mwansa et al., 2024).

Ante problemas típicos, piensa en discrepancias de transporte cuando un troncal no permite la red virtual esperada en errores de puerta de enlace cuando una estación responde localmente pero no atraviesa segmentos y en políticas mal ordenadas que bloquean flujos legítimos, diagnostica de forma sistemática comparando tablas, verificando etiquetas visibles en el enlace compartido y observando el camino efectivo según la decisión de enrutamiento. Ajusta pertenencias, habilita identificadores faltantes y corrige prioridades de reglas, registrando cada cambio y su efecto sobre las pruebas repetidas, la evidencia previa te ayudará a aislar causas sin depender de conjeturas o de intervenciones improvisadas (IEEE, 2022a; IEEE, 2022b).

En resumen, consolidaste segmentación, transporte etiquetado y enrutamiento entre redes virtuales con un paquete de evidencias replicable y ordenado. Este laboratorio prepara el terreno para el próximo capítulo de gestión y monitoreo, donde medirás latencia, pérdida y rendimiento y elaborarás mapas de cobertura inalámbrica que retroalimenten decisiones de diseño, mantendrás la misma disciplina de nomenclatura, capturas y versiones para que cada métrica se relacione con políticas y topologías declaradas, cerrando

el ciclo de diseño y verificación continua en el campus (IEEE, 2022a; Mwansa et al., 2024).

Cierre de capitulo

Este capítulo convirtió la interconexión y la segmentación en una práctica ordenada que sostiene desempeño, seguridad y claridad operativa. Pasaste de comprender cómo un conmutador aprende direcciones y reenvía tramas eficientes, a diseñar dominios lógicos que contienen la difusión y reducen la superficie de ataque, observaste que la identidad de cada segmento no depende del cableado físico, sino de una definición consistente en el plano de conmutación, esta comprensión te permite explicar por qué una red bien segmentada ofrece menos ruido, menos colisiones y diagnósticos más precisos.

Reconociste que el etiquetado estandarizado preserva esa identidad cuando varios segmentos viajan por el mismo enlace compartido, identificaste cómo los identificadores y las prioridades sostienen la separación y habilitan tratamientos preferentes cuando la política lo requiere, a partir de esa base construiste un plan de segmentación con nombres comprensibles, prefijos coherentes y puertas de enlace claras para cada red virtual, esta disciplina documental prepara auditorías, evita solapamientos y favorece ampliaciones sin reconfiguraciones traumáticas.

Llevaste la comunicación entre segmentos al punto de enrutamiento con interfaces virtuales o subinterfaces eligiendo la opción adecuada según escala y presupuesto, aplicaste políticas explícitas que permiten solo lo necesario entre redes, manteniendo un criterio de mínima confianza sustentado por evidencia, comprobaste conectividad con mensajes de eco, resolviste nombres autorizados y verificaste que los rechazos aparezcan exactamente donde la política los define, la combinación de pruebas, capturas y marcas temporales construyó una cadena de custodia replicable y defendible ante revisiones técnicas.

Consolidaste todo en una práctica guiada que reunió segmentación, transporte etiquetado y enrutamiento inter redes con resultados observables, diagnosticaste problemas típicos como discrepancias de transporte, puertas de enlace incorrectas o reglas mal ordenadas, sosteniéndote en tablas, filtros y contadores verificables. Aprendiste a corregir la pertenencia de puertos, habilitar identificadores faltantes y ajustar prioridades, evitando suposiciones y decisiones improvisadas, el resultado operativo es una red que escala con orden y se explica por sí misma ante cualquier inspección responsable.

Este cierre te deja una metodología completa para diseñar, implementar y demostrar segmentación con criterios medibles de éxito, en el próximo capítulo abordarás gestión y monitoreo, donde traducirás tu diseño en indicadores de latencia, fluctuación, pérdida

y rendimiento, junto con mapas de cobertura inalámbrica. Aprenderás a instrumentar consultas de administración simple y sistemas de gestión que convierten eventos aislados en decisiones de mejora continua, llevarás la misma disciplina de nomenclatura, capturas y versiones para que cada métrica dialogue con tus políticas y con la topología declarada.

CAPITULO 6: GESTIÓN Y MONITOREO

«Cuando puedes medir aquello de lo que hablas y expresarlo en números, sabes algo sobre ello.»

Lord Kelvin

Introducción

La gestión y el monitoreo convierten el diseño de red en un sistema observable que aprende de su propio comportamiento y se corrige con evidencia, en este capítulo pondremos instrumentos a trabajar para responder preguntas concretas sobre disponibilidad, capacidad y experiencia de usuarios reales, pasaremos de suposiciones generales a métricas específicas que permitan priorizar acciones correctivas con impacto medible y documentado, el objetivo es que cada decisión técnica pueda explicarse, repetirse y auditarse sin depender de intuiciones aisladas.

Comenzaremos instrumentando lecturas con administración simple de red y con sistemas de gestión que consultan indicadores clave de equipos y enlaces, verás cómo la base de información y los identificadores de objeto se traducen en gráficas, alertas y reportes comprensibles para operación y docencia, integraremos estas lecturas con mediciones activas de latencia, fluctuación, pérdida y rendimiento para caracterizar la salud del camino extremo a extremo, con este marco los números dejan de ser piezas sueltas y se vuelven una historia coherente sobre el estado real del servicio.

Profundizaremos en estudios de cobertura inalámbrica para transformar planos y mapas en decisiones de canal, potencia y ubicación de puntos de acceso, aprenderás a interpretar mapas de calor, interferencias y solapamientos, relacionándolos con quejas habituales y con los resultados de tus indicadores de red, daremos espacio a la calidad de servicio como herramienta conceptual para priorizar tráfico sensible sin caer en configuraciones complejas innecesarias, todo quedará unido por una documentación clara que acompañe cada captura, parámetro y hallazgo relevante.

Cerraremos con una práctica de gestión de incidencias y mejora continua que conecte métricas, umbrales y acciones verificables en ciclos repetibles, verás cómo un registro bien llevado acelera diagnósticos, facilita defensa de decisiones y reduce recurrencia de fallas comunes.

La meta es graduarte con una red que no solo funciona, sino que se explica sola a través de sus datos y evoluciona con cada medición responsable, con esta base, los capítulos finales consolidarán una operación madura que sostiene el aprendizaje y el trabajo cotidiano sin sorpresas desagradables.

6.1. SNMP, MIB y NMS

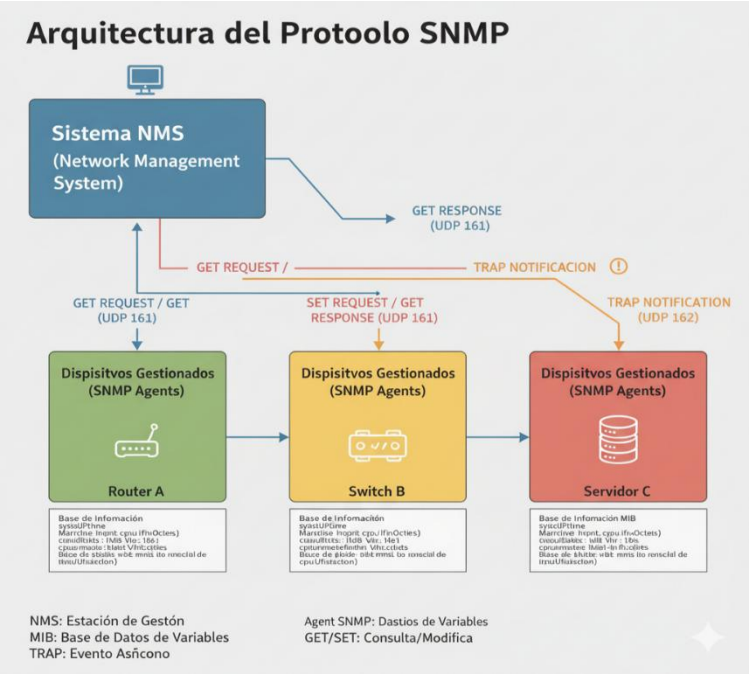
La observabilidad útil comienza cuando las consultas están bien estructuradas y se leen desde una fuente confiable de estados, en

redes académicas y empresariales, esa disciplina la aporta SNMP con un gestor que consulta a agentes y con respuestas estandarizadas que pueden correlacionarse en el tiempo. La adopción de credenciales modernas y transporte seguro permite que los mismos datos de operación alimenten alertas y reportes sin exponer secretos innecesarios, favoreciendo decisiones repetibles y auditables en el día a día (Vaughn, 2023; Sheffer et al., 2022).

La arquitectura de SNMP se apoya en tres actores que cooperan con responsabilidades claras. Los agentes residen en los equipos y exponen variables operativas, el gestor centraliza consultas y notificaciones, y el control de acceso se implementa con modelos de seguridad de la versión tres y con transporte cifrado compatible con TLS uno punto tres. El ciclo normal alterna lecturas periódicas y eventos asincrónicos, logrando una vista estable del estado sin saturar la red y alineándose con las recomendaciones vigentes de uso seguro de TLS y DTLS en servicios gestionados (Vaughn, 2023; Sheffer et al., 2022).

Figura 29

Representación de la arquitectura de SNMP



Nota. Imagen de la representación de la arquitectura de SNMP. Fuente. Elaboración propia.

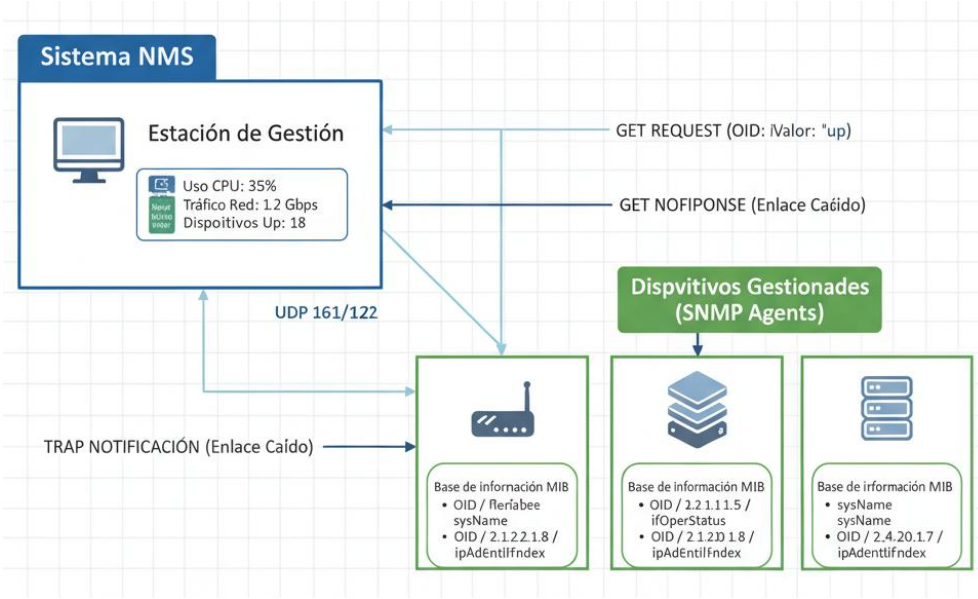
La base de información de gestión organiza datos en un árbol jerárquico donde cada objeto posee un identificador único, ese identificador permite recuperar valores específicos como contadores de interfaz o estados administrativos, posibilitando que distintos fabricantes describan variables de forma interoperable. Un ejemplo comprensible es consultar el estado operativo de una interfaz y

verificar coherencia con tráfico reciente, demostrando cómo una sola lectura bien contextualizada permite anticipar riesgos antes de que escalen a incidentes visibles en el servicio (Alhilali et al., 2023).

Un sistema de gestión de red consolida inventario, umbrales y alertas en paneles que priorizan la acción operativa, los cuadros mínimos que debe revisar un operador muestran disponibilidad de interfaces críticas, utilización de enlaces, temperatura y eventos recientes, junto con líneas de base para distinguir anomalías de variaciones normales. La literatura reciente subraya que, aunque el sondeo clásico con SNMP sigue siendo valioso, debe integrarse con telemetría y flujos para lograr granularidad y oportunidad adecuadas en redes modernas a gran escala (Yaseen, 2025).

Figura 30

Representación de la arquitectura de SNMP y trabajo en entornos reales



Nota. Imagen de la representación de la arquitectura de SNMP y trabajo en entornos reales. Fuente. Elaboración propia.

Para dejar evidencia conviene registrar cada lectura con marca temporal, dispositivo, objeto consultado y valor observado, acompañando capturas del analizador cuando un evento desencadene investigación, ese registro breve facilita reproducibilidad y acelera diagnósticos, especialmente cuando se correlaciona con cambios de configuración o con tickets de incidente. Un reporte técnico recomendado incluye contexto del equipo, objetivos de la consulta,

resultados relevantes y una interpretación que conecte los valores con hipótesis verificadas, manteniendo trazabilidad entre mediciones y decisiones adoptadas (Alhilali et al., 2023).

En síntesis, un monitoreo básico efectivo combina agentes confiables, un modelo de datos claro y paneles que convierten lecturas en acciones verificables, la seguridad del transporte y de las credenciales evita que la observabilidad abra nuevas superficies de ataque, cumpliendo con las mejores prácticas actuales para TLS y DTLS en entornos gestionados. Con esta plataforma conceptual establecida, avanzaremos hacia indicadores de desempeño que transforman lecturas puntuales en métricas que miden la salud real de la red y orientan la mejora continua (Vaughn, 2023; Sheffer et al., 2022).

6.2. KPIs de red: latencia, fluctuación, pérdida y rendimiento

Los indicadores de desempeño orientan decisiones de capacidad, priorización y diseño porque traducen percepciones en evidencia comparable, la latencia se manifiesta como tiempos de respuesta lentos, la fluctuación provoca cortes o eco en voz y video, la pérdida degrada calidad perceptible y el rendimiento efectivo condiciona transferencias y sincronizaciones. Cuando las métricas se vuelven series temporales claras, es posible relacionar umbrales con acuerdos de servicio, ajustar colas o ampliar enlaces de manera justificada, una

red observable permite invertir con precisión y evaluar impacto real de cada cambio sobre la experiencia de usuarios.

La latencia suele medirse como tiempo de ida y vuelta entre dos puntos representativos del recorrido extremo a extremo, un aumento sostenido eleva tiempos de inicio de sesión, cargas de páginas y establecimiento de sesiones interactivas, aun cuando el ancho de banda nominal parezca suficiente. La fluctuación describe la variación entre muestras sucesivas y afecta directamente aplicaciones de tiempo real, que requieren llegadas regulares para mantener decodificación fluida, estos diseños modernos de transporte y control de congestión buscan reducir colas y variabilidad para sostener interactividad consistente bajo carga diversa (Briscoe et al., 2023; Iyengar & Thomson, 2021).

En servicios de voz y video, pequeñas variaciones acumuladas producen congelamientos, artefactos o desalineación perceptible, aun con tasas agregadas adecuadas, protocolos contemporáneos optimizan establecimiento, migración de ruta y recuperación ante cambios para mantener latencia baja y estable durante sesiones prolongadas. La combinación de control de congestión sensible y señales explícitas del camino reduce el tiempo en cola, suaviza la entrega y mejora continuidad audiovisual, estas técnicas permiten sostener interactividad cuando múltiples flujos compiten por enlaces

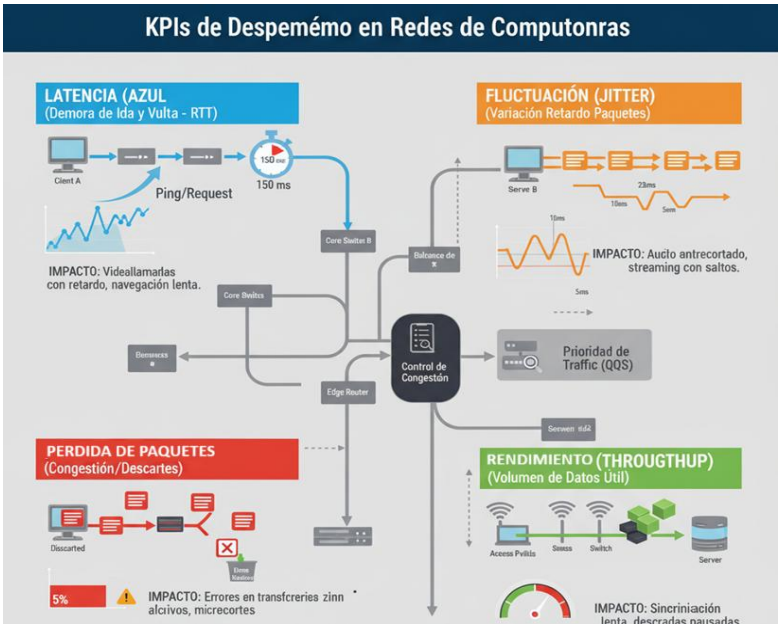
compartidos y cambian las condiciones del medio (Briscoe et al., 2023; Iyengar & Thomson, 2021).

La pérdida suele originarse en colas saturadas, errores de radio o descartes por políticas y su impacto depende de la recuperación del transporte y de la sensibilidad de la aplicación, pérdidas pequeñas pero correlacionadas afectan más a tiempo real que pérdidas aisladas, porque vacían búferes y rompen la continuidad. Controladores de congestión y algoritmos de detección de pérdida ajustan envío y reenvío para evitar colapso del camino, manteniendo equilibrio entre velocidad y estabilidad, medir pérdida junto con latencia y fluctuación permite distinguir congestión de fallas físicas o interferencias ambientales (Iyengar & Swett, 2021; Eddy, 2022).

El rendimiento efectivo difiere de la capacidad nominal porque incluye cabeceras, confirmaciones, retransmisiones y comportamiento del control de congestión, en trayectos con alta latencia, ventanas y startup del protocolo limitan la tasa útil antes de alcanzar equilibrio estable, la coexistencia de flujos sensibles y de gran volumen exige políticas que eviten que el llenado de colas deteriore todos los servicios simultáneamente. Diseños recientes de servicio de baja latencia buscan combinar alto rendimiento con colas cortas mediante señalización explícita y control más reactivo (Briscoe et al., 2023; Eddy, 2022).

Figura 31

Representación de KPI de red



Nota. Representación de KPIs de despemémo en redes de computadoras. Fuente. Elaboración propia.

Un procedimiento breve y reproducible define ventanas de medición, destinos estables y condiciones del entorno antes de recoger muestras, conviene registrar ubicación, tecnología de acceso, hora, carga de fondo y versión de las herramientas para permitir comparaciones honestas entre jornadas, para latencia y fluctuación se emplean sondas periódicas con intervalos fijos y muestras suficientes para estimar dispersión, mientras rendimiento se evalúa con

transferencias controladas que cubran tamaño y duración realistas. En inalámbrico, el estándar reciente habilita agendamiento y acceso múltiple que influyen en latencia percibida, por lo que debe anotarse canal, ancho y densidad de clientes al analizar resultados (IEEE, 2021).

Las métricas orientan acciones de mejora cuando se interpretan junto con topología, políticas y cambios operativos documentados, umbrales de latencia y fluctuación guían priorización de tráfico, límites de colas o segmentación adicional, mientras curvas de rendimiento detectan cuellos de botella reales y no supuestos. En dominios inalámbricos, configuraciones de eficiencia y coexistencia afectan capacidad, pérdida y tiempos de acceso, por lo que deben evaluarse con escenarios representativos y repetibles, este marco prepara el terreno para el estudio de cobertura, donde mapas de calor y análisis de canal traducen indicadores en decisiones de ubicación, potencia y planificación de frecuencias (IEEE, 2021; Briscoe et al., 2023)

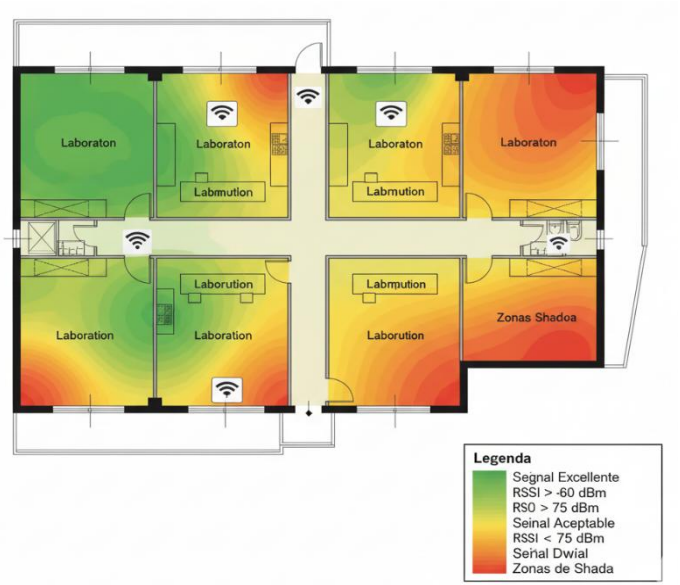
6.3. Site Survey con NetSpot

Un estudio de cobertura permite ubicar puntos de acceso donde realmente aportan calidad, reducir interferencias y equilibrar capacidad con experiencia de usuario, el alcance típico incluye aulas, pasillos y oficinas, con énfasis en zonas críticas de alta densidad y áreas con quejas recurrentes, el objetivo es transformar un plano en

decisiones de canalización y potencia verificables, de modo que el mapa de calor refleje uniformidad suficiente y márgenes razonables. La planificación debe considerar bandas disponibles, anchos de canal y coexistencia con redes vecinas para evitar solapamientos innecesarios (IEEE, 2021).

Figura 32

Diagrama de mapa de calor de red



Nota. Imagen representativa de Diagrama de mapa de calor de red de acuerdo a la distribución. Fuente. Elaboración propia.

La preparación comienza con un plano a escala y una malla de puntos de medición que cubra bordes, interiores y pasos entre recintos.

Define parámetros de escaneo coherentes con el entorno, anota banda, ancho de canal, potencia del adaptador y modelo del dispositivo de medición, para asegurar repetibilidad, conserva la misma altura del equipo, velocidades de desplazamiento similares y franjas horarias comparables, ya que ocupación y puertas abiertas alteran las lecturas, un flujo de trabajo claro en la herramienta facilita crear el proyecto, cargar el plano y calibrar distancias para que las métricas correspondan a la geometría real.

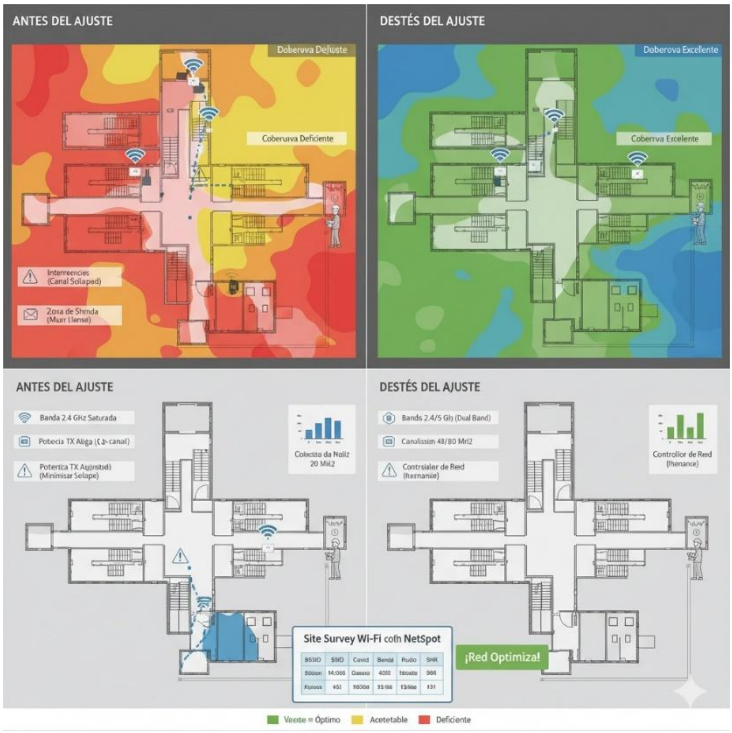
Durante el levantamiento recolecta muestras caminando con pausas breves en cada punto, evitando sesgos por movimiento continuo que promedian en exceso, repite mediciones en esquinas, pasillos angostos y detrás de mobiliario para capturar sombras y variaciones reales, evita obstáculos temporales no representativos como carritos o puertas parcialmente cerradas, y documenta cualquier condición especial observada, si el edificio tiene varios niveles, registra escaleras y vacíos que permitan acoplamientos inesperados entre plantas.

El análisis se centra en el mapa de calor y en la distribución de niveles por área, comparando valores promedio y mínimos alcanzados, define umbrales aceptables según el uso, buscando que zonas de trabajo sostengan niveles estables sin caídas abruptas, detecta zonas de sombra donde la señal cae por debajo de la meta y correlaciónalas con materiales, distancias y solapes de canal, complementa con

lectura de ocupación de canales y solapamientos para distinguir atenuación física de interferencia co-canal o adyacente (Giménez et al., 2023).

Figura 33

Mapa de calor de red real



Nota. Mapa de calor de red real ates y después del ajuste. Fuente. Elaboración propia.

Las recomendaciones priorizan ajustes de canal y potencia que reduzcan solapes y mantengan celdas contiguas con bordes definidos,

en 2.4 GHz conviene evitar canales adyacentes solapados y, en 5 y 6 GHz, elegir anchos prudentes cuando la densidad sea alta, priorizando capacidad útil y latencia estable sobre picos teóricos. Reubica puntos de acceso que queden ocultos por estructuras y documenta el antes y el después con mapas comparables, manteniendo versiones y marcas temporales, vincula cada cambio con una expectativa medible, y pudiendo elevar mínimos de señal y disminuir retransmisiones en aulas críticas (IEEE, 2021; Giménez et al., 2023).

Como cierre, el estudio entrega un plano con cobertura homogénea, canales coordinados y potencias acordes al entorno, junto con un expediente reproducible, los resultados alimentan decisiones de mantenimiento y configuran la base para políticas de priorización de tráfico, en el siguiente tema abordarás calidad de servicio, donde las colas y los marcados complementarán la cobertura lograda para sostener voz, video y aplicaciones interactivas en escenarios reales.

6.4. Calidad de servicio (QoS)

Las redes modernas alojan aplicaciones con necesidades muy distintas que compiten por recursos finitos, por lo que la calidad de servicio organiza preferencias para sostener experiencias aceptables, cuando varias cargas coinciden en un mismo enlace, las decisiones sobre marcación, colas y control del envío evitan que flujos sensibles padezcan esperas excesivas. Voz y video dependen de latencia baja y

fluctuación acotada, mientras transferencias masivas toleran demoras moderadas a cambio de mayor rendimiento sostenido. Las políticas de calidad de servicio convierten esos compromisos en acciones medibles que se reflejan en indicadores de salud y percepción del usuario.

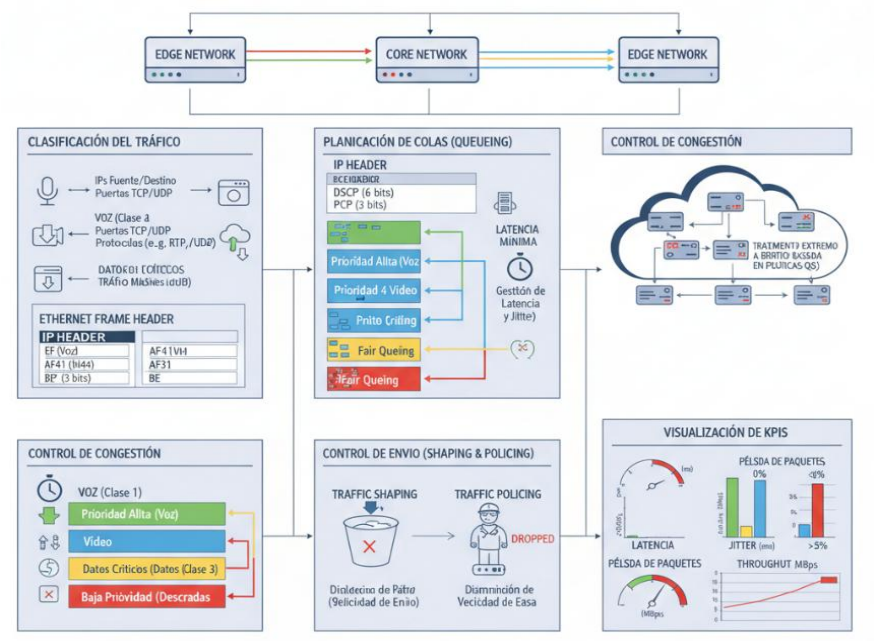
La marcación identifica tráfico que requiere tratamiento diferenciado y permite que cada salto aplique decisiones coherentes, en la cabecera de IP se utiliza el campo de servicios diferenciados, mientras en redes conmutadas el encabezado de enlace puede transportar prioridad por clase para influir en el despacho. La clasificación combina atributos como dirección, puertos y protocolos con señales de aplicación para ubicar flujos en categorías operativas, una marcación consistente facilita que los dispositivos respeten prioridades y que los análisis posteriores expliquen por qué un paquete recibió cierto trato en cada cola intermedia (IEEE, 2022).

Cuando la red y los extremos admiten notificación explícita de congestión, las marcas de congestión permiten reducir envíos sin esperar pérdidas, mejorando continuidad y latencia, la arquitectura de baja latencia y baja pérdida propone un uso refinado de esas señales y control de congestión escalable para mantener colas cortas aun con alta utilización. Esta visión desplaza el foco desde la longitud del búfer hacia el comportamiento del remitente, y habilita servicios interactivos más estables bajo carga diversa, adoptar estas pautas

eleva la probabilidad de converger en ritmos de envío que eviten colas persistentes y picos de variabilidad (Briscoe et al., 2023; De Schepper & Briscoe, 2023).

Figura 34

Representación de QoS en la de red



Nota. Estructura de la representación de QoS en la de red. Fuente. Elaboración propia.

Las colas y su planificación determinan el orden de salida y, por tanto, la latencia y la fluctuación percibidas por cada tipo de flujo, estrategias que aíslan clases sensibles y limitan el tiempo en cola

reducen congelamientos en video y mantienen conversaciones naturales en voz, incluso cuando coexisten transferencias voluminosas, el acoplamiento entre gestión activa de colas y control de congestión escalable busca que las señales sean frecuentes y suaves, evitando ráfagas y acumulaciones innecesarias, la coordinación entre marcación en el borde y planificación en el núcleo convierte el diseño en una experiencia consistente de extremo a extremo (De Schepper & Briscoe, 2023; Briscoe et al., 2023).

El control del envío complementa a las colas mediante moldeado y limitación que suavizan ráfagas o acotan tasas para proteger a otros flujos, un moldeado bien calibrado reduce variabilidad sin sacrificar demasiada capacidad, mientras la limitación previene que aplicaciones voraces degraden servicios críticos. En transportes modernos, el ajuste de ventanas y la detección de pérdida o congestión reaccionan a marcas y tiempos de ida y vuelta para estabilizar la trayectoria, la combinación adecuada evita colapsos por colas saturadas y mantiene equilibrio entre rendimiento agregado y experiencia individual (Iyengar & Thomson, 2021; Iyengar & Swett, 2021).

La validación se apoya en pruebas con cargas controladas y en registros de colas y contadores por clase para confirmar que la política surte efecto, resulta clave observar marcaciones en capturas, verificar ocupación y tiempo de espera por cola y correlacionar con

cambios en latencia y fluctuación. Cuando hay notificación de congestión, conviene revisar marcas de congestión en tránsito y la respuesta de los remitentes ante esas señales, documentar objetivos, parámetros y resultados con marcas temporales y versiones de herramientas produce evidencia replicable que guía ajustes posteriores (De Schepper & Briscoe, 2023; IEEE, 2022).

En conjunto, introducir calidad de servicio exige comenzar con pocos objetivos claros, validar resultados y escalar gradualmente hacia perfiles más finos, las pautas prácticas recomiendan priorizar voz y señalización, estabilizar video interactivo, y mantener transferencias a tasas que no dañen la experiencia del resto. Estas decisiones se integran con la gestión de incidencias, donde bitácoras, umbrales y métricas orientan correcciones oportunas y sostenibles, con esta base, el siguiente tema unirá estas políticas con procedimientos de operación que aseguren continuidad, trazabilidad y mejora continua.

6.5. Gestión de incidencias y bitácoras

Un procedimiento de gestión de incidencias evita pérdidas de información clave, acelera la restauración del servicio y convierte cada evento en aprendizaje organizacional, definir roles desde el primer minuto reduce ambigüedades: quién declara la incidencia, quién lidera el diagnóstico técnico, quién comunica a usuarios y quién captura la evidencia. La asignación temprana de responsabilidades permite coordinar prioridades, proteger la

trazabilidad y sostener decisiones auditables durante todo el ciclo, la literatura reciente enfatiza además la necesidad de una cultura sin culpa para que las causas reales afloren y los equipos aprendan de manera sostenida a partir de los hechos (National Institute of Standards and Technology, 2025; Patterson et al., 2024).

El registro mínimo debe incluir fecha y hora con zona, alcance e impacto percibido, síntomas observables, acciones ejecutadas y responsables asociados, además de referencias a bitácoras y capturas, la claridad de estos campos facilita auditoría posterior, comparación entre eventos y cálculo honesto de tiempos de detección, reconocimiento y resolución. Un plan de gestión de registros describe qué fuentes se consultan, cómo se protegen y durante cuánto tiempo se conservan, de modo que los datos sostengan análisis replicables, esta disciplina de log management es condición para investigar sin sesgos y cumplir obligaciones regulatorias y académicas (Scarfone & Souppaya, 2023).

El diagnóstico debe avanzar por capas con comprobaciones breves, correlacionando síntomas de usuario con estados del medio, del enlace y de la red. Leer contadores de interfaces, revisar tablas y políticas, y observar eventos de cambio permite aislar causas sin depender de conjeturas. Cuando un síntoma sugiere congestión o pérdida, conviene complementar con mediciones reproducibles y con correlación de trazas y registros. Integrar logs, métricas y trazas en

una misma cronología reduce el tiempo de hipótesis y mejora la calidad de las conclusiones. (Gómez, 2023; National Institute of Standards and Technology, 2025).

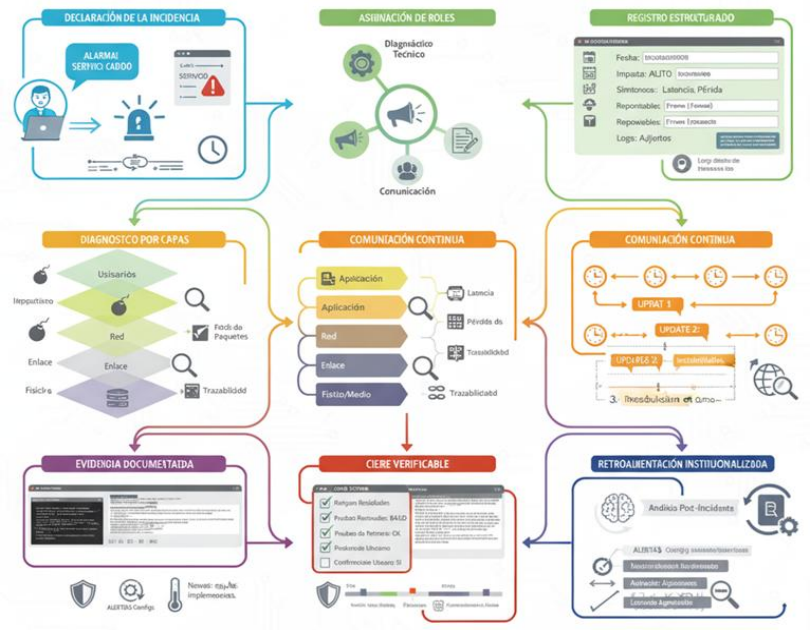
La comunicación efectiva sostiene la operación mientras el equipo técnico trabaja, por lo que deben establecerse canales, frecuencia de actualizaciones y una ventana de pruebas acordada con los interesados, informes breves y puntuales sobre impacto, mitigaciones temporales y próximos hitos mantienen la confianza y evitan esfuerzos duplicados. Documentar quién autorizó cada cambio y en qué momento protege la trazabilidad y permite reconstruir con precisión la línea temporal del evento, esta coordinación facilita postmortems objetivos donde el foco está en el sistema y no en la culpa individual. (Patterson et al., 2024).

Las condiciones de solución deben ser explícitas, verificables y acordadas antes de cerrar la incidencia, incluyendo pruebas de retorno a la normalidad y riesgos residuales, el expediente debe reunir evidencias clave como capturas con marcas temporales, extractos de logs relevantes, parámetros modificados y versiones de las herramientas utilizadas. La retrospectiva identifica causas primarias y condiciones contribuyentes, mientras la perspectiva prioriza mejoras según impacto y esfuerzo estimado, evitando listas extensas sin dueño ni fecha, este cierre orientado a resultados fortalece la memoria técnica de la organización y acelera futuras recuperaciones.

(National Institute of Standards and Technology, 2025; Scarfone & Souppaya, 2023).

Figura 35

Flujo de gestión de incidencias



Nota. Flujo de gestión de incidencias estructurado. Fuente. Elaboración propia.

El aprendizaje se institucionaliza cuando las mejoras quedan incorporadas en guías, automatizaciones y umbrales de alerta que se revisan periódicamente, priorizar acciones por severidad histórica, frecuencia y costo de oportunidad asegura que el esfuerzo se invierta donde aporta más resiliencia. La correlación continua entre

indicadores, bitácoras y topología declarada permite evaluar si las acciones reducen efectivamente tiempos de detección y restauración, con cada iteración, la organización afina su capacidad de anticiparse y responde con mayor precisión a variaciones del entorno. (Patterson et al., 2024; Gómez, 2023).

En síntesis, un enfoque sistemático de gestión de incidencias estandariza registros, ordena el diagnóstico por capas, asegura comunicación transparente y convierte la evidencia en mejoras sostenibles. Este marco entrega tiempos de restauración más cortos, menor recurrencia de fallas y decisiones defendibles ante auditorías o evaluaciones académicas, en el siguiente tema abordaremos mejora continua, donde estos aprendizajes se transforman en ciclos planificados de revisión, métricas y acciones que consolidan una operación estable y evolutiva (National Institute of Standards and Technology, 2025).

6.6. Mejora continua

Los ciclos iterativos convierten la operación diaria en aprendizaje acumulado, siempre que las metas sean observables y estén vinculadas con niveles de servicio acordados, definir objetivos medibles para disponibilidad, tiempos de respuesta y estabilidad reduce discusiones subjetivas y orienta decisiones de inversión. Un enfoque de mejora continua establece cadencias fijas para revisar métricas, registrar hallazgos y ajustar políticas sin depender de

emergencias, este marco integra retrospectivas con acciones concretas que cierran brechas detectadas entre objetivos y resultados reales (Patterson et al, 2024; National Institute of Standards and Technology, 2025).

Las métricas clave nacen de fuentes complementarias: telemetría de dispositivos y aplicaciones, series de mediciones activas extremo a extremo y resultados de estudios de cobertura Wi-Fi, integrar estos datos con registros de gestión e incidencias permite correlacionar picos de latencia, pérdida o fluctuación con cambios de configuración y eventos de capacidad. Una plataforma de observabilidad coherente consolida métricas, trazas y logs, ofreciendo contexto suficiente para interpretar variaciones y evitar conclusiones apresuradas, con esta base, los tableros pasan de mostrar valores aislados a explicar historias causales verificables (Gómez, 2023).

El plan de acción debe caber en una página con responsables, plazos, riesgos y criterios de éxito claramente definidos, cada acción se prioriza por impacto esperado en la experiencia del usuario, costo y complejidad operativa, evitando listas extensas sin dueño ni fecha, se recomienda vincular cada tarea a una métrica específica y a un umbral objetivo, de modo que el equipo sepa qué cambiar y cómo medirá el efecto, este formato acelera coordinación, reduce ambigüedades y facilita seguimiento ejecutivo y técnico (Patterson et al., 2024).

La validación exige mediciones comparables antes y después, con ventanas temporales y condiciones de entorno documentadas, repetir pruebas bajo horarios, cargas y ubicaciones equivalentes permite atribuir mejoras al cambio aplicado y no a variaciones circunstanciales, si el resultado no alcanza el umbral, el plan se ajusta o se descarta, registrando supuestos, aprendizajes y próximos pasos. Esta disciplina sostiene decisiones defendibles y evita ciclos interminables de ajustes marginales sin evidencia (National Institute of Standards and Technology, 2025).

La documentación convierte la mejora en patrimonio institucional cuando conserva evidencias, versiones de herramientas y procedimientos actualizados, registrar recetas de medición, capturas, consultas y parámetros garantiza que cohortes futuras repliquen los resultados y comparen tendencias. Actualizar guías y automatizaciones reduce la carga manual y disminuye la variabilidad entre equipos, reforzando la calidad de servicio cotidiana, reutilizar plantillas consolida un lenguaje común que acelera la incorporación de personas nuevas al proceso (Gómez, 2023).

Sostener hábitos de revisión evita que la red dependa de heroicidades puntuales y habilita una evolución estable, medible y predecible, este capítulo se cierra con una invitación a preparar el proyecto integrador, donde aplicarás metas, métricas y planes de acción en un caso completo, llevarás un enfoque que une observabilidad, gestión de

incidencias y mejora continua para demostrar, con evidencia, decisiones que fortalecen desempeño y confiabilidad. De este modo, cada iteración elevará la madurez del servicio y la claridad operativa del campus o la empresa (Patterson et al., 2024; National Institute of Standards and Technology, 2025).

Cierre del capitulo

Este capítulo convirtió la gestión y el monitoreo en una práctica cotidiana que hace visible el estado real de la red, aprendiste a instrumentar consultas estructuradas con administración simple, a interpretar bases de información y a apoyarte en sistemas de gestión que consolidan inventario, umbrales y alertas. Entendiste que sin una fuente confiable de estados las decisiones se diluyen, mientras con paneles claros y series temporales coherentes cada hallazgo se vuelve accionable, la observabilidad dejó de ser un lujo para transformarse en una condición básica del diseño operativo.

Tradujiste la experiencia del usuario en indicadores comprensibles y medibles, conectando latencia, fluctuación, pérdida y rendimiento con efectos percibidos en voz, video y aplicaciones interactivas. Definiste ventanas de medición y condiciones de entorno para comparar campañas con honestidad metodológica, evitando conclusiones apresuradas por variables no controladas, descubriste que el rendimiento efectivo depende de cabeceras, retransmisiones y control de congestión, por lo que dimensionar solo por tasas

nominales conduce a decisiones frágiles, con estas métricas pudiste priorizar acciones y justificar inversiones con evidencia reproducible.

Llevaste el análisis al dominio inalámbrico mediante levantamientos de cobertura que pusieron en el mapa la realidad de pasillos, aulas y laboratorios. Construiste y leíste mapas de calor, detectaste sombras y propusiste ajustes de canal y potencia con metas verificables, vinculaste esa topología radio con políticas de calidad de servicio para que la marcación, las colas y el control del envío sostengan continuidad sin sacrificar estabilidad, al documentar el antes y el después consolidaste una cadena de custodia que permite evaluar el impacto de cada cambio con precisión suficiente.

Estandarizaste la gestión de incidencias y las bitácoras para que cada evento aporte aprendizaje en lugar de solo urgencia, definiste roles y registros mínimos, ordenaste el diagnóstico por capas y estableciste una comunicación clara con ventanas de prueba acordadas, cerraste cada caso con evidencias, condiciones de solución y una retrospectiva que prioriza mejoras por impacto y esfuerzo razonable. Finalmente, integraste estos hallazgos en ciclos de mejora continua que fijan metas observables y actualizan guías y automatizaciones con cadencia sostenida.

Con esta base estás listo para el proyecto integrador, donde demostrarás de extremo a extremo que el diseño se sostiene con

métricas, que las políticas reflejan necesidades reales y que la operación aprende con cada iteración, diseñarás, medirás y ajustarás con la misma disciplina de nomenclatura, capturas y versiones que practicaste aquí, defendiendo decisiones con evidencia y no con suposiciones. El objetivo final es entregar una red que funcione, se explique con sus datos y mejore en ciclos previsibles, preparada para crecer sin perder orden ni confiabilidad.

CAPITULO 7: GESTIÓN Y MONITOREO

«Los programas deben escribirse para que los lean las personas, y solo accidentalmente para que los ejecuten las máquinas.»

Harold Abelson

Introducción

El proyecto integrador convierte todo lo aprendido en una propuesta completa, defendible y respaldada por evidencias, la idea central es transformar necesidades reales de un campus o una pequeña empresa en una red que funcione, se explique con sus datos y pueda crecer sin perder orden, trabajarás con alcance y supuestos claros, criterios de éxito medibles y una línea de tiempo realista, la meta no es solo que la red opere, sino que cada decisión pueda justificarse frente a una rúbrica experta y a una auditoría técnica básica.

Comenzarás levantando requerimientos y delimitando el problema con precisión suficiente para evitar ambigüedades posteriores. A partir de allí elaborarás el diseño lógico y físico con diagramas consistentes, plan de direccionamiento, segmentación por redes virtuales y enlaces troncales coherentes, ese diseño incluirá políticas de enrutamiento adecuadas al tamaño del dominio y a su ritmo de cambio previsto, cada elemento quedará descrito con nombres, prefijos y dependencias que faciliten pruebas, operación y mantenimiento.

El siguiente paso será implementar la solución en simulación y emuladores, configurando funciones clave y validando conectividad extremo a extremo, integrarás controles de seguridad con autenticación, listas de acceso y transporte cifrado donde corresponda, cuidando que la postura de protección no rompa el servicio, además, instrumentarás monitoreo básico y mediciones de desempeño para observar latencia, fluctuación, pérdida y rendimiento, relacionándolos con decisiones de topología y de calidad de servicio. Toda la evidencia se registrará con capturas, versiones de herramientas y marcas temporales que permitan reproducción fiel.

Finalmente cerrarás el ciclo con documentación clara, un acta de aceptación firmada electrónicamente y una defensa breve de decisiones y resultados, presentarás hallazgos, limitaciones y mejoras propuestas, mostrando cómo el diseño responde a los objetivos y cómo las métricas confirman su comportamiento esperado. Con esta metodología, el proyecto integrador deja de ser un ejercicio aislado y se convierte en un prototipo operativo y auditable, estás listo para demostrar que puedes diseñar, implementar, medir y sostener una red con criterios profesionales y con evidencia suficiente.

7.1. Requerimientos y alcance

El proyecto integrador tiene como propósito convertir necesidades reales en decisiones de diseño justificables y medibles, con actores

definidos y metas educativas u operativas claras, participan responsables académicos o de negocio, personal técnico y usuarios representativos que aportan criterios de éxito y restricciones del entorno, el nivel de servicio esperado debe quedar expresado en términos comprensibles, como disponibilidad percibida en horarios críticos, tiempos de respuesta para aplicaciones institucionales y márgenes de crecimiento razonables, este encuadre evita ambigüedades y prepara la defensa técnica ante una rúbrica experta y una revisión por pares.

Los requerimientos funcionales describen qué servicios de red deben existir y para quién, considerando tipos de usuarios, zonas y flujos característicos, se identifican necesidades de conectividad cableada e inalámbrica, autenticación institucional, publicación controlada de servicios y acceso remoto seguro. También se documentan dependencias con aplicaciones críticas, como plataformas de aprendizaje, sistemas administrativos y repositorios de investigación, incluyendo ventanas de mantenimiento y requisitos de resolución de nombres, estas relaciones condicionan el diseño lógico, la elección de tecnologías y la priorización de pruebas.

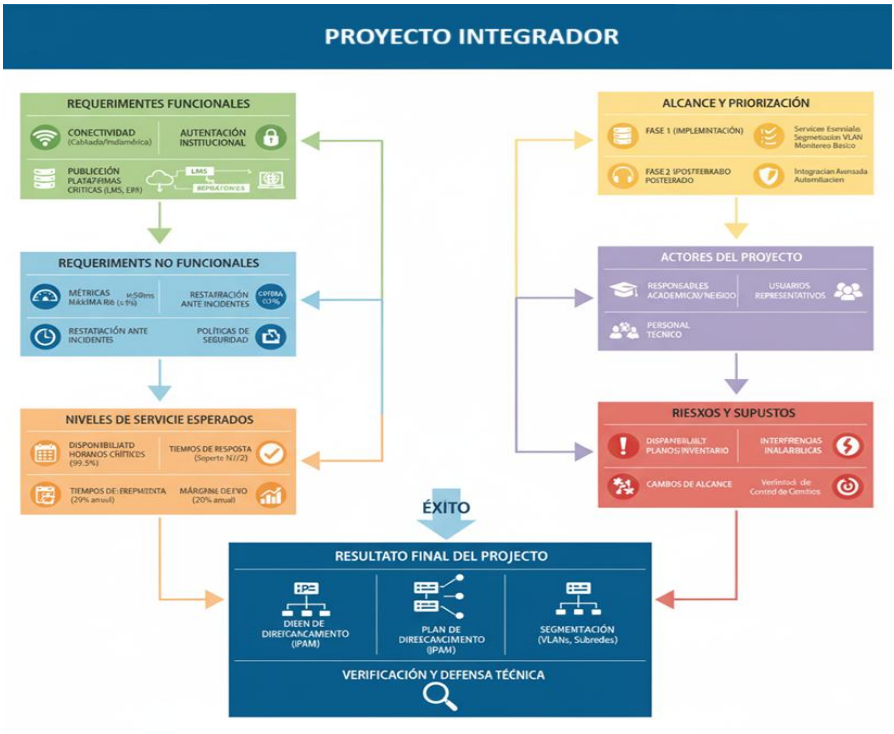
Los requerimientos no funcionales establecen disponibilidad objetiva, capacidad por área, márgenes de seguridad y pautas de crecimiento ordenado, se fijan criterios de aceptación medibles, como latencia máxima entre sedes, pérdida tolerable en troncales,

densidad de usuarios por celda inalámbrica y tiempos de restauración ante incidentes. La seguridad se expresa como políticas verificables de segmentación, control de acceso y cifrado en tránsito, con evidencias esperadas en capturas y registros, al vincular metas con métricas, el proyecto gana trazabilidad y foco operativo.

Los supuestos y riesgos se declaran para reducir incertidumbre y orientar mitigaciones con responsables claros, resulta razonable suponer disponibilidad de planos actualizados, inventario mínimo de equipos y acceso a emuladores o simuladores para pruebas previas, entre los riesgos típicos aparecen retrasos logísticos, incompatibilidades de versiones, interferencias radioeléctricas y cambios de alcance no controlados, cada riesgo se acompaña de impacto probable, acciones preventivas y planes de contingencia que preserven hitos y niveles de servicio.

Figura 36

Representación general del Proyecto Integrador de Saberes (PIS)



Nota. Representación general de los requerimientos par ale éxito del Proyecto Integrador de Saberes Fuente. Elaboración propia.

La priorización y el alcance definen qué se entrega en esta etapa y qué se posterga a fases futuras, con criterios explícitos de valor y esfuerzo. Se prioriza habilitar servicios esenciales, asegurar segmentación y conectividad extremo a extremo y dejar monitoreo básico operativo, quedan fuera optimizaciones finas o integraciones

no críticas, que se planifican con metas y fechas tentativas, este recorte deliberado facilita una entrega defendible y reduce el riesgo de desalineación entre expectativas y capacidades disponibles.

En síntesis, el mapa de requisitos integra propósito, servicios, niveles de servicio, riesgos y prioridades en un documento que guía decisiones y pruebas, a partir de aquí se desarrolla el diseño lógico y físico con diagramas consistentes, plan de direccionamiento y segmentación, preparando la verificación y la defensa del proyecto, la estructura recomendada para especificar y trazar requisitos se alinea con prácticas estandarizadas de ingeniería que facilitan evaluación y mantenimiento a lo largo del ciclo de vida (ISO/IEC/IEEE, 2018).

7.2. Diseño lógico y físico

La visión lógica organiza la red por capas, delimita dominios de difusión y ubica áreas funcionales con propósitos claros, el tráfico principal fluye desde acceso hacia distribución y núcleo, separando control, datos y gestión para mantener orden y trazabilidad, las fronteras lógicas establecen qué segmentos pueden comunicarse y bajo qué condiciones, preservando independencia entre aulas, administración y servicios, esta estructura reduce ruido, facilita diagnósticos y prepara la aplicación coherente de políticas verificables de extremo a extremo.

El plan de direccionamiento define prefijos, subredes y puertas de enlace por segmento con una convención de nombres estable, cada VLAN recibe un bloque propio sin solapamientos, documentando máscaras, etiquetas y rutas previstas para crecimiento razonable, en dominios duales conviene anticipar transición hacia preferencia por la versión más reciente del protocolo de Internet, manteniendo interconexión controlada con servicios heredados, una planificación explícita mejora seguridad operativa y simplifica auditorías de alcance entre sedes y servicios (RFC 9099; RFC 9386).

La segmentación agrupa dispositivos con riesgos y funciones similares en redes virtuales, mientras los enlaces troncales transportan múltiples etiquetas entre equipos, las zonas de seguridad definen políticas permitidas entre segmentos, como acceso restringido desde aulas a servicios centrales y publicación controlada hacia Internet. El etiquetado preserva identidades lógicas en tránsito y habilitas prioridades cuando la calidad de servicio lo requiera, este diseño sostiene separación y coherencia sin depender del cableado físico subyacente (IEEE, 2022a).

El diseño físico ubica equipos considerando rutas de cableado, energía, ventilación y accesibilidad segura para mantenimiento, los troncales se dimensionan con redundancia selectiva y caminos diferenciados, minimizando puntos únicos de fallo razonables para el contexto. Los puntos de acceso siguen criterios de cobertura y

capacidad acordes con densidad y materiales del entorno, la documentación incluye inventario, planos y rutas con etiquetado consistente para acelerar cambios y reparaciones futuras (IEEE, 2022b).

La verificabilidad exige datos que permitan validar el diseño en simulación antes de cualquier despliegue real, se definen pruebas de conectividad, tablas de reenvío, etiquetas visibles y políticas efectivas entre segmentos autorizados. La evidencia requerida incluye diagramas, archivos de configuración, capturas con filtros y marcas temporales reproducibles, estos artefactos sostienen la defensa técnica del proyecto y facilitan revisión por pares y seguimiento de mejoras.

A manera de resumen, las decisiones clave integran capas lógicas, direccionamiento claro, segmentación consistente y un trazado físico mantenible con evidencia replicable, el siguiente paso traslada este diseño a simulación y emuladores para confirmar rutas, políticas y resiliencia antes del piloto, con esta base, el proyecto avanza desde la intención arquitectónica hacia resultados medibles y defendibles en pruebas controladas (RFC 9099; IEEE, 2022a).

7.3. Implementación en simulación y emuladores

Comienza creando un proyecto limpio, cargando los dispositivos previstos y estableciendo parámetros globales de reloj, zona horaria

y banners informativos, aplica una convención de nombres que codifique rol, ubicación y número lógico, y prepara una hoja de inventario con puertos y funciones. Documenta en el campo de notas del proyecto los objetivos, versiones de la herramienta y supuestos operativos, guarda el archivo con nomenclatura versionada y registra un cambio de logos (changelog) breve por cada ajuste relevante (Allison, 2022).

Construye el plano lógico configurando direccionamiento por segmento, redes virtuales y transporte etiquetado en los troncales, define puertas de enlace por VLAN mediante interfaces virtuales o subinterfaces y aplica rutas estáticas o dinámicas según el diseño, verifica que no existan solapamientos de prefijos y que los identificadores de VLAN coincidan en ambos extremos, asegura consistencia entre nombres, prefijos y etiquetas para que las capturas posteriores resulten auto explicativas (IEEE, 2022).

Activa servicios y políticas de infraestructura alineados con requisitos: DHCP por segmento, resolución de nombres, traducción en el borde y listas de control entre VLAN. Mantén el principio de mínimo privilegio permitiendo solo flujos justificados y registrando excepciones con su motivo, cuando corresponda, integra marcación de prioridad y colas básicas para proteger tráfico sensible, documenta parámetros clave, rangos asignados, reservas y dependencias de cada servicio (Mwansa et al., 2024).

Verifica conectividad con eco hacia puertas de enlace, pruebas autorizadas entre segmentos y resoluciones de nombres hacia servidores definidos, confirma caminos efectivos con seguimiento de ruta y usa el modo de simulación para observar ARP, DHCP y etiquetas 802.1Q, corroborando que el reenvío ocurre según el diseño, repite pruebas con ventanas temporales claras y anota condiciones del entorno para comparaciones honestas, registra cualquier desviación y su corrección inmediata (Allison, 2022; IEEE, 2022).

Reúne evidencia guardando el proyecto con versión, exportando capturas de pantalla de tablas, troncales y políticas, y anexando archivos de simulación relevantes, estructura el informe con secciones de diseño, configuración y validación, una matriz de pruebas con resultados y una conclusión breve, incluye marcas temporales, versiones de herramienta y, si es posible, huellas hash de archivos adjuntos para trazabilidad, esta carpeta técnica permitirá replicación por pares y defensa ante rúbrica experta.

Con la implementación funcional y la evidencia consolidada, el estado del proyecto queda listo para fortalecer seguridad y cumplimiento, el siguiente paso afina controles de acceso, registros y cifrado, y alinea las políticas con métricas de desempeño observadas en las pruebas, mantén la misma disciplina de

documentación y repetibilidad para que cada mejora sea medible y defendible en iteraciones posteriores (Mwansa et al., 2024).

7.4. Seguridad y cumplimiento

Las decisiones de seguridad y cumplimiento deben responder a amenazas reales del entorno y a objetivos claros de protección definidos por el negocio, en un proyecto académico o empresarial, la prioridad es reducir exposición, preservar confidencialidad e integridad y mantener trazabilidad sin obstaculizar el servicio, la configuración segura del transporte, especialmente con TLS moderno, es un pilar para credenciales y datos en tránsito, y debe alinearse con guías actuales que desaconsejan suites obsoletas y recomiendan parámetros robustos, la gobernanza del registro y la respuesta ante incidentes completan el cuadro para cumplir regulaciones y demostrar diligencia responsable en auditorías técnicas. (Sheffer et al., 2022; NIST, 2025).

El control de acceso parte de una segmentación consistente con redes virtuales y zonas, reforzada por listas que permiten solo lo necesario entre segmentos definidos, la administración de identidades básica exige credenciales únicas y perfiles mínimos por rol, evitando cuentas compartidas y registrando cambios con responsables y fechas, las excepciones deben justificarse por caso de uso, documentarse con vigencia limitada y revisarse en ventanas planificadas para no convertirse en puertas permanentes, esta

disciplina reduce movimiento lateral, facilita auditoría y preserva coherencia entre políticas y comportamiento efectivo del tráfico.

La protección en tránsito combina cifrado de aplicación con TLS vigente y túneles IPsec cuando se requiere encapsular dominios o sedes completas, las recomendaciones actuales para TLS y DTLS orientan versiones, suites y validaciones de certificado, mientras perfiles cripto para IPsec especifican algoritmos y tamaños de clave adecuados para alta seguridad, en escenarios con recursos limitados, una implementación mínima de ESP mantiene interoperabilidad y reduce complejidad sin renunciar a propiedades críticas de protección, la consistencia de parámetros y la verificación periódica evitan derivas de configuración que reabran riesgos mitigados. (Sheffer et al., 2022; Corcoran & Jenkins, 2022; Migault & Guggemos, 2023).

La privacidad exige tratar evidencias y registros con criterio, evitando exponer información personal o sensible en capturas y reportes, la literatura resalta límites y riesgos de la anonimización si no se aplican técnicas y controles adecuados, por lo que conviene minimizar datos y aplicar principios de necesidad y proporcionalidad. En redes con IPv6, el uso de direcciones temporales aleatorizadas reduce correlaciones triviales entre sesiones y mitiga rastreo por terceros, sin impedir el registro operativo responsable, las políticas deben definir retención, acceso y eliminación segura con

responsables claros y periodos explícitos (Gadotti et al., 2024; Gont et al., 2021).

La evidencia y la auditoría se sostienen con bitácoras completas y capturas selectivas que documenten configuración, eventos y pruebas, con marcas temporales y versiones de herramientas, un expediente mínimo cita archivos y filtros usados, relaciona hallazgos con indicadores y conserva huellas criptográficas para garantizar integridad, las guías más recientes de respuesta ante incidentes recomiendan integrar estos registros con el ciclo de gestión del riesgo, de modo que cada evento produzca mejoras verificables y acciones repetibles, esta trazabilidad permite demostrar cumplimiento y defender decisiones técnicas frente a pares y revisores. (NIST, 2025).

A manera de conclusión, el perfil de seguridad del proyecto integra segmentación y listas, transporte cifrado y prácticas de privacidad con retención responsable de evidencias, el cierre operativo requiere verificar que las políticas efectivamente se apliquen y que el desempeño permanezca dentro de umbrales aceptables para voz, video y servicios críticos, el siguiente paso enlaza estos controles con monitoreo e indicadores, de modo que la red se explique con sus datos y cada ajuste pueda medirse y sostenerse en el tiempo (Sheffer et al., 2022; Corcoran & Jenkins, 2022).

7.5. Entrega y defensa

La entrega de los documentos finales (dossier final), debe incluir todos los insumos necesarios para entender, verificar y mantener la solución sin depender del equipo autor, organiza el paquete en un orden lógico que comience por un resumen ejecutivo breve y continúe con el diseño lógico y físico, los diagramas actualizados, el plan de direccionamiento y segmentación, y las políticas de enrutamiento, traducción y acceso, añade una sección de topología inalámbrica con criterios de canalización y potencia, seguida por la matriz de pruebas ejecutadas y sus resultados principales, cierra con un anexo técnico que detalle parámetros, versiones de herramientas, convenciones de nombres y supuestos operativos validados.

Incorpora como evidencia los archivos del proyecto de simulación, las capturas de pantalla relevantes y los registros generados durante las pruebas, cuidando coherencia en los nombres y las versiones, emplea una convención de nomenclatura que incluya fecha en formato ISO, etapa y alcance, de modo que versiones previas puedan rastrearse sin ambigüedades, mantén una carpeta nombrada como “artifacts”, con subdirectorios para configuraciones, capturas crudas del analizador y exportes de reportes, acompañados por un archivo de índice que explique contenido y relación con los requisitos, calcula y documenta huellas hash de los archivos clave para asegurar integridad en transferencias y revisiones.

Formaliza la aceptación mediante un acta firmada electrónicamente que identifique claramente a las personas responsables, el alcance entregado y los criterios de aceptación cumplidos, utiliza una herramienta de firma confiable que emita un certificado de finalización y un registro de auditoría con marcas temporales, direcciones de red y eventos de apertura y firma, conserva el documento firmado y su auditoría en el repositorio del proyecto, anotando ubicación, control de versiones y periodo de retención acordado, esta trazabilidad aporta no repudio y facilita auditorías posteriores sin reconstrucciones costosas.

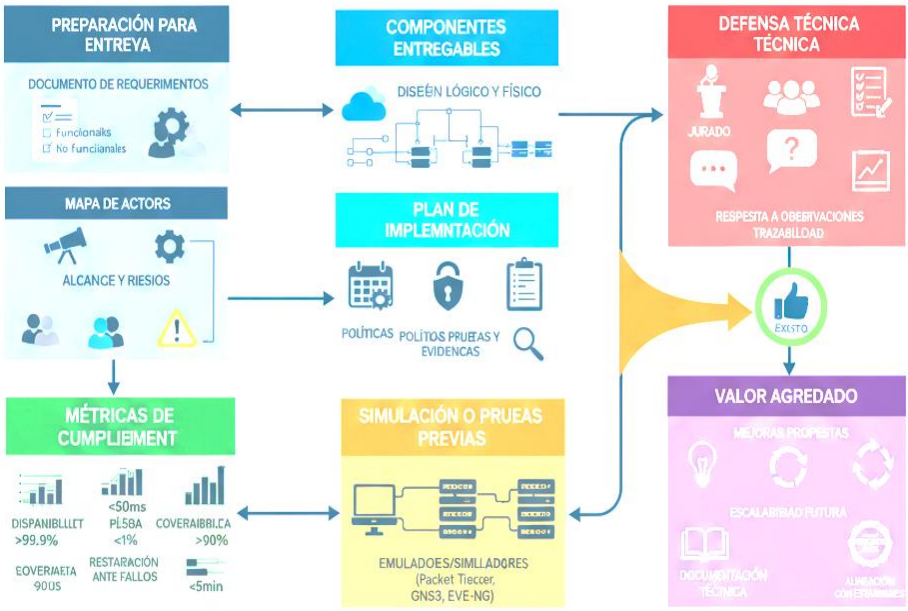
Estructura la defensa técnica como una presentación breve y enfocada en requisitos, diseño, pruebas y resultados, con una narrativa que conecte decisiones y evidencias, abre con el problema, los objetivos y los supuestos, continúa con los diagramas clave y el plan de direccionamiento, y muestra políticas representativas con su efecto observable, dedica una sección a resultados de pruebas con dos o tres métricas críticas, y termina con riesgos remanentes y mejoras propuestas, gestiona el tiempo con una agenda visible y checkpoints claros para preguntas, reservando un minuto final para conclusiones y siguientes pasos.

Mapea cada requerimiento de la rúbrica a una evidencia concreta del dossier y marca el estado de cumplimiento con una breve justificación verificable, habilita un formulario o sección de

retroalimentación donde el jurado registre observaciones y recomendaciones priorizadas, y convierte esos comentarios en un pequeño plan de acción con responsables y fechas, si alguna evidencia resulta insuficiente, anota la corrección prevista y la métrica que confirmará su eficacia, evitando respuestas defensivas y privilegiando claridad y mejora continua, esta práctica cierra el ciclo de aprendizaje y prepara una siguiente iteración más sólida.

Figura 37

Flujo de entrega y defensa del PIS



Nota. Estructura referencial del Flujo de entrega y defensa del PIS. Fuente. Elaboración propia.

El proyecto se considera logrado cuando la solución funciona según lo esperado, la evidencia lo demuestra sin ambigüedades y la aceptación queda formalizada con firma y trazabilidad, este cierre no es un punto final, sino la base para continuidad operativa y nuevas mejoras guiadas por métricas y retroalimentación, con el dossier completo, la defensa sustentada y los compromisos de mantenimiento definidos, concluye el capítulo e inicia la etapa de evolución y refinamiento, en la que cada iteración fortalecerá desempeño, seguridad y claridad operativa del entorno.

Cierre del capítulo y del libro.

El capítulo culminó integrando requerimientos, diseño, implementación en simulación, seguridad, monitoreo y formalización de la aceptación en un conjunto coherente, convertiste necesidades reales en artefactos verificables con nombres claros, prefijos consistentes, políticas justificadas y métricas que confirman el comportamiento esperado, registraste evidencias con capturas, versiones y marcas temporales, de modo que la réplica del experimento no dependa de memoria frágil ni de interpretaciones ambiguas, la defensa técnica demostró que cada decisión responde a objetivos medibles y a riesgos contextualizados, sosteniendo conclusiones con datos y no con suposiciones.

Al finalizar, el proyecto no solo funcionó según lo previsto, también quedó listo para operar y evolucionar con criterios sostenibles, estableciste umbrales para indicadores clave, definiste ventanas de mantenimiento y documentaste procedimientos de recuperación que reducen tiempos de restauración, formalizaste la aceptación con trazabilidad completa y convertiste observaciones del jurado en acciones priorizadas por impacto y esfuerzo razonable, el resultado es una solución que puede explicarse, transferirse y auditarse sin depender de personas específicas.

La principal lección es que la calidad emerge de la preparación, la verificación y la disciplina documental, no de atajos extraordinarios, diseñar, medir y ajustar en ciclos cortos produce mejoras reales y reduce la incertidumbre ante cambios inevitables del entorno, con ese enfoque, la infraestructura se vuelve un sistema vivo que aprende de sus datos y que mejora cada vez que se ejecuta un plan de pruebas honesto, la metodología ya es parte de tu caja de herramientas y no un requisito aislado de examen.

Cerramos el capítulo invitándote a mantener la misma actitud de evidencia y claridad en despliegues futuros, lleva contigo las plantillas, los criterios operativos y las métricas que construiste, y actualízalos cuando cambie el contexto tecnológico o institucional, una red bien gobernada no es solo estable hoy, también es

comprensible y mejorable mañana con pasos concretos y responsabilidades claras.

El libro completo te acompañó desde fundamentos hasta un proyecto que se defiende con datos y documentos precisos, iniciaste reconociendo capas, PDU y protocolos, planificaste direccionamiento con prefijos estables y observaste tramas y paquetes para entender el recorrido extremo a extremo, exploraste transmisión y codificación, mediste errores y rendimiento, y elegiste medios adecuados a distancia, costo y resiliencia, aplicaste seguridad con principios claros, integridad verificable, transporte cifrado y gobierno de evidencia que resiste auditorías serias.

Diseñaste redes de área amplia con criterios explícitos de capacidad, alcance y continuidad, comparaste enrutamiento estático y dinámico, y administraste traducción y túneles sin perder trazabilidad, segmentaste el campus con redes virtuales, habilitaste enrutamiento inter VLAN y evitaste bucles con control de la capa de enlace, instrumentaste monitoreo con administración simple, definiste indicadores de latencia, fluctuación, pérdida y rendimiento, y mejoraste cobertura inalámbrica con mapas de calor replicables, finalmente uniste todo en un expediente técnico que cualquiera puede revisar y reproducir con justicia metodológica.

La propuesta central que recorre estas páginas es que el diseño es inseparable de la verificación y de la documentación, porque solo así las decisiones sobreviven al tiempo, un conjunto de métricas bien elegidas sustituye discusiones vagas por acuerdos operativos, y una evidencia ordenada transforma opiniones en aprendizajes que permanecen, la cultura de mejora continua evita que la red dependa de heroicidades y habilita iteraciones pequeñas con retornos medibles, ningún entorno es estático, por eso la metodología vale tanto como la configuración misma.

Te invitamos a continuar cultivando hábitos de medición honesta, nombres consistentes y pruebas reproducibles, compartiendo con tu comunidad los artefactos que generan confianza, mantén actualizadas tus referencias, revisa periódicamente parámetros criptográficos y políticas de acceso, y valida que las herramientas sigan alineadas con objetivos reales, cada nuevo proyecto será otra oportunidad para demostrar que un enfoque basado en evidencia reduce riesgos, acelera decisiones y eleva la calidad de la experiencia, que este cierre sea un punto de partida para redes que funcionen, se expliquen con sus datos y mejoren en ciclos previsibles.

Referencias Bibliográficas:

Alhilali, A. H., Al Farawn, A., & Mjhool, A. Y. (2023). Design and implement a real-time network traffic management system using SNMP protocol. Eastern-European Journal of Enterprise Technologies, 5(9), 35–44. https://doi.org/10.15587/1729-4061.2023.286528

Allison, J. (2022). Simulation-based learning via Cisco Packet Tracer to enhance computer networking education. En Proceedings of ACM ITiCSE 2022 (pp. 1–6). ACM. https://doi.org/10.1145/3502718.3524739

Biryukov, A., Dinu, D., Khovratovich, D., & Josefsson, S. (2021). Argon2 memory-hard function for password hashing and proof-of-work applications (RFC 9106). RFC Editor. https://doi.org/10.17487/RFC9106

Briscoe, B., De Schepper, K., Bagnulo, M., & White, G. (2023). Low Latency, Low Loss, and Scalable Throughput (L4S) Internet Service: Architecture (RFC 9330). RFC Editor. https://doi.org/10.17487/RFC9330

Campbell, B., Bradley, J., Sakimura, N., & Jones, M. (2020). OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens (RFC 8705). RFC Editor. https://doi.org/10.17487/RFC8705

Chang, Y.-F., Tai, W.-L., & Fan, K.-H. (2022). Offline user authentication ensuring non-repudiation and anonymity. Sensors, 22(24), 9673. https://doi.org/10.3390/s22249673

Chroboczek, J. (2020). The Babel routing protocol (RFC 8966). RFC Editor. https://doi.org/10.17487/RFC8966

Colitti, L., & Linkova, J. (2020). Discovering PREF64 in Router Advertisements (RFC 8781). RFC Editor. https://doi.org/10.17487/RFC8781

Corcoran, L., & Jenkins, M. (2022). Commercial National Security Algorithm (CNSA) Suite Cryptography for Internet Protocol Security (IPsec) (RFC 9206). RFC Editor. https://doi.org/10.17487/RFC9206

Corcoran, L., & Jenkins, M. (2022). Commercial National Security Algorithm (CNSA) Suite Cryptography for IPsec (RFC 9206). RFC Editor. https://doi.org/10.17487/RFC9206

De Schepper, K., & Briscoe, B. (2023). Dual-Queue Coupled Active Queue Management (AQM) for Low Latency, Low Loss, and Scalable Throughput (L4S) (RFC 9332). RFC Editor. https://doi.org/10.17487/RFC9332

De Schepper, K., & Briscoe, B. (Eds.). (2023). The Explicit Congestion Notification (ECN) Protocol for Low Latency, Low Loss, and Scalable Throughput (L4S) (RFC 9331). RFC Editor. https://doi.org/10.17487/RFC9331

Deering, S., & Hinden, R. (2017). Internet protocol, version 6 (IPv6) specification (RFC 8200). RFC Editor. https://doi.org/10.17487/RFC8200

DocuSign. (2024, January 12). View a contract's audit trail. https://support.docusign.com/s/document-item?_LANG=enus&bundleId=zzg1606752647158&topicId=vvh1606752561471.html

DocuSign. (2025, July 26). History and certificate of completion. https://support.docusign.com/s/document-item?_LANG=enus&bundleId=oeq1643226594604&language=en_US&rsc_301=&topicId=hha1578456343641.html

Eddy, W. (2022). Transmission Control Protocol (TCP) (RFC 9293). RFC Editor. https://doi.org/10.17487/RFC9293

ETSI. (2024, January). ETSI EN 319 142-1 V1.2.1: PAdES baseline signatures—Building blocks. https://cdn.standards.iteh.ai/samples/68046/3d9a1d7083e84ecaa99dffcf5eecb978/ETSI-EN-319-142-1-V1-2-1-2024-01-.pdf

ETSI. (2024, June 17). ETSI EN 319 102-1 V1.4.1: Electronic signatures and infrastructures; Procedures for creation and validation of AdES—Part 1: Creation and validation. https://www.etsi.org/deliver/etsi_en/319100_319199/31910201/01.04.01_60/en_31910201v010401p.pdf

ETSI. (2024, June). ETSI EN 319 401 V3.1.1: Electronic signatures and trust infrastructures; General policy requirements for trust service providers. https://www.etsi.org/deliver/etsi_en/319400_319499/319401/03.01.01_60/en_319401v030101p.pdf

Fuller, V., & Li, T. (2006). Classless inter-domain routing (CIDR): The Internet address assignment and aggregation plan (RFC 4632). RFC Editor. https://doi.org/10.17487/RFC4632

Gadotti, A., Rocher, L., Houssiau, F., & Creţu, A.-M. (2024). Anonymization: The imperfect science of using data while preserving privacy. Science Advances, 10(29), eadn7053. https://doi.org/10.1126/sciadv.adn7053

Gadotti, A., Vigo, M., Darby, P., Tolmie, P., Singh, J., Garfield, S., & Jamnik, M. (2024). Anonymization: The imperfect science of using data while minimizing privacy risks. Science Advances, 10(36), eadn7053. https://doi.org/10.1126/sciadv.adn7053

GCHQ. (2025). CyberChef [Aplicación web]. https://gchq.github.io/CyberChef/

Geels, J., Park, Y., Das, S., Kumar, D., & Choffnes, D. (2024). Ordinary users do not understand digital signatures. Proceedings of the ACM on Human-Computer Interaction, 8(CSCW2), Article 487. https://doi.org/10.1145/3679318.3685402

Giménez-Guzmán, J. M., Marsá-Maestre, I., de la Hoz, E., Orden, D., & Herranz-Oliveros, D. (2023). Channel selection in uncoordinated IEEE 802.11 networks using graph coloring. Sensors, 23(13), 5932. https://doi.org/10.3390/s23135932

Gómez Blanco, D. (2023). Practical OpenTelemetry: Adopting open observability standards across your organization. Apress. https://doi.org/10.1007/978-1-4842-9075-0

Gont, F., Krishnan, S., & Narten, T. (2021). Temporary address extensions for stateless address autoconfiguration in IPv6 (RFC 8981). RFC Editor. https://doi.org/10.17487/RFC8981

Gont, F., Krishnan, S., & Narten, T. (2021). Temporary Address Extensions for Stateless Address Autoconfiguration (SLAAC) in IPv6 (RFC 8981). RFC Editor. https://doi.org/10.17487/RFC8981

Hillman, D., Harel, Y., & Toch, E. (2023). Evaluating organizational phishing awareness training on an enterprise scale. Computers & Security, 132, 103364. https://doi.org/10.1016/j.cose.2023.103364

IEEE. (2021). IEEE Std 802.11ax-2021: IEEE standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications—Amendment 1:

Enhancements for high efficiency WLAN. https://doi.org/10.1109/IEEESTD.2021.9442429

IEEE. (2021). IEEE Std 802.11ax-2021: Wireless LAN MAC and PHY—Amendment 1: Enhancements for High-Efficiency WLAN. https://doi.org/10.1109/IEEESTD.2021.9442429

IEEE. (2022). IEEE Std 802.1Q-2022: IEEE Standard for Local and Metropolitan Area Networks—Bridges and Bridged Networks. https://doi.org/10.1109/IEEESTD.2022.10004498

IEEE. (2022a). IEEE Std 802.1Q-2022: Bridges and Bridged Networks. https://doi.org/10.1109/IEEESTD.2022.10004498

IEEE. (2022a). IEEE Std 802.3-2022: IEEE standard for Ethernet. https://standards.ieee.org/ieee/802.3/10422/

IEEE. (2022b). IEEE Std 802.1Q-2022: IEEE standard for local and metropolitan area networks—Bridges and bridged networks. https://doi.org/10.1109/IEEESTD.2022.10004498

IEEE. (2022b). IEEE Std 802.3-2022: Ethernet. https://doi.org/10.1109/IEEESTD.2022.9869410

International Telecommunication Union. (2020). Ethernet ring protection switching (Recommendation ITU-T G.8032/Y.1344). International Telecommunication Union. https://www.itu.int/rec/T-REC-G.8032

Internet Engineering Task Force. (2021). Operational Security Considerations for IPv6 Networks (RFC 9099). RFC Editor. https://doi.org/10.17487/RFC9099

Internet Engineering Task Force. (2023). IPv6 Deployment Status (RFC 9386). RFC Editor. https://doi.org/10.17487/RFC9386

ISO/IEC. (1994). Information technology—Open Systems Interconnection—Basic Reference Model: The basic model (ISO/IEC 7498-1:1994). International Organization for Standardization. https://www.iso.org/standard/20269.html

ISO/IEC/IEEE. (2018). ISO/IEC/IEEE 29148:2018—Systems and software engineering—Life cycle processes—Requirements engineering. https://doi.org/10.1109/IEEESTD.2018.8559686

Iyengar, J., & Swett, I. (2021). QUIC Loss Detection and Congestion Control (RFC 9002). RFC Editor. https://doi.org/10.17487/RFC9002

Iyengar, J., & Thomson, M. (2021). QUIC: A UDP-Based Multiplexed and Secure Transport (RFC 9000). RFC Editor. https://doi.org/10.17487/RFC9000

Kabir, M. H., Kabir, M. A., Islam, M. S., Mortuza, M. G., & Mohiuddin, M. (2021). Performance analysis of mesh based enterprise network using RIP, EIGRP and OSPF routing protocols. Engineering Proceedings, 10(1), 47. https://doi.org/10.3390/ecsa-8-11285

Leurent, G., & Peyrin, T. (2020). SHA-1 is a shambles: First chosen-prefix collision on SHA-1 and application to the PGP Web of Trust. Proceedings of the 2020 ACM

Conference, 1299–1316. https://www.usenix.org/conference/usenixsecurity20/presentation/leurent

Liu, X., Sarda, P., & Choudhary, V. (2020). A YANG data model for the Routing Information Protocol (RIP) (RFC 8695). RFC Editor. https://doi.org/10.17487/RFC8695

Migault, D., & Guggemos, T. (2023). Minimal IP Encapsulating Security Payload (ESP) (RFC 9333). RFC Editor. https://doi.org/10.17487/RFC9333

Mwansa, G., Ngandu, M. R., & Dasi, Z. S. (2024). Enhancing practical skills in computer networking: Evaluating the unique impact of simulation tools, particularly Cisco Packet Tracer, in resource-constrained higher education settings. Education Sciences, 14(10), 1099. https://doi.org/10.3390/educsci14101099

National Institute of Standards and Technology. (2020). Guide to IPsec VPNs (NIST SP 800-77r1). https://doi.org/10.6028/NIST.SP.800-77r1

National Institute of Standards and Technology. (2020). Security and privacy controls for information systems and organizations (NIST SP 800-53 Rev. 5). https://doi.org/10.6028/NIST.SP.800-53r5

National Institute of Standards and Technology. (2025). Incident response recommendations and considerations for

cybersecurity risk management (NIST SP 800-61r3). https://doi.org/10.6028/NIST.SP.800-61r3

National Institute of Standards and Technology. (2025). Incident response recommendations and considerations for cyber risk management (NIST SP 800-61r3). https://doi.org/10.6028/NIST.SP.800-61r3

Patterson, C. M., Nurse, J. R. C., & Franqueira, V. N. L. (2024). "I don't think we're there yet": The practices and challenges of organisational learning from cyber security incidents. Computers & Security, 139, 103699. https://doi.org/10.1016/j.cose.2023.103699

Pauly, T., & Smyslov, V. (2022). TCP encapsulation of Internet Key Exchange protocol (IKE) and IPsec packets (RFC 9329). RFC Editor. https://doi.org/10.17487/RFC9329

Petit-Huguenin, M., Salgueiro, G., Rosenberg, J., Wing, D., Mahy, R., & Matthews, P. (2020). Session Traversal Utilities for NAT (STUN) (RFC 8489). RFC Editor. https://doi.org/10.17487/RFC8489

Postel, J. (1981). Internet Control Message Protocol (RFC 792). RFC Editor. https://doi.org/10.17487/RFC0792

Psenak, P., Ginsberg, L., Henderickx, W., Tantsura, J., & Drake, J. (2023). OSPF application-specific link attributes (RFC 9492). RFC Editor. https://doi.org/10.17487/RFC9492

Rescorla, E. (2022). The Datagram Transport Layer Security (DTLS) Protocol Version 1.3 (RFC 9147). RFC Editor. https://doi.org/10.17487/RFC9147

Richer, J. (2021). JSON Web Token (JWT) Profile for OAuth 2.0 Access Tokens (RFC 9068). RFC Editor. https://doi.org/10.17487/RFC9068

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture (NIST SP 800-207). https://doi.org/10.6028/NIST.SP.800-207

Scarfone, K., & Souppaya, M. (2023). Cybersecurity log management planning guide (NIST SP 800-92r1, initial public draft). https://doi.org/10.6028/NIST.SP.800-92r1.ipd

Sheffer, Y., Hardt, D., & Jones, M. B. (2020). JSON Web Token (JWT) Best Current Practices (RFC 8725). RFC Editor. https://doi.org/10.17487/RFC8725

Sheffer, Y., Holz, R., & Saint-André, P. (2022). Recommendations for secure use of TLS and DTLS (RFC 9325). RFC Editor. https://doi.org/10.17487/RFC9325

Sheffer, Y., Saint-André, P., & Farrell, S. (2021). Deprecating TLS 1.0 and TLS 1.1 (RFC 8996). RFC Editor. https://doi.org/10.17487/RFC8996

Sheffer, Y., Saint-André, P., & Fossati, T. (2022). Recommendations for secure use of Transport Layer Security (TLS) and

Datagram Transport Layer Security (DTLS) (RFC 9325). RFC Editor. https://doi.org/10.17487/RFC9325

Sheffer, Y., Saint-André, P., & Fossati, T. (2022). Recommendations for secure use of TLS and DTLS (RFC 9325). RFC Editor. https://doi.org/10.17487/RFC9325

Smyslov, V. (2022). Intermediate exchange in the Internet Key Exchange protocol version 2 (IKEv2) (RFC 9242). RFC Editor. https://doi.org/10.17487/RFC9242

Song, H., Qin, F., Martinez-Julia, P., Ciavaglia, L., & Wang, A. (2022). Network telemetry framework (RFC 9232). RFC Editor. https://doi.org/10.17487/RFC9232

Talaulikar, K., & Psenak, P. (2023). Advertising Layer 2 bundle member link attributes in OSPF (RFC 9356). RFC Editor. https://doi.org/10.17487/RFC9356

TP-Link. (2025). Configuring ACL [Guía en línea]. https://www.tp-link.com/us/configuration-guides/configuring_acl/

TP-Link. (2025). TP-Link Emulators [Panel web]. https://www.tp-link.com/us/support/emulator/

Vaughn, K. (2023). Updates to the TLS Transport Model for SNMP (RFC 9456). RFC Editor. https://doi.org/10.17487/RFC9456

Wireshark Foundation. (2025). Wireshark user's guide. https://www.wireshark.org/docs/wsug_html_chunked/

Wu, B., Zheng, G., & Wang, Z. (2021). A YANG data model for Terminal Access Controller Access Control System Plus

(TACACS+) (RFC 9105). RFC Editor. https://doi.org/10.17487/RFC9105

Wu, Q., Boucadair, M., López, D., Xie, C., & Geng, L. (2021). A framework for automating service and network management with YANG (RFC 8969). RFC Editor. https://doi.org/10.17487/RFC8969

Yaseen, N. (2025). From counters to telemetry: A survey of programmable network-wide monitoring. Network, 5(3), 38. https://doi.org/10.3390/network5030038

EDITORIAL
edulearn
Academy SAS

ISBN: 978-9942-7393-3-9