



Introducción a las Redes

Guía didáctica

++
++
++
++
++
++



Facultad:

Ingenierías y Arquitectura



Carrera:

Redes y Analítica de Datos



Autora:

Patricia Jeanneth Ludeña González

Universidad Técnica Particular de Loja

Introducción a las Redes

Guía didáctica

Patricia Jeanneth Ludeña González

Diagramación y diseño digital:

Ediloja Cia. Ltda.

Marcelino Champagnat s/n y París

edilojacialtda@ediloja.com.ec

www.ediloja.com.ec

ISBN digital - 978-9942-47-496-4

Año de edición: Octubre, 2025

Edición: primera edición

El autor de esta obra ha utilizado la inteligencia artificial como una herramienta complementaria. La creatividad, el criterio y la visión del autor se han mantenido intactos a lo largo de todo el proceso.

Loja-Ecuador



Los contenidos de este trabajo están sujetos a una licencia internacional Creative Commons

Reconocimiento-NoComercial-CompartirIgual 4.0 (CC BY-NC-SA 4.0). Usted es libre de **Compartir** – copiar y redistribuir el material en cualquier medio o formato. **Adaptar** – remezclar, transformar y construir a partir del material citando la fuente, bajo los siguientes términos: **Reconocimiento** – debe dar crédito de manera adecuada, brindar un enlace a la licencia, e indicar si se han realizado cambios. Puede hacerlo en cualquier forma razonable, pero no de forma tal que sugiera que usted o su uso tienen el apoyo de la licenciante. **No Comercial** – no puede hacer uso del material con propósitos comerciales. **Compartir igual** – Si remezcla, transforma o crea a partir del material, debe distribuir su contribución bajo la misma licencia del original. No puede aplicar términos legales ni medidas tecnológicas que restrinjan legalmente a otras a hacer cualquier uso permitido por la licencia. <https://creativecommons.org/licenses/by-nc-sa/4.0/>

8 de octubre, 2025

Índice

1. Datos de información	7	Índice
1.1. Presentación de la asignatura	7	
1.2. Competencias genéricas de la UTPL.....	7	
1.3. Competencias del perfil profesional	7	
1.4. Problemática que aborda la asignatura.....	8	
2. Metodología de aprendizaje	8	I Bimestre
3. Orientaciones didácticas por resultados de aprendizaje	10	
 Primer bimestre	 10	
Resultado de aprendizaje 1.....	10	
Contenidos, recursos y actividades de aprendizaje recomendadas.....	11	
 Semana 1	 12	
 Unidad 1. Fundamentos de redes	 12	
1.1. Conceptos básicos de redes	13	
1.2. Características de redes	22	
1.3. Modelos de referencia	27	
1.4. Encapsulamiento.....	38	
Actividades de aprendizaje recomendadas	40	
 Semana 2	 43	
1.5. Configuración de dispositivos de red	43	
Actividades de aprendizaje recomendadas	67	
Autoevaluación 1.....	71	
		II Bimestre
		Solucionario
		Referencias



Resultado de aprendizaje 2	75
Contenidos, recursos y actividades de aprendizaje recomendadas.....	75
Semana 3	76
Unidad 2. Comunicación entre dispositivos	76
2.1. Capa física.....	77
Actividades de aprendizaje recomendadas	94
Semana 4	97
2.2. Sistemas de numeración	97
2.3. Capa de enlace.....	106
Actividad de aprendizaje recomendada.....	112
Semana 5	113
2.4. Protocolo Ethernet	113
Actividades de aprendizaje recomendadas	127
Semana 6	131
2.5. Capa de red.....	131
Actividad de aprendizaje recomendada.....	151
Semana 7	153
2.6. Protocolo IPv4.....	153
2.7. Protocolo IPv6.....	164
Actividad de aprendizaje recomendada.....	172
Semana 8	174
Actividades finales del bimestre.....	174
Actividad de aprendizaje recomendada	176



Segundo bimestre	179
Resultado de aprendizaje 2	179
Contenidos, recursos y actividades de aprendizaje recomendadas.....	179
Semana 9	180
2.8. Protocolo ICMP	180
2.9. Resolución de direcciones IP-MAC	186
Actividades de aprendizaje recomendadas	198
Semana 10	202
2.10. Configuración de enrutadores	202
Actividades de aprendizaje recomendadas	213
Semana 11	216
2.11. División en subredes.....	216
Actividades de aprendizaje recomendadas	232
Autoevaluación 2	236
Semana 12	241
Unidad 3. Comunicación entre aplicaciones.....	241
3.1. Capa de transporte	241
3.2. Protocolo UDP	244
3.3. Protocolo TCP	248
Actividad de aprendizaje recomendada	258
Semana 13	260
3.4. Capas superiores	260
Actividades de aprendizaje recomendadas	272
Autoevaluación 3	274

Resultado de aprendizaje 3	279
Contenidos, recursos y actividades de aprendizaje recomendadas.....	279
Semana 14	280
Unidad 4. Fundamentos de seguridad e implementación.....	280
4.1. Fundamentos de seguridad	280
Actividades de aprendizaje recomendadas	296
Semana 15	299
4.2. Implementación de redes LAN.....	299
Actividades de aprendizaje recomendadas	316
Autoevaluación 4.....	320
Semana 16	326
Actividades finales del bimestre.....	326
Actividades de aprendizaje recomendadas	327
4. Solucionario.....	330
5. Glosario.....	341
6. Referencias bibliográficas	344
7. Anexos.....	346



1. Datos de información

1.1. Presentación de la asignatura



UTPL

1.2. Competencias genéricas de la UTPL

- Orientación a la innovación y a la investigación.
- Pensamiento crítico y reflexivo.
- Organización y planificación del tiempo.

1.3. Competencias del perfil profesional

Diseñar y evaluar la infraestructura de redes de telecomunicaciones mediante la aplicación de tecnologías emergentes siguiendo estándares

internacionales para brindar conectividad sostenible y de calidad a la sociedad.

1.4. Problemática que aborda la asignatura

La asignatura Introducción a las redes se enfoca en brindar una visión general de cómo se estructuran las redes de computadoras modernas, qué protocolos se usan para transportar datos y qué requisitos básicos deben cumplir las redes para la puesta en marcha de servicios en aplicaciones de diferente índole. La materia no solo cubre conceptos, sino también brinda competencias en la puesta en marcha de equipos a través de configuración de equipos de redes y la detección de fallos con herramientas básicas, estas habilidades le permitirán ser competente en su ejercicio profesional al enfrentarse a problemas similares en redes reales.



2. Metodología de aprendizaje

La asignatura de Introducción a las redes brinda la oportunidad de fortalecer su currículo profesional a través de la formación para la certificación de redes Cisco Certified Networking Associate (CCNA) en su nivel 1. Por tanto, usted tendrá acceso a la plataforma Netacad donde podrá revisar todos los contenidos, herramientas y materiales de formación disponibles.

En esta asignatura se usarán metodologías activas con un **enfoque práctico**, a través de simulación con Packet Tracer y evaluación de

tráfico usando Wireshark, para abordar los temas fundamentales de redes.

Las unidades se aprenderán a través de la metodología de **Aula Invertida Digital**. La teoría y los conceptos se estudiarán previamente a través de la revisión de los módulos correspondientes en la plataforma Netacad y videos, tutoriales y lecturas interactivas recomendadas en la guía didáctica y en la plataforma virtual. Los recursos estarán disponibles en cualquier momento, permitiendo que usted pueda avanzar a su propio ritmo.

Además, se usará la metodología de **Aprendizaje Basado en Problemas**. Los tipos de problemas que se le propondrán serán similares a los que podrían encontrarse cuando se desempeñe como profesional. La resolución de problemas pondrá a prueba sus conocimientos sobre redes y su habilidad para razonar y determinar posibles escenarios de solución de manera creativa. La metodología se divide en varios pasos, siendo los más importantes:

- Propuesta de escenarios prácticos para la aplicación de conceptos clave. Los problemas serán planteados en escenarios hipotéticos que simulen situaciones de red reales. Por ejemplo, para entender la configuración de direcciones IP, usted deberá configurar subredes, asignar direcciones IP a dispositivos y realizar pruebas de conectividad. Estos ejercicios le permitirán experimentar con la configuración y diagnóstico de redes de forma práctica y efectiva.
- Desarrollo de estrategias de solución de problemas. Usted trabajará con Packet Tracer para resolver problemas de conectividad, configuración de dispositivos y análisis de tráfico. Se le brindará un conjunto de herramientas y metodologías de solución de problemas (como el uso de comandos como ping, traceroute y simulación de fallos de red) para identificar y solucionar problemas en las redes simuladas con base en un guion.



3. Orientaciones didácticas por resultados de aprendizaje

Resultado de aprendizaje 1



Primer bimestre

- Describe los principios fundamentales de las redes en la configuración de dispositivos y su infraestructura con el objetivo de desarrollar soluciones de telecomunicaciones sostenibles y de calidad.

Este resultado de aprendizaje se alcanzará con el estudio de la unidad 1. Para alcanzarlo, desarrollaremos un trabajo sistemático y colaborativo que le permitirá dominar los fundamentos de las redes. Comenzando por identificar el papel protagónico que desempeñan las redes de telecomunicaciones en la sociedad digital, para luego abordar temas más técnicos, como son los principios de diseño y operación de infraestructuras de redes; y, las bases para una configuración de dispositivos orientada a la calidad, la seguridad y la sostenibilidad.

El integrar teoría y práctica para comprender este panorama, le permitirá evaluar y seleccionar tecnologías, de forma sostenible y con criterios de calidad, pues sabrá a qué necesidades reales responde cada decisión técnica. El desarrollo de estas competencias se sustentará en estrategias didácticas integradas: análisis crítico de contenidos y recursos, laboratorios de simulación en Packet Tracer y verificación de comprensión en la plataforma Netacad. Así, cada actividad fomentará el pensamiento sistémico, la argumentación fundamentada y la destreza

índice

I Bimestre

II Bimestre

Solucionario

Referencias

técnica necesarias para responder a las demandas actuales del ámbito profesional de redes y analítica de datos.

Contenidos, recursos y actividades de aprendizaje recomendadas



Sem 1 Sem 2 Sem 3 Sem 4 Sem 5 Sem 6 Sem 7 Sem 8



Semana 1

¡Bienvenido a los contenidos de la unidad 1!

En la presente semana se analizará el papel estratégico que desempeñan las redes en la sociedad digital, vinculándolo con la forma en que se organizan los dispositivos y medios de transmisión dentro de una arquitectura de comunicaciones. Más adelante, revisaremos los principales entornos de despliegue de redes y sus atributos de rendimiento, fiabilidad y escalabilidad, para luego profundizar en los modelos de referencia OSI y TCP/IP que describen, capa por capa, las funciones esenciales que permiten el intercambio de datos entre sistemas computacionales de manera estructurada. Con ello, usted adquirirá la capacidad de diagnosticar y optimizar infraestructuras, una competencia clave para su futuro desempeño profesional como ingeniero capaz de diseñar soluciones de red robustas, seguras y alineadas a las demandas de una economía cada vez más interconectada. Para que amplíe sus conocimientos, le invito a analizar el tema de Fundamentos de redes en la bibliografía básica. Adicionalmente, le recomiendo revisar el video introductorio que ofrece una perspectiva integral de los temas que abordaremos en la [unidad 1](#).

Como pudo observar en el material audiovisual, las redes no son simplemente cables y dispositivos conectados, sino sistemas organizados que siguen modelos estructurados como TCP/IP y OSI. Esta base conceptual que acaba de revisar será fundamental para comprender cómo los datos viajan de un punto a otro de manera ordenada y eficiente.

Unidad 1. Fundamentos de redes

Índice

I Bimestre

II Bimestre

Solucionario

Referencias

1.1. Conceptos básicos de redes

Antes de comenzar, piense en el instante en que abre una aplicación de mensajería para saludar a un ser querido, en la compra que realiza por Internet o en la clase en línea de la materia que ahora mismo cursa. Detrás de cada acción existe una infraestructura de red que transporta datos, ya sean estas voz, video o texto; y cada una de estas acciones implica una precisión de milisegundos.



La red más conocida y masificada es Internet, que es una red de redes con alcance mundial. Se ha preguntado alguna vez: ¿qué es en realidad Internet? Le invito a revisar el video [¿Qué es internet?](#), donde se explica de forma sencilla qué es esta red, cómo surgió y cómo funciona. Se define a Internet como un "conjunto de redes interconectadas que permiten la comunicación entre dispositivos en todo el mundo, mediante cables o conexiones inalámbricas", siendo esta una excelente definición.

1.1.1. Rol de las redes en el contexto actual

Áreas sostenidas por redes de computadoras

En el mundo actual hay varias áreas que tienen como columna vertebral las redes de computadoras (ver figura 1), entre ellas podemos mencionar:

- **Conectividad ubicua:** las redes posibilitan el acceso continuo a servicios de salud, educación, banca, entretenimiento y gobierno electrónico, incluso en zonas remotas gracias a tecnologías móviles y satelitales.
- **Economía digital:** plataformas de comercio electrónico, FinTech y logística dependen del intercambio seguro y fiable de información. El desempeño de una pasarela de pagos, por ejemplo, descansa

en latencias bajas y altos niveles de disponibilidad de red, que son características clave de las redes modernas.

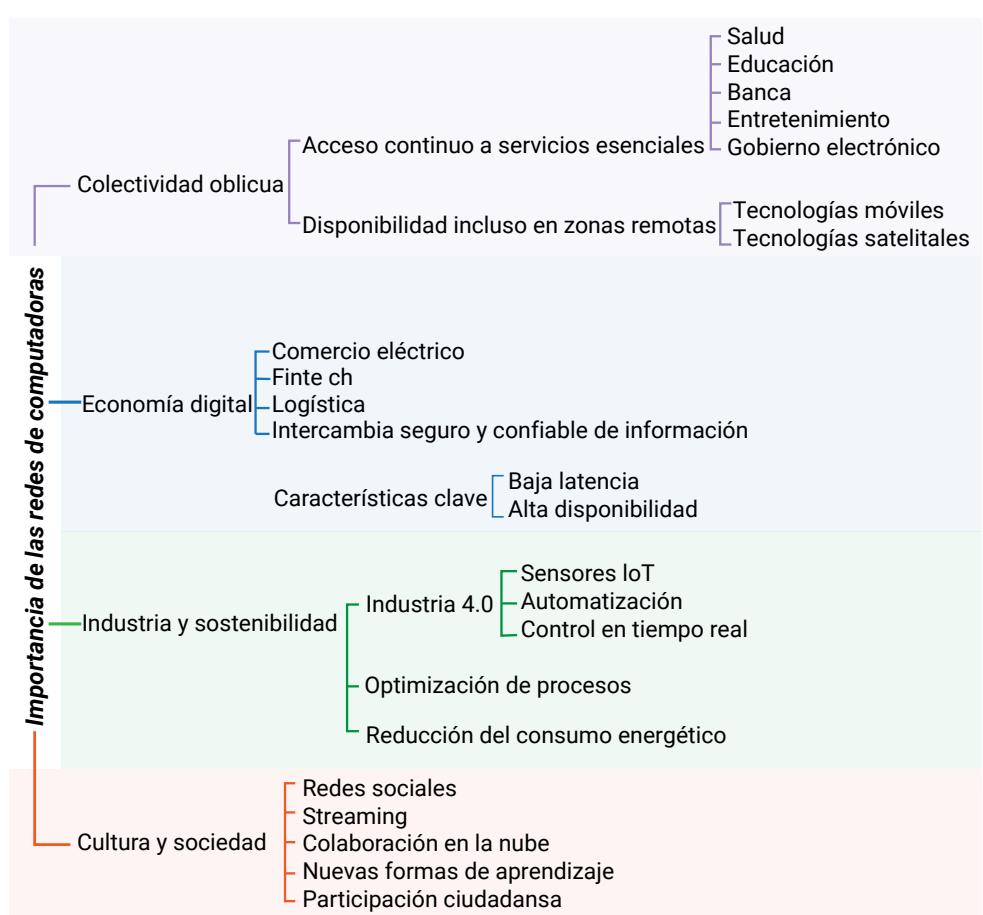
- **Industria y sostenibilidad:** la Industria 4.0 integra sensores IoT que recogen datos para optimizar procesos y reducir el consumo energético. Sin las redes, la automatización y el control en tiempo real no serían posibles y, por tanto, la eficiencia se disminuiría notablemente.
- **Cultura y sociedad:** redes sociales, streaming y colaboración en la nube modelan nuevas formas de comunicación, aprendizaje y participación ciudadana. Apliquemos este concepto a su experiencia: ¿cuántas redes sociales usa a nivel personal?, ¿cuáles de ellas usan *Internet* para intercambio de información?

Todas estas aplicaciones tienen un nexo común: la red de computadoras que permite que los sistemas computacionales intercambien datos.

Reflexione: ¿qué actividades de su rutina dependen de *Internet*? , ¿cómo afectaría a su rutina si *Internet* dejara de funcionar hoy? Seguramente muchas de sus actividades se volverían un caos.

Figura 1

Mapa mental sobre áreas sostenidas por redes de computadores



Nota. Ludeña, P., 2025.

Según Fernández (2024): "casi dos tercios de los habitantes del planeta Tierra están conectados a la red" (párr.1). Para América Latina los usuarios de Internet han crecido considerablemente en la última década, a febrero 2025 en Ecuador son alrededor de 15,2 millones las personas que acceden a la red, mientras que las cifras son mucho mayores para otros países de la región como Colombia (41,1 millones) o Brasil (183 millones) (Statista, 2025). El crecimiento del tráfico en Internet exige

profesionales capaces de diseñar, gestionar y asegurar infraestructuras tecnológicas, generando nichos laborales (WEForum, 2025) (Hays, 2025) como son:

- Administración de redes (Network Administrator): configuración, monitoreo y soporte de redes LAN, WAN y WLAN.
- Ingeniería de redes (Network Engineer): diseño y optimización de topologías, selección de equipos y protocolos.
- Seguridad de redes (Network Security Specialist): implementación de políticas de firewall, VPN, IDS/IPS y respuesta ante incidentes.
- Arquitectura de redes en la nube (Cloud Network Architect): integración de redes locales con entornos de nube híbrida y multicloud.
- Especialista en IoT/OT: despliegue y mantenimiento de redes para sensores industriales y edificios inteligentes.

Como puede notar todas estas áreas son ámbitos donde usted se podrá desempeñar cuando culmine sus estudios, de ahí que es importante que aproveche al máximo su formación.

1.1.2. Estructura de redes de computadores

Las redes de computadores, en su versión más elemental, tiene la misma estructura de la comunicación entre personas, en la Figura 2, se puede apreciar estos elementos: quien habla, quien escucha, el mensaje y el canal de comunicación. En la Figura 3, usted podrá ver los elementos básicos de la comunicación entre computadores: emisor/receptor que serán los dispositivos finales, el medio de interconexión que suele incorporar algunos dispositivos intermediarios y el mensaje que se envía como datos usando el medio para transportarlos.

Figura 2

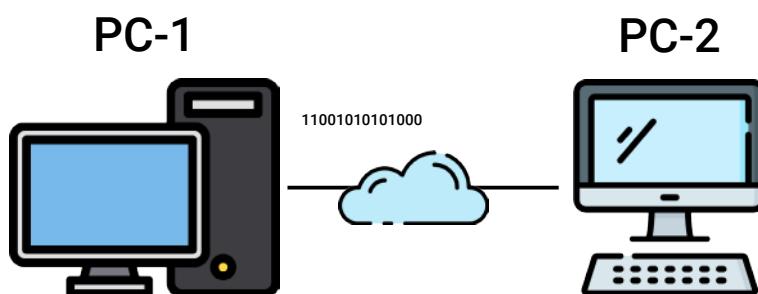
Elementos básicos de la comunicación interpersonal



Nota. Ludeña, P., 2025.

Figura 3

Elementos básicos de la comunicación entre computadoras



Nota. Ludeña, P., 2025.

Imagine la red como una ciudad dinámica: los **dispositivos finales** son los hogares, los **dispositivos intermediarios** son los semáforos y redondeles que ordenan el tráfico, y los **medios de interconexión** son las calles, avenidas y vías rápidas que conectan cada punto. Ahora, en el siguiente modulo didáctico revisaremos en detalle los elementos de red, desde los

dispositivos donde se originan y terminan los datos hasta los caminos invisibles por los que estos viajan.

Estructura de Redes de Computadores

Como pudo observar a lo largo del módulo, la estructura de las redes de computadores sigue principios similares a los sistemas de comunicación que utilizamos diariamente. Las analogías presentadas, desde la comunicación interpersonal hasta el tránsito urbano, le han permitido comprender que los conceptos técnicos tienen fundamentos lógicos y organizados. Notará que cada elemento cumple funciones específicas y complementarias, creando un ecosistema tecnológico donde la eficiencia depende de la correcta interacción entre dispositivos finales, intermediarios y medios de interconexión.

1.1.3. Topologías de red

En el mundo de las redes de computadores usted se encontrará con diagramas que representarán la estructura de las redes, estos diagramas se denominan **topologías** y son la documentación obligatoria que como ingenieros debemos manejar. La función de los diagramas es brindar un mapa visual de cómo se conectan los equipos dentro de la red. Existen dos tipos de topologías:

- a. **Topología física:** es la representación de la manera en que los cables, los puntos de acceso inalámbrico, los switches y los routers están dispuestos físicamente en el espacio. Es decir, tenemos una referencia concreta de dónde se ubica cada dispositivo, qué medio (cobre, fibra o inalámbrico) le permite enlazarse con el siguiente dispositivo y la distancia real entre ellos.
- b. **Topología lógica:** es el diagrama que representa la trayectoria que siguen los datos sobre la infraestructura física, es decir qué enlaces se usan para el viaje efectivo de los datos, qué nodos actúan como puntos de conmutación, qué rutas se usan para priorizar el tráfico

y con qué reglas se está enrutando o reenviando las estructuras de datos.

En la Tabla 1, encontrará un cuadro que resume algunas diferencias clave entre la topología física y la lógica para que pueda interiorizar qué diagrama debe usar en cada ocasión.

Tabla 1

Comparación entre topología física y topología lógica en redes

Aspecto	Topología física	Topología lógica
Enfoque	Distribución concreta del hardware	Flujo de la información y reglas de enrutamiento
Visibilidad	Representación de un plano del cableado	Refleja las tablas de rutas o conexión de protocolos lógicos.
Modificación	Refleja cambios en cables y dispositivos	Refleja cambios dados por software en configuración
Dependencia	Suele cambiar poco luego de la instalación.	Puede variar de acuerdo con las configuraciones o según el tráfico.

Nota. Ludeña, P., 2025.

Como puede notar, cada topología se encarga de representar un aspecto particular de la red. Recuerde que ambas describen interconexiones entre nodos y que un buen diseño de red exige un uso combinado y eficiente de ambas topologías.

Continuando con nuestra analogía del sistema vial de una ciudad, la topología física serían los planos del trazado de calles, puentes y túneles donde se especifica dónde están las avenidas, cuántos carriles tiene y cómo se unen a cada uno de los barrios. Mientras que la topología lógica constituiría el plan de itinerarios de las líneas de autobús donde se especifica qué ruta sigue cada línea, dónde hacen paradas y con qué frecuencia sale cada turno. Entonces, dos barrios podrían estar conectados por las mismas avenidas, pero tener rutas de autobuses distintas que sigan recorridos distintos. De la misma manera, los dispositivos finales podrían tener los mismos medios conectados, pero

seguir rutas distintas a destinos diversos, inclusive tener rutas diferentes dependiendo de la congestión que se presente en la red en determinado momento del día.

Para afianzar el tema de topologías, le invito a revisar el video [Redes: topología Física vs. Lógica](#), el objetivo es que usted pueda diferenciar entre la topología física y lógica y que conozca qué tipos de topologías hay y qué aplicación se les da debido a sus ventajas y desventajas. En el video se define la topología como “la disposición de los dispositivos y sus interconexiones para transmitir datos”, así mismo, se define qué es una topología física y una topología lógica, apunte estos conceptos y compárelos con los estudiados. Luego de ver el video, reflexione:



- ¿Cuáles son los tipos de topologías físicas que se presentan en el video?
- ¿Cuál es la ventaja de usar una topología de anillo?
- ¿Cuál cree usted que presenta mayores ventajas para un entorno de campus en la actualidad? ¿Por qué?
- ¿Qué tipo de topología describe la red punto a punto?

1.1.4. Tipos comunes de redes

Las redes se pueden clasificar dependiendo del tamaño del área de cobertura y la cantidad de usuarios conectados, en la Tabla 2, usted puede encontrar esta clasificación de menor a mayor cobertura.

Tabla 2

Clasificación de redes según su alcance y cobertura

Acrónimo	Nombre	Cobertura aproximada	Uso típico
PAN	Personal Area Network	Unos pocos metros (entorno corporal o escritorio)	Conexión Bluetooth entre teléfono, auriculares y reloj inteligente.
LAN	Local Area Network	Hasta un edificio o planta (decenas a cientos de metros)	Red cableada o Wi-Fi de oficina, aula, hogar o laboratorio.

Acrónimo	Nombre	Cobertura aproximada	Uso típico
WLAN	Wireless LAN	Misma escala que una LAN, pero exclusivamente inalámbrica	Acceso Wi-Fi en campus o cafeterías.
CAN	Campus/ Corporate Area Network	Varios edificios dentro de un recinto (hasta kilómetros)	Red de toda una universidad o parque industrial interrelacionado.
MAN	Metropolitan Area Network	Una ciudad o área metropolitana	Conexiones de operador que enlazan sedes empresariales o redes municipales.
WAN	Wide Area Network	Países o continentes	Redes de proveedores de servicios, enlaces troncales de Internet.
GAN	Global Area Network	Cobertura mundial	Infraestructura global de Internet, redes satelitales intercontinentales.

Nota. Ludeña, P., 2025.

Una de las principales características de esta clasificación es que cada red de orden inferior puede integrarse dentro de una red de mayor orden, por ejemplo: una red LAN forma parte de una red WAN. Adicionalmente, el alcance es condicionado por la tecnología de conexión física y los protocolos de interconexión empleados. Finalmente, conforme se avanza en el orden de las redes se aumenta la complejidad en términos de latencia, velocidad de conexión y gestión de dispositivos.

Una vez que hemos introducido la clasificación de los tipos de redes, es momento de profundizar en los tipos de redes que más se suelen usar para ejemplificar el funcionamiento de las redes actuales. Le invito a revisar la siguiente presentación interactiva que presenta de manera visual y comparativa las características fundamentales de las redes LAN y WAN, incluyendo ejemplos prácticos de su uso en el entorno doméstico, empresarial y global.

Tipos de Redes LAN y WAN

Como pudo constatar en la información, las redes LAN y WAN representan dos escalas diferentes pero complementarias de conectividad. Habrá notado que mientras las redes LAN optimizan la colaboración en espacios reducidos con alta velocidad y bajo retardo, las redes WAN amplían las posibilidades de comunicación a nivel geográfico, permitiendo que organizaciones distribuidas funcionen como una sola entidad. La reflexión final sobre sus actividades cotidianas le ha demostrado que, sin darse cuenta, utiliza ambos tipos de redes constantemente: desde compartir archivos en su hogar (LAN) hasta acceder a servicios globales como el sistema académico universitario (WAN).

1.2. Características de redes

En la actualidad, las redes no solo deben conectar dispositivos, sino que son deseables características que permitan tener una mejor experiencia como usuarios. Los usuarios modernos quieren que su conexión a redes de computadoras sea continua, eficiente y confiable, incluso en entornos dinámicos y exigentes como empresas, centros de datos, servicios de *streaming*, plataformas educativas, y sistemas financieros. Para profundizar en estos aspectos fundamentales, escuche atentamente el siguiente audio que explica de manera clara y práctica los cuatro pilares que sostienen el funcionamiento óptimo de las redes contemporáneas.

Los cuatro pilares esenciales de las redes modernas.

Como pudo escuchar en el audio, estos pilares trabajan de manera interdependiente para garantizar una experiencia de usuario óptima. Habrá notado que estos pilares no son conceptos aislados, sino que se complementan entre sí para crear redes robustas y eficientes. La introducción general que escuchó le ha proporcionado el contexto necesario para comprender por qué estas características son fundamentales en el diseño de redes contemporáneas.

A continuación, le presento cuatro pilares sobre los cuales se construyen las redes actuales:

1.2.1. Tolerancia a fallos

La tolerancia a fallas es la capacidad de una red para seguir funcionando correctamente, incluso cuando ocurren errores o fallos en alguno de sus componentes. Para ello, la red deberá limitar la cantidad de equipos que se ven afectados durante la falla y diseñar la mejor estrategia de recuperación rápida. Por esta razón, las redes modernas afrontan los fallos incorporando redundancia en su diseño, traducida como: múltiples caminos, enlaces duplicados, conmutadores de respaldo y protocolos que reaccionan automáticamente ante una interrupción.



Por ejemplo, si un enlace entre dos switches se interrumpe, protocolos como STP (Spanning Tree Protocol) redirigen el tráfico automáticamente por otra ruta disponible, sin afectar la conectividad del usuario final. Este comportamiento es vital en entornos críticos como hospitales, servicios de emergencia, centros bancarios o redes industriales, donde el fallo de una parte del sistema no puede, bajo ningún concepto, significar la caída total de la red.

1.2.2. Escalabilidad

La escalabilidad es la capacidad de una red para crecer y adaptarse, ya sea en términos de usuarios, equipos o aplicaciones, sin perder rendimiento ni requerir rediseños profundos. Esto implica que una red bien diseñada puede comenzar con 10 dispositivos, y escalar hasta miles, integrando nuevas sedes, servidores, dispositivos IoT, o servicios en la nube sin necesidad de rehacer todo desde cero. Para lograr la escalabilidad, las redes modernas deben seguir estándares internacionales y protocolos comunes, de tal forma que se pueda asegurar interoperabilidad con equipos de otros fabricantes. Otras estrategias de escalabilidad pasan por el uso de VLAN, direcciones IP

jerárquicas, subredes bien planificadas, redes modulares y protocolos de enrutamiento dinámico. También se recurre a soluciones virtualizadas y SDN (Software Defined Networking) para facilitar la expansión y el control centralizado.

1.2.3. Calidad de servicio

La Calidad de Servicio (Quality of Service – QoS) se refiere a la capacidad de una red para priorizar el tráfico de datos según su importancia o tipo, garantizando que los servicios críticos tengan la velocidad y disponibilidad que necesitan, especialmente en entornos congestionados. La congestión es un fenómeno que se presenta cuando el volumen de tráfico excede los recursos de la red, de tal forma que se pierden paquetes y se degrada el rendimiento.

La calidad de servicio es especialmente importante para las aplicaciones modernas que se centran en la transmisión de datos multimedia. Por ejemplo, en una videollamada, el tráfico de voz y video en tiempo real debe llegar sin retrasos ni interrupciones. QoS permite darle prioridad sobre otros tipos de tráfico, como descargas de archivos o navegación web, para ello se aplican políticas que clasifican, etiquetan y gestionan el tráfico en función de criterios como el protocolo, el puerto, la aplicación o el tipo de servicio y se configura los equipos intermediarios para que puedan priorizar el tráfico con base en estas políticas. En redes corporativas, educativas o gubernamentales, QoS es esencial para mantener la experiencia del usuario y la productividad operativa.

1.2.4. Seguridad

La seguridad en redes modernas implica una arquitectura completa que proteja los datos, dispositivos y usuarios frente a amenazas internas y externas, como accesos no autorizados, ataques cibernéticos, *malware*, suplantación de identidad y pérdida de información. Las instituciones que no consideran mecanismos de seguridad están expuestas a

ataques que pueden suponer grandes pérdidas económicas, sanciones legales y daños a su reputación.

En la actualidad el bien máspreciado es la información y por ende las redes por las cuales viaja, por tanto, ustedes como posibles administradores de red deberán afrontar entonces dos perfiles de seguridad: seguridad a nivel de infraestructura de red y seguridad de la información propiamente dicha.

- La **seguridad de infraestructura** incluye toda la parte física de los dispositivos y las interconexiones, y comprende no solo evitar el acceso no autorizado a las zonas de equipos o a los puertos de comunicación, sino también el proporcionar un ambiente adecuado para el correcto funcionamiento de los equipos.
- La **seguridad de la información** se encarga de proteger las estructuras de datos que se transportan por las redes y las que se encuentran archivadas en dispositivos de almacenamiento. Este tipo de seguridad debe cumplir tres requisitos fundamentales:
 1. **Confidencialidad:** asegura que únicamente los receptores previstos y con autorización puedan acceder a la información y leer su contenido.
 2. **Integridad:** garantiza que los datos permanezcan sin modificaciones durante su traslado desde el dispositivo inicial hasta el destinatario.
 3. **Disponibilidad:** implica que los usuarios autorizados puedan acceder a los servicios y a la información de manera fiable y en el momento oportuno.

En la figura 4, encontrará un mapa mental con las principales características que requieren las redes actuales.

Figura 4

Pilares fundamentales de las redes de computadoras modernas



Nota. Ludeña, P., 2025.

Como puede ver los cuatro pilares son: tolerancia a fallos, escalabilidad, calidad de servicio y seguridad. La tolerancia a fallos asegura la continuidad del servicio incluso ante errores o caídas de componentes, gracias a mecanismos de redundancia como enlaces duplicados, caminos alternativos y protocolos de recuperación automática, indispensables en sectores críticos como hospitales o bancos. Por su parte, la escalabilidad permite que una red pueda crecer en usuarios, equipos o aplicaciones sin perder rendimiento, aplicando estándares internacionales, direccionamiento jerárquico, redes modulares, VLANs y

tecnologías avanzadas como SDN, lo que facilita integrar desde pocos dispositivos hasta miles de equipos conectados globalmente.

A estos pilares se suman la calidad de servicio (QoS) y la seguridad. La QoS garantiza que los servicios esenciales, como videollamadas o aplicaciones en tiempo real, mantengan un rendimiento óptimo incluso en situaciones de congestión, mediante políticas que priorizan tráfico crítico sobre el no esencial. Finalmente, la seguridad protege tanto la infraestructura física de la red como la información que circula en ella, asegurando confidencialidad, integridad y disponibilidad de los datos frente a amenazas ciberneticas y accesos no autorizados. Estos elementos son esenciales para construir redes modernas, confiables y preparadas para los retos actuales y futuros.



Considere que debe implementar una red en una organización, ordene las características presentadas en esta guía en orden de importancia de acuerdo con su criterio. ¿De qué depende esa selección?

A medida que avanza en su formación como ingeniero en redes y analítica de datos, aprenderá a diseñar, configurar y optimizar redes que se cumplan con estas cuatro características fundamentales, permitiéndole construir infraestructuras robustas, inteligentes y preparadas para los desafíos del futuro digital.

1.3. Modelos de referencia



Imagine que quiere enviar un regalo de cumpleaños a un familiar que vive en otra ciudad, obviamente usted quiere que el paquete llegue intacto, al destinatario correcto y antes de la fecha de cumpleaños. Para lograr este cometido se deberán llevar a cabo varias etapas claramente identificadas.

Por ejemplo, una vez comprado el obsequio usted deberá ponerlo en una funda de regalo, posteriormente lo pondrá en una caja con material amortiguador si el regalo es frágil y pondrá en el paquete la guía de envío con la declaración del valor del paquete para poder tener el seguro de viaje. Ya en la oficina de envíos usted entrega el paquete y se le asignará un número de seguimiento para poder clasificarlo en los centros logísticos. A lo largo del viaje pasará por varios centros o incluso aeropuertos que determinarán la mejor ruta para que llegue a su destino. Al llegar a la ciudad de destino, se enviará al centro de distribución que lo pondrá en un vehículo específico para ser entregado en la puerta del destinatario. La acción compleja de enviar paquetería se divide en varias acciones coordinadas que realizan distintas oficinas, los esfuerzos individuales hacen que se obtenga el resultado deseado, este es el sentido del modelo de referencia. En el caso de las redes de computadores el problema es cómo llevar los datos de un dispositivo final a otro atravesando varios dispositivos intermediarios, medios y redes.

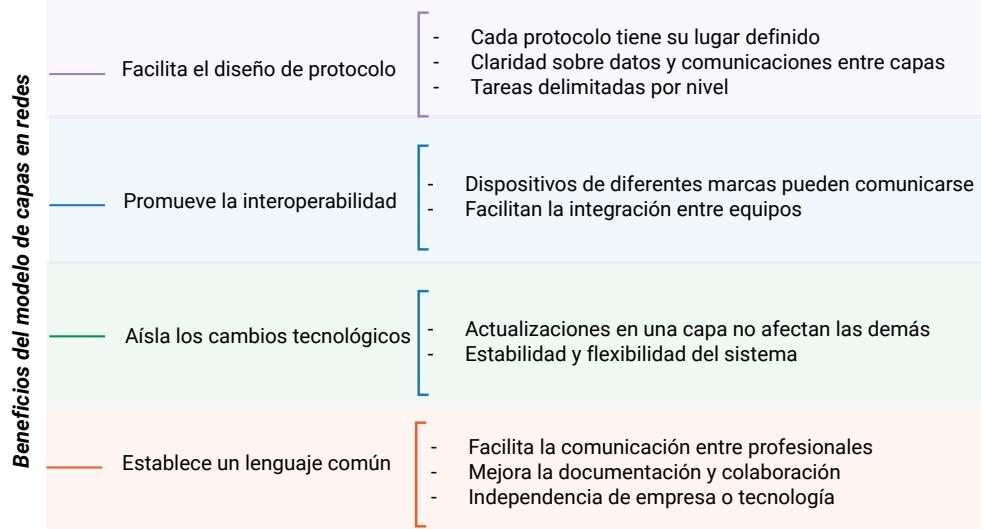
Un **modelo de referencia** funciona del mismo modo que el manual operativo de la empresa de mensajería: organiza todo el proceso en capas, asigna funciones concretas a cada etapa y normaliza los procedimientos para que cualquier oficina, en cualquier país, pueda integrarse sin contratiempos.

Cada capa se ocupará de solventar una parte de la solución y la coordinación entre capa dará la solución al problema. Así, siguiendo nuestra analogía, de la misma forma que el mensajero no necesita saber qué contiene la caja; solo le interesa su etiqueta y la ruta de entrega, en una red, cada capa se limita a gestionar su propia tarea y confía en que las demás cumplirán la suya. Esta separación de responsabilidades permite identificar fallos con rapidez, introducir nuevas tecnologías sin rediseñar todo el sistema y garantizar que, al igual que el regalo que quería enviar, los datos lleguen completos, seguros y a tiempo.

En la Figura 5, puede analizar un mapa mental que describe algunas ventajas de utilizar un modelo en capas para modelar las redes de computadores.

Figura 5

Beneficios del modelo de capas para abordar la interconexión de computadores



Nota. Ludeña, P., 2025.

Cada rama representa un beneficio específico, entre ellos tenemos: facilitar el diseño de protocolos, promover la interoperabilidad, aislar los cambios tecnológicos y establecer un lenguaje común, lo que permite que las redes se desplieguen y conecten todas las redes a nivel mundial.

Las funciones de cada capa se especifican a través de reglas, estas reglas conforman protocolos. Los protocolos usados en redes deben cumplir con algunos requisitos, entre ellos:

- Identificación de emisor y receptor a través del direccionamiento.

- Codificación de datos, que es convertir los datos en formas que puedan viajar en los medios.
- Formato y encapsulamiento estandarizado de estructuras de datos.
- Tamaño estandarizado de estructura de datos.
- Sincronización de envío. Los temporizadores son importantes para tareas como control de flujo, tiempos de respuesta y métodos de acceso.
- Opciones de entrega y, si fuera el caso, acuses de recibo.

El cumplimiento de requisitos dependerá de la capa en la que opere y la índole del protocolo, por ejemplo, si es de comunicaciones de red, de seguridad o de enrutamiento o de detección de servicios en general. Los protocolos deben poder trabajar unos con otros para poder garantizar la interconexión de computadores, por ello se diseñan para ser interoperables, comunicarse y proveerse servicios entre capas. El conjunto de protocolos que trabajan cooperativamente para conseguir un propósito de comunicación se denomina suite de protocolos.

A continuación, se presentan los modelos de referencia OSI y TCP/IP que son lo más usados en el ámbito de redes de computadores.

1.3.1. Modelo OSI

El modelo de interconexión de sistemas abiertos o simplemente modelo OSI por sus siglas en inglés (Open Systems Interconnection) es un marco de trabajo especificado en la ISO/IEC 7498-1 (ISO, 1994). OSI establece siete capas para el proceso de intercambio de datos entre computadores. En la Tabla 3, se pueden encontrar las funciones de las capas del modelo de mayor a menor: Aplicación, Presentación, Sesión, Transporte, Red, Enlace de datos y Física.

Tabla 3

Funciones y protocolos por capa del modelo OSI

Capa	Funciones principales	Protocolos usados
1. Aplicación	<ul style="list-style-type: none"> ▪ Provee servicios directos a los usuarios, es decir, de proceso a proceso (correo, transferencia de archivos, navegación web). ▪ Determina la sintaxis de los datos y mecanismos de autenticación de la aplicación. 	HTTP/S, FTP, SMTP, IMAP, DNS, Telnet, SNMP
2. Presentación	<ul style="list-style-type: none"> ▪ Provee una representación común a los datos que vienen de la capa de aplicación. ▪ Traduce datos entre formatos de la aplicación y formato de red (codificación ASCII/EBCDIC, conversión de imágenes, audio, video). ▪ Compresión y descompresión. ▪ Cifrado y descifrado de la información. 	SSL/TLS, JPEG, MPEG, ASCII, UTF-8
3. Sesión	<ul style="list-style-type: none"> ▪ Establece, administra y finaliza sesiones o diálogos entre aplicaciones en hosts distintos. ▪ Sincroniza la comunicación y gestiona puntos de restauración (checkpoints). ▪ Control de diálogo. 	RPC, NetBIOS, PPTP, SQL Net
4. Transporte	<ul style="list-style-type: none"> ▪ Segmenta y reensambla información; garantiza la entrega completa y ordenada. ▪ Control de flujo y de congestión. ▪ Puede ofrecer confiabilidad (orientación a conexión) o no (no orientada a conexión). 	TCP, UDP, SCTP

Capa	Funciones principales	Protocolos usados
5. Red	<ul style="list-style-type: none"> ▪ Direccionamiento lógico (IP). ▪ Enrutamiento lógico: determina la mejor ruta entre redes (subredes, dominios). ▪ Fragmentación de paquetes para adaptarse a diferentes tramos de red. 	IPv4, IPv6, ICMP, OSPF, RIP, BGP
6. Enlace de datos	<ul style="list-style-type: none"> ▪ Transfiere tramas entre nodos adyacentes en la misma red física. ▪ Control de acceso al medio (MAC), detección y corrección de errores de trama. ▪ Subcapas: LLC (Logical Link Control) y MAC (Media Access Control). 	Ethernet, IEEE 802.11, PPP, HDLC, Frame Relay, VLAN (802.1Q)
7. Física	<ul style="list-style-type: none"> ▪ Define características eléctricas, ópticas o de radio de la conexión (voltajes, pines, modulaciones). ▪ Conversión de bits en señales y viceversa. ▪ Sincronización de reloj y tasas de transmisión. 	10BASE-T, 1000BASE-X, DSL, T1/E1, RS-232, fibra óptica, radio Wi-Fi

Nota. Ludeña, P., 2025.

Frecuentemente, en la literatura de redes de computadores, las capas de este modelo se mencionan sólo por su número de orden y no por su nombre.

Retomando el ejemplo del servicio de paquetería, ahora asociaremos el proceso con el modelo de referencia OSI. El obsequio serían los datos que queremos enviar, la funda de regalo sería la capa de Aplicación, el material de amortiguación y la caja será la capa de Presentación. Cuando usted le pone la guía de envío está organizando cómo viajará el paquete igual que la capa de Sesión lo hace con los datos. La clasificación del paquete en el centro logístico es un proceso similar

a lo que ocurre en la capa de Transporte y luego la distribución que se hace en cada uno de los terminales es el mismo rol que la capa de Red realiza al determinar las mejores rutas para que el paquete llegue a destino. Finalmente, el agrupamiento de las cajas en la ciudad de destino es similar al proceso de la capa de Enlace y la entrega en la puerta del destinatario es lo que ocurre en la capa Física del modelo. Como se puede ver cada una de las capas se encarga de un proceso que contribuye al objetivo global.

1.3.2. Modelo TCP/IP

El modelo de referencia TCP/IP representa la base de cómo funciona Internet y es mantenido por la Internet Engineering Task Force en el RFC 1122 (IETF, 1989). Debe su nombre a los protocolos TCP e IP que son protocolos complementarios (Sánchez Rubio, 2020). En la Tabla 4, está la descripción de las capas de este modelo y su relación a la descripción de siete capas del modelo OSI.

Tabla 4

Relación entre las capas del modelo TCP/IP y las capas del modelo OSI

Capa	Funciones principales	Relación con OSI
Aplicación	<ul style="list-style-type: none"> ▪ Incorpora las capas 7, 6 y 5 del modelo OSI. ▪ Relación de aplicación de usuario a aplicación de usuario. ▪ Protocolos de servicios de red (HTTP, SMTP, FTP). 	Aplicación Presentación Sesión Transporte
Transporte	<ul style="list-style-type: none"> ▪ Fiabilidad de extremo a extremo, control de flujo, puertos de comunicación. ▪ Gestión de errores y reordenación de segmentos, si fuera el caso. 	Transporte

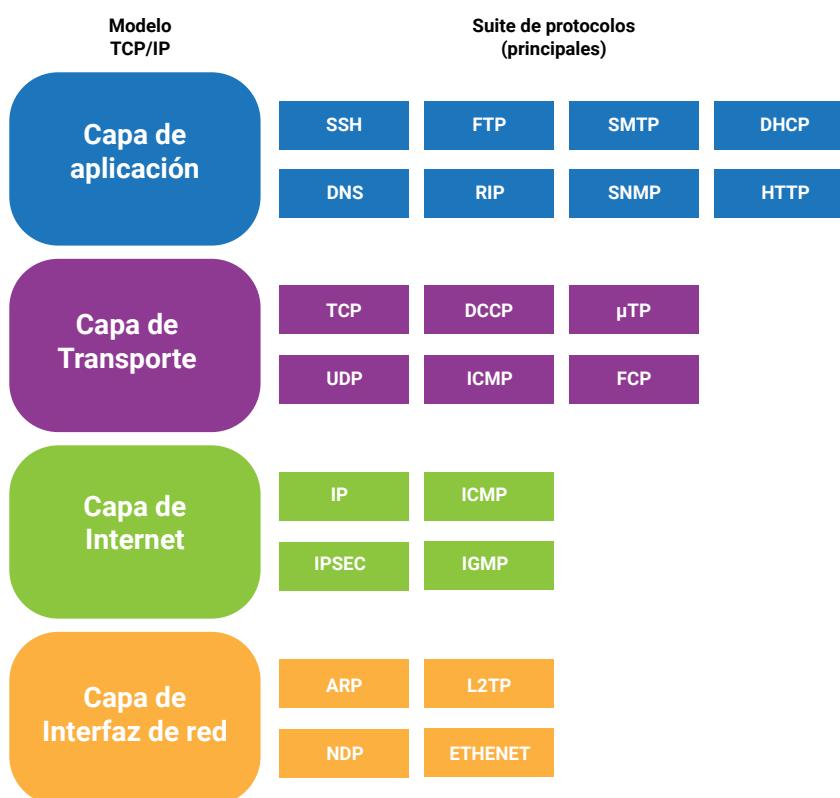
Capa	Funciones principales	Relación con OSI
Internet	<ul style="list-style-type: none"> ▪ Direccionamiento IP. ▪ Encaminamiento lógico global, fragmentación. 	Red
Acceso a red	<ul style="list-style-type: none"> ▪ Interacción con cualquier tecnología de red subyacente. ▪ Definición de tramas, MAC, acceso al medio y señalización física. 	Enlace de datos Física

Nota. Ludeña, P., 2025.

En la Figura 6, usted encontrará los principales protocolos que componen la suite TCP/IP, clasificados por capas funcionales, lo que facilita la comprensión de cómo fluye la información desde una aplicación hasta la red física.

Figura 6

Suite de protocolos para TCP/IP



Nota. Tomado de Suite de Protocolos TCP/IP [Ilustración], por GISEPROI, 2016, [WikimediaCommons](#), CC BY 4.0.

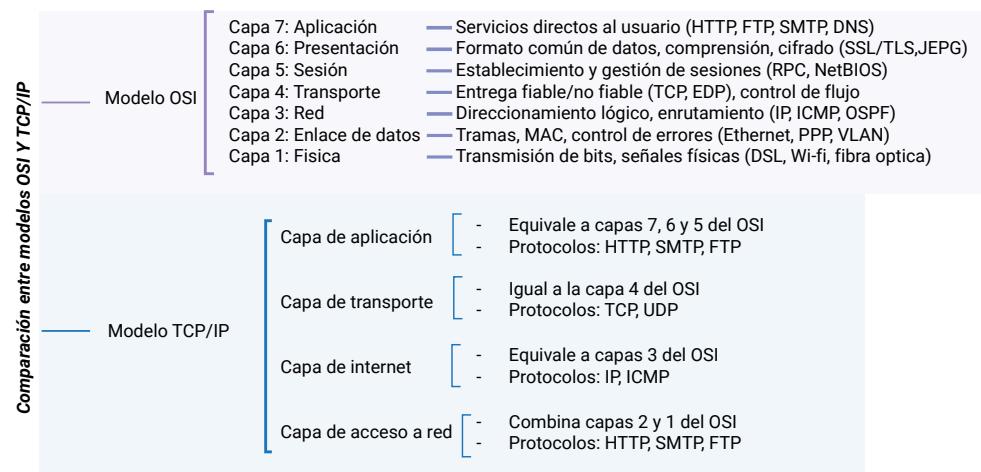
El modelo TCP/IP es la base de Internet y de prácticamente todas las redes modernas, por lo que su estudio es indispensable para estudiantes, profesionales y cualquier persona interesada en redes. Por ejemplo, puede notar que el protocolo Ethernet de las capas inferiores, luego puede conectarse con el protocolo IP de la Capa de Internet, que luego puede conectarse con UDP en capa de transporte y finalmente con DNS en Capa de Aplicación. Al visualizar los protocolos en sus respectivas capas, ya sean Aplicación, Transporte, Internet o Interfaz de Red, se clarifican los roles específicos que cada protocolo desempeña en el

proceso de comunicación de datos y como el trabajo coordinado entre capas permite que se consiga el objetivo de comunicación.

Ahora que hemos revisado los dos modelos de referencia, le invito a que analice el mapa mental de la Figura 7 donde se puede comparar las funciones de ambos modelos y los protocolos que se suelen utilizar en cada una de ellas.

Figura 7

Comparación estructural de los modelos de referencia OSI y TCP/IP



Nota. Ludeña, P., 2025.

Recuerde que las tres capas superiores del Modelo OSI para el Modelo OSI/TCP se unen en una sola capa y que las capas inferiores se unen en la de Acceso de Red, para darle simplicidad al modelo como se puede notar.

¿Es familiar alguno de estos protocolos para usted? ¿En qué contexto ha escuchado de alguno de estos protocolos?

¿Qué tanto sabe sobre modelos de referencia de redes de computadores?

En esta actividad realizará un repaso sobre las principales características de los dos modelos de referencia estudiados: OSI y TCP/IP. El siguiente módulo didáctico combina mapas conceptuales visuales con un quiz dinámico que le permitirá explorar de manera autónoma las similitudes, diferencias y aplicaciones prácticas de ambos modelos, evaluando al mismo tiempo su nivel de comprensión mediante preguntas contextualizadas.



Modelos de referencia por capas para la comunicación de redes

Como pudo experimentar en la herramienta interactiva, los modelos OSI y TCP/IP representan enfoques complementarios para comprender el funcionamiento de las redes.

Luego de desarrollar la actividad, conteste en su cuaderno de apuntes o en un documento de Word estas preguntas de reflexión:



- ¿De qué manera la estructura de siete capas del modelo OSI ayuda a comprender mejor el flujo de datos en una red, en comparación con la organización en cuatro capas del modelo TCP/IP?
- ¿Qué ventajas y desventajas presenta el modelo TCP/IP al ser más práctico y ampliamente adoptado frente al enfoque más teórico y detallado del modelo OSI?

1.4. Encapsulamiento

Imagine que envía un documento secreto a través de un servicio de mensajería: primero, se coloca en un sobre interno, luego en uno externo con la dirección, y finalmente en una caja resistente que la agencia de correo pueda transportar. Cuando la caja llegue al destino, el destinatario deberá realizar el proceso inverso, hasta llegar al documento propiamente dicho.

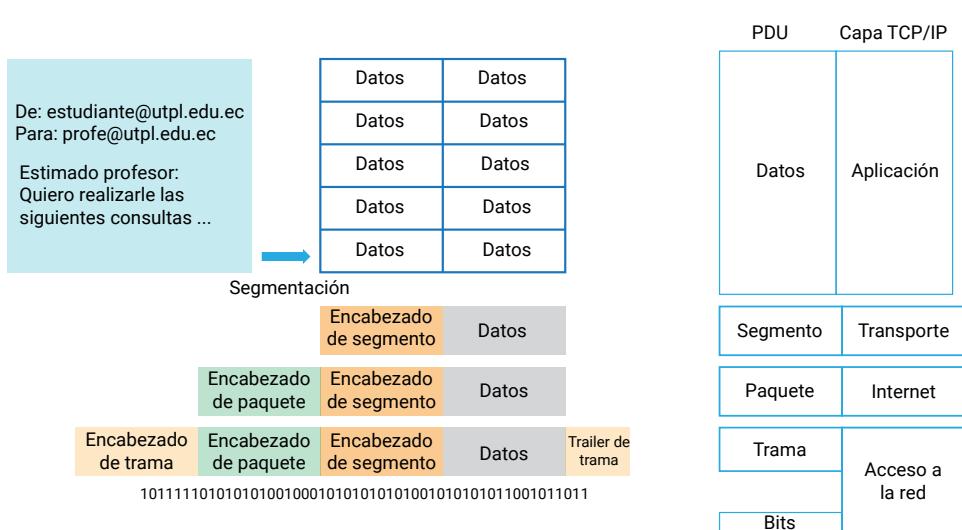
Este proceso es la perfecta analogía para el proceso de encapsulado, cada una de las capas incorpora bits al inicio (denominada cabecera) y a veces luego de los datos, con el objetivo de realizar las funciones propias de su nivel. La única consideración que debemos hacer es que, a diferencia del ejemplo, los datos no se envían como un todo, no es posible enviar los documentos completos. En redes, los datos enviados desde aplicaciones deben segmentarse en partes pequeñas que puedan ser transportadas en unidades de datos de protocolo (PDU por sus siglas en inglés) para que puedan ser manejadas por cada capa. Entonces, los datos de la aplicación se convierten en las siguientes PDUs sucesivamente: segmento (capa de transporte), paquete (capa de red), trama (capa de enlace) y finalmente bits (capa física).

En el host receptor se da el proceso inverso, el desencapsulamiento, en el cual cada capa elimina su encabezado y pasa la carga útil hacia arriba.

En la Figura 8, se puede ver el proceso de encapsulamiento en el envío de un correo electrónico. El correo se segmenta en partes de datos para enviarse a la capa de transporte.

Figura 8

Proceso de encapsulamiento de datos en el modelo TCP/IP



Nota. Ludeña, P., 2025.

Cada una de esas partes se encapsula añadiendo bits como cabecera en una estructura denominada segmento, y luego se pasa a la siguiente capa. En la capa de Internet se arma un paquete, poniendo un encabezado a la carga útil que viene de la capa de transporte. El paquete se pasa a la siguiente capa, donde se añade bits al inicio y al final para obtener una trama, la estructura de la trama dependerá del medio que se usa para interconectar los equipos. Finalmente, la trama se codifica en bits para enviar los datos sobre el medio de comunicación.

Le invito a ver el video titulado “[Proceso de encapsulamiento de datos en Modelos OSI y TCP/IP](#)”, en el cual se explica cómo se da el proceso de encapsulamiento y desencapsulamiento. Note que en el video se ejemplifica el proceso para la comunicación Web que usa los protocolos HTTP, TCP, IP y Ethernet. En cada capa se va agregando información crucial para que el mensaje pueda llegar al destino. Es interesante ver cómo actividades cotidianas tienen tras de sí, varias tareas que deben

desarrollarse de manera organizadas para que la comunicación fluya de manera eficiente.



Una vez que haya observado este proceso en acción a través del video, podrá responder con mayor fundamento la siguiente pregunta reflexiva: ¿Qué ventajas trae el proceso de encapsulamiento a la comunicación de datos?

Es momento de evaluar los conocimientos adquiridos durante la primera semana de estudio. A continuación, encontrará un juego interactivo de unir con líneas que le permitirá verificar su comprensión de los conceptos fundamentales sobre estructura de redes, tipos de dispositivos, modelos de referencia y características esenciales de las redes modernas.

Fundamentos de redes de computadores

Como pudo comprobar al completar el juego, dominar la terminología técnica es fundamental para construir una base sólida en el estudio de redes de computadoras. Su desempeño en este ejercicio refleja qué tan bien ha asimilado los fundamentos teóricos que le servirán como cimiento para los temas más avanzados que abordaremos en las próximas semanas. Si experimentó dificultades con alguna asociación, le recomiendo revisar nuevamente los recursos de la semana antes de continuar con los siguientes contenidos.



Actividades de aprendizaje recomendadas

Continuemos con el aprendizaje mediante su participación en las actividades que se describen a continuación:

Actividad 1. Comenzamos el camino a nuestra certificación

La asignatura Introducción a las redes es parte del componente de formación para la certificación de redes, y durante el transcurso del

ciclo, en paralelo, obtendremos la microcertificación de formación en el primer nivel CCNA de Cisco. Por tanto, en esta primera actividad deberá crear su cuenta en la plataforma de formación [Netacad](#) siguiendo los pasos que llegarán a su cuenta de correo institucional y revisando el siguiente manual: [anexo 1. Cómo crear una cuenta en academia Netacad](#). El objetivo es que pueda tener acceso a todo el material de consulta disponible en la plataforma, así como también las actividades interactivas como animaciones y verificadores de sintaxis para comandos; y también las evaluaciones de módulos y evaluación final que le permitirá obtener su microcertificación. Si tiene alguna dificultad en su registro, no dude en contactar con su tutor.

Actividad 2. Lectura de los contenidos propuestos

Ingresé a la plataforma [Netacad](#) y revise el módulo 1: Las redes en la actualidad y el módulo 3: Protocolos y modelos. El objetivo es que pueda reafirmar los contenidos teóricos sobre los conceptos básicos de redes y las características de redes. Adicionalmente, podrá revisar las bases de los modelos de referencia OSI y TCP/IP.

Estrategia de trabajo:

- Planifique un tiempo semanal para la lectura de los materiales sugeridos.
- Tenga a mano un cuaderno de apuntes o un documento Word donde pueda tomar nota de las ideas principales. Este material le será de mucha utilidad para cuando necesite hacer el repaso general en la semana 8.
- Desarrolle las actividades. Verifique su comprensión.
- Realice las autoevaluaciones disponibles para los módulos 1 y 3 con el objetivo de evaluar su comprensión sobre los contenidos.

Retroalimentación:

En las autoevaluaciones, la plataforma Netacad le corregirá las preguntas, indicando las respuestas erróneas. Esto le permitirá identificar cuáles son los conceptos que debe reforzar para que los vuelva a repasar.

Las actividades pueden ser repetidas cuantas veces sean necesarias hasta que usted se sienta satisfecho con sus resultados.

índice

I Bimestre

II Bimestre

Solucionario

Referencias



Sem 1 Sem 2 Sem 3 Sem 4 Sem 5 Sem 6 Sem 7 Sem 8



Semana 2

En esta semana revisaremos cómo configurar dispositivos para que se puedan comunicar entre sí. En la comunicación entre computadoras, cuando un paquete de datos se envía al destinatario, atraviesa varios dispositivos intermediarios, los cuales son los responsables de determinar los caminos por los cuales deberán retransmitirse las unidades de datos, de manera eficiente y segura hacia su destino. Tanto los dispositivos finales, como los intermediarios, deben tener configuradas sus interfaces y los protocolos de red que van a funcionar que van a intervenir en la comunicación.



Aprender a configurar estos equipos es fundamental en la tarea de administrar redes de computadoras y usted, como futuro ingeniero en Redes y Analítica de Datos, deberá garantizar que la infraestructura de red soporte tráfico masivo, análisis en tiempo real y servicios críticos sin interrupciones. Además, el dominio de la CLI y de las interfaces de administración le brinda una ventaja competitiva en el mercado laboral para desplegar redes y poder detectar fallos.

Para reforzar el tema de Configuración de dispositivos de red, puede revisar la bibliografía básica. A continuación, se detallará la configuración de los dispositivos que intervienen en la comunicación entre computadoras.

1.5. Configuración de dispositivos de red

Los equipos usados en red, ya sean: *router*, *switch* o *firewall*, son computadoras que tienen funciones y prestaciones específicas. Estos dispositivos ejecutan un Sistema Operativo de Red (*Network Operating*

Índice

I Bimestre

II Bimestre

Solucionario

Referencias

System NOS), durante el componente de redes de la malla curricular utilizaremos equipos Cisco para la experimentación, por tanto, usaremos el Cisco IOS como sistema operativo; y, con fines didácticos, usaremos el simulador Packet Tracer para poder desarrollar la parte práctica.

De manera muy simplificada, los dispositivos se dividen en tres componentes: *hardware*, *kernel* y *shell*. En la tabla 5, se realiza una descripción de cada uno de estos componentes.

Tabla 5

Componentes principales de un dispositivo de red

Componente	Descripción
Hardware	Parte física del dispositivo: chips de conmutación, interfaces, fuentes de poder.
Kernel	Administra CPU y memoria, decide cómo y cuándo reenviar los paquetes. Es la interfaz entre el hardware y el software del dispositivo.
Shell (CLI/GUI)	Interpreta los comandos que usted escribe y muestra los resultados.

Nota. Ludeña, P., 2025.

Las solicitudes que recibe el Shell pueden ser introducidas a través de la CLI (interfaz de línea de comandos) o GUI (interfaz gráfica de usuario). En CLI el usuario interactúa con el sistema operativo tecleando órdenes en forma de texto. Cada instrucción se introduce en un prompt y el dispositivo responde, también en texto, con información o confirmaciones. Usar CLI tiene como ventaja la rapidez, la automatización de tareas y la reducción de carga en el procesador, mientras que la desventaja es que se deben recordar los comandos y la sintaxis usada. La GUI, en cambio, presenta menús, botones, casillas y ventanas manipulables con el ratón o pantalla táctil. Su mayor ventaja es que resulta intuitiva y visual, adecuada para quienes se inician o necesitan un vistazo rápido a estadísticas de rendimiento. A cambio, puede limitar el acceso a opciones avanzadas y consumir más recursos.

1.5.1. Introducción a Cisco Internetwork Operating System (IOS)

Cisco IOS (Cisco, 2025), es el NOS que impulsa la mayoría de los routers y switches de nivel empresarial de Cisco. Apareció por primera vez en la década de 1980 y ha evolucionado hasta convertirse en un entorno muy potente. Cisco IOS se carga como imagen binaria en la memoria flash y se ejecuta íntegramente en RAM después del arranque.

Características de Cisco IOS

Entre sus características más relevantes tenemos las que se detallan en la siguiente infografía, que presenta de manera visual y organizada los aspectos técnicos fundamentales del sistema operativo Cisco IOS.

Características de Cisco IOS.

Como pudo observar en la infografía, el Cisco IOS presenta características técnicas que lo consolidan como un sistema operativo especializado para dispositivos de red. Habrá notado que cada elemento mostrado tiene un propósito específico en el diseño del sistema.

Una de las principales características de Cisco IOS es la compatibilidad de sintaxis, la cual permite que todos sus equipos manejen un grupo de comandos básicos, reduciendo así la curva de aprendizaje.

1.5.2. Sintaxis de un comando en Cisco IOS

La sintaxis es el formato que precisa qué elementos deben escribirse y cómo debe redactarse la orden para que el dispositivo la reconozca, interprete y ejecute. Al igual que en gramática, se define un uso del sujeto, verbo y complemento en la oración y se establecen unas relaciones entre ellos, así mismo la sintaxis en CLI definirá los elementos esenciales y relaciones entre ellos dentro de una instrucción.

1. **Palabras clave (keywords):** son términos específicos definidos en Cisco IOS, por tanto, se escriben literalmente como aparecen en la ayuda, por ejemplo: **show, interface, ip**. Funcionan como el verbo y los sustantivos de la oración. Las instrucciones usan palabras claves para especificar los comandos y subcomandos.
2. **Argumentos o parámetros:** valores no predefinidos que el usuario sustituye con valores específicos para completar la orden. Pueden ser palabras, números, valores o expresiones que especifican la naturaleza de la acción, por ejemplo: números de puerto, direcciones IP, nombres de host, contraseñas, etc. Podrían ser obligatorios u opcionales.
3. **Orden y jerarquía:** la posición de cada elemento es estricta, por lo cual cambiar el orden provoca un error de sintaxis.
4. **Convenciones tipográficas:**
 - a. **Negrita:** representan los comandos y las palabras clave.
 - b. **Cursiva:** representan los argumentos.
 - c. **Corchetes [a]:** indican elementosopcionales.
 - d. **Llaves {a}:** indican elementos obligatorios.
 - e. **Llaves y barra vertical { a |b }:** muestran alternativas exclusivas "a" o "b" (seleccione una).
 - f. **Corchetes, Llaves y barra vertical [a { b | c }]:** indican una elección de un elemento obligatorio "b" o "c" dentro de un elemento opcional "a".
 - g. **Angulares < > :** indican argumentos que se deben reemplazar con un valor específico.

- 5. Restricciones de contexto:** algunos comandos solo son válidos en modos de configuración específicos (por ejemplo, **ip address** dentro de la configuración de interfaz).

En la figura 9, se puede ver un ejemplo de la sintaxis para el comando **ip route** de Cisco IOS, el cual se usa para configurar rutas estáticas, con la opción de integrar entornos de Routing Virtual (VRF).

Figura 9

Ejemplo de sintaxis para el comando *ip route* en Cisco IOS

```
R1(config)#ip route [vrf <nombre-VRF>] {<IP-Dest> <Mask> | <IP-Dest>/<Pref>} {<SigSalto> | <IntSalto>} [name <Tag>]
    comando [tabla VRF opcional] {elección obligatoria para declarar destino} {elección obligatoria en definir ruta} [etiqueta opcional]
```

Ejemplo: Se añade una ruta estática en el router denominado R1 a la tabla de enrutamiento virtual "vrf_Clientes" que tiene como destino la red con dirección IP 192.168.10.0 y máscara 255.255.255.0 y prefijo /24, el siguiente salto es el router 2 con dirección 10.10.10.1 a la cual se llega por la interfaz de salida g0/1. No se pone una etiqueta a la ruta creada. Para la configuración de la ruta se usa la máscara de red y la especificación de la dirección del siguiente salto, entonces, la instrucción quedaría:

```
R1(config)#ip route vrf vrf_Clientes 192.168.10.0 255.255.255.0 10.10.10.1
```

Nota. Ludeña, P., 2025.

De acuerdo con la sintaxis el comando permite definir rutas de red precisas hacia destinos específicos, de dos opciones a escoger: una dirección de siguiente salto o una interfaz de salida y una dirección de siguiente salto. En el ejemplo de aplicación se puede ver su aplicación a un caso realista.

IMPORTANTE:

- Cisco IOS es “case-insensitive”, es decir, no distingue entre mayúsculas y minúsculas. Por lo tanto, escribir SHOW y show equivale a lo mismo.
- Para acceder a la ayuda contextual de Cisco IOS escriba el signo de interrogación “?” en la línea de comandos en cualquier punto del comando, esto presentará un listado de palabras válidas que se pueden usar en esa posición.

- Cisco IOS tiene un verificador sintaxis, si el usuario introduce un comando inválido presentará un error indicando que no se puede procesar la instrucción.
- Se pueden usar abreviaturas de comandos en instrucciones, siempre y cuando éstas no sean ambiguas y presenten confusión con otras palabras clave. Es necesario asegurarse de tener un mínimo de caracteres que hagan que el token sea único.
- Cisco IOS permite completar automáticamente un comando, siempre y cuando los caracteres ya escritos no presenten coincidencias con otros comandos, haciendo el token sea único.
- Los elementos de una instrucción se separan con espacios.
- Los comandos son especificados para cada modo de configuración específico, es decir que no todos los comandos pueden operar en toda la estructura de Cisco IOS.

Adicionalmente, Cisco IOS presenta un conjunto de atajos y combinaciones de teclas de acceso directo que usted puede consultar en la Tabla 6.

Tabla 6

Teclas de acceso rápido y atajos útiles en la configuración de dispositivos con Cisco IOS

Tecla / Combinación	Acción inmediata	Uso frecuente / Comentario práctico
Tab	Autocompleta la palabra clave o argumento.	Ahorra tecleo y evita errores ortográficos.
?	Muestra ayuda contextual para la posición actual del cursor.	Indispensable cuando no recuerda la sintaxis exacta.
Ctrl + P ó ↑	Recupera el comando anterior en el historial.	Repite o edita órdenes recientes sin volver a escribirlas.

Tecla / Combinación	Acción inmediata	Uso frecuente / Comentario práctico
Ctrl + N ó ↓	Avanza al siguiente comando del historial.	Útil tras retroceder varias entradas.
Ctrl + A	Mueve el cursor al inicio de la línea.	Permite insertar texto al principio de un comando largo.
Ctrl + E	Mueve el cursor al final de la línea.	Agiliza la edición cuando el cursor quedó en mitad del texto.
Ctrl + B	Retrocede un carácter.	Ajuste fino sin usar flechas en terminales antiguas.
Ctrl + F	Avanza un carácter.	Idem anterior, en dirección opuesta.
Esc + B	Retrocede una palabra completa.	Navegación rápida por segmentos largos.
Esc + F	Avanza una palabra completa.	Igual que el anterior, hacia adelante.
Ctrl + U o Ctrl + X	Borra desde el cursor hasta el inicio de la línea.	Reescribe por completo sin volver a llamar al historial.
Ctrl + K	Borra desde el cursor hasta el final de la línea.	Cancela la parte sobrante de un comando mal tecleado.
Ctrl + W	Elimina la palabra situada antes del cursor.	Corrige rápidamente un argumento aislado.
Ctrl + R	Repite y refresca la línea actual en pantalla.	Muy útil si la salida de logs rompe la visibilidad del prompt.
Ctrl + L	Limpia la ventana (redibuja la pantalla).	Mejora la lectura cuando hay paginado excesivo.
Ctrl + C	Interrumpe la operación o comando en curso.	Detiene un ping o sale de un menú de configuración.
Ctrl + Shift + 6	Rompe procesos prolongados (p. ej., ping continuo).	Detiene rápidamente pruebas o traceroutes extensos.
Ctrl + Shift + 6 luego X	Suspende una sesión Telnet/SSH anidada y vuelve al dispositivo anterior.	"Escapatoria" cuando se encadena acceso a varios equipos.
Ctrl + Z	Finaliza el modo de configuración y regresa al prompt EXEC privilegiado (#).	Atajo clásico para "salir y guardar" sin exit sucesivos.
Enter (en paginación)	Avanza una línea cuando aparece --More--.	Examina resultados con detalle.

Tecla / Combinación	Acción inmediata	Uso frecuente / Comentario práctico
Barra espaciadora	Avanza una página completa en la salida con --More--.	Recorre listados largos con rapidez.

Nota. Adaptado de *Entrenamiento intensivo sobre IOS*, por Instituto Sa Palomera, 2020, [sapalomera](#).

Los comandos de acceso rápido y métodos abreviados más usados son Ctrl+Z para interrumpir los procesos, el TAB para completar los comandos, la Barra espaciadora para visualizar páginas completas de información y las flechas para recuperar comandos, mientras más practique su uso, más habilidad tendrá en la configuración de equipos.

1.5.3. Acceso a Cisco IOS

El modo CLI de Cisco IOS es la única puerta de entrada de todas las operaciones de configuración y monitoreo de equipos Cisco, por tanto, es fundamental que usted conozca cómo poder acceder a esta interfaz. Existen tres mecanismos de acceso para acceder a Cisco IOS: consola, Telnet y SSH. Estas vías describen dos procesos diferentes: acceso local y acceso remoto.

1.5.3.1. Acceso local

Este proceso, llamado también “fuera de banda”, es realizado a través del puerto de consola. A través de consola se puede realizar la configuración de equipos desde 0, es decir, su disponibilidad no depende de que las interfaces estén activas ni de que exista conectividad LAN/WAN; por ello resulta imprescindible para la puesta en marcha, la recuperación de contraseñas y la resolución de fallos graves.

Físicamente, los dispositivos más antiguos ofrecen un conector RJ-45 rotulado como CONSOLE, al que se conecta un cable directo cuyo trenzado invierte el orden de los pines y termina en un adaptador DB-9 (serial). Si su ordenador carece de puerto serie, ese adaptador

se convierte mediante un conversor USB-a-serial en un puerto COM virtual. En equipos modernos, estos enlaces se simplifican con puertos mini-USB o USB-C, lo que elimina la necesidad de cables especiales y aprovecha controladores FTDI que el sistema operativo de su ordenador detecta automáticamente. En la Figura 10 usted puede ver la ubicación del puerto de consola en la parte posterior de un router marca Cisco, el cable azul plano conectado al puerto es un cable de consola RJ-45 a DB9, característico de la marca Cisco.

Figura 10

Ubicación del puerto de consola en un router Cisco serie 2800



Nota. Tomado de *Cisco 2800 close-up - IMG 1009 [Fotografía]*, por Jemimus, 2006, [WikimediaCommons](#), CC BY 4.0.

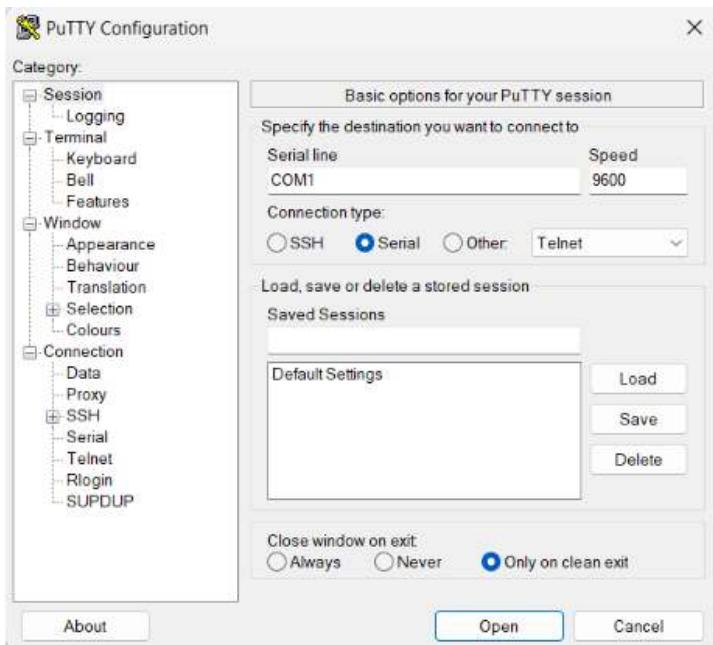
El puerto suele estar etiquetado como “CONSOLE” y se encuentra próximo a los puertos auxiliares o Ethernet, como se aprecia claramente en la imagen.

Una vez establecido el enlace físico, se requiere un programa de emulación de terminal. En Windows resultan habituales PuTTY, Tera Term o SecureCRT; en Linux y macOS basta el comando screen o utilidades como minicom. Todos ellos dialogan con el puerto COM virtual configurado, aplicando siempre los parámetros predeterminados de

Cisco: 9600 baudios, 8 bits de datos, sin paridad, 1 bit de parada y sin control de flujo (es decir, "9600 8 N 1"), en la Figura 11, puede ver cómo se configura el acceso serial a consola desde la herramienta PuTTY.

Figura 11

Configuración de sesión serial en PuTTY para acceso por consola a dispositivos de red



Nota. Ludeña, P., 2025.

Si al abrir la sesión la salida se muestra ilegible, conviene probar otras velocidades (19 200, 38 400 o 115 200 bps) hasta encontrar texto coherente; esto es más frecuente cuando el administrador anterior ajustó los parámetros y no lo documentó.

El flujo típico consiste en conectar el cable, lanzar el emulador de terminal, seleccionar el puerto COM y presionar Enter hasta que aparezca el prompt Router> o el asistente de configuración inicial. Desde ese estado ya se puede navegar por el Cisco IOS.

1.5.3.2. Acceso remoto

Cuando el administrador no está físicamente junto al dispositivo de red que quiere monitorear, se habilita el acceso remoto a través de líneas VTY. Las líneas VTY son líneas terminales virtuales que aceptan conexiones a través de protocolos de acceso remotos como son Telnet o SSH. A diferencia de la conexión local, la conexión remota exige que al menos una interfaz activa tenga configurada una dirección IP, una puerta de enlace por defecto (default Gateway) y una ruta entre su red local y la red donde se encuentra el administrador. Es aconsejable que la línea VTY cuente con autenticación mínima, es decir, usuario local y contraseña; y, si fuera el caso clave de cifrado, esto dependerá del protocolo que se está usando.

- a. **Telnet:** este protocolo transmite tanto las credenciales como todo el tráfico en texto plano, usando el protocolo TCP en el puerto 23 en capa de transporte. Basta con declarar una contraseña en las líneas VTY, activar login y permitir especificar el protocolo a usar, como se puede ver en la Figura 12.

Figura 12

Configuración de acceso telnet en un dispositivo Cisco

```
switch(config)#line vty 0 15
switch(config-line)#password ClaveVTY
switch(config-line)#login
switch(config-line)#transport input telnet
```

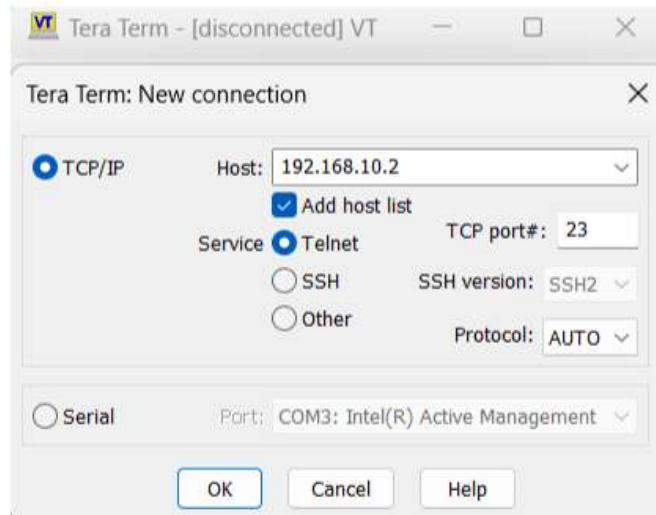
Nota. Ludeña, P., 2025.

De cara al cliente, para acceder con Telnet al equipo se puede usar emuladores de terminal como PuTTY o Tera Term y configurar el cliente apropiado (ver Figura 13); o, a través de líneas de comandos desde Linux o Windows. Telnet tiene como desventaja la inseguridad inherente a transmitir en texto plano, puesto que una herramienta de análisis de tráfico podría capturar las credenciales y acceder a la sesión, o inclusive

directamente leer los datos que están siendo enviados y modificarlos. Por ello, el uso de Telnet se reduce hoy a laboratorios aislados o a situaciones de emergencia cuando no se dispone de otro método.

Figura 13

Acceso remoto por Telnet desde Tera Term a un dispositivo de red



Nota. Ludeña, P., 2025.

- b. **Secure Shell (SSH):** el protocolo SSH cifra todo el tráfico usando algoritmos como AES, de esta forma protege los datos contra espionaje y manipulación. SSH usa el protocolo TCP en el puerto 22 en la capa de transporte. Para habilitar SSH es necesario establecer credenciales, activar login y además crear las llaves de encriptación. En la Figura 14, está la configuración de habilitación de SSH, como usted puede constatar la configuración es mucho más compleja que para el protocolo Telnet.

Figura 14

Configuración del acceso seguro por SSH en dispositivos Cisco

```
switch(config)#ip domain-name redesUTPL.edu
switch(config)#crypto key generate rsa
% You already have RSA keys defined named
switch.redes.edu .
% Do you really want to replace them? [yes/no]: yes
The name for the keys will be: switch.redesUTPL.edu
Choose the size of the key modulus in the range of
360 to 4096 for your
General Purpose Keys. Choosing a key modulus
greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-
exportable...[OK]

switch(config)#ip ssh version 2
*Mar 1 0:9:45.937: %SSH-5-ENABLED: SSH 2 has been
enabled
switch(config)#username admin secret S3gura!
switch(config)#line vty 0 15
switch(config-line)#login local
switch(config-line)#transport input ssh
```

Nota. Ludeña, P., 2025.

Para el acceso al equipo a través de SSH, se puede acceder con OpenSSH (ssh admin@192.168.10.1), PuTTY, SecureCRT, KiTTY, MobaXterm, Termius o cualquier cliente compatible con claves públicas. Usar SSH tiene complejidad en la gestión de claves y algoritmos de cifrado, sin embargo, es un bajo precio a pagar, por el beneficio que se obtiene en cuanto a privacidad y reducción de riesgo de ataques de suplantación.

En la Tabla 7, usted podrá revisar la comparación sobre las características de Telnet y SSH.

Tabla 7

Comparación entre Telnet y SSH

Característica	Telnet	SSH
Cifrado	Ninguno (texto claro)	Completo (confidencialidad e integridad)
Puerto TCP	23	22
Autenticación	Solo contraseña	Contraseña y/o clave pública
Copia de archivos	Ninguna	SCP/SFTP integrados
Uso recomendado	Laboratorio cerrado, dispositivos muy antiguos	Producción, redes públicas, exigencias de cumplimiento
Riesgo principal	Captura de credenciales, manipulación de sesión	Gestión inadecuada de claves; mayor uso de CPU

Nota. Ludeña, P., 2025.

Con base en lo revisado, reflexione sobre el uso de estos protocolos: cuando usted introduce una contraseña mediante Telnet y sabe que viaja en texto claro, ¿qué responsabilidad ética asume sobre la información y los usuarios que dependen de esa red? Ahora bien, ¿qué impacto tendría que un atacante intercepte las credenciales de administración por Telnet? Si en su organización educativa o laboral, quisiera migrarse al uso de SSH, ¿qué acciones concretas se tomarían en este proceso para no interrumpir la operación normal de la red? Y finalmente, usted como futuro profesional en Redes y Analítica de Datos, ¿de qué manera aprovecharía los registros de sesión que se obtienen de SSH para elaborar métricas de uso y detectar patrones de ataque?

¿Qué método de acceso usar?

En su ejercicio profesional seguramente le tocará interactuar con equipos de redes, para ello esta actividad se ha diseñado para que usted pueda determinar en qué situaciones deberá usar el acceso por consola y en qué situaciones deberá optar por ingresar por Telnet o SSH.



Checklist para determinar qué método de acceso utilizar

Como pudo analizar durante el juego interactivo, la elección del método de acceso correcto depende de múltiples factores contextuales y de seguridad. Habrá notado que el acceso por consola es fundamental en situaciones donde la conectividad de red no está disponible o cuando se requiere configuración inicial, mientras que Telnet/SSH son apropiados para administración remota cuando ya existe conectividad de red establecida.

Luego de desarrollar la actividad, a su criterio responda en su cuaderno de apuntes o en un documento de Word las siguientes preguntas:



- ¿Cuál es el mejor método para realizar la configuración inicial de equipos?
- Considerando las características de los métodos de acceso ¿cuál es el método más seguro y por qué?

1.5.4. Navegación básica en Cisco IOS

Cisco IOS tiene una estructura jerárquica de modos de ejecución de comandos. Hay tres modos de principales:

1. **Modo EXEC de usuario:** modo inicial al acceder al dispositivo, con comandos básicos de monitorización. Desde este modo se puede acceder al modo de EXEC con privilegios con el comando enable.

2. **Modo EXEC privilegiado:** permite acceder a todos los comandos, incluyendo configuración y administración. Desde este modo se puede acceder al modo de configuración global usando el comando configure terminal.
3. **Modos de configuración:** permiten modificar la configuración del dispositivo, como la configuración global, de interfaz, etc. Desde este modo se puede acceder a los modos de subconfiguración de línea y de interfaz.

En la Tabla 8, puede ver el detalle de estos niveles y sus características principales.

Tabla 8

Estructura jerárquica de los modos de operación en Cisco IOS

Nivel	Prompt típico	Permisos	Uso frecuente
Modo de ejecución de usuario	Switch>	Lectura	Ver estado: ping, show ip int brief.
(User EXEC)			
Modo de ejecución con privilegios	Switch#	Lectura + escritura global	Copiar archivos, reiniciar: show run, copy.
(Privileged EXEC)			
Configuración global	Switch(config)#	Cambios permanentes	Configurar hostname, enable secret, banner motd.
(Global Config)			
Subconfiguración	Switch(config-if)#	Ajustes puntuales	Configurar VLAN, puertos, activación de interfaces
	Switch(config-line)#		Establecer contraseñas para acceso a través de líneas

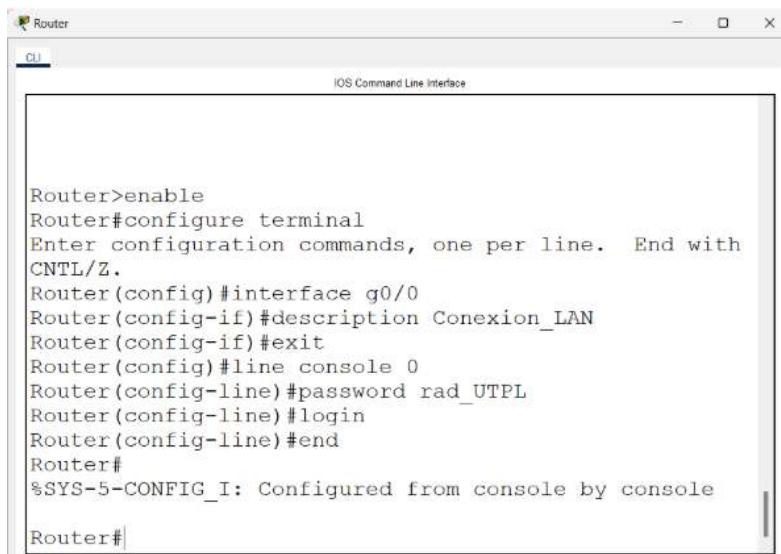
Nota. Ludeña, P., 2025.

Para retornar a un modo se usa el comando exit y para volver directamente al modo EXEC con privilegios desde un modo de

subconfiguración se usa el comando end o las teclas Ctrl + Z. En la Figura 15, puede revisar un ejemplo completo de navegación donde se ve los comandos de acceso a los niveles de ejecución hasta los niveles de subconfiguración y los comandos de retorno a niveles.

Figura 15

Ejemplo de navegación y configuración en Cisco IOS desde la CLI



```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with
CTRL/Z.
Router(config)#interface g0/0
Router(config-if)#description Conexion_LAN
Router(config-if)#exit
Router(config)#line console 0
Router(config-line)#password rad_UTPL
Router(config-line)#login
Router(config-line)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#|
```

Nota. Ludeña, P., 2025.

La configuración se realiza para la interfaz g0/0, es decir, la Gigabit Ethernet identificada con 0/0 y se le da configura una descripción que permita identificar la funcionalidad. Además, se configura la línea de consola con contraseña y se solicita que se pida la contraseña para acceder.

IMPORTANTE:

En su paso por el eje de formación en redes de telecomunicaciones, comenzando por la asignatura de Introducción a las redes, le recomendamos mantener un **cuaderno de ingeniería** personal

donde registre, de forma clara y ordenada, todos los comandos de configuración que vaya aprendiendo. Este cuaderno puede ser digital o físico, y debe incluir desde comandos básicos como los usados para navegación entre modos de ejecución, configuraciones básicas como asignación de direcciones IP; hasta comandos más complejos relacionados con protocolos de enrutamiento, diagnóstico de red y gestión de dispositivos. Más allá de ser una simple libreta de apuntes, este recurso se convierte en un registro técnico valioso que refleja su evolución en el dominio de las tecnologías de redes.

El cuaderno de ingeniería le servirá como guía de consulta rápida, especialmente cuando enfrente escenarios reales donde deberá configurar o solucionar problemas en redes más complejas. A futuro, como profesional en Redes y analítica de datos, contar con este repositorio personal de conocimiento facilitará la implementación de soluciones, la documentación de proyectos y la preparación para certificaciones como Cisco CCNA. Además, refleja una actitud profesional orientada al orden, la trazabilidad y la mejora continua, siendo estas tres cualidades altamente valoradas en el mundo laboral.

1.5.5. Configuración básica de dispositivos

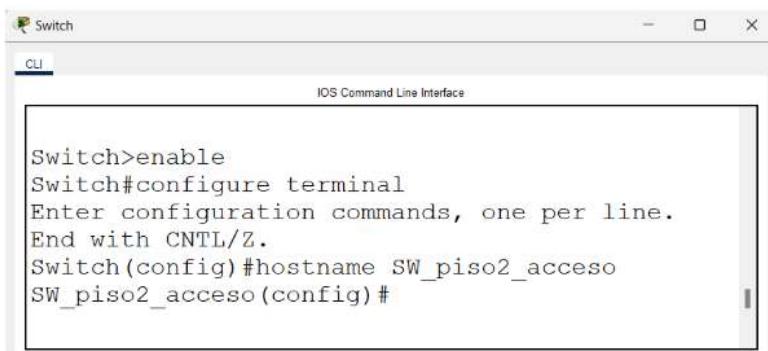
La configuración de dispositivos se realiza desde el modo de configuración global y se almacenará en el archivo running-config en la memoria volátil del equipo. Toda configuración siempre partirá de una planificación previa de la topología que se desea implantar en la red. Es necesario que se documente todo el proceso de configuración para que se construya un archivo histórico de la red para que pueda ser utilizado para un análisis posterior ya sea por fallos o repotencialización de la red.

El primer paso para la configuración suele ser la individualización del nombre del dispositivo, puesto que todos los equipos por defecto tienen el mismo nombre de fábrica, por ejemplo, un router Cisco tiene como nombre "Router" y un switch "Switch". En la Figura 16 puede ver el ejemplo de configuración del nombre de equipo para un Switch Cisco 2960.

Asignar un nombre descriptivo facilita la identificación del equipo en el diagnóstico remoto y automatiza la generación de inventarios.

Figura 16

Asignación de nombre a un switch Cisco mediante CLI



```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
Switch(config)#hostname SW_piso2_acceso
SW_piso2_acceso(config)#
```

Nota. Ludeña, P., 2025.

El usuario empieza accediendo al modo privilegiado con el comando enable, seguido de configure terminal para ingresar al modo de configuración global. Luego, se ejecuta el comando hostname SW_piso2_acceso, lo cual cambia el nombre del switch al indicado. Inmediatamente, el prompt cambia para mostrar el nuevo nombre, indicando que el cambio fue aplicado con éxito.

IMPORTANTE:



- El nombre del equipo debe iniciar con una letra.
- No se permiten espacios en blanco.
- Tiene que concluir con una letra o un número.
- Solo puede contener letras, números y guiones.
- La longitud total no puede alcanzar los 64 caracteres.
- Aconsejable que se incluya ubicación, función y nivel, por ejemplo, "SW_piso2_acceso".

Como vimos en la Sección 1.5.3 de esta Guía Didáctica, existen varias formas de acceder a Cisco IOS y desde el sistema operativo podemos controlar la función del equipo, por esto, es importante dotar de seguridad el acceso al mismo. La seguridad básica es establecer una contraseña para el acceso tanto a la línea de consola como a las líneas VTY activando el comando `login`, y de modo de ejecución de usuario al modo de ejecución con privilegios. De acuerdo con estudios, el 80% de los accesos no autorizados en redes pequeñas se debe a contraseñas débiles o a que los usuarios dejan contraseñas por defecto. Por esta razón es necesario que se creen contraseñas fuertes y que se establezcan mecanismos de protección para evitar la violación de contraseñas. El ataque más frecuente suele ser a través de fuerza bruta, por esta razón es aconsejable limitar el número de intentos fallidos en un lapso de tiempo a través de la instrucción `login block-for <tiempo_bloqueo_seg> attempts <intentos> within <lapso_seg>`. En la Figura 17, puede ver la configuración de contraseñas para las líneas de acceso al sistema operativo de equipos Cisco.

Figura 17

Configuración de contraseñas en líneas de consola y VTY en un switch Cisco

```
Switch1
CLI
IOS Command Line Interface

SW_piso2_acceso>enable
SW_piso2_acceso#configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
SW_piso2_acceso(config)#enable secret
Rad_u7p1$L
SW_piso2_acceso(config)#line console 0
SW_piso2_acceso(config-line)#password COnsola!
SW_piso2_acceso(config-line)#login
SW_piso2_acceso(config-line)#exit
SW_piso2_acceso(config)#line vty 0 4
SW_piso2_acceso(config-line)#password
Vty@Acceso
SW_piso2_acceso(config-line)#login
SW_piso2_acceso(config-line)#transport input
ssh
SW_piso2_acceso(config-line)#exit
SW_piso2_acceso(config)#login block-for 180
attempts 3 within 10
```

Nota. Ludeña, P., 2025.

El usuario empieza accediendo al modo privilegiado con el comando enable, seguido de configure terminal para ingresar al modo de configuración global. Luego, se ejecuta el comando enable secret para establecer una contraseña para acceder al modo de usuario con privilegios. Y a continuación, se configuran las líneas de acceso, estableciendo contraseñas. Finalmente, el acceso se bloquea luego de 3 intentos fallidos.

IMPORTANTE:

- Es recomendable que las contraseñas para equipos en producción tengan entre 10 a 12 caracteres.
- Deben ser una mezcla de mayúsculas, minúsculas, números y símbolos.
- La contraseña debe ser única, no reutilizar las contraseñas de otros servicios.
- Cambiar frecuentemente las contraseñas o tras cambios de personal.
- Se puede configurar contraseñas con el comando password que escribirá las almacenará en texto plano o con el comando secret que las almacenará encriptadas.

Es recomendable poner un mensaje disuasorio que anuncie una política de bloqueo o advertencias con consecuencias legales por el acceso no autorizado a los equipos, dichos mensajes se pueden configurar a través de un banner usando el comando Banner motd #<Aviso>#. También, es importante limitar el tiempo de inactividad con exec-timeout <minutos> <segundos> y activar logging synchronous para que los mensajes no interrumpan la escritura. En la Figura 18, puede ver las configuraciones indicadas para un switch, donde luego de 3 minutos de inactividad se desconectará la línea de consola, de igual forma se puede configurar esta opción para líneas VTY.

Figura 18

Configuración de tiempo de inactividad y mensaje de advertencia en un switch Cisco

The screenshot shows a terminal window titled "Switch" with the title bar "CLI" and "IOS Command Line Interface". The window displays the following configuration session:

```
SW_piso2_acceso>enable
SW_piso2_acceso#conf t
Enter configuration commands, one per line. End with
CTRL/Z.
SW_piso2_acceso(config)#
SW_piso2_acceso(config)#
SW_piso2_acceso(config)#
SW_piso2_acceso(config)#line console 0
SW_piso2_acceso(config-line)#logging synchronous
SW_piso2_acceso(config-line)#exec-timeout 3 0
SW_piso2_acceso(config-line)#exit
SW_piso2_acceso(config)#! banner motd #
Enter TEXT message. End with the character '#'.
*****
** Acceso restringido. Todo uso ser monitoreado y
registrado.
Usuarios no autorizados sern procesados segn la ley.
*****
```

The configuration includes enabling global configuration mode, entering configuration mode, setting the console line to log synchronous messages, and defining an exec timeout of 3 minutes and 0 seconds. It concludes with a banner message indicating restricted access and legal consequences for unauthorized users.

Nota. Ludeña, P., 2025.

El usuario accede al modo de configuración global con conf t y luego entra a la línea de consola (line console 0). Allí, habilita la sincronización de mensajes del sistema con el comando logging synchronous, y configura la desconexión automática por inactividad con exec-timeout 3 0, lo que significa 3 minutos y 0 segundos.

Después, sale del modo de línea con el comando exit; y, utiliza el comando banner motd # para crear un mensaje de advertencia. El mensaje, delimitado por el símbolo #, indica que el acceso está restringido, será monitoreado y que los usuarios no autorizados serán procesados legalmente.

Las contraseñas que se crean con el comando password se escriben en texto plano, es decir, que si alguien accede al archivo de configuración

puede leer las contraseñas. Por eso es importante encriptar las contraseñas añadiendo el comando `service password-encryption`, el cual cifrará las credenciales en la NVRAM.

Todas las configuraciones realizadas se escriben en el archivo `running-config`, el cual se almacena en la memoria RAM del dispositivo. Esto significa que si bien es cierto todas las configuraciones son efectivas inmediatamente, no se guardan automáticamente y si el equipo se reinicia se perderán las configuraciones realizadas. Si se quieren conservar las configuraciones es necesario que se copien al archivo `startup-config`. Este archivo se almacena en la memoria NVRAM del equipo y permite que el dispositivo retenga la configuración incluso después del apagado o reinicio del mismo. Para pasar las configuraciones se usará el comando **copy** `running-config startup-config`.

Ahora reflexione las siguientes preguntas: ¿Qué nivel de confianza siente usted al utilizar la CLI de Cisco IOS después de los ejercicios practicados, y cuáles comandos considera indispensables para su futura labor como ingeniero en Redes y Analítica de Datos? Al comparar la interfaz de línea de comandos con herramientas gráficas de administración, ¿Se le dificultó usar la CLI? ¿en qué situaciones profesionales cree usted que la CLI aportará mayor agilidad o precisión en la resolución de problemas? ¿Qué estrategias personales (por ejemplo, atajos de teclado, plantillas de configuración, guías de sintaxis) piensa implementar para mejorar su velocidad y reducir errores al configurar dispositivos en entornos reales?



Actividades de aprendizaje recomendadas

Reforcemos el aprendizaje resolviendo las siguientes actividades.

Actividad 1. Lectura de los contenidos propuestos

Ingresé a la plataforma [Netacad](#) y revise el módulo 2: Configuración básica de switches y terminales. El objetivo es que pueda reafirmar los contenidos teóricos sobre los conceptos básicos de redes y las características de redes. Adicionalmente, podrá revisar las bases de los modelos de referencia OSI y TCP/IP.

Estrategia de trabajo:

- Reserve un momento cada semana para revisar los materiales recomendados.
- Utilice un cuaderno o un documento digital para anotar las ideas clave; este registro será especialmente útil para repasar antes de la evaluación en la semana 8.
- Complete las secciones. Verifique su comprensión y comprobador de sintaxis del módulo.
- Realice la autoevaluación del módulo 2 para medir su nivel de aplicación de los comandos presentados en esta unidad.

Retroalimentación:

Al acabar la autoevaluación, la plataforma le mostrará qué respuestas fueron incorrectas, ayudándole a identificar los temas que requieren mayor atención. Recuerde que puede repetir las actividades las veces que considere necesarias hasta alcanzar un dominio satisfactorio del contenido.

Actividad 2. ¡Configuremos equipos!

En esta actividad resolveremos un problema típico de redes. Imagine que ha sido contratado recientemente como técnico de LAN. Su primera misión crucial es demostrar sus habilidades ante el administrador de red, configurando una pequeña red de área local (LAN). En el escenario propuesto tiene equipos con la configuración de fábrica; con base en las técnicas estudiadas, realizará las configuraciones iniciales para switches y dispositivos finales para implementar una red sencilla.

Estrategia de trabajo:

- Revise los comandos que se le han presentado en esta semana.
- Tenga a mano su cuaderno de ingeniería, que le será de mucha utilidad para el desarrollo de esta actividad.
- Desarrolle la actividad propuesta siguiendo el guion disponible en la misma.

[Práctica 2.9.1 de CCNA-1: configuración básica de comutadores y dispositivos finales.](#)

En esta actividad usted podrá practicar lo aprendido sobre Cisco IOS y pasar de la teoría a la acción al construir desde cero una red funcional, tal como lo haría en su actividad laboral.

Para evaluar el éxito en la resolución del problema usted realizará pruebas de conectividad y podrá utilizar comandos de monitoreo para extraer información de funcionamiento, las mismas que le permitirán a futuro determinar fallos en red y resolver algunas preguntas de reflexión que encontrará al final de la práctica.

Retroalimentación:

En esta actividad de Packet Tracer podrá ver su progreso como porcentaje, además pueden hacer clic en la pestaña *Check Results* para ver los ítems que se consideran para medir su progreso y verificar cuáles

están pendientes o no están correctamente ejecutados. Adicionalmente, se puede usar la opción *Reset Activity* para generar un nuevo conjunto de requisitos (se perderán las configuraciones realizadas).

Finalizada la actividad, con base en lo aprendido, conteste las siguientes preguntas de reflexión:

1. Al iniciar la configuración, ¿qué pasos considera que son los más críticos para establecer una base segura en los switches y por qué la encriptación de contraseñas es una práctica tan fundamental en este proceso?
2. Durante la configuración de los switches con Cisco IOS, ¿hubo algún comando o configuración que le confundiera en un inicio? Si es así, ¿cómo logró resolverlo?
3. ¿Qué herramienta o comando utilizó principalmente para verificar la conectividad entre los PC y los switches, y qué información obtuvo?

Actividad 3. Es hora de medir nuestro avance

En la plataforma Netacad encontrará el Examen de punto de control: Examen básico de conectividad de red y comunicaciones (módulos 1-3), que le propondrá cuestiones sobre los conceptos de la unidad 1.

Le invito cordialmente a desarrollar la evaluación correspondiente a los módulos del curso CCNA 1 en la plataforma Netacad. Superar esta actividad le permitirá avanzar hacia la microcertificación oficial, un logro que fortalecerá su perfil académico y profesional. Aproveche esta oportunidad para destacar en un entorno laboral cada vez más competitivo. Su esfuerzo marcará la diferencia.

Actividad 4. Autoevaluación 1

Estimado estudiante, a continuación, usted tiene unas preguntas para que pueda medir su nivel de conocimiento sobre los contenidos de la unidad 1.

Estrategia de trabajo

- Resolver la autoevaluación sin revisar material adicional.
- Revisar el solucionario disponible al final de la guía.

Una vez comprendida la actividad, realice la autoevaluación para comprobar sus conocimientos.

índice

I Bimestre

II Bimestre

Solucionario

Referencias



Autoevaluación 1

Lea cada pregunta con atención y seleccione la alternativa que considere correcta.

1. La red de *Internet* es administrada por un único organismo centralizado que dicta todas sus normas de funcionamiento, asegurando una gestión uniforme a nivel mundial.
 - a. Verdadero.
 - b. Falso.
2. Al configurar contraseñas en equipos Cisco con el comando *password*, estas se almacenan encriptadas por defecto en el archivo *running-config*, protegiéndolas de accesos no autorizados al archivo de configuración.
 - a. Verdadero.
 - b. Falso.
3. ¿Cuál es el propósito principal de la Calidad de Servicio (QoS) en una red moderna?
 - a. Garantizar que todos los tipos de tráfico reciban la misma prioridad para evitar discriminación.
 - b. Priorizar el tráfico de datos según su importancia o tipo para asegurar la velocidad y disponibilidad de servicios críticos.
 - c. Reducir la cantidad total de tráfico de red para minimizar la congestión.
 - d. Cifrar todos los datos que transitan por la red para proteger su confidencialidad.

4. En el Modelo OSI, ¿qué capa es responsable de establecer, administrar y finalizar sesiones o diálogos entre aplicaciones en hosts distintos?
- Capa de transporte.
 - Capa de red.
 - Capa de sesión.
 - Capa de presentación.
5. ¿Qué comando o combinación de teclas permite regresar directamente al modo EXEC privilegiado (Switch#) desde cualquier modo de subconfiguración en Cisco IOS?
- exit
 - Ctrl + C
 - end o Ctrl + Z
 - disable
6. ¿Cuál de los siguientes principios de seguridad de la información garantiza que los datos permanezcan sin modificaciones durante su tránsito desde el dispositivo inicial hasta el destinatario?
- Integridad.
 - Confidencialidad.
 - Disponibilidad.
 - Autenticidad.

7. Al seleccionar el medio de interconexión apropiado para el despliegue de una red, ¿qué dos factores son importantes considerar para asegurar una solución de telecomunicaciones de calidad?
- La distancia máxima o alcance deseado para la conexión.
 - El tipo de sistema operativo del dispositivo final que se conectará.
 - La capacidad de transmisión de datos requerida (velocidad de transmisión del medio).
 - El modelo de madurez de Richardson del sistema a implementar.
8. Comparado con Telnet, ¿qué dos ventajas clave ofrece Secure Shell (SSH) para el acceso remoto seguro a dispositivos Cisco IOS?
- Cifrado completo de todo el tráfico y las credenciales.
 - Menor uso de recursos de CPU en el dispositivo de red.
 - Mayor facilidad de configuración para usuarios principiantes debido a su interfaz simplificada.
 - Inclusión de funcionalidades para copia de archivos como SCP/SFTP.
9. Relacione cada tipo de red con su cobertura geográfica aproximada.

Tipos de red	Cobertura aproximada
1. LAN	A. Unos pocos metros (entorno corporal o escritorio).
2. WAN	B. Hasta un edificio o planta (decenas a cientos de metros).
3. PAN	C. Países o continentes.
4. GAN	D. Cobertura mundial.

10. Asocie cada componente de la estructura simplificada de los dispositivos de red Cisco con su descripción.

Componente	Descripción
1. Hardware	A. Interpreta los comandos que el usuario escribe y muestra los resultados, permitiendo la interacción directa con el sistema operativo del dispositivo.
2. Kernel	B. Parte física del dispositivo, incluyendo <i>chips de conmutación</i> , interfaces y fuentes de poder.
3. Shell	C. Administra la CPU y la memoria del dispositivo, y toma decisiones fundamentales sobre cómo y cuándo reenviar los paquetes, actuando como interfaz entre el <i>hardware</i> y el <i>software</i> .

[Ir al solucionario](#)

Resultado de aprendizaje 2

- Analiza la comunicación entre dispositivos y aplicaciones en redes considerando el modelo de capas OSI y TCP/IP, garantizando el desempeño y la conectividad eficientes.

Para alcanzar este resultado de aprendizaje, se propone que usted consolide una visión integral de la comunicación extremo a extremo, comprendiendo cómo las funciones de las capas física, de enlace y de red se articulan con los protocolos Ethernet, IP, ARP e ICMP para garantizar la transferencia eficiente y segura de datos. Al analizar los procesos que ocurren desde que una señal abandona el dispositivo emisor hasta que la aplicación de destino recibe la información, usted podrá diagnosticar problemas comunes, interpretar capturas de tráfico y explicar, con propiedad técnica, el rol de cada capa dentro de los modelos OSI y TCP/IP.

Para lograrlo se combinarán estrategias de aprendizaje activo: laboratorios guiados en Packet Tracer, análisis colaborativo de capturas en Wireshark, ejercicios de cálculo y aplicación de configuración de routers y switches que incluyan pruebas de conectividad con ping y traceroute.

Contenidos, recursos y actividades de aprendizaje recomendadas



Sem 1 Sem 2 Sem 3 Sem 4 Sem 5 Sem 6 Sem 7 Sem 8



Semana 3

Esta semana exploraremos la capa física, la base tangible sobre la que descansa todo el entramado de redes. Al adentrarse en este tema, usted descubrirá cómo los *bits* se convierten en pulsos eléctricos, haces de luz o señales de radio que atraviesan cables de cobre, fibras ópticas y enlaces inalámbricos para transportarse a otros equipos.

Comprender el propósito, las características y la selección adecuada de cada medio le otorgará la capacidad de diseñar infraestructuras robustas, optimizar el desempeño y anticipar problemas de atenuación e interferencias, competencias esenciales para su futuro como ingeniero de Redes y Analítica de Datos.

Realice las actividades recomendadas y haga una reflexión de los contenidos estudiados porque estos serán los cimientos que sostendrán capas superiores como la de enlace y la de red. Para que complemente su conocimiento sobre los contenidos de esta semana, le invito a revisar las unidades sobre Capa física en la bibliografía básica y el video introductorio de la [unidad 2](#).

Como pudo notar en la introducción, la comunicación en redes es un proceso complejo que ocurre en múltiples capas simultáneamente. Lo que observó sobre la interacción entre la capa física, de enlace y de red ilustra cómo cada protocolo tiene un rol específico para garantizar que los datos lleguen correctamente a su destino, desde la señal eléctrica hasta el enrutamiento inteligente.

Unidad 2. Comunicación entre dispositivos

Imagine que la información fuese un flujo constante de productos almacenados en cajas, que deben ser transportados de un sitio a otro dentro de un gran país. Para mover esas cajas de datos existen distintos

índice

I Bimestre

II Bimestre

Solucionario

Referencias

caminos físicos y todos tienen un único punto de salida, que sería el centro de paquetería. Dicho centro representa la capa física, es decir, donde el proceso de envío a través de estas rutas posibles es efectivo. Para el caso de redes de computadoras, donde se pasa del mundo digital al mundo tangible de las señales.

2.1. Capa física.

2.1.1. Funciones de la capa física

La capa física en el modelo OSI actúa como punto de contacto entre los computadores e interconexiones propiamente dichas. Proporciona los medios para transportar los *bits* que vienen de capas superiores y se encarga de que lleguen correctamente.

Las funciones de la capa física se agrupan en cinco pilares, los cuales se presentan de manera visual y organizada en la siguiente infografía que le permitirá identificar y comprender las responsabilidades fundamentales de esta capa base del modelo OSI.

[Funciones de la capa física \(modelo OSI\).](#)

Como pudo observar en la infografía, la capa física constituye el fundamento sobre el cual se construye toda la comunicación de datos en las redes. Habrá notado que los cinco pilares presentados no son independientes, sino que trabajan de manera coordinada para garantizar que la información digital se transforme correctamente en señales físicas y viceversa.

Para ampliar su conocimiento, revise las siguientes descripciones de cada pilar:

1. **Transporte de bits:** la capa física convierte la trama que viene de la capa de enlace en una secuencia de señales que se introducen en el medio de transporte seleccionado. Estas señales pueden

ser; pulsos eléctricos, pulsos luminosos u ondas de radio. Ya en el receptor, la capa física se encarga del proceso inverso, es decir, de tomar las señales y reconstruir los *bits* para entregarlos a la capa de enlace.

2. **Especificación de interfaces:** en la capa física se definen normas mecánicas, eléctricas, ópticas, de temporización y de sincronización para el funcionamiento del *hardware*, de tal forma que equipos de distintos fabricantes puedan conectarse físicamente sin problemas.
3. **Codificación y señalización:** convierte los *bits* (0 y 1) del mundo digital a códigos estandarizados (por ejemplo: Manchester, 4B/5B, 8B/10B, etc.), y define su representación en patrones para cada tipo de medio.
4. **Control de ancho de banda y rendimiento:** cada medio se caracteriza por una velocidad máxima nominal que establece parámetros teóricos para el enlace de conexión, teniendo en cuenta atenuación, interferencias y fenómenos físicos. Estos parámetros permiten calcular el posible rendimiento del enlace en términos de latencia y rendimiento.
5. **Topologías y puntos de acceso:** la topología física establece cómo se disponen los equipos y las conexiones físicas que los unen.

2.1.2. Características de la capa física

Antes de ahondar en los medios, las especificaciones y números, imagine que está viendo su serie favorita de Netflix en 4K mientras alguien en casa realiza una videollamada y otro descarga un videojuego de 50 GB y que todo esto ocurre sin ningún problema. Detrás de esa aparente magia se esconden las características de la capa física, por ejemplo: los reglamentos que permiten que equipos de marcas distintas se entiendan, los medios estandarizados por donde viajan los *bits*, el

alfabeto que los convierte en pulsos y la manera en que esos pulsos eluden el ruido para cruzar largas distancias sin corromperse.



Le invito a revisar el video titulado “[Resumen capa física y medios de red](#)”, donde podrá revisar el concepto y funcionamiento de la capa física. Sobre todo, céntrese en la explicación de los soportes físicos que transportan las señales que hacen posible que los equipos se comuniquen.

A continuación, con los elementos que hemos introducido, las principales características de esta capa serán explicadas en detalle.

1. Estándares usados en la capa física

Como los reglamentos de tránsito que permiten que vehículos de distintas marcas circulen sin contratiempos, los estándares en capa física determinan los lineamientos con los cuales trabajarán el *hardware* de red en cuanto a medios, codificación, señalización, conectores, etc. Podemos citar muchas organizaciones que han creado estándares relacionados con la capa física, entre ellos:

- Organización Internacional para la Estandarización (ISO).
- Asociación de las Industrias de las Telecomunicaciones (TIA) y Asociación de Industrias Electrónicas (EIA).
- Unión Internacional de Telecomunicaciones (ITU).
- Instituto Nacional Estadounidense de Estándares (ANSI).
- Instituto de Ingenieros Eléctricos y Electrónicos (IEEE).
- Autoridades nacionales reguladoras de las telecomunicaciones, incluida la *Federal Communication*.
- Commission (FCC) de los Estados Unidos y el Instituto Europeo de Estándares de Telecomunicaciones (ETSI).

Algunos ejemplos de estándares usados en capa física son: IEEE 802.3 para Ethernet, IEEE 802.11 para wifi, ITU-T G.652 para fibra, TIA/EIA 568 para cableado estructurado, entre otros. En ellos se definen voltajes, longitudes de onda, conectores y distancias máximas. Conocerlos le garantiza interoperabilidad y facilita la resolución de fallos cuando dos equipos tienen conflictos de conexión. ¿Ha escuchado acerca de alguno de estos estándares?, ¿conoce algún otro similar?

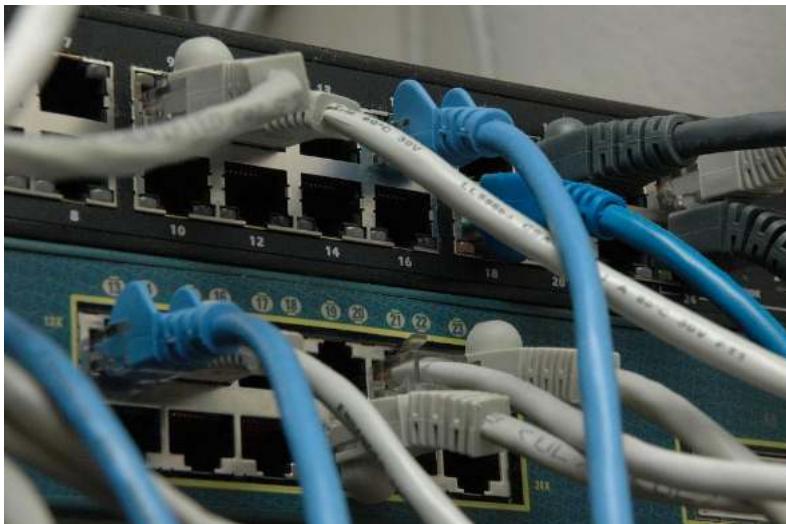
2. Componentes físicos

La capa física especifica todo el *hardware* o parte tangible que el computador usa para interconectarse con otros equipos. El primer componente físico para conectarse a la red que tiene todo dispositivo es la tarjeta de interfaz de red (NIC por sus siglas en inglés). La NIC permite la conexión cableada o la conexión inalámbrica, y así un dispositivo puede tener diferentes tipos de NIC activos a la vez.

Los puntos de unión de los dispositivos a la red se denominan interfaces, y para esa unión utilizan conectores especiales, dependiendo del tipo de interfaz y del medio de conexión. En la figura 19, puede ver un *switch* y las interfaces de conexión con cables UTP y conectores RJ-45.

Figura 19

Interfaces Ethernet y conectores RJ-45 en switches de red



Nota. Tomado de Network switches [Fotografía], por ShakataGaNai, 2008, [WikimediaCommons](#), CC BY 4.0.

Para las conexiones cableadas los materiales del cable también constituirán un componente físico y dependiendo de su naturaleza requerirán un aislamiento especial e infraestructura de soporte. Adicionalmente, la estructura, forma y armado de los cables responderán a un estándar que especificará el orden de pines, diámetro, enchapado entre otros.

3. Codificación

Si los datos fueran mensajes en clave Morse, la codificación sería el alfabeto que convierte cada letra en puntos y rayas. Los códigos como NRZ, Manchester o 8B/10B, son esquemas de bits que transforman los 0 y 1 en patrones de señal para que sean resistentes al ruido y sean fácilmente identificables en el receptor. La codificación, entonces, es el proceso mediante el cual la capa física traduce los bits (0 y 1) que recibe

de la capa de enlace a un patrón de señal eléctrica, óptica o de radio que pueda viajar por el medio elegido.

4. Señalización

Mientras la codificación define el idioma, la señalización indica cómo se pronuncia: modulaciones (ASK, FSK, QAM), amplitud, frecuencia y temporización. Imagine a un ciclista con una linterna en la noche, él podrá parpadear, variar la intensidad o cambiar de color para transmitir información. Del mismo modo, la señalización permite exprimir más bits por segundo sin cambiar de medio.

5. Ancho de banda, latencia y tasas de transferencia

Los medios físicos tienen características diferentes que determinan velocidades de transferencias de datos diferentes, esta velocidad se traduce en **ancho de banda**. El ancho de banda es la capacidad que tiene un medio para transmitir datos medidos en bits por segundo (es frecuente usar prefijos como mega 10⁶bps – Mbps y giga 10⁹bps – Gbps para indicar sus múltiplos).

La **latencia** se refiere al tiempo (medido en milisegundos ms) que demoran los datos para ir desde un punto a otro de la red, es frecuente usar el término de retardo también. La latencia será el resultado de los tiempos de propagación en medios, transmisión, conmutación, tiempo en búfer, encolado en dispositivos intermedios, procesado en equipos, etc.

La **tasa de transferencia efectiva** (*Throughput*) es la velocidad real a la que se entregan los datos a nivel de usuario. Se mide en bits por segundo y, en la práctica, siempre será menor al ancho de banda disponible.

La **capacidad de transferencia útil** (*Goodput*) es la medida de datos utilizados que han sido transferidos en un periodo de tiempo concreto

descontando los bits de cabeceras, retransmisiones, acuses de recibo y establecimiento de sesiones. Está medido en bits por segundo.

En nuestra analogía de tránsito automovilístico, el ancho de banda sería el número de carriles de una autopista, cuantos más carriles más carros a la vez podrán transitarla; la latencia sería el tiempo de viaje y los tiempos de espera en semáforos y peajes; el *Throughput* será el número de autos por segundo que realmente pasan por una intersección sin contar desvíos o congestión en algún sector de la ciudad; y el *Goodput*, serán los vehículos que llegan con un producto específico y se descontaría los que no llevan la paquetería o se han regresado por alguna razón.



Reflexione sobre cómo el conocimiento de estas métricas le puede ayudar a identificar errores en redes. ¿Cuáles de estas métricas sería crucial para transmisiones multimedia? ¿Cómo el análisis de *Throughput* nos permite determinar cuellos de botella?

2.1.3. Medios cableados

En redes de computadoras, los medios cableados, también conocidos como medios guiados, son el medio físico a través del cual viajan los datos que se han codificado en señales. Estos medios incluyen cables de cobre y fibra óptica.

2.1.3.1. Cables de cobre

Este tipo de medio usan el cobre como material conductor para llevar las señales de un dispositivo a otro debido a que es económico, fácil de instalar y bastante conductor. Los datos son transformados en pulsos eléctricos para ser transportados, sin embargo, este tipo de señales son sensibles a la interferencia electromagnética (EMI), interferencias de radiofrecuencia (RFI) y susceptibles a las pérdidas debidas a la atenuación por distancia.

Se tiene dos tipos de medios de cobre: cable coaxial y par trenzado.

a. **Cable coaxial:**

El cable coaxial consta de un conductor interno llamado núcleo central rodeado por una capa de material aislante dieléctrico, una malla metálica y una cubierta externa plástica (ver Figura 20).

Figura 20

Estructura interna de un cable coaxial



Nota. Tomado de *Coaxial cable cutaway-es* [Ilustración], por Begoon, 2024, [WikimediaCommons](#), CC BY 4.0.

Suele usarse para conectar redes de televisión por cable y redes Ethernet. El cable coaxial usa varios tipos de conectores, entre ellos, tipo N, tipo F y BNC.

b. **Par trenzado:**

Este medio consta de cuatro pares de cables de cobre aislados y trenzados entre sí para reducir la interferencia y codificados en colores. A su vez se divide en dos tipos: **UTP** (*Unshielded Twisted Pair*) y **STP** (*Shielded Twisted Pair*). El primero no tiene blindaje adicional y es común en redes locales, mientras que el segundo se caracteriza por contar con una capa adicional blindada para evitar interferencias, en la Figura 21, puede ver un cable UTP comúnmente usado en redes domiciliares.

Figura 21

Cable UTP con conectores RJ-45 para redes Ethernet

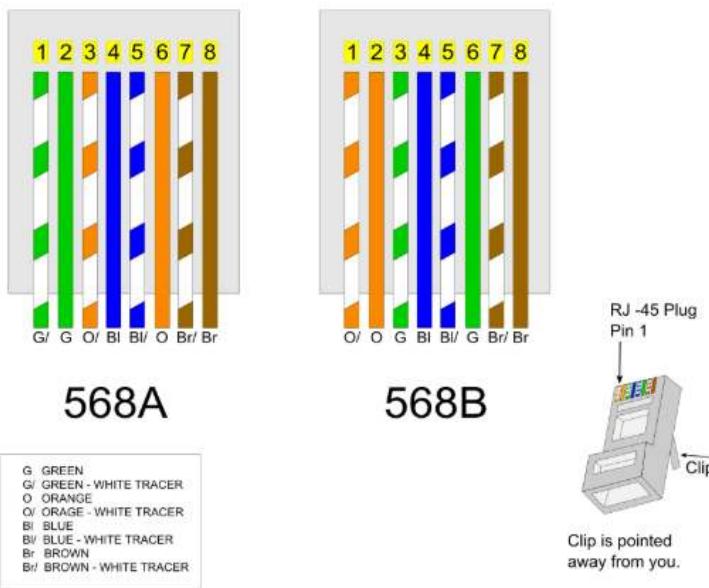


Nota. Tomado de *UTP cable-blue* [Fotografía], por Hatschepsut, 2007, [WikimediaCommons](#), CC BY 4.0.

Este tipo de cables, frecuentemente, tienen chaquetas azules. Sin embargo, lo más importante es definir qué categoría de cable se va a utilizar porque de ello depende su uso. Las categorías Cat-5e a Cat-6a ofrecen velocidad de 1 a 10 Gbps en tramos de hasta 100m, mientras que las categorías Cat-7 y Cat-8 pueden conseguir 25-40 Gbps incorporando blindajes dobles. Los pares trenzados suelen usar conectores RJ-45 para conectarse a las interfaces de los dispositivos. El armado de los cables puede seguir la norma 568A o 568B (ver Figura 22 para el detalle de la norma).

Figura 22

Normas T568A y T568B para el armado de cables de red Ethernet



Nota. Tomado de *568 A and 568 B [Ilustración]*, por charner1963, 2018, [WikimediaCommons](#), CC BY 4.0.

La diferencia entre las dos normas se encuentra en los pares 1-2 y 3-6, que se invierten. Dependiendo de la norma usada en cada extremo se puede tener cables directos (ambos extremos la misma norma) o cruzados (cada extremo una norma). Los **cables directos** se usan para conectar dos dispositivos de diferente nivel, por ejemplo, un computador y un switch. Por otro lado, un **cable cruzado** se usa para conectar dos dispositivos del mismo nivel, por ejemplo, dos computadores.

2.1.3.2. Fibra óptica

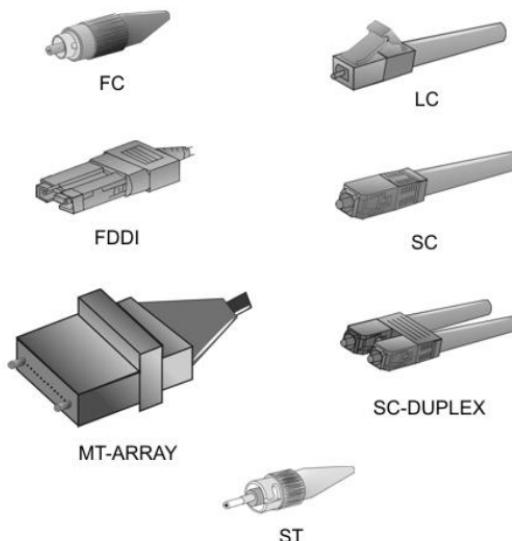
En la fibra óptica los datos son transmitidos como pulsos de luz a través de hilos de vidrio o plástico. Este medio ofrece alta velocidad y ancho de banda, además de inmunidad a la interferencia electromagnética. Hay dos tipos de fibra óptica: fibra monomodo y fibra multimodo.

- La **fibra monomodo** consta de un núcleo pequeño (125 micras) y usa un láser como emisor de luz, la pureza de su haz de luz y la baja dispersión que tiene le permite alcanzar largas distancias (alrededor de cientos de kilómetros).
- La **fibra multimodo** tiene un núcleo más grande y usa focos LED como emisores, por lo cual envía haces de luz en diferentes ángulos. La fibra multimodo se divide a su vez en fibra de índice a salto de índice y fibra a gradiente de índice dependiendo del índice de refracción de la fibra.

Este tipo de medio usa varios conectores, entre los cuales podemos citar FC, LC, FDDI, SC y ST, en la Figura 23, puede ver el aspecto de los conectores, cada uno tiene características específicas en cuanto a forma, mecanismo de conexión y aplicaciones.

Figura 23

Tipos de conectores de fibra óptica en redes de comunicación



Nota. Tomado de *tipos de conductores de fibra optica [Ilustración]*, por Elsanto510.ULE, 2007, [WikimediaCommons](#), CC BY 4.0.

La selección del conector depende del tipo de equipo, del entorno de instalación y de la necesidad de transmisión (simplex o dúplex). Por ejemplo, los conectores LC y SC son ampliamente usados en switches y paneles de distribución por su tamaño compacto y fiabilidad. El conector MT-Array se utiliza para enlaces de alta densidad, mientras que los ST y FC eran comunes en instalaciones más antiguas.

En la Tabla 9, usted puede encontrar una comparación entre los medios cableados para que la tenga como referencia cuando requiera elementos para seleccionar el medio ideal para una red concreta.

Tabla 9

Comparación de medios de transmisión cableados en la capa física

Criterio	Par trenzado (Cat 5e-8)	Coaxial	Fibra multimodo	Fibra monomodo
Velocidad típica	1–40 Gb/s	100 Mb/s–10 Gb/s	1–100 Gb/s	10–400 Gb/s
Distancia sin repetidores	≤ 100 m	≤ 500 m	≤ 550 m	≥ 40 km
EMI / Seguridad	Media / Baja	Alta / Media	Inmune / Alta	Inmune / Muy alta
Coste del medio	Bajo	Medio	Medio	Alto
Uso actual	LAN, PoE, ToR	HFC, CCTV	Data center, campus	Backbone, FTTH, 5G

Nota. Ludeña, P., 2025.

Note que las conexiones de redes LAN a nivel de usuario suelen usar par trenzado por sus distancias cortas de hasta 100 m, mientras que las conexiones de campus utilizan cable coaxial o fibra óptica con hasta 550 m de longitud.

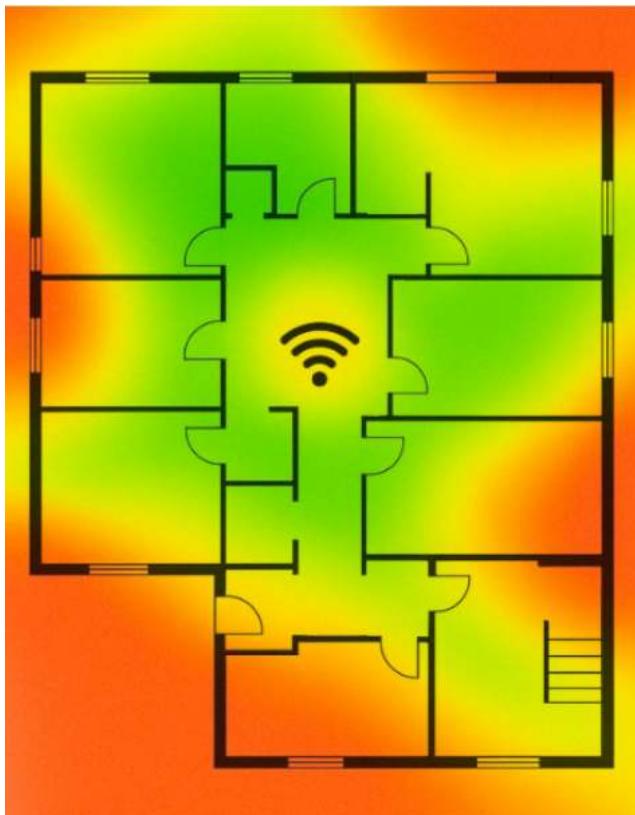
2.1.4. Medios inalámbricos

En los medios inalámbricos o también denominados medios no guiados, los datos se codifican en bits que se transportan como ondas de radio o microondas. Las señales se producen como variaciones de frecuencia,

fase o amplitud. La cobertura y alcance de estos medios depende de los obstáculos que se encuentren en la trayectoria y la potencia con la que se envía la señal, en la Figura 24, se puede ver la cobertura de un punto de acceso (Access point - AP) inalámbrico.

Figura 24

Mapa de calor de un Access point en un plano de oficinas



Nota. Ludeña, P., 2025.

En el mapa de calor presentado, las zonas más alejadas al AP tendrán menos recepción que las zonas más cercanas, las señales que deben atravesar más paredes llegarán con menos potencia a las zonas más alejadas del plano.

Al no tener un medio guiado las señales no están aisladas de interferencias externas y son susceptibles a interferencias procedentes de elementos comunes que operan en las mismas bandas de frecuencias, por ejemplo, microondas. Adicionalmente, la ausencia de protección física hace que estas señales puedan ser interceptadas por lo que es necesario reforzar la seguridad en términos de encriptación y autenticación.

Existen varios tipos de medios inalámbricos usados para redes, entre los principales se pueden citar:

- Wi-Fi (IEEE 802.11): estándar dominante en interiores (WLAN), con variantes desde 11 Mbps (802.11b) hasta 1,3 Gbps (802.11ac) usando antenas en configuración MIMO y opera en frecuencias de 2,4 GHz y 5 GHz.
- Bluetooth (IEEE 802.15.1): estándar dominante en área personal WPAN, conecta periféricos a pocos metros con bajo consumo.
- Zigbee (IEEE 802.15.4): ideal para IoT y aplicaciones industriales, prioriza el ahorro energético sobre la velocidad, para ello opera con baja velocidad de datos y baja potencia.
- WiMAX (IEEE 802.16) y redes celulares 4G/5G: proporcionan banda ancha de varios kilómetros, soportando movilidad y traspasos (handoff) entre celdas.

Siguiendo con nuestra analogía de los múltiples caminos físicos que pueden seguir un servicio de paquetería, podríamos tener calles secundarias, autopistas, rutas aéreas, entre otras. Cada una de ellas tendrá unas características propias, pero de seguro entre las más importantes es la rapidez con la que pueden hacer que los productos lleguen a su destino. De la misma forma los medios físicos los clasificaremos en dos grandes grupos: medios inalámbricos y medios cableados.

Las calles secundarias equivalen al cable de cobre UTP o coaxial, serían rutas económicas, sencillas de instalar y suficientes para la entrega diaria en distancias cortas, aunque la presencia de tráfico (atenuación e interferencias) limite su velocidad.

La autopista de varios carriles sería análoga a las conexiones con fibra óptica, donde la luz recorre kilómetros casi sin perder fuerza; vías veloces e ideales para tráfico pesado y entregas urgentes.

Las rutas aéreas son los enlaces inalámbricos, puesto que no requieren obra civil y ofrecen libertad de movimiento, pero dependen del clima y de la congestión del espectro radioeléctrico, por lo que requieren control estricto de potencia y seguridad.

Al igual que en la analogía todos los medios son válidos y funcionales, depende de los requerimientos de envío, el ambiente donde se deba montar la red, la densidad de usuarios, la disponibilidad del presupuesto, la velocidad requerida y los objetivos trazados para seleccionar el medio que se adapte de mejor forma a la red.

Finalmente, en la Tabla 10 encontrará las ventajas y desventajas de los medios inalámbricos en relación con los medios cableados.

Tabla 10

Ventajas y desventajas de los medios inalámbricos frente al cableado

Aspecto	Ventajas frente a cableado	Desventajas
Movilidad	Conexión sin ataduras; roaming entre celdas	Cobertura limitada y handoff complejo
Coste y tiempo de despliegue	Sin obras civiles; ideal en edificios históricos	Requiere planificación de canales y energía
Flexibilidad	Escalable para dispositivos IoT	Interferencias y congestión en bandas libres
Seguridad	Autenticación dinámica; segmentación lógica fácil	Tráfico susceptible a escucha si se configura mal

Aspecto	Ventajas frente a cableado	Desventajas
Ancho de banda sostenido	10 – 100 Mb/s reales para muchas aplicaciones	Inferior a fibra/cobre; sensible a la distancia y obstáculos

Nota. Ludeña, P., 2025.

En esta comparación se destacan cinco aspectos fundamentales: movilidad, coste y tiempo de despliegue, flexibilidad, seguridad y ancho de banda sostenido. Entre las principales ventajas del medio inalámbrico se encuentra la conexión sin cables, ideal para entornos móviles, su instalación sin obras físicas, la escalabilidad para dispositivos IoT, la facilidad de autenticar usuarios y la capacidad de ofrecer velocidades entre 10 y 100 Mb/s para diversas aplicaciones.

Sin embargo, también se presentan desventajas importantes. La cobertura inalámbrica puede ser limitada y el traspaso entre celdas (handoff) complejo, además de requerir planificación de canales, energía y ser sensible a interferencias. La seguridad puede verse comprometida si no se configura adecuadamente y el rendimiento, aunque útil para muchas aplicaciones, sigue siendo inferior a medios cableados como fibra óptica. Esta comparación sirve para tomar decisiones fundamentadas sobre el tipo de red a implementar según el entorno y los requisitos del usuario.

¿Qué tanto sabe sobre medios de transmisión?

Los medios de transmisión constituyen las vías por donde circulan los datos que se transmiten a todo el mundo, de ahí la importancia. El objetivo de esta actividad es poder reconocer las principales características de los medios de transmisión para que pueda seleccionar en qué condiciones deberá usar una u otra opción, o inclusive habrá situaciones en que la mejor solución incluya un despliegue combinando varias tecnologías. A continuación, resuelva el juego de unir con líneas:



Medios de transmisión en redes

Como pudo comprobar al completar la actividad, cada medio de transmisión presenta ventajas y limitaciones específicas que determinan su aplicabilidad en diferentes escenarios. La actividad le ha permitido consolidar conocimientos sobre las características técnicas distintivas de cada tecnología.

Ahora que comprende las características de cada medio, si ya estuviera ejerciendo su profesión y debe implementar redes de telecomunicaciones:

- ¿Qué medio de transmisión usaría para una conexión de varios kilómetros?
- ¿Cuál medio cableado tiene un costo más bajo?
- ¿Qué medio de transmisión es más afectado por condiciones climáticas?

Es hora de poner en práctica sus conocimientos sobre medios de transmisión y diseño de redes mediante un caso de estudio real. En esta actividad práctica enfrentará el desafío de tomar decisiones técnicas fundamentadas para resolver un problema de conectividad empresarial. El caso le presentará un escenario corporativo con múltiples variables y restricciones, donde deberá aplicar los conceptos aprendidos sobre características de medios de transmisión, consideraciones de distancia, velocidad, costo y seguridad para proponer soluciones óptimas.

Conectividad de Campus Corporativo

Como pudo experimentar a través del caso de estudio, el diseño de infraestructuras de red requiere un análisis integral que va más allá de las especificaciones técnicas individuales. Habrá notado que cada decisión técnica debe equilibrar múltiples factores: rendimiento, costo, tiempo de implementación, seguridad y escalabilidad futura.



Actividades de aprendizaje recomendadas

Es hora de reforzar los conocimientos adquiridos resolviendo las siguientes actividades:

Actividad 1. Lectura de los contenidos propuestos

Ingresé a la plataforma [Netacad](#) y revise el módulo 4: Capa física. Revise las funciones de esta capa y la clasificación de los medios de transmisión que se pueden usar para interconectar dispositivos y armar redes.

Estrategia de trabajo:

- En el espacio semanal que usted haya determinado para esta asignatura, revise el módulo recomendado.
- Registre las ideas principales en su cuaderno de apuntes de manera sistemática y ordenada.
- Complete las actividades tituladas. Verifique su comprensión que tiene disponible en la plataforma para el módulo 4.
- Resuelva la autoevaluación del módulo 4 y mida su avance.

Retroalimentación:

Finalizada la autoevaluación, verifique sus respuestas y repase los conceptos que le generaron duda o estuvieron errados. Recuerde que puede repetir la actividad cuantas veces crea oportuno.

Actividad 2. ¡Vamos a conectar equipos!

En esta actividad interactiva, de Packet Tracer decidirá cuál es la mejor opción para interconectar equipos. El objetivo es que usted entienda cómo los dispositivos se conectan físicamente entre sí y que a partir de esa conexión se desarrolla la comunicación entre los equipos. Usted dispondrá del modo físico que le permitirá seleccionar, diferenciar y conectar los componentes de red.

Estrategia de trabajo:

- Repase la información sobre los dispositivos físicos y los medios de transmisión que se estudiaron esta semana.
- Abra el Packet Tracer y revise los tipos de cables disponibles para interconectar dispositivos.
- Tenga a mano su cuaderno de ingeniería para consultar los comandos de monitoreo y verificación de conectividad.
- Desarrolle la actividad propuesta siguiendo el guion disponible en la misma.

Práctica 4.7.2 de CCNA-1: conectar la capa física.

En esta actividad usted podrá identificar y comprender las características físicas de los dispositivos de red. Se familiarizará con los módulos, los puertos de consola y las interfaces Gigabit Ethernet y Serial. También deberá seleccionar el tipo de cable adecuado para cada conexión, identificando el tipo de dispositivo y de interfaz.

Retroalimentación:

En esta actividad de Packet Tracer podrá ver su progreso como porcentaje, además pueden hacer clic en la pestaña *Check Results* para ver los ítems que se consideran para medir su progreso y verificar cuáles están pendientes o no están correctamente ejecutados.

Finalizada la actividad, le invito a responder las siguientes preguntas de reflexión:

1. ¿Cómo cree que afectaría la selección equivocada de tipo de cable para una conexión?
2. ¿Identificó problemas de conexión en la red a través de los indicadores visuales en Packet Tracer?, ¿en la vida real, qué elementos le pueden ayudar a identificar problemas de conectividad de manera visual?
3. Si una interfaz muestra un estado de *down down*, ¿qué se puede inferir sobre la comunicación en la capa física y cómo podría afectar a una aplicación que intenta usar la red?



Sem 1 Sem 2 Sem 3 Sem 4 Sem 5 Sem 6 Sem 7 Sem 8



Semana 4

Los computadores hablan un lenguaje binario y a través de él se realizan todos los procesos de comunicación, es decir, que el sistema binario es la base para entender el mundo digital. Con base en este sistema se construyen otras estructuras de identificadores a nivel de varias capas de los modelos de referencia que se manejan en sistemas decimales y hexadecimales. Por esta razón, en esta semana nos centraremos en los sistemas de numeración, enfocándonos en comprender la estructura de cada sistema y los métodos de conversión entre sistemas de numeración que nos permitirán conocer cómo los equipos dialogan y algoritmos de red dialogan entre sí. Dominar estas bases le capacitará para traducir direcciones IP, calibrar máscaras de subred, interpretar tramas Ethernet y, más adelante, optimizar modelos de datos en análisis de tráfico. Considere que, al igual que un arquitecto debe leer planos, el profesional en Redes y Analítica de Datos requiere fluidez numérica para construir infraestructuras seguras y extraer conocimiento de grandes volúmenes de información. Le animo a abordar cada conversión y ejercicio de codificación con curiosidad y disciplina; esta destreza será su aliada cuando diseñe soluciones de direccionamiento, planifique redes, automatice configuraciones o evalúe el rendimiento de redes reales.

2.2. Sistemas de numeración

Cuando una computadora habla, no lo hace con letras ni con los números que usamos a diario, sino con *bits*. Estos *bits* son unos y ceros, que viajan por los medios físicos en forma de señales, como lo vimos la semana pasada. Entender cómo se agrupan esos *bits* para representar cantidades nos abre la puerta a temas tan variados como las direcciones IP, la configuración de máscaras o la lectura de tramas. En la tabla 11, encontrará la descripción de la notación que emplea cada dirección usada en redes y un ejemplo de la notación.

Índice

I Bimestre

II Bimestre
Solucionario

Referencias

Tabla 11

Notación y sistemas de numeración en direcciones MAC, IPv4 e IPv6 que se utilizan en redes de computadores

Dirección	Número de bits	Notación usada	Ejemplo
Dirección MAC	48 bits	Hexadecimal 12 dígitos hexadecimales, divididos en seis grupos de dos dígitos hexadecimales separados por guiones o dos puntos	00:1A:2B:3C:4D:5E
Dirección IPv4	32 bits	Decimal punteado 4 números decimales separados por puntos. Cada número decimal se traduce de un grupo de 8 bits denominado octeto	192.168.100.1
Dirección IPv6	128 bits	Hexadecimal 8 grupos de cuatro dígitos hexadecimales separados por dos puntos	2001:0db8:0001:0000:0000:0ab9:C0A8:0102

Nota. La tabla presenta una comparación entre las direcciones más utilizadas en redes de computadores, mostrando su longitud en bits, el sistema de numeración empleado y un ejemplo representativo. Ludeña, P., 2025.

Esta información es fundamental para introducir el tema de conversión entre sistemas de numeración, como binario, decimal y hexadecimal, dado que cada tipo de dirección usa una representación distinta para facilitar su lectura y operación en diferentes capas del modelo OSI.

En redes, es esencial interpretar estas notaciones correctamente para configurar equipos, analizar tráfico o realizar subredes. Entender cómo se representan y convierten estas direcciones le permite prepararse para realizar tareas críticas de administración, seguridad y diagnóstico en redes modernas.

Los sistemas a los que haremos referencia son, obviamente binario por ser la base del lenguaje digital, el sistema decimal y el sistema hexadecimal. Para tener un fin práctico, trabajaremos con direcciones

IP y direcciones MAC, aunque más adelante estudiaremos en detalle su estructura y funcionamiento, por el momento sólo puntualizaremos el número de bits que tiene cada dirección y cómo agrupan sus dígitos.

En primer lugar, vamos a recordar cómo se conforman los sistemas numéricicos:

- El sistema decimal emplea diez símbolos (0-9) y asigna a cada dígito un valor 10^n según su posición; por ejemplo, 2 154 se descompone en $2 \times 10^3 + 1 \times 10^2 + 5 \times 10^1 + 4 \times 10^0$ para dar 2154.
- En cambio, el sistema binario trabaja con solo dos símbolos (0 y 1) y potencias de base 2; por ejemplo, una palabra de 8 bits sería 1100 0000.
- El sistema hexadecimal (base 16) maneja 16 símbolos (0-9 y de A-F) por lo que es capaz de reunir cuatro bits en un solo dígito hexadecimal 0-F.

Para realizar la conversión entre sistemas de numeración usaremos los valores posicionales de base 2, en la Tabla 12, tiene los valores posicionales para una palabra de 8 bits.

Tabla 12

Valores posicionales para una palabra de 8 bits

Posición en número	7	6	5	4	3	2	1	0
Cálculo en base 2	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Valor posicional	128	64	32	16	8	4	2	1

Nota. Ludeña, P., 2025.

Estos valores se extraen elevando la base 2 a la potencia de la posición, donde la posición se cuenta desde la derecha y empieza desde 0. Para una palabra de 8 bits el bit más a la derecha tendrá valor posicional 0 y el más a la izquierda tendrá valor posicional 128.

2.2.1. Conversión binaria-decimal-binaria

Para convertir un número binario a decimal se multiplica cada dígito binario por el valor posicional correspondiente (comenzando desde la derecha) y se suman los resultados. En la Tabla 13, se detalla la conversión del número binario 10011010 a decimal, obteniéndose como resultado 154.

Tabla 13

Ejemplo de conversión de número binario a decimal paso a paso

Posición	7	6	5	4	3	2	1	0
Valor posicional	128	64	32	16	8	4	2	1
Número binario	1	0	0	1	1	0	1	0
Operación	128×1	$+64 \times 0$	$+32 \times 0$	$+16 \times 1$	$+8 \times 1$	$+4 \times 0$	$+2 \times 1$	$+1 \times 0$
	128	+0	+0	+16	+8	+0	+2	+0
	$128 + 0 + 0 + 16 + 8 + 0 + 2 + 0 = 154$							
Número decimal	154							

Nota. Ludeña, P., 2025.

Reflexione: ¿cuál es el mayor número decimal que puede obtenerse en un octeto? Es decir, cuando tenemos el número binario 11111111. Este número es importante porque sería el mayor número que podría obtener en cada sección separada por un punto en una dirección IPv4.

Para realizar el proceso contrario, es decir, convertir un número decimal a binario, hay dos métodos que presentaremos a continuación.

1. **Método por divisiones:** se divide el número decimal entre 2 y se anota el residuo de cada división. Luego se toma el cociente y se vuelve a repetir el proceso hasta que el cociente sea 0. El número binario será los residuos en orden inverso.

Ejemplo: convertir 13 a binario.

- Dividimos el número $13 / 2 = 6$ y anotamos el residuo: 1
- Dividimos el cociente $6 / 2 = 3$ y anotamos el residuo: 0

- Dividimos el cociente $3 / 2 = 1$ y anotamos el residuo: 1
- Dividimos el cociente $1 / 2 = 0$ y anotamos el residuo: 1

Los residuos que se anotó son 1011, por tanto, el número binario que estamos buscando serán estos dígitos binarios en orden inverso, es decir, 1101. Respuesta: 13 en binario es 1101.

2. **Método de comparación:** el número decimal se compara con el valor posicional del bit más significativo, para palabras de 8 bits sería 128. Si el número es mayor o igual al valor posicional se anota un 1 y se resta el valor posicional al número decimal. El resultado se vuelve a comparar con el siguiente valor posicional. Si el número es menor al valor posicional se escribe 0 y se pasa al siguiente valor posicional. Se sigue iterando hasta comparar todos los valores posicionales o hasta que el número llegue a 0, en cuyo caso se completarán las siguientes con ceros.

Ejemplo: convertir 140 a binario

- 140 es mayor o igual a 128? Si, anotamos 1 y restamos $140 - 128 = 12$
- 12 es mayor o igual a 64? No, anotamos 0 y continuamos con el siguiente valor posicional
- 12 es mayor o igual a 32? No, anotamos 0 y continuamos con el siguiente valor posicional
- 12 es mayor o igual a 16? No, anotamos 0 y continuamos con el siguiente valor posicional
- 12 es mayor o igual a 8? Si, anotamos 1 y restamos $12 - 8 = 4$
- 4 es mayor o igual a 4? Si, anotamos 1 y restamos $4 - 4 = 0$ el número ha llegado a 0 paramos las iteraciones y completamos con ceros los bits restantes (dos posiciones).

Respuesta: 140 en decimal es 10001100 en binario.

2.2.2. Conversión hexadecimal-decimal-hexadecimal

Para convertir números hexadecimales a decimales y viceversa pasaremos por el sistema binario, en la Figura 25, se puede ver las equivalencias de valores en los tres sistemas de numeración estudiados.

Figura 25

Equivalencias entre sistemas decimal, binario y hexadecimal

Decimal	Binario	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

Nota. Ludeña, P., 2025.

Por ejemplo, el número decimal 12 en binario es 1100 y en hexadecimal es C. Los dígitos hexadecimales funcionan muy bien para simplificar

grandes cadenas de dígitos binarios, como en el caso de direcciones IPv6, puesto que agrupa 4 bits binarios y los reemplaza con un solo dígitos hexadecimales. Los sistemas hexadecimal y decimal usan símbolos iguales y pueden presentarse confusiones, para evitar equivocaciones es común usar el prefijo "0x" antes del número hexadecimal (0x3A) o agregar "H" o la base 16 al final del número hexadecimal (3AH o $3A_{16}$).

Para la **conversión de hexadecimal a decimal**, se convierte los dígitos hexadecimales en grupos de 4 dígitos binarios, para completar palabras de 8 bits, esas palabras se convierten a decimal usando el método de valores posicionales presentado en la sección anterior y se obtiene el resultado.

Ejemplo: convertir D2H a decimal

Comenzamos convirtiendo cada dígito hexadecimal en binario. D es 1101 y 2 es 0010 en binario. La palabra de 8 bits será 11010010. En la Tabla 14, puede ver el procedimiento paso a paso para convertir el número binario 11010010 a su forma decimal utilizando la posición y el valor posicional de cada bit.

Tabla 14

Conversión del número binario 11010010 a su equivalente decimal

Posición	7	6	5	4	3	2	1	0
Valor posicional	128	64	32	16	8	4	2	1
Número binario	1	1	0	1	0	0	1	0
Operación	128×1	$+64 \times 1$	$+32 \times 0$	$+16 \times 1$	$+8 \times 0$	$+4 \times 0$	$+2 \times 1$	$+1 \times 0$
	128	+64	+0	+16	+0	+0	+2	+0
Número decimal	210							

Nota. Ludeña, P., 2025.

Entonces, el número D2H es 210 en decimal.

Para la **conversión decimal a hexadecimal**, se traduce el decimal a un binario de 8 bits con cualquiera de los dos métodos que se presentaron en la sección anterior, luego se divide la palabra en dos grupos de 4 dígitos binarios y se sustituye cada grupo por su símbolo hexadecimal equivalente (revisar Figura 25).

Ejemplo: convertir 168 a hexadecimal



Primero convertimos 168 a binario

- 168 es mayor o igual a 128? Si, anotamos 1 y restamos $168 - 128 = 40$
- 40 es mayor o igual a 64? No, anotamos 0 y continuamos con el siguiente valor posicional
- 40 es mayor o igual a 32? Si, anotamos 1 y restamos $40 - 32 = 8$
- 8 es mayor o igual a 16? No, anotamos 0 y continuamos con el siguiente valor posicional
- 8 es mayor o igual a 8? Si, anotamos 1 y restamos $8 - 8 = 0$, el número ha llegado a 0 paramos las iteraciones y completamos con ceros los bits restantes (tres posiciones).

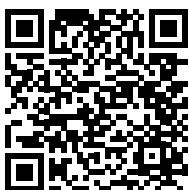
El número binario es 1010 1000. Hacemos dos grupos de cuatro bits y buscamos su equivalencia en hexadecimal, así: 1010 es AH y 1000 es 8H entonces el número en hexadecimal es A8H.

La habilidad de transformar sistemas de numeración es muy importante para un ingeniero en Redes y analítica de datos, porque le permitirá interpretar rápida y rigurosamente la información que circula por la red y las configuraciones que están presentes en los dispositivos que deberá administrar.

¡Ponga a prueba sus habilidades y resuelva este misterio!

Usted es un agente secreto que debe resolver un misterio. A lo largo de la actividad se le darán pistas que incluyen conversión de números. Anote las pistas para lograr abrir un sospechoso maletín. ¿Será capaz de resolver el misterio y encontrar el mensaje que guarda el maletín?

Participe en el siguiente juego de escape interactivo donde deberá aplicar sus conocimientos sobre sistemas de numeración para descifrar códigos secretos y completar las misiones que lo llevarán a obtener su insignia como agente profesional.



La misión del agente secreto

Como pudo experimentar durante la dinámica, la conversión entre sistemas de numeración es una habilidad práctica que trasciende el ámbito académico. Este ejercicio refuerza que las competencias técnicas en sistemas de numeración no son solo ejercicios teóricos, sino herramientas fundamentales para el análisis y configuración en entornos tecnológicos reales.



Luego de desarrollar la actividad, conteste en su cuaderno de apuntes o en un documento de Word las siguientes preguntas de reflexión:

- ¿Cuál es la funcionalidad de los valores posicionales en la conversión de sistemas numéricos?
- ¿Qué se puede intuir si el último bit de un número binario es uno?

2.3. Capa de enlace

La capa de enlace es la segunda capa dentro del modelo OSI, es decir, la capa que se encuentra entre la capa de red y la capa física. Por lo tanto, recibirá el paquete de la capa de red y se asegurará de que pueda acceder al medio a través del encapsulado en una trama apropiada. La capa física recibe la trama de la capa de red y la convierte en señales que introduce en los medios para que viajen a través de la red, como lo vio en la Sección 2.1 de esta Guía Didáctica.

2.3.1. Funciones de la capa de enlace

La capa de enlace actúa como un verdadero organizador local entre el hardware y la lógica de red, por lo tanto, su primera función es brindar servicios a la capa de red y ser una interfaz entre esta capa lógica y los medios físicos del equipo. Entonces recibe los paquetes de la capa de red, les añade información esencial para su transporte inmediato y, al mismo tiempo, se pone de acuerdo con la capa física para decidir cuándo y cómo estos bits deben salir al medio sin colisionar. Para profundizar en el análisis detallado de estas responsabilidades críticas, escuche atentamente el siguiente podcast que explora las funciones específicas de la capa de enlace y su papel fundamental en la comunicación eficiente entre dispositivos de red.

Funciones de la capa de enlace

Como pudo escuchar en el podcast, la capa de enlace desempeña un papel coordinador esencial que va mucho más allá de simplemente pasar datos entre capas. Habrá notado que esta capa actúa como un verdadero "director de tráfico local" que debe tomar decisiones complejas en tiempo real: desde el control de acceso al medio hasta la detección y corrección de errores.

Para sistematizar este conocimiento, las funciones de la capa de enlace se pueden resumir en los siguientes aspectos:

- a. **Encapsulamiento y delimitación de tramas:** la capa de enlace toma los paquetes que le entrega la capa de red y los encapsula en tramas, marcando claramente el inicio y el fin de la trama con cabeceras y tráileres. Este proceso, denominado framing como un anglicismo, permite que el receptor reconstruya la información exacta y la entregue intacta a la capa superior.
- b. **Dirección física y entrega local:** la capa de enlace se encarga de agregar en la cabecera las direcciones MAC de origen y destino, con ello garantiza que la información llegue solo al dispositivo correcto dentro de la red local. Este direccionamiento físico evita que los paquetes se propaguen innecesariamente y sienta la base para el aprendizaje de tablas de direcciones MAC en switches y procesos como resolución de direcciones ARP.
- c. **Detección y control de errores:** mediante campos de verificación, como el CRC o FCS ubicados en el tráiler, la capa de enlace comprueba la integridad de cada trama. Si el receptor, luego de realizar la suma de comprobación, detecta inconsistencias, descartará la trama para evitar que las capas superiores reciban tramas corruptas y se propaguen errores.
- d. **Control de acceso al medio:** cuando varios nodos comparten el mismo canal (cobre, fibra o espectro), la capa de enlace aplica reglas como CSMA/CD en Ethernet o CSMA/CA en Wi-Fi para evitar colisiones.

Para afianzar su conocimiento en la Tabla 15, puede ver el resumen de las funciones principales de la capa de enlace y cuál es su impacto en la operación de redes de computadores.

Tabla 15

Funciones de la capa de enlace en el Modelo OSI

Función	Descripción técnica	Beneficio operativo
Framing	Delimita dónde inicia y termina la unidad de datos (trama) con campos de cabecera y tráiler.	Permite que el receptor sincronice la lectura y ensamle los bits en información significativa.
Direccionamiento físico	Inserta la dirección MAC origen y destino (48 bits) para la entrega local.	Garantiza que solo el dispositivo correcto procese la trama, reduciendo tráfico innecesario.
Detección de errores	Calcula el FCS/CRC en el tráiler y lo contrasta en destino.	Descarta tramas dañadas antes de que contaminen capas superiores.
Control de acceso al medio (MAC)	Aplica reglas como CSMA/CD (Ethernet) o CSMA/CA (Wi-Fi) para evitar o gestionar colisiones.	Optimiza el uso del canal compartido y mantiene la integridad de los datos.

Nota. Ludeña, P., 2025.

Cada función de la capa tiene un beneficio operativo que le permite una ejecución eficiente. ¿Cuál cree usted que es la principal función de cara a la interoperabilidad de las redes actuales?

2.3.2. Subcapas de enlace de datos

La capa de enlace de datos se divide en dos subcapas:

- Control de enlace lógico (LLC por sus siglas en inglés *Logical Link Control*).
- Control de acceso al medio (MAC por sus siglas en inglés *Media Access Control*).

2.3.2.1. Subcapa LLC

Esta subcapa gestiona la comunicación entre la capa de enlace y las capas superiores, comenzando con la capa de red. En esta capa se dan las operaciones de multiplexación, demultiplexación y detección de errores.

Los servicios proporcionados por esta subcapa se encuentran especificados en el estándar IEEE 802.2 para propósito general y permite identificar qué servicio superior (IPv4, IPv6, ARP) debe recibirla.

2.3.2.2. Subcapa MAC

La subcapa MAC define el formato de trama específico (Ethernet II, 802.11, 802.15) dependiendo del medio con el que se cuenta en capa física. Esta subcapa encapsula los datos incorporando bits para delimitar la trama, sincronizar la transmisión, proporcionar direccionamiento y detectar errores.

MAC controla el hardware del dispositivo para enviar y recibir datos en el medio. Los dispositivos pueden configurarse para estar en modo semidúplex (half-duplex) o dúplex completo (full-duplex), esto se refiere a cómo se transmite la información. En semidúplex la comunicación es bidireccional pero no simultánea, es decir, sólo un dispositivo puede enviar a la vez, mientras que en full-duplex, ambos dispositivos pueden enviar y transmitir y recibir datos a la vez. Cuando los equipos están en semidúplex pueden colisionar y dañar las transmisiones, por ello es importante especificar qué dispositivo transmitirá en cada momento. La subcapa MAC gestiona las reglas de acceso al medio, ya sea CSMA/CD o CSMA/CA en medios con contienda, back-off exponencial, RTS/CTS, etc. Adicionalmente, para el control de errores esta subcapa realiza los cálculos para generar la secuencia de verificación de trama (FCS) y en el receptor se encarga de realizar la suma de comprobación.



Para afianzar sus conocimientos sobre las subcapas de la capa de enlace, le invito a revisar el video titulado "[Capa de Enlace de Datos Modelos OSI](#)". En el video podrá revisar algunas animaciones sobre cómo opera cada una de las subcapas. Revise cómo la capa MAC tiene como objetivo la codificación de datos, creación de tramas y el envío de las mismas por la red, mientras que la subcapa LLC se encarga de la interfaz entre el software y el hardware. Luego de revisarlo, establezca las principales diferencias entre ellas.

2.3.3. Switch o comutador

El switch o comutador es el dispositivo de capa de enlace, ya que toma decisiones con base en la información que proporciona la trama, principalmente, la dirección MAC de origen y la dirección MAC de destino.

El switch recibirá una trama por uno de sus puertos y su función será retransmitir la trama por el puerto o los puertos apropiados para que llegue a su destino. Para tomar esta decisión el comutador tiene una tabla de direcciones MAC, también llamada CAM, que contiene pares direcciones MAC-puerto por el cual se puede alcanzar dicha dirección.

Al encenderse el switch, la tabla estará vacía, por lo cual su primera tarea será poblar la tabla, para ello cada vez que una trama pasa por el switch, el equipo registra la dirección de origen y el número de puerto por el cual se recibió la trama. Con esta información se agrega una entrada en la tabla y una marca de tiempo, teniendo la certeza que a través de ese puerto se puede llegar al equipo que tiene esa dirección MAC. La marca de tiempo es importante para garantizar que la información se mantiene actualizada.

Para el reenvío de la trama se analiza la dirección MAC de destino y se puede tener dos casos. Primero, existe una entrada en la tabla para dirección de destino, en cuyo caso el switch retransmite la trama por el

puerto que se indica en la tabla. Y el segundo caso es cuando no existe una entrada coincidente en la tabla, en este caso el switch retransmite la trama por todos sus puertos salvo por el que recibió la trama. De esta manera intenta que la trama eventualmente llegue al destino.



Este proceso puede ser visto de forma dinámica en el video denominado “[Cómo el switch logra reenviar tramas a la computadora correcta](#)”, en el cual con una animación se verá cómo las direcciones que el switch encuentra en la trama son usadas para realizar sus funciones. Note principalmente la difusión a través de la cual se busca la dirección MAC, de hecho, este mecanismo es una vulnerabilidad que tiene este protocolo. El protocolo ARP mencionado en el video será estudiado extensamente en la Sección 2.9 de esta Guía Didáctica.

Las entradas almacenadas en la tabla pueden eliminarse si el temporizador vence, por lo general el temporizador se establece predeterminadamente en 5 minutos para evitar que la tabla crezca indefinidamente y que se tenga información desactualizada.

Es momento de evaluar su comprensión de los conceptos técnicos fundamentales abordados durante esta semana de estudio. El siguiente quiz le permitirá demostrar su dominio sobre sistemas de numeración (conversiones binaria-decimal-hexadecimal), funciones y subcapas de la capa de enlace (LLC y MAC), y características operativas de switches y comutadores.

[Sistemas de numeración y capa de enlace](#)

Como pudo verificar al completar la actividad, puede determinarse que la comprensión de los sistemas de numeración y de la capa de enlace resulta esencial para interpretar, configurar y analizar de manera rigurosa las redes de comunicación.



Actividad de aprendizaje recomendada

Es momento de aplicar sus conocimientos a través de la actividad que se ha planteado a continuación:

Lectura de los contenidos propuestos

Ingresé a la plataforma [Netacad](#) y revise el módulo 5: Sistemas numéricos y el módulo 6: Capa de enlace de datos. Analice las técnicas de conversión entre sistemas numéricos y revise los ejemplos proporcionados. Además, se comenzará el estudio de la capa de enlace con la definición de sus funciones y sus características.

Estrategia de trabajo:

- Reserve un horario determinado para revisar la plataforma Netacad y desarrollar las actividades recomendadas.
- Tome nota de las ideas claves y los algoritmos de resolución de problemas de conversión de sistemas numéricos.
- Complete las secciones. Verifique su comprensión en la plataforma.
- Compruebe su avance resolviendo las autoevaluaciones correspondientes.

Retroalimentación:

Resuelva las autoevaluaciones sin revisar apuntes de tal forma que su resultado le permita determinar secciones que deben ser reforzadas a futuro.



Sem 1 Sem 2 Sem 3 Sem 4 Sem 5 Sem 6 Sem 7 Sem 8



Semana 5

Estimado estudiante, esta semana centraremos nuestra atención en el Protocolo Ethernet, el estándar que desde hace más de cuatro décadas sostiene la mayor parte del tráfico local en oficinas, centros de datos, campus universitarios e incluso infraestructuras industriales. El protocolo ha sufrido algunas mejoras a lo largo de los años, por eso, nuestro objetivo principal será comprender la arquitectura de la trama, el método de acceso básico y la evolución de las velocidades que a lo largo de los años han permitido hacer más eficientes las redes de área local. Estos conocimientos le permitirán a futuro tener habilidades para la toma de decisiones sobre detección de fallas a nivel de cableado y conmutación, competencias que el perfil de egreso del ingeniero en Redes y Analítica de Datos exige para diseñar infraestructuras resilientes y extraer métricas significativas del flujo de datos. Le invito a reforzar el tema de Protocolo Ethernet revisando la bibliografía básica.

2.4. Protocolo Ethernet

Ethernet es un protocolo que opera en las dos capas inferiores del modelo de referencia OSI, es decir, capa física y capa de enlace de datos.

Evolución de Ethernet

Para comprender mejor cómo Ethernet se convirtió en la tecnología dominante en redes locales, es fundamental conocer su desarrollo histórico y los hitos que marcaron su evolución. La siguiente infografía de línea de tiempo presenta de manera cronológica y visual los momentos clave en la historia de Ethernet.

[Evolución histórica del estándar Ethernet.](#)

índice

I Bimestre

II Bimestre

Solucionario

Referencias

Como pudo observar en la línea de tiempo, la evolución de Ethernet ilustra perfectamente cómo la innovación tecnológica surge de la combinación entre investigación académica y colaboración industrial. Habrá notado que el desarrollo no fue lineal, sino que involucró múltiples actores y refinamientos sucesivos: desde la inspiración inicial en la red ALOHA, pasando por el prototipo de Xerox, hasta la estandarización colaborativa DIX y la posterior adopción por IEEE.

A comienzos de la década de 1970, Bob Metcalfe y David Boggs, inspirados por la red ALOHA, construyeron en Xerox PARC la primera LAN que compartía un único cable coaxial grueso y ofrecía 3 Mbps; la bautizaron Ethernet en alusión al éter luminífero que, según la física del siglo XIX, permitía propagar la luz. El éxito del prototipo motivó a DEC, Intel y Xerox a publicar en 1978 el estándar DIX (*Digital Equipment Corporation, Intel and Xerox*) de 10 Mbps, lo que se conoce como Ethernet DIX. Posteriormente, el IEEE con base en este realizó algunas modificaciones y en 1983 publicó un nuevo estándar, sentando las bases de todas las evoluciones posteriores. En la actualidad, el protocolo de Ethernet IEEE 802.3 (IEEE, 2022) se ha consolidado como la tecnología predominante en centros de datos, campus y entornos industriales gracias a su sencillez, bajo costo y escalabilidad.

Ethernet es un estándar de comunicación por cable, es decir, un medio guiado y, por tanto, permite tener un nivel básico de seguridad, al tener un control de acceso a la conexión a nivel físico. En contraparte, el número de puertos de conexión a un switch será el limitante para determinar el número máximo de dispositivos que se pueden conectar a la red.



En Ethernet se tienen diversas tecnologías como Fast Ethernet, Gigabit Ethernet, entre otras. Los subestándares tienen una nomenclatura específica:

Rapidez de transmisión + Tipo de señalización utilizada + Información sobre el medio físico.

Ejemplo:

Si tenemos 10BaseT significa que el estándar permite una transmisión de 10 megabits por segundo, en banda base y el medio físico es par trenzado.

En la tabla 16, usted podrá encontrar la especificación de los subestándares de Ethernet con la velocidad, el tipo de medio y el alcance máximo para cada uno de ellos.

Tabla 16

Especificaciones para subestándares de Ethernet

Denominación general	Velocidad estándar	Subestándar	Tipo de medio	Alcance máximo
Ethernet	10 Mbps	10Base2	Coaxial	185 m
		10Base5	Coaxial	500 m
		10BaseT	Par trenzado	100 m
		10BaseF	Fibra óptica	2000 m
		10BaseFL	Fibra óptica	2000 m
Fast Ethernet	100 Mbps	100BaseT4	Par trenzado (UTP Cat3)	100 m
		100BaseTX	Par trenzado (UTP Cat5)	100 m
		100BaseFX	Fibra óptica	2000 m
Giga Ethernet	1 Gbps	1000BaseT	Par trenzado (UTP Cat 5e o 6)	100 m
		1000BaseSX	Fibra óptica multimodo	550 m
		1000BaseLX	Fibra óptica monomodo	5000 m

Denominación general	Velocidad estándar	Subestándar	Tipo de medio	Alcance máximo
10 Giga Ethernet	10 Gbps	10GBaseSR	Fibra óptica multimodo	82 m
		10GBaseCX4	Coaxial	15 m
		10GBaseLX4	Fibra óptica multimodo	240 – 300 m
			Fibra óptica monomodo	10 Km
		10GBaseLR	Fibra óptica monomodo	10 Km
		10GBaseER	Fibra óptica monomodo	40 Km
		10GBaseLRM	Fibra óptica multimodo	220 m
		10GBaseSW	Fibra óptica multimodo	82 m
		10GBaseLW	Fibra óptica monomodo	10 Km
		10GBaseEW	Fibra óptica monomodo	40 Km
10GBaseT	<100 m		Par trenzado (UTP Cat 6 o 7)	<100 m
		10GBaseKX4	Placa base (Backplane)	1 m (4 vías)
10GBaseKR	1 m (1 sola vía)		Placa base (Backplane)	1 m (1 sola vía)

Nota. Ludeña, P., 2025.

Adicionalmente, existen en la actualidad algunos estándares de mayor velocidad que se conocen como Ultra-High-Speed Ethernet, por ejemplo: 25GBASE-SR/-LR cuyo medio es la fibra óptica, 25GBASE-T que usa cable Cat 8 y tiene alcance máximo de 30 m, 40GBASE-SR4 y -LR4, 100GBASE-SR4/-LR4, 200G y 400GBASE que se obtienen usando enlaces de fibra óptica en paralelo.



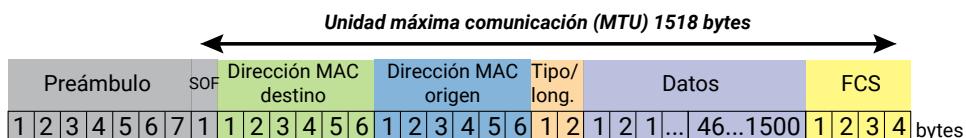
Reflexione sobre la gran variedad de opciones que usted tiene para implementar soluciones de red en diferentes escenarios. Una solución completa puede incluir una combinación de varios estándares, por ejemplo, 1000BaseT para llegar a los usuarios finales en escritorios, 10GBaseSR para conectar los equipos ubicados en los racks dentro del cuarto de comunicaciones y 40GBaseLR4 en el core de la red, todo dependerá de los requisitos, costo, compatibilidad y los planes de expansión de la red.

2.4.1. Trama de Ethernet

La base del protocolo Ethernet es la estructura de su unidad de datos de protocolo, denominada **trama**. De hecho, la principal diferencia entre las dos especificaciones en uso se encuentra en la estructura de la trama, pues en Ethernet DIX el campo que indica el tipo de protocolo, en IEEE 802.3 es el campo de longitud de trama (Tanenbaum & Wetherall, 2021). En la Figura 26, puede ver la estructura de la trama para el estándar Ethernet y el orden de los campos que la componen.

Figura 26

Estructura de la trama Ethernet



Nota. Ludeña, P., 2025.

Una trama Ethernet comienza con un octeto distribuido en dos secciones: preámbulo de sincronización de 7 bytes y el delimitador Start-of-Frame Delimiter (SOF) de 1 byte. Estos 8 bytes no se toman en cuenta para el cálculo del tamaño de la trama por cuanto sólo se usan para la sincronización entre el emisor y el receptor.

A continuación, se tienen los campos de direcciones MAC. Es importante notar que de acuerdo con la estructura primero se ubica la dirección MAC de destino y luego la de origen, esto tiene una función en los métodos de reenvío de tramas que posteriormente revisaremos. Los siguientes 2 bytes son el campo longitud/tipo (dependiendo del estándar usado), por ejemplo, si el contenido corresponde a un paquete IPv4 el campo tendrá el valor 0x0800.

Los datos de la trama, es decir, el paquete que viene de la capa de red y se está encapsulando en la trama, se ubican en el campo de carga útil y puede tener una extensión de entre 46 a 1500 bytes. Y finalmente,

va el tráiler, este es el campo Secuencia de verificación de trama o FCS (*Frame Check Sequence*) que tiene 4 bytes y usa un algoritmo de Comprobación de redundancia cíclica o CRC por sus siglas en inglés, para detectar si la trama recibida ha tenido errores durante la transmisión. En la Tabla 17, está la descripción resumida de los campos y las longitudes de cada uno de ellos.

Tabla 17

Resumen de los campos de la trama Ethernet

Campo	Tamaño (bytes)	Descripción
Preámbulo	7 bytes	Patrón de bits similar a 101010...1011 que indica al receptor que comienza la transmisión de bits.
Delimitador de inicio de trama / SFD	1 byte	Permite que emisor y receptor sincronicen relojes antes de que lleguen datos útiles
Dirección MAC de destino	6 bytes	Dirección física o MAC del receptor. Si todos los bits de la dirección son 1, la trama se envía a todos los equipos de la red local.
Dirección MAC de origen	6 bytes	Dirección física o MAC del emisor.
Tipo o	2 bytes	En Ethernet II indica el protocolo de la capa 3 que recibirá la carga (IPv4 0x0800, ARP 0x0806, IPv6 0x86DD, etc.).
Longitud en 802.3		En 802.3, valores ≤ 1536 representan la longitud de la carga y obligan a insertar un encabezado LLC para identificar el protocolo superior.
Datos	46 – 1500 bytes	Contiene el paquete IP u otra PDU. Si la carga es menor de 46 bytes, se añade relleno para alcanzar el tamaño mínimo de trama.
FCS	4 bytes	Secuencia de redundancia cíclica que permite al receptor detectar errores de bit.

Nota. Ludeña, P., 2025.

Con la especificación de la longitud de los campos se puede determinar que la trama completa tendrá tamaño entre 64 y 1518 bytes. Si existen

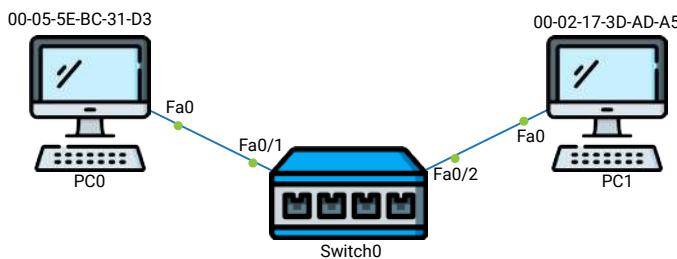
tramas más pequeñas al valor mínimo, el receptor las considerará como fragmentos de colisiones y se descartarán; y si existen tramas más grandes que el tamaño máximo las considerará como tramas gigantes y también las descartará.

Tanto la cabecera como el tráiler son añadidos por la subcapa MAC de la capa de enlace de datos, que se encarga tanto de la encapsulación como del acceso al medio, mientras que la subcapa LLC señala al protocolo de red al que pertenece la carga útil.

Veamos un ejemplo práctico. Suponga que tenemos la red de la Figura 27, donde la PC0 con dirección MAC 00-05-5E-BC-31-D3 quiere comunicarse con la PC1 cuya dirección MAC es 00-02-17-3D-AD-A5. El protocolo de capa de red será IPv4 y transportará un paquete de 500 bytes.

Figura 27

Ejemplo de trama Ethernet para comunicación entre dispositivos en una red LAN



7 bytes	1 bytes	6 bytes	6 bytes	2 bytes	46 - 1500 bytes
Preambulo	SOF	Dirección MAC destino	Dirección MAC origen	Tipo/longitud	Datos
101010...1011	1	00-02-17-3D-AD-A5	00-05-5E-BC-31-D3	0X0800	paquete de 500 bytes

Nota. Ludeña, P., 2025.

Ahora analice cómo se llenarían los campos de la trama correspondiente. La tarjeta de PC1 crea la trama comenzando con el preámbulo, añade la MAC de PC1, su propia MAC de origen, el valor 0x0800 por el tipo de dato transporta, el paquete que entregó la capa de red, que en este caso tiene un tamaño de 500 bytes. Y, finalmente, se añade el FCS calculado para la trama. La trama viajará a través del medio y el switch, el cual la retransmitirá apropiadamente para que llegue a PC1. Una vez que llegue al destino, PC1 validará el FCS para comprobar que la trama no tiene errores, si en efecto, no tiene errores la pasará a la capa siguiente.

Reflexione las siguientes preguntas:

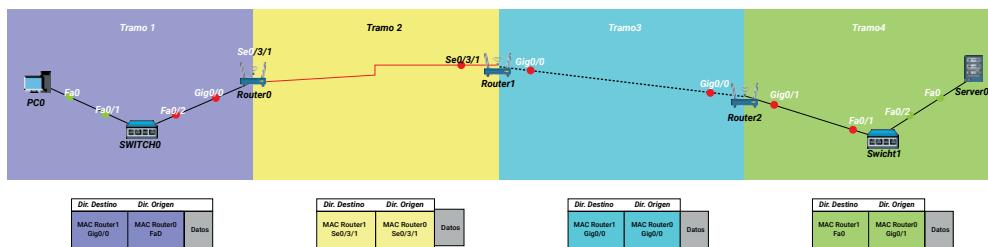


- ¿Cuándo es necesario que se armen tramas?
- ¿La información de direcciones MAC de origen y destino cambian a lo largo de la ruta de un paquete o siempre son las mismas?

El formato de trama que se ha presentado en esta sección es para el protocolo Ethernet, pero hay muchos formatos de tramas como protocolos de capas inferiores. Entonces, en esencia cada vez que se cambia de medio de transmisión se cambiará el formato de la trama. Por otra parte, considere ahora la trayectoria para un mensaje que va desde la PC0 a un servidor identificado como Server0, descrita en la Figura 28. Cada red de la topología está indicada como un tramo de la trayectoria con un color diferente para su fácil diferenciación.

Figura 28

Evolución de las tramas Ethernet en el camino de origen a destino



Nota. Ludeña, P., 2025.

Los datos se entregan única y exclusivamente entre equipos que se encuentran dentro de la misma red y, por tanto, en cada tramo la trama cambiará los datos de dirección MAC de origen y dirección MAC de destino. Note como en cada tramo se tiene una nueva dirección MAC de origen y de destino, de acuerdo con las interfaces involucradas en esa parte del trayecto, corresponde al destino y al origen correspondiente (las siglas Fa corresponden a FastEthernet, Gig a GigabitEthernet y Se a Serial). Por ejemplo, en el tramo 1 la trama tiene como destino la MAC de la interfaz G0/0 del Router0, y como origen la MAC del PC. Mientras, en el tramo 2 la dirección de destino es la dirección MAC de la interfaz serial identificada como 0/3/1 del Router1 y la dirección de origen es la dirección MAC de la interfaz serial 0/3/1 del Router 0. A medida que la trama pasa por los routers (Router0, Router1 y Router2), sus encabezados de capa 2 se actualizan, manteniendo constante únicamente el contenido de los datos.

Estructura de trama Ethernet

En esta actividad usted deberá recordar la estructura de la trama Ethernet y la descripción de cada uno de los campos que la componen. Este ejercicio interactivo ha sido diseñado para que usted pueda hacer varios intentos y compruebe sus conocimientos que a futuro le permitirán detectar fallos en el funcionamiento de los equipos de redes. Proceda a realizar el siguiente juego de arrastrar y soltar donde organizará

correctamente los componentes de la trama según su secuencia y funcionalidad específica dentro del protocolo Ethernet.



Estructura de la trama de Ethernet

Como pudo comprobar al trabajar con la estructura de la trama Ethernet, cada campo tiene una función específica y crítica en el proceso de comunicación de datos. Su capacidad para identificar y ubicar correctamente estos componentes demuestra su comprensión de cómo los datos se organizan y protegen durante la transmisión.

Luego de desarrollar la actividad, conteste en su cuaderno de apuntes o en un documento de Word las siguientes preguntas de reflexión:



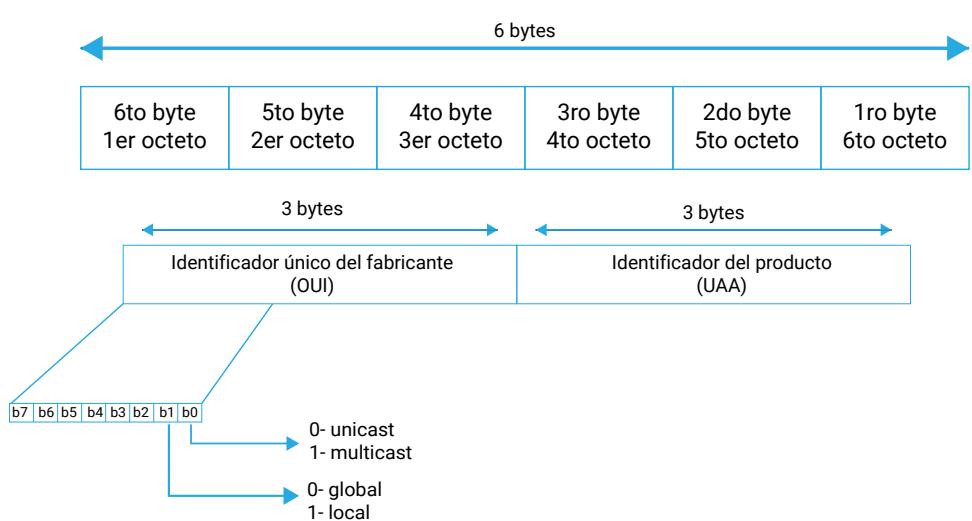
- ¿Cuál es el fin práctico de que la dirección MAC de destino vaya antes que la dirección MAC de origen en la trama Ethernet?
- ¿Cuál es el tamaño máximo de una trama Ethernet?
- ¿Qué pasa si el switch recibe una trama de 40 bytes?

2.4.2. Direcciones MAC

Como se pudo dar cuenta para la capa de enlace la dirección MAC o dirección física es el elemento esencial para tomar decisiones, por tanto, es importante que usted conozca cómo está conformada la misma. La dirección física que cada interfaz Ethernet tiene es asignada de fábrica y consta de 48 bits, representados en 12 dígitos hexadecimales. En la Figura 29, usted puede revisar la estructura de la dirección MAC.

Figura 29

Estructura y significado de los campos en una dirección MAC



Nota. Ludeña, P., 2025.

La dirección MAC se divide en dos partes, los tres primeros octetos son conocidos como **identificador único** de fabricante y los tres octetos restantes son los denominados **identificador del producto**, o conocidos como OUI y UAA, respectivamente por sus siglas en inglés. El OUI es asignado a cada fabricante por el IEEE y garantiza la unicidad global de la dirección, es decir que no pueden existir dos direcciones MAC iguales. Los identificadores de producto son asignados a criterio del fabricante para individualizar cada tarjeta, podrían tener formatos para especificar el tipo de dispositivo y modelo.

Dentro del primer octeto destacan dos bits: el b0 - I/G (Individual/ Group) indica si el destino es unidifusión = 0, multidifusión = 1, y el b1 - U/L (Universally/Locally administered) señala si la MAC es de fábrica = 0 o reasignada por software = 1.

Para ilustrar, retomemos los datos de PC0 que usamos en el ejemplo anterior, la dirección MAC es 00-05-5E-BC-31-D3. El OUI es 00-05-5E

que corresponde al fabricante Cisco Systems, ahora analizaremos los bits del primer octeto 00, entonces I/G = 0 que significa unidifusión y U/L = 0 que indica que tiene administración global, es decir, sigue la regulación de IEEE. El identificador de producto es BC-31-D3.

Ahora, le invito a revisar el video titulado "[¿Qué es una dirección MAC?](#)", con el objetivo de que pueda afianzar los conocimientos sobre direcciones físicas. En este recurso puede ver la estructura de la dirección, revise particularmente los ejemplos para identificar la OUI de la dirección MAC. Luego de ver el video, responda en su cuaderno de apuntes o en un documento de Word las siguientes preguntas de reflexión:

- ¿Cuándo una empresa quiere fabricar tarjetas de red, quién le asigna el OUI que deberán tener todas sus tarjetas?
- ¿Cuál es la ventaja de tener direcciones MAC únicas para cada dispositivo a nivel mundial?

2.4.3. Métodos de reenvío de switch

Existen tres métodos de reenvío que un switch puede utilizar para retransmitir cada trama, depende de las características que tiene la red para decidir cuál de ellos implementar porque cada uno de ellos tiene características diferentes en términos de latencia, confiabilidad y procesamiento. A continuación, se presentan los métodos de reenvío para luego discutir los escenarios de aplicación.

1. Conmutación de almacenamiento y reenvío (store-and-forward)

Piense en un agente de aduanas que retiene el paquete, lo inspecciona por completo y solo lo libera si pasa todas las revisiones, ese es exactamente el proceso que realiza el switch en este método. El switch recibe toda la trama, comprueba el CRC y descarta de inmediato cualquier trama corrupta; sólo si la trama no tiene errores el switch busca la MAC de destino para buscar en la tabla CAM y la envía por el puerto correcto. Este método elimina la propagación de errores y

permite aplicar QoS, pues el equipo ya tiene la trama completa para clasificarla. La ventaja de este método es que aporta confiabilidad, pero la desventaja es que, por los procesos que realiza, añade latencia y necesita un espacio de memoria intermedia para almacenar la trama para el análisis.

2. Conmutación de corte (cut-through) y avance rápido (fast-forward):

En este método el switch actúa como un corredor de postas, que tan pronto como recibe la dirección MAC de destino (recuerde que en la trama la dirección MAC de destino está dispuesta al inicio, los primeros 6 bytes), comienza a reenviar el resto de los bits de la trama al puerto adecuado sin esperar al final de la trama. La ventaja que tiene este método es que tiene una latencia mínima, lo que la convierte en ideal para transmisión de datos sensibles al retardo. La principal desventaja es que se pueden propagar errores y al transmitir inmediatamente incluso se pueden transmitir tramas de menos de 64 bytes que serán descartadas en el destino.

3. Conmutación de corte (cut-through) sin fragmentos (fragment-free):

Para encontrar un punto medio entre los métodos anteriores se tiene esta técnica sin fragmentos, en donde el switch almacena los primeros 64 bytes y verifica rápidamente que no existan errores para luego retransmitir el resto de los bits de la trama. De esta forma se reduce la probabilidad de propagar tramas dañadas y al mismo tiempo no se agrega demasiada latencia.

Ahora que conoce las características técnicas de cada método, es momento de aplicar este conocimiento a escenarios reales. Reflexione sobre las siguientes preguntas:



¿cuándo debería utilizar cada uno de estos métodos?

Suponga una red corporativa, donde la prioridad es la integridad de los datos y la coexistencia de servicios (voz, video, aplicaciones de negocio). ¿Qué método usaría y por qué?

En contraste, considere un escenario completamente diferente: suponga un centro de baja latencia, donde los servidores de trading electrónico intercambian mensajes de pocos bytes en enlaces de 100 Gbps, ¿qué método usaría y por qué?

Como puede observar en estos ejemplos, al conocer las ventajas y las limitaciones de cada método, usted podrá ajustar sus conmutadores al perfil de tráfico y a los objetivos y características de cada servicio y tipo de red.

Su conocimiento en tecnologías de red será puesto a prueba mediante un caso de estudio que simula las complejidades del mundo profesional. En esta simulación asumirá la responsabilidad de diseñar una solución de conectividad para una organización con múltiples perfiles de usuario y aplicaciones críticas.

Implementación de Red Ethernet Corporativa

El análisis que ha realizado a través de este caso demuestra cómo la teoría de redes se transforma en valor empresarial cuando se aplica con criterio técnico sólido y visión estratégica. Habrá observado que las decisiones óptimas emergen del equilibrio inteligente entre performance técnico, viabilidad económica y adaptabilidad futura, requiriendo no solo dominio conceptual sino también habilidades de análisis crítico y comunicación técnica.



Actividades de aprendizaje recomendadas

Continuemos con el aprendizaje mediante su participación en la actividad que se describe a continuación:

Actividad 1. Lectura de los contenidos propuestos

Ingresé a la plataforma [Netacad](#) y revise el módulo 7: Switching Ethernet. Este módulo se centra en el estudio del Protocolo Ethernet por ser el más utilizado en redes LAN, con este objetivo se presenta la estructura de la trama estándar y los campos que la componen para evaluar la funcionalidad práctica de cada uno de ellos. Con base en este protocolo se presenta la gestión de tramas en un switch a través de la tabla de direcciones y los métodos de reenvío.

Estrategia de trabajo:

- En el espacio de tiempo reservado para esta asignatura, ingrese a la plataforma Netacad y desarrolle las actividades recomendadas.
- Ejecute las animaciones disponibles en el subtema 7.2 del módulo 7 en la plataforma para revisar visualmente el procesamiento de tramas que realizan los switches.
- Revise los videos sobre las tablas de direcciones en switches para comprobar cómo se toman las decisiones dentro del switch con base en las direcciones MAC de destino.
- Tome nota de las ideas claves en su cuaderno de apuntes.
- Realice la autoevaluación cuando se sienta preparado.

Retroalimentación:

En las autoevaluaciones, la plataforma Netacad le corregirá las preguntas, identifique qué áreas debe volver a reforzar.

Actividad 2. ¿Cuál es mi dirección MAC?

En esta actividad descubrirá cómo, a través de comandos, puede conocer la dirección MAC de los dispositivos en los principales sistemas operativos. El conocimiento de esta información es muy importante para las actividades de monitoreo que se realizan dentro del área de TI.

Estrategia de trabajo:

- Identifique qué sistema operativo usa en sus dispositivos.
- Siga estos sencillos pasos, de acuerdo con el sistema operativo específico, y registre los resultados obtenidos para cada interfaz disponible en su equipo (cableadas e inalámbricas).

1. Windows 10/11

1. Abra Símbolo del sistema (Tecla Windows + R → cmd).
2. Ejecute: ipconfig /all.
3. Busque la línea de tarjeta Ethernet o wifi y anote el campo Dirección física. Recuerde que el formato de la dirección será dado en hexadecimal así XX-XX-XX-XX-XX-XX.

2. GNU/Linux

1. Abra la terminal.
2. Escriba ip link show o ifconfig -a

3. Localice la interfaz (eth0, enp3s0, wlan0...) y copie la dirección que encontrará luego de link/ether luego de HWaddr.

3. macOS

1. Abra Terminal.
 2. Ejecute ifconfig en0 (Wi-Fi) o ifconfig en1 (Ethernet).
 3. La línea ether xx:xx:xx:xx:xx:xx muestra la dirección MAC.
- En cada caso, verifique el número de dígitos hexadecimales que compone la dirección MAC.

Retroalimentación:

Ahora realice una investigación sobre el fabricante de su tarjeta de red. Ingrese a la página web: [MAC Address Lookup](#) y escriba su dirección MAC. Luego de realizar la investigación, responda las siguientes interrogantes:

- ¿Qué información le ofrece esta aplicación?
- ¿Por qué se puede mapear al fabricante a través de su dirección MAC?

Repita el proceso para todas las direcciones MAC de las interfaces disponibles en su dispositivo.

Recuerde que los primeros seis dígitos corresponden al OUI de su fabricante (podría consultarla en [ieee.org](#)), de esa forma es fácil extraer la información sobre su tarjeta de red. Con esta actividad, usted relacionará la teoría de la estructura MAC con la realidad de la interfaz de red.

Actividad 3. Es hora de medir nuestro avance

En la plataforma Netacad encontrará el Examen de punto de control: Examen de conceptos de Ethernet (módulos 4-7), que le propondrá cuestiones sobre los conceptos de las secciones 2.1 a la 2.4 de esta guía didáctica.

Le animo a completar la evaluación, ya que esta actividad no solo representa un paso clave para aprobar el módulo, sino que también le abre la posibilidad de obtener una microcertificación. Este reconocimiento es altamente valorado en el mercado laboral y añadirá un distintivo importante a su currículo. ¡Confío en su capacidad para alcanzarlo!



Semana 6

En esta semana empezaremos el estudio de la capa de red que actúa como el sistema circulatorio de *Internet*, es decir, se encarga de llevar los datos hacia cada rincón de la red de redes. Usted aprenderá cuáles son las funciones de la capa de red y cómo cumple con ellas, cómo se identifican los equipos en capa de red; y, también, conocerá qué dispositivo y cómo transporta los paquetes desde la red de origen al destino final. Estos conceptos le permitirán tener una base sólida para obtener habilidades en el diseño de infraestructuras de telecomunicaciones, diagnóstico de fallos y optimización de calidad de servicio, que son competencias esenciales para un ingeniero en Redes y Analítica de Datos.

2.5. Capa de red

Para comprender cómo funciona la capa de red, imagine que cada paquete de datos es un repartidor de un local comercial que debe hacer una entrega a una casa cuya dirección le ha sido dada con ubicación por GPS. El repartidor lleva el producto (datos) en una maleta de reparto (paquete) y llevará consigo la dirección. Al principio deberá conducir por las calles del barrio que son aledañas al local comercial; luego, llegará a la avenida principal y avenidas de circunvalación; y, eventualmente, llegará a las calles secundarias aledañas a la casa, que constituye su destino final. Pese a que el GPS determina una ruta desde el origen hasta el destino, en cada bifurcación u obstáculo (por ejemplo, tráfico imprevisto) es capaz de recalcular la ruta. En el caso de la capa de red, el barrio del origen y del destino son las redes locales y las bifurcaciones hacia avenidas principales y avenidas de circunvalación son *routers*, siendo las avenidas redes de mayor amplitud e incluso el núcleo de *Internet*. En el ejemplo, el GPS traza la ruta que debe seguir el repartidor. En el caso de la capa de red, cada *router* debe tomar la decisión de la

ruta en la que debe tomar el paquete en cada segmento de red hasta llegar al destino.

2.5.1. Funciones de la capa de red

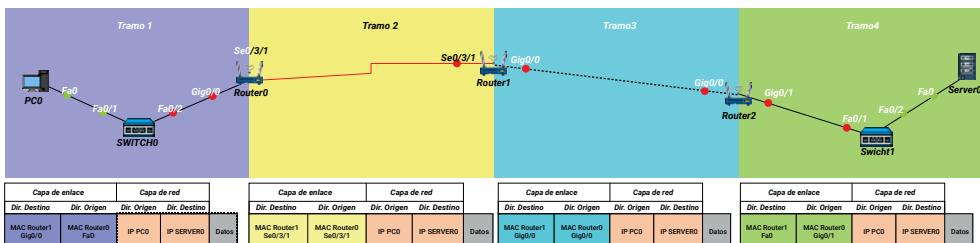
La capa de red tiene varias funciones esenciales para la comunicación de computadoras; de hecho, su importancia es tal que está presente de manera individual tanto en el modelo de referencia OSI como en el modelo TCP/IP, donde se le denomina capa de *Internet*.

A continuación, se mencionarán las funciones de la capa de red que permiten transportar datos a través de diferentes redes.

1. Direcciónamiento lógico global: la capa de red se encarga de asignar direcciónamiento lógico a través de la configuración de direcciones IP en cada interfaz de red. La dirección IP, ya sea IPv4 o IPv6, es un identificador único que permanece constante a lo largo de todos los trayectos que atraviesa el paquete hasta llegar a su destino (ver figura 30), siguiendo nuestra analogía del repartidor serían las direcciones de origen y destino que fueron ingresadas en el GPS, aunque la ruta cambie, estos puntos no van a cambiar.

Figura 30

Comportamiento de paquetes IP y tramas Ethernet a lo largo de la ruta de comunicación



Nota. Ludeña, P., 2025.

Revisemos el flujo de comunicación entre el computador (PC0) y un servidor (Server0), a través de varios dispositivos de red: dos switches y tres routers. El recorrido está dividido en cuatro tramos. En cada tramo se muestra cómo las direcciones MAC de origen y destino cambian según las interfaces del siguiente salto, pero las direcciones IP de origen (PC0) y destino (Server0) permanecen constantes en todos los tramos. En la información enviada se puede constatar que, en la capa de enlace, se actualizan las MACs para reflejar el siguiente salto físico; mientras que, en la capa de red, siempre se mantiene IP origen: PC0 e IP destino: Server0.



Recuerde que cuando se estudió las direcciones MAC origen y destino que se incluían en la trama, éstas cambian en cada trayecto de red porque deben identificar la fuente y receptor de cada tramo y el formato de trama depende del medio físico.

2. **Encapsulamiento y desencapsulamiento de segmentos:** la capa de red se encarga de encapsular la estructura de datos que proviene de la capa de transporte, denominada segmento. Para ello agrega una cabecera con campos específicos, la cabecera promedio tendrá una extensión de 20 bytes si es IPv4 o 40 bytes si es IPv6. Cuando llega al destino, la capa de red homóloga realiza el proceso inverso y entrega a la capa superior el segmento.
3. **Reenvío (forwarding):** como se explicó en la analogía, la capa de red es la encargada de decidir en cada intersección por dónde enviar los paquetes. Para ello, cada que un paquete llega a un router, se consulta la tabla de encaminamiento por cuál interfaz se debería reenviar ese paquete, para, posteriormente, enviarlo al enlace de salida adecuado.
4. **Enrutamiento (routing):** una de las tareas más importantes de la capa de red es armar la tabla de rutas para que el router pueda tomar decisiones de encaminamiento. La tabla tiene

una línea por cada ruta disponible, sólo las mejores rutas son almacenadas en la tabla. Las rutas pueden ser aprendidas automáticamente, configuradas estáticamente al ser introducidas por un administrador de red o ser aprendidas dinámicamente a través de un protocolo de enrutamiento como OSPF o BGP. El enrutamiento incluye las tareas de mantenimiento y actualización, retirando rutas inválidas y anunciando alternativas para mantener la conectividad.

5. **Fragmentación y adaptación al tamaño de trama:** cuando un paquete encuentra un enlace con menor Unidad de Transmisión Máxima (MTU), el protocolo IPv4 puede dividirlo en fragmentos para que cada pieza se ajuste al nuevo límite y llegue al destino, donde se reensambla para ser entregado a las capas superiores.

A su criterio, ¿cuál de las funciones de capa de red presentadas es la más importante y por qué? ¿cuál de estas funciones puede aportar estadísticas que luego podría analizar para mejorar la eficiencia de la red?

2.5.2. Características de la capa de red

Estimado estudiante, le invito a observar el video donde explorará las características esenciales que definen el comportamiento de esta capa crítica del modelo OSI, analizando cómo sus propiedades técnicas específicas han revolucionado la conectividad mundial. Comprenderá por qué ciertos atributos como el direccionamiento jerárquico, el enrutamiento dinámico y la independencia del medio físico no son simplemente especificaciones técnicas, sino elementos fundamentales que han permitido la expansión exponencial de las redes de comunicación a escala planetaria.

[Características de la capa de red](#)

El análisis que ha realizado sobre las características de la capa de red revela la elegancia ingenieril detrás de uno de los diseños de protocolo más exitosos en la historia de las telecomunicaciones. Ha podido apreciar cómo propiedades aparentemente técnicas como la conmutación de paquetes, el direccionamiento lógico y la capacidad de interconexión entre redes heterogéneas se traducen directamente en capacidades operacionales que transformaron la comunicación humana.

La capa de red opera en base al protocolo IP, por tanto, las características del protocolo se asocian directamente a la capa de red. Las características que distinguen al protocolo IP le han permitido tener un alcance global, de ahí que Internet, por ejemplo, tenga un alcance planetario.

Una de las primeras características importantes es el direccionamiento lógico y su estructura jerárquica. Cada interfaz de un equipo de red recibe un identificador único de red (IPv4, IPv6 o ambos). Este identificador pertenece a un grupo denominado **red**. Todos los equipos que componen la red local compartirán una misma dirección de red.

La capa de red, al trabajar con direcciones lógicas, ofrece facilidades para que las redes puedan añadir nodos sin colapsar, pues los enrutadores solo almacenan en sus tablas rutas a las direcciones de las redes de destino (como prefijos) no a cada uno de los dispositivos que se encuentran en ellas.

Otra característica importante es que la capa de red es independiente de los medios. El mismo paquete IP puede viajar sobre cobre, fibra o radio sin modificar su formato, por ejemplo, como se pudo haber dado cuenta en la Figura 30, el paquete pasó de viajar en cables UTP directos a cable serial, luego a cable cruzado y nuevamente a UTP directo y no cambió su estructura. La capa de red únicamente se acopla a la Unidad de Transmisión Máxima que cada enlace soporta y, si lo necesita, puede fragmentar el paquete y reensamblarlo en destino. Esto posibilita

la interconexión de redes heterogéneas, superando diferencias de tecnología, tamaño de trama o política administrativa.

Finalmente, el protocolo IP en la capa de red ofrece un servicio denominado de **mejor esfuerzo**. Esto es servicio sin conexión, lo que quiere decir que no establece circuitos virtuales previos, tampoco garantiza que los paquetes llegaran en orden a su destino, es más, ni si quiera garantiza que los paquetes llegarán.



La capa de red simplemente intenta entregar los paquetes que le han sido dados y delega la confiabilidad a capas superiores. Esto tiene mucho sentido si consideramos que las capas inferiores (física, enlace y red) son las encargadas de transportar los datos por todos los dispositivos intermediarios que se requiera, y es necesario mantener su operación ligera y eficiente.

2.5.3. Direccionamiento IP

El direccionamiento es una de las principales funciones de la capa de red. La dirección IP se divide en dos porciones: porción de red y porción de host.

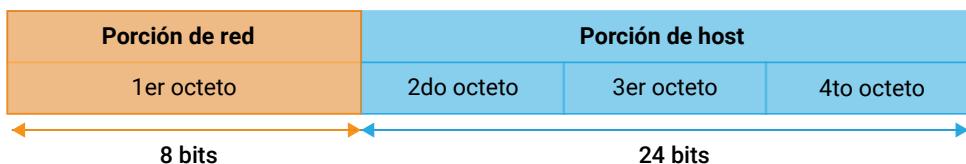
- La **porción de red** es la parte de la dirección que identifica a la red a la que pertenece un dispositivo, por tanto, todos los hosts que pertenecen a la misma red tendrán la misma porción de red. Los bits que componen esta porción se cuentan desde la izquierda y el total de bits que pertenecen a esta porción se denomina longitud de prefijo.
- La **porción de host** son los bits que permiten identificar a un dispositivo específico dentro de una red, esta porción debe ser única para cada red.

Como analogía, pensemos en una dirección, la porción de red sería como el nombre de la calle y la porción de red sería el número de la casa en esa calle. Así como hay muchas casas en una misma calle, así mismo, puede haber muchos hosts en una misma red local, pero cada host tendrá una identificación única. En la Figura 31, puede ver un ejemplo de la distribución en porciones de una dirección IPv4.

Figura 31

Ejemplo de distribución de bits de una dirección IPv4

Dirección IPv4: 32 bits



Nota. Ludeña, P., 2025.

La sección anaranjada es la porción de red y comienza desde la izquierda ocupando el primer octeto es decir 8 bits; mientras que la porción de host en color azul ocupará los tres octetos restantes, los 24 bits restantes.

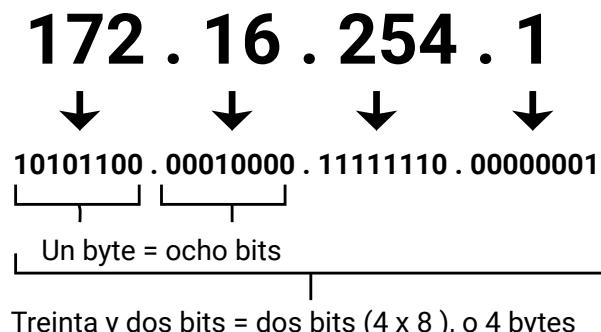
Dependiendo del protocolo que se use, IPv4 o IPV6, el número de bits de la dirección y la representación será diferente.

En IPv4, la dirección es una palabra de 32 bits que se representa en cuatro octetos decimales, como 172.16.254.1, en la Figura 32, usted puede ver la distribución de los bits y octetos para este ejemplo.

Figura 32

Ejemplo de dirección IPv4 en formato binario y punto decimal para 172.16.254.1

Direccion IPV4



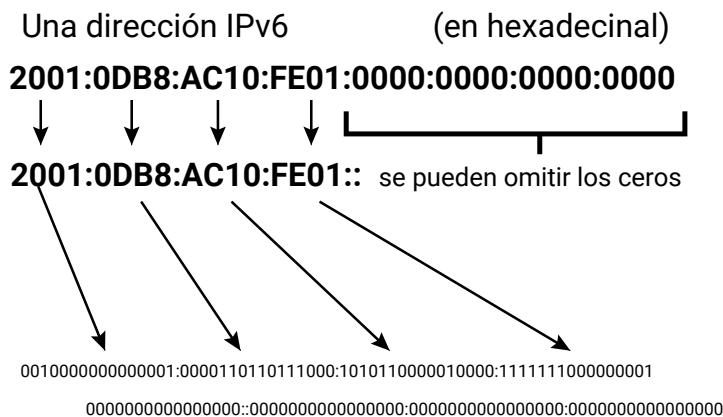
Nota. Tomado de *Ipv4 address Spanish* [Ilustración], por Loadmaster, 2013, [WikimediaCommons](#), CC BY 4.0.

Esta notación suele ir acompañada de una barra y un número, por ejemplo 172.16.254.1/24, esta notación indica la longitud del prefijo, es decir, indica cuántos bits pertenecen a la porción de red, en el ejemplo, 24 bits pertenecen a la porción de red y en consecuencia sólo 8 bits quedarían en la porción de host. En consecuencia, también podemos calcular cuántas direcciones posibles direcciones de host se tendrían, basta con elevar la base 2 al número de bits en la porción de hosts. Así para el ejemplo tendríamos 256 posibles direcciones ($2^8=256$), el rango de direcciones iría desde 0 a 255.

En IPv6 la dirección se compone de 128 bits representados en ocho hexáctetos en formato hexadecimal, por ejemplo 2001:0DB8:AC10:FE01:0000:0000:0000:0000 (ver Figura 33), acompañado de una barra y un número, por ejemplo, /64 que, al igual que en IPv4, indica la longitud de la porción de red, denominada longitud de prefijo y marca la frontera entre el prefijo de red y la parte de interfaz.

Figura 33

Ejemplo de dirección IPv6 en formato hexadecimal



Nota. Tomado de *Ipv6 address-es-corrected* [Ilustración], por KugXel, 2015, [WikimediaCommons](#), CC BY 4.0.

Debido al gran número de bits que poseen suelen y pese a que las direcciones IPv6 usan formato hexadecimal, se han planteado dos reglas de compresión para acortar su escritura y facilitar su memorización.

1. **Omitir ceros iniciales en cada hexteto:** dentro de cada bloque de 4 dígitos hexadecimales (hexteto) se pueden suprimir los ceros que encabezan cada grupo. Por ejemplo: 03F2 se puede representar como 3F2 y 0000 como 0. Los ceros intermedios o finales no se pueden omitir porque generaría ambigüedad, por ejemplo, el hexteto 1050 no podría ser reemplazado por un formato comprimido.
2. **Los dos puntos dobles (::) pueden sustituir una única secuencia continua de hextetos 0000:** la regla sólo puede usarse una vez por dirección para evitar ambigüedad. El número exacto de hextetos omitidos se determina por la longitud total (debe haber 8 hextetos en la dirección completa).

En la Tabla 18, encontrará unos ejemplos de aplicación de las reglas de compresión para direcciones IPv6.

Tabla 18

Ejemplos de compresión de direcciones IPv6 aplicando reglas de abreviación

Dirección completa	Aplicación regla 1	Aplicación regla 1 + 2
2001:0db8:0000:0000:0000:00a0:0100	2001: db8:0:0:0:a0:100	2001:db8::a0:100
FE80:0000:0000:0000:021C:7EFF:FE11:92D0	FE80: 0:0:0:21C:7EFF:FE11:92D0	FE80::21C:7EFF:FE11:92D0
0000:0000:0000:0000:0000:0000:0001	0:0:0:0:0:0:1	::1

Nota. Ludeña, P., 2025.

Analice la primera y la última columna con detenimiento, ¿cree que es útil la aplicación de las reglas de compresión? ¿utilizaría estas reglas en el ejercicio de su carrera? ¿por qué?

Todos los equipos que componen la red local compartirán una misma dirección de red, una misma máscara de red y una misma dirección de difusión o de broadcast. ¿Pero qué son estos conceptos? ¿Para qué se usan? A continuación, lo descubriremos.

- **La dirección de red** es el identificador lógico que representa toda la red, es decir, que cuando mencionamos la red estamos mencionando al grupo de hosts de la red local. Piense que la red local es una familia, entonces la dirección de red es el apellido de la familia, por ejemplo, Suárez Mendoza. Cuando decimos los Suárez Mendoza nos referimos a todos en general. La dirección de red es usada por los routers para agregar entradas en sus tablas de rutas.
- **La dirección de difusión o broadcast** está establecida sólo para IPv4. En esta dirección todos los bits de la porción de host se ponen a 1. El paquete enviado a esa dirección llega simultáneamente a todos los nodos en la red local.

- **La máscara de red** es una cadena de 32 bits cuyo objetivo es delimitar que parte de la dirección es porción de red y qué parte es porción de host para IPv4. Para esto, pone unos en todos los bits que pertenecen a la porción de red y pone ceros en todos los bits que pertenecen a la porción de host. Se expresa en notación decimal punteada (255.255.255.0) o como longitud de prefijo (/24).

En la Tabla 19, puede ver los valores por octeto de una máscara de red.

Tabla 19

Posibles valores de la máscara para una dirección IPv4

Número de bits en 1	Número binario en el octeto	Equivalente decimal
0	00000000	0
1	10000000	128
2	11000000	192
3	11100000	224
4	11110000	240
5	11111000	248
6	11111100	252
7	11111110	254
8	11111111	255

Nota. Ludeña, P., 2025.

Por ejemplo, si la dirección tiene un prefijo /19 la máscara de red abarcaría dos octetos completos (16 bits) y 3 bits del tercer octeto, entonces de acuerdo con la tabla, el primer octeto con 8 bits tendría valor 255, el segundo octeto con 8 bits tendría valor 255, el tercer octeto con tres bits tendría valor de 224 y el cuarto octeto con 0 bits tendría el valor de 0, así la máscara para esta dirección es 255.255.224.0.

La máscara de red permite a hosts y routers determinar, mediante operaciones lógicas simples, si dos direcciones están en la misma red o si el tráfico debe a otra red.

Alguna vez se ha preguntado ¿cómo un computador sabe si el destino al que quiere llegar está en su red local o en una red remota?

Para resolver esta inquietud, se sigue un proceso que involucra la dirección IP de origen, dirección IP del destino, la máscara de red y la operación AND. Y que le explicaré a través de un ejemplo.

Ejemplo:

Supongamos que el computador PC 192.168.10.25/24 quiere enviar un paquete al servidor 192.168.20.10.

Paso 1. Encontrar la máscara de red. La dirección del equipo es 192.168.10.25 y al tener prefijo /24 se sabe que se tienen 24 bits en la porción de red, lo que quiere decir que los primeros 24 bits de la máscara estarán en 1 y los demás en 0, que en formato decimal punteado sería 255.255.255.0.

Paso 2. Luego se aplica la operación AND bit a bit entre la dirección IP del dispositivo y la máscara de red, en la Tabla 20, usted dispone de los resultados de aplicar AND para los posibles operadores.

Tabla 20

Operación AND

Bit 1	Bit 2	AND
0	0	0
0	1	0
1	0	0
1	1	1

Nota. Ludeña, P., 2025.

La operación AND sólo tendrá resultado 1 cuando los dos operadores sean 1, en el resto de los casos será 0, por esto se asocia su comportamiento a una multiplicación.

El resultado de la operación AND entre las dos direcciones es la dirección de red para el computador PC y para todos los equipos que están en la

red local, en la Tabla 21, puede ver las operaciones bit a bit dando como resultado la dirección 192.168.10.0.

Tabla 21

Determinación de la dirección de red del dispositivo origen (paso 2)

Descripción	Dirección IP	Primer octeto	Segundo octeto	Tercer octeto	Cuarto octeto
PC	192.168.10.25	11000000	10101000	00001010	00011001
Máscara	255.255.255.0	11111111	11111111	11111111	00000000
Red PC	192.168.10.0	11000000	10101000	00001010	00000000

Nota. Ludeña, P., 2025.

Paso 3. Si la dirección de destino pertenece a la red local debería tener la misma dirección de red. Entonces, para comprobarlo aplicaremos la operación AND entre la dirección IP del destino 192.168.20.10/24 y la máscara de red. En la Tabla 22, puede ver las operaciones bit a bit y el resultado que es la dirección 192.168.20.0

Tabla 22

Operación AND entre dirección IP de destino y máscara de red (paso 3)

Descripción	Dirección IP	Primer octeto	Segundo octeto	Tercer octeto	Cuarto octeto
Servidor	192.168.20.10	11000000	10101000	00010100	00001010
Máscara	255.255.255.0	11111111	11111111	11111111	00000000
Resultado	192.168.20.0	11000000	10101000	00010100	00000000

Nota. Ludeña, P., 2025.

Paso 4. Se comparan los resultados obtenidos en los Paso 2 y 3. Si son iguales el destino pertenece a la red local y se puede hacer la entrega. Si los resultados son diferentes el destino es remoto y los paquetes deben ser enviados a un router para salir hacia otras redes. En el ejemplo, el destino está en una red remota, por tanto, el dispositivo debe enviar los paquetes a la puerta de enlace predeterminada para poder, eventualmente, alcanzar la red del destino.

La puerta de enlace predeterminada o Gateway por defecto es la interfaz del router encargado de dirigir el tráfico hacia otras redes. Si

imaginamos una red como una habitación, la puerta de enlace sería la salida hacia un pasillo que conecta a otras habitaciones, así que siempre que se quiera ir a otras habitaciones (redes), es necesario pasar por esa puerta.

Sus características principales se presentan a continuación:



- La dirección IP de la puerta de enlace debe estar dentro del mismo rango que los demás dispositivos de la red local.
- El Gateway por defecto puede recibir datos desde la red local y enviarlos hacia redes remotas
- La puerta de enlace debe ser una interfaz de un dispositivo que permita el enrutamiento de capa 3.
- Sin una puerta de enlace predeterminada no puede haber comunicación remota.

2.5.4. Clasificación de direcciones por entrega

Las direcciones de acuerdo con el enfoque de entrega se clasifican en:

1. **Unidifusión (unicast):** un único remitente entrega a un único destino, por ejemplo, una PC con dirección 172.16.4.1 envía un documento hacia la impresora con dirección 172.16.4.253.
2. **Multidifusión (multicast):** un emisor envía el paquete a un grupo de destinatarios. Para evitar conflictos el alcance se limita solo a quienes se han unido a una dirección de grupo, como 224.0.0.9 en IPv4 o FF02::1:FFXX:XXXX para nodo solicitado en IPv6, ahorrando ancho de banda al resto de la red .
3. **Difusión IPv4 (Broadcast):** el emisor envía un paquete a todos los hosts del dominio, para ello en la dirección de destino se pone 255.255.255.255 o la dirección de red con bits de host en 1; los routers bloquean esa señal para que no inunde redes externas.

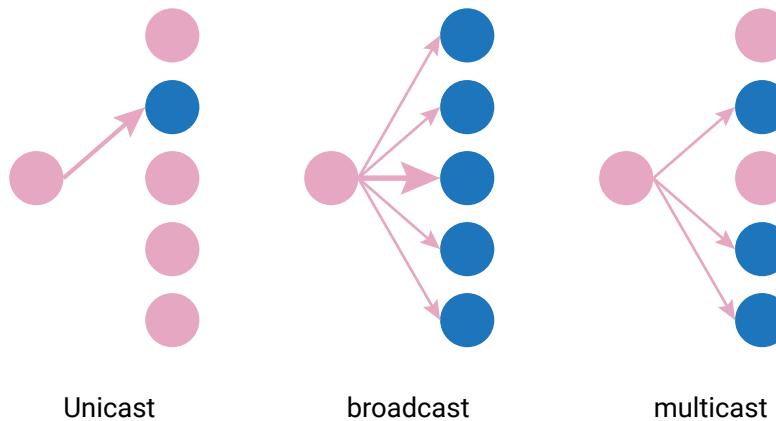
4. **Anycast IPv6:** varias interfaces comparten la misma dirección; la red entrega el paquete al miembro más próximo, técnica muy usada en DNS y CDNs para reducir latencia.

Pese a que existen estos tipos de tráfico, no todos se usan con la misma frecuencia, en la práctica, usted empleará unidifusión para el 99 % del tráfico de usuario, multidifusión para servicios como videoconferencia o descubrimiento de vecinos en IPv6, difusión IPv4 para arranque de red en servicios como DHCP para obtener direccionamiento dinámico o ARP para conocer direcciones MAC; y, anycast IPv6 para balancear servicios globales.

Para concluir con este tema, le invito a revisar la Figura 34 donde se visualiza gráficamente el tipo de entrega que realiza cada método.

Figura 34

Diferencias en la entrega de unidifusión, multidifusión y difusión



Nota. Tomado de *Difference unicast multicast broadcast [Ilustración]*, por AbdollahFani, 2017, [WikimediaCommons](#), CC BY 4.0.

2.5.5. Router

El router o enrutador es el equipo de capa de red o capa tres del modelo OSI, puesto que toma decisiones de enrutamiento con base en

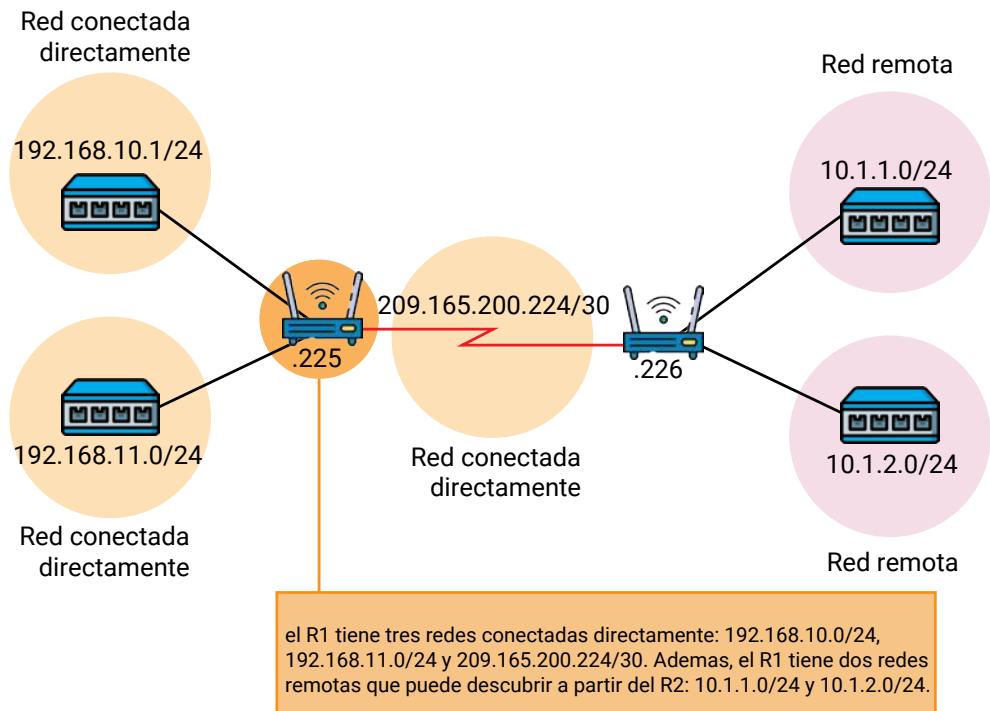
la información contenida en el paquete. El router realiza dos funciones complementarias: enrutamiento y retransmisión.

El **enrutamiento** en un router se basa en mantener una tabla de rutas, donde cada entrada es una ruta a un destino concreto. Las rutas que se almacenan en la tabla de rutas pueden tener como destino redes directamente conectadas y redes remotas, es decir redes a las cuales se debe acceder usando otros routers.

En la Figura 35, se tiene un ejemplo de los tipos de rutas.

Figura 35

Identificación de redes conectadas directamente y redes remotas



Nota. Tomado de *Decisión de reenvío de paquetes del router [Ilustración]*, por Cisco Networking Academy, s.f., CISCO, CC BY 4.0.

Para el router R1 las redes 192.168.10.0, 192.168.11.0 y 209.165.200.224 son redes directamente conectadas, mientras las redes 10.1.1.0 y 10.1.2.0 son redes remotas y deberá acceder a ellas a través del router R2. Las rutas se añaden a la tabla de rutas de manera estática a través de la configuración manual de cada una de las rutas o de manera dinámica usando protocolos de enrutamiento dinámico como OSPF o BGP.

En la tabla de enrutamiento cada entrada contiene al menos las siguientes columnas:

- **Origen de la ruta:** informa el modo en que se descubrió la ruta, es identificado por un código. Los códigos más comunes incluyen: L que identifica una interfaz configurada y activa del router C identifica una red directamente conectada al router, S identifica una ruta configurada estáticamente, O identifica una ruta aprendida a través del protocolo OSPF y * identifica una ruta predeterminada.
- **Red de destino:** se especifica a través del prefijo de red y longitud, por ejemplo 10.20.0.0/16.
- **Distancia administrativa:** Permite determinar la confiabilidad del origen de la ruta. Los valores más bajos indican rutas más confiables, por ejemplo, rutas a redes directamente conectadas tienen distancia administrativa 0 y rutas estáticas tienen distancia administrativa 1 por defecto.
- **Métrica:** identifica un valor asignado para llegar a la red remota, esto puede ser asociado al coste, retardo o ancho de banda.
- **Próximo salto:** identifica la dirección IP de la interfaz del router al que se deben entregar los paquetes para que sigan su viaje hacia el destino. La dirección IP debe pertenecer a una red directamente conectada al router.

- **Interfaz de salida:** identifica la interfaz de salida del router por la cual el paquete deberá salir para ser reenviado.
- **Marca de hora:** las rutas dinámicas guardan un temporizador para que, en caso de que dejen de actualizarse, sean eliminadas para evitar bucles.

En la Figura 36, usted puede ver una tabla de enrutamiento extraída de un router Cisco, donde puede identificar todos los elementos antes descritos.

Figura 36

Visualización de rutas estáticas en la tabla de enrutamiento de un router

```
Router>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is 10.10.11.101 to network 0.0.0.0

 10.0.0.0/8 is variably subnetted, 9 subnets, 6 masks
S*   10.10.0.0/21 [1/0] via 10.10.11.101
S     10.10.8.0/23 [1/0] via 10.10.11.101
C     10.10.10.0/24 is directly connected, GigabitEthernet0/0
L     10.10.10.1/32 is directly connected, GigabitEthernet0/0
C     10.10.11.0/26 is directly connected, GigabitEthernet0/1
L     10.10.11.1/32 is directly connected, GigabitEthernet0/1
S     10.10.11.96/30 [1/0] via 10.10.11.101
C     10.10.11.100/30 is directly connected, Serial0/0/0
L     10.10.11.102/32 is directly connected, Serial0/0/0
S*   0.0.0.0/0 [1/0] via 10.10.11.101
```

Nota. Ludeña, P., 2025.

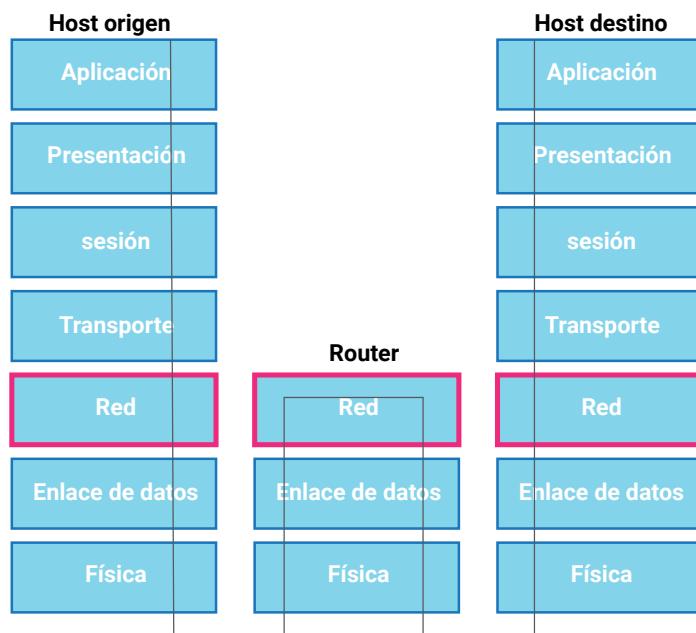
Para la entrada en el recuadro rojo se lee la información de la siguiente manera: la ruta ha sido configurada manualmente (código S), la red de destino es 10.10.0.0/21 con distancia administrativa 1 (por defecto)

y métrica 0, el siguiente salto es la interfaz del siguiente router con dirección IP 10.10.11.101.

La otra función que es la **retransmisión** es realizada luego de consultar la tabla de enrutamiento, con base en la consulta se determina por cuál interfaz saldrá el paquete. La conmutación interna dentro del router debe hacerse en el menor tiempo posible para que no se añada latencia en el proceso de comunicación. Asociada a este proceso el router debe realizar el proceso de desencapsulamiento y encapsulamiento, ya que debe extraer el paquete de la trama para revisar la información de la cabecera IP y luego armar una nueva trama para reenviar el paquete por la interfaz de salida como se ve en la Figura 37.

Figura 37

Encapsulamiento de datos en el modelo OSI durante el reenvío por un router



Nota. Tomado de *OSI model router [Ilustración]*, por xcrespo11, 2012, WikimediaCommons, CC BY 4.0.

Note que el router al ser un dispositivo de capa 3, sólo desencapsula hasta esta capa. Es decir, recibe la información desde los medios de capa física, extrae la trama, desencapsula el paquete y lo analiza. Resuelve el enrutamiento y envía el paquete a la interfaz adecuada, encapsula el paquete en una nueva trama y la envía por el medio adecuado.

Estructura de tabla de enrutamiento

En esta actividad usted deberá recordar la estructura de la tabla de enrutamiento e identificar los datos que componen cada entrada de una ruta descrita. El principal objetivo de esta actividad es que pueda reconocer los diferentes tipos de rutas y los elementos más importantes para describir rutas en un router.



Identificación de elementos de tabla de enrutamiento

Su desempeño en esta actividad de emparejamiento demuestra la consolidación de conocimientos esenciales sobre la estructura interna de las tablas de enrutamiento, un componente fundamental que determina la eficiencia y precisión del forwarding de paquetes en redes complejas. Ha logrado establecer las conexiones correctas entre conceptos que, aunque técnicamente específicos, representan la base operacional sobre la cual los routers toman millones de decisiones de enrutamiento cada segundo.

Con base en la información disponible en la tabla de enrutamiento de la actividad interactiva, conteste en su cuaderno de apuntes o en un documento de Word las siguientes interrogantes:



- ¿Qué significa la letra D al inicio de la línea? ¿Quién ha configurado esta ruta, es decir, el router automáticamente o un administrador de red?
- ¿Qué indica el prefijo /24 en la ruta 192.168.1.0/24? ¿Cuántas direcciones IP se podrían tener en esta red?
- ¿Qué rol cumple la dirección 192.168.3.1?

Excelente, hemos completado la semana 6. Los invito a realizar el siguiente *quiz* para aplicar los conceptos estudiados.

Capa de Red y Enrutamiento IP

Como pudo comprobar durante la actividad, la capa de red constituye el núcleo lógico que permite la comunicación global en redes de datos. Su desempeño refleja qué tan sólidamente ha asimilado conceptos críticos como el direccionamiento jerárquico que hace posible la escalabilidad de Internet, las funciones diferenciadas de enrutamiento y reenvío que ejecutan los routers, y las características de servicio "mejor esfuerzo" que definen el comportamiento del protocolo IP



Actividad de aprendizaje recomendada

Reforcemos el aprendizaje resolviendo las siguientes actividades.

Lectura de los contenidos propuestos

Ingresé a la plataforma [Netacad](#) y revise el módulo 8: Capa de red, en el cual revisará las funciones y características de esta capa 3 del Modelo OSI.

Estrategia de trabajo:

- Organice un horario semanal para revisar los contenidos recomendados.
- Mantenga disponible un cuaderno o archivo digital para anotar los conceptos más importantes; este recurso será de gran ayuda al momento de repasar en la semana 8.
- Complete las actividades de la sección. Verifique su comprensión.
- Realice las autoevaluaciones correspondientes al módulo 8 para medir su nivel de entendimiento sobre los temas tratados.

Retroalimentación:

Durante las autoevaluaciones, la plataforma Netacad le mostrará cuáles respuestas fueron incorrectas, permitiéndole reconocer qué conceptos aún necesitan ser fortalecidos. Le sugiero revisar cuidadosamente las explicaciones de cada pregunta y volver a consultar los materiales relacionados.



Semana 7

Esta semana estudiaremos el protocolo IP en sus versiones 4 y 6, para comprender el alcance de la capa de red. Primero, revisaremos el protocolo IPv4, la estructura de paquete que maneja y los tipos de direcciones que se distinguen en este protocolo, para luego analizar cómo se configuran las direcciones IPv4. Posteriormente, se estudiará el protocolo IPv6, ahondando en las diferencias que existen con las especificaciones de paquete para IPv4 y los tipos de direcciones que se definen para este protocolo. También se especificarán los mecanismos para la configuración de direcciones dinámicas IPv6. El conocimiento de estos conceptos les permitirá seleccionar el protocolo que más se adapta a sus requerimientos de red y de manera eficiente brindar direccionamiento a las redes, siendo esta una de las habilidades más buscadas en entornos laborales en la actualidad.

2.6. Protocolo IPv4



El Protocolo de Internet, o simplemente IP, por sus siglas en inglés (*Internet Protocol*), en su versión 4 se publicó en 1981 en la RFC 791 (DARPA, 1981), y rápidamente se convirtió en la base de las redes de la época. Dos años después, el 1 de enero de 1983, ARPANET adoptó oficialmente el modelo de referencia TCP/IP y con ello el estándar IP tuvo un alcance global, demostrando así que podía escalar fácilmente y ofrecer interoperabilidad a redes heterogéneas.

En el estándar se plantea una estructura de direccionamiento con 43 bits, capaz de ofrecer, casi, 4295 millones de direcciones (2^{32}), que para inicios de los 80 parecía un espacio suficiente. En este nuevo ecosistema se desarrollaron servicios como web, correo electrónico y las primeras aplicaciones multimedia. El protocolo IPv4 se ha enfrentado a grandes

Índice

I Bimestre

II Bimestre

Solucionario

Referencias

contratiempos debidos a su éxito masivo y ha debido reinventarse con el paso de los años, por ejemplo, encontrar soluciones al inminente agotamiento de direcciones. Y pese a todas las dificultades, este protocolo no pierde vigencia y, desde el punto de vista técnico, es considerado una piedra angular, de ahí su importancia en la formación de un ingeniero en Redes y Analítica de Datos.

2.6.1. Paquete IPv4

El estándar define que el paquete IPv4 añade a los datos una cabecera. Esta cabecera se compone de una parte fija de 20 bytes, y, opcionalmente, una parte denominada **opciones** que puede hacer crecer el tamaño de la cabecera hasta 60 bytes. La cabecera suele estar ordenada en palabras de 32 bits y se lee de izquierda a derecha y cuenta con catorce campos, como se puede ver en la figura 38.

Figura 38

Cabecera de paquete del protocolo IPv4

Version	Longitud del encabezado de internet	Servicios diferenciados (DS)		Longitud total						
		DSCP	ECN							
Identificación				Indicador	Desplazamiento de fragmentos					
Tiempo de vida (TTL)	Protocolo		Checksum de cabecera							
Dirección IP de origen										
Dirección IP de destino										
Opciones										
Datos										

Nota. Ludeña, P., 2025.

En la Tabla 23, usted encontrará la descripción y el uso de cada campo que componen la cabecera IPv4.

Tabla 23

Descripción de campos de la cabecera IPv4

Campo	Longitud	Descripción	Función
Versión	4 bits	Indica la versión del protocolo; para IPv4 su valor es 0100.	Permite la convivencia con IPv6 en la red.
Longitud de cabecera (IHL)	4 bits	Número de palabras de 32 bits que ocupa la cabecera; mínimo 5.	Determina dónde comienza la carga útil o datos.

Campo	Longitud	Descripción	Función
Tipo de servicio o Servicios diferenciados DS	8 bits	Diferenciación de servicios y notificación de congestión (DiffServ/ECN).	Base para QoS y priorización de tráfico multimedia.
Longitud total	16 bits	Tamaño completo del paquete (cabecera + datos).	Límite teórico 65 535 bytes; en la práctica \leq 1500 bytes para que pueda ser transportado en Ethernet.
Identificación	16 bits	Gestionan la fragmentación cuando el datagrama supera la MTU de un enlace.	Cada fragmento hereda la misma identificación para ser reensamblado en destino.
Indicador o banderas	3 bits		
Desplazamiento de fragmentos	13 bits		
Tiempo de vida (TTL)	8 bits	Contador de saltos que se decrementa en cada router; al llegar a 0 el paquete se descarta.	Previene bucles de enrutamiento, evita que los paquetes estén deambulando eternamente por la red.
Protocolo	8 bits	Especifica la PDU de capa 4 que transporta (TCP = 6, UDP = 17, ICMP = 1, etc.).	Enlaza la capa de red con la de transporte.
Checksum de cabecera	16 bits	Verifica errores solo en la cabecera; se recalcula en cada salto porque el TTL varía.	Si la suma de comprobación no concuerda, el router descarta el paquete.
Dirección IP de origen	32 bits	Identifica al emisor.	Insertada por el host al crear el paquete.
Dirección IP de destino	32 bits	Identifica al receptor final.	Los routers la usan para encontrar la ruta en la tabla de enrutamiento.
Opciones y Relleno	0-40 bytes	Funciones poco usadas (timestamp, security, record route).	No tienen funciones explícitas suelen reducir el rendimiento; por ello se eliminaron en IPv6.

Nota. Ludeña, P., 2025.

El dispositivo origen construye la cabecera original fijando la Versión, la Longitud de cabecera, el tipo de servicio, Longitud total, su propia dirección IP, la dirección IP del destino y el resto de los campos, calcula la Suma de comprobación y envía el paquete a la red local. Si el destino es remoto, el paquete recorrerá varios saltos, en cada uno de esos saltos visitará un router. Cada router decrementará el TTL, recalculará la suma de comprobación y reenviará el paquete según el campo Protocolo y las direcciones de la cabecera original.



Para comprender la utilidad de los campos Identificación, Banderas y Desplazamiento para fragmentar, le invito a ver el video titulado "[¿MTU para que sirve en realidad?](#)", el cual explica qué es la unidad máxima de transmisión. Analice cómo la fragmentación permite que la información viaje por medios de diferente MTU de acuerdo con la tecnología que se tenga en cada tramo de red, así en cada router se puede ajustar el valor de tamaño.

El protocolo IPv4 brinda la posibilidad de fragmentar el paquete si el siguiente enlace de la ruta tiene una MTU menor, asegurando que cada fragmento se ajuste al nuevo tamaño.

El dispositivo destino usa la suma de comprobación para detectar errores en el paquete, si no se detectan errores el paquete se pasa a la capa de transporte.

2.6.2. Tipos de direcciones IPv4

El direccionamiento para el protocolo IPv4 originalmente se dividía en cinco clases estrictas, definidas por los bits que se destinaban para la porción de red, en la Figura 39 usted puede encontrar las clases de direcciones IPv4 y las porciones de red y de host para cada una de ellas.

Figura 39

Clasificación de direcciones IPv4 por clases

Clase A	Red	Host		
Octet	1	2	3	4
Clase B	Red		Host	
Octet	1	2	3	4
Clase C	Red			Host
Octet	1	2	3	4
Clase D	Host			
Octet	1	2	3	4

Nota. Tomado de *Clase direcciones IP [Ilustración]*, por Verona ULE, 2008, [WikimediaCommons](#), CC BY 4.0.

Ahora describiremos cada una de las clases definidas:

- **Clase A** (1.0.0.0/8 a 126.0.0.0/8): la porción de red es delimitada por el primer octeto de la dirección IP, por tanto, el prefijo es /8. Los 8 bits determinan que se puedan tener 256 redes capaces de albergar ≈ 16 millones de hosts cada una, por ejemplo 10.0.0.1.
- **Clase B** (128.0.0.0/16 – 191.255.0.0/16): en esta clase se toman los dos primeros octetos para la porción de red, dando como resultado un prefijo /16. Esta clase puede tener 16 384 redes de hasta 65 534 hosts, por ejemplo 172.16.0.35.
- **Clase C** (192.0.0.0/24 – 223.255.255.0/24): para esta clase se reservan los tres primeros octetos para la porción de red para obtener el prefijo /24. El número de redes llega a 2 097 152 redes de 254 hosts en esta clase, por ejemplo 192.168.5.10.
- **Clase D** (224.0.0.0–239.255.255.255): esta clase se utiliza para identificar grupos de multidifusión, por ejemplo 224.0.0.9 para OSPF. No hay necesidad de asignar octetos o bits a las distintas direcciones de red o de host.

- **Clase E** (240.0.0.0–255.255.255.255): está clase se reserva para fines de investigación y experimentación solamente.

Usar estas clases aportaban simplicidad a la búsqueda de destinos en las tablas de rutas dentro de los enrutadores, pero la desproporción en el número de redes disponibles y el tamaño que podían tener esas redes en cada clase, ya que en unos casos sobraban miles de direcciones y en otros casos faltaban direcciones para hosts, hicieron que se pensará en un esquema que se adaptará mejor a los requerimientos de las redes. Es así como, en 1993 se adopta un direccionamiento sin clases denominado CIDR, que permite prefijos de cualquier longitud y una asignación mucho más eficiente.

Como se mencionó antes IPv4 tuvo mucha popularidad y con la masificación de Internet debió afrontar el problema de agotamiento de direcciones. En ese entonces se propusieron dos soluciones complementarias que permitieron contener el problema.

Primero se estableció una nueva clasificación de direcciones IPv4, de acuerdo con su ámbito de acción, las direcciones que pueden ser enrutadas en el núcleo de Internet se denominan **direcciones IP públicas** (enrutables globalmente y administradas por IANA) y las que tienen un carácter netamente organizacional se denominaron **direcciones IP privadas** y se definieron en RFC 1918.

Para las direcciones privadas se reservaron tres bloques 10.0.0.0/8, 172.16.0.0/12 y 192.168.0.0/16. De esta forma el esquema de direccionamiento interno podía ser replicado una y otra vez, sin agotar las direcciones públicas, ya que únicamente el uso de direcciones públicas es necesario cuando se quiere atravesar Internet.

Para esto se planteó la segunda solución, denominada **Traducción de direcciones de red o simplemente NAT**, la cual permite traducir decenas o cientos de direcciones privadas a una sola dirección pública en el límite de la organización, por lo general en un router de borde. Cuando retorna

la comunicación se produce el proceso inverso, para lo cual se lleva un registro del tráfico de salida y así se le asigna a cada destinatario interno el flujo de datos correspondiente.

Hay algunas direcciones reservadas que no se pueden asignar a interfaces de dispositivos, entre ellas:



- **Loopback** (127.0.0.0/8): se usa para realizar pruebas locales de pila TCP/IP; el host responde a 127.0.0.1 sin salir a la red.
- **Link-local/APIPA** (169.254.0.0/16): el sistema autogenera una dirección en este rango cuando no hay DHCP disponible.
- **Documentación** (RFC 5737): 192.0.2.0/24, 198.51.100.0/24, 203.0.113.0/24; se usan en ejemplos y nunca deben aparecer en producción.
- **0.0.0.0/32** indica host desconocido o este equipo durante la inicialización
- **255.255.255.255/32** es la difusión limitada dentro del dominio de capa 2.

Ahora es momento de evaluar su comprensión la clasificación de direcciones IPv4. Describa con sus propias palabras la diferencia entre una dirección IP pública y una dirección IP privada. ¿Qué papel desempeña el mecanismo NAT en esta distinción? ¿Qué desventajas puede detectar en el uso de esta solución?

Piense ahora en la dirección de loopback, plantee dos casos prácticos donde usted pueda utilizar esta dirección en su ejercicio profesional.

2.6.3. Tipos de direccionamiento para IPv4

El direccionamiento puede ser de dos tipos: estático y dinámico.

1. **El direccionamiento estático:** consiste en asignar manualmente a cada interfaz un identificador lógico, esto es una dirección IPv4

que permanecerá fijo hasta que el administrador lo cambie. La dirección IP se introduce directamente en la configuración del sistema operativo o del dispositivo, junto con su máscara de red o la longitud de prefijo, la puerta de enlace y la dirección IP del servidor DNS, por ejemplo, en la Figura 40, usted puede ver la configuración para una PC con sistema operativo Windows.

Figura 40

Configuración manual de dirección IP en un dispositivo con Windows

Editar configuración de IP

Manual

IPv4

Activado

Dirección IP
192.168.10.10

Máscara de subred
255.255.255.0

Puerta de enlace
192.168.10.1

DNS preferido
8.8.8.8

DNS a través de HTTPS
Desactivado

DNS alternativo

Guardar Cancelar

Nota. Ludeña, P., 2025.

La ventaja de este método es que el administrador tiene control absoluto de la conectividad del equipo, que resulta indispensable para equipos como servidores, impresoras de red y equipos intermediarios (switches, routers, firewalls, etc.). Sin embargo, también trae desventajas, puesto que la configuración y mantenimiento manual hace que el método sea propenso a errores de tipografía y genera una carga administrativa significativa.

- El direccionamiento dinámico:** en el direccionamiento dinámico se delega la configuración de los datos a un servicio automatizado, sin intervención del administrador de red. La ventaja de este método es que el dispositivo puede pedir los servicios cuántas veces lo requiera, es más, los servicios pueden ser requeridos por varios dispositivos al mismo tiempo y recibirán la configuración de red válida para el segmento de red. En entornos con dispositivos móviles o en redes de usuarios invitados, este esquema es altamente recomendado. El administrador deberá precautelar la disponibilidad de recursos para quienes lo requieran en la preconfiguración del servidor de direcciones y manejar esquemas de gestión de recursos.

En la Tabla 24 usted podrá encontrar un cuadro comparativo de direccionamiento estático versus dinámico que le permitirá determinar cuándo deberá cada uno de ellos.

Tabla 24

Tabla comparativa de direccionamiento estático versus dinámico

Aspecto	Dirección estática	Dirección dinámica
Asignación	Manual, fija	Automática
Gestión masiva	Laboriosa; alto riesgo de error humano	Centralizada; escalable con bases de datos
Idoneidad	Servidores, infraestructuras, enlaces de ruteo	Usuarios finales, redes IoT, visitantes

Aspecto	Dirección estática	Dirección dinámica
Cambios de topología	Requieren reconfigurar equipo por equipo	Clientes renuevan o reciben nueva configuración en nuevas solicitudes
Dependencias	Sin servicios adicionales; solo configuración local	Requiere servidor DHCP

Nota. Ludeña, P., 2025.

La dirección estática se describe como una asignación manual y fija, adecuada para servidores y dispositivos que requieren estabilidad en la red, aunque requiere intervención manual en caso de cambios de topología. Por el contrario, la dirección dinámica se asigna automáticamente por un servidor DHCP, facilitando la gestión masiva y el reacomodo de equipos en redes cambiantes.

En IPv4 el direccionamiento dinámico se realiza a través del protocolo DHCP definido en RFC 2131. DHCP maneja un modelo cliente-servidor, eso significa que el host solicita dirección IP y el servidor le arrendará una dirección (las direcciones disponibles son configuradas por el administrador dentro de un grupo, denominado pool), adicional al a dirección el servidor DHCP entrega parámetros de red (máscara de red, puerta de enlace y dirección de DNS).

Revisemos un ejemplo didáctico del proceso.

El administrador define en un servidor DHCP un pool de direcciones, por ejemplo, desde 192.168.1.100 a 192.168.1.200 y establece los siguientes parámetros de red: máscara (255.255.255.0), puerta de enlace (192.168.1.1), DNS (8.8.8.8) y tiempo de arrendamiento de dirección (8 horas).

El usuario al encender su computador aún no conoce su dirección IP. El sistema marca su interfaz con la dirección 0.0.0.0 y envía un mensaje DHCPDISCOVER a la dirección de difusión 255.255.255.255 para que llegue a todos los dispositivos de la red local, con su MAC

como dirección de origen como única identidad. El servidor recibe la difusión, verifica que la MAC no tenga ya una reserva y responde con un mensaje DHCPOFFER, que contiene una propuesta de direccionamiento, por ejemplo: 192.168.1.108 por 8 h y el resto de los parámetros de red. El host recibe las ofertas (si hubiera varias), elige una y envía un DHCPREQUEST en difusión, confirmando la IP deseada. El servidor valida que la dirección siga libre y responde con DHCPACK. El sistema del usuario configura los datos en su tarjeta de red y comienza a usarlos para comunicarse por la red. Este proceso será estudiado en detalle en la Sección 3.4.4. de esta Guía didáctica.

2.7. Protocolo IPv6

En 2011 los últimos registros regionales de direcciones IPv4 colapsaron debido al crecimiento exponencial de dispositivos conectados a Internet. Pero el problema no era sólo numérico, puesto que ya se habían diseñado estrategias para alargar el espacio de direcciones como las direcciones privadas y NAT, esto ocasionó que se pierda la comunicación de extremo a extremo, añadió latencia y añadió complejidad a la comunicación de redes. Por otra parte, la cabecera IPv4 fue pensada para las características de las redes originarias y campos como la suma de comprobación que debía recalcularse cada vez que se actualizaba el TTL reducían el rendimiento general de la red.

Todas estas limitaciones hicieron que el IETF diseñara IPv6 y lo publicara en el RFC 2460. Este nuevo protocolo amplía el espacio de direcciones a 128 bits, que, en teoría, hace que el agotamiento de direcciones sea imposible. En la Figura 41, puede ver la evolución del espacio de direcciones para varias recomendaciones y protocolos.

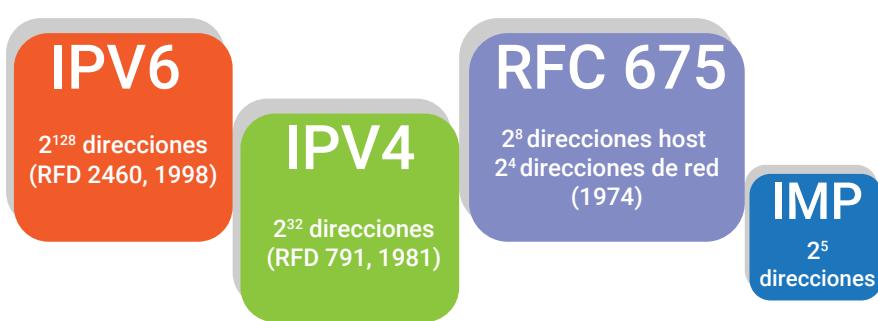
Figura 41*Evolución del Espacio de Direcciones IP desde IMP a IPv6*

Diagrama que muestra el crecimiento masivo del espacio de direcciones de cada protocolo.

Cada bloque es la cascada magnifica una pequeña área en el bloque precedente.

Nota. Tomado de [CascadaIP-es](#) [Ilustración], por Verona ULE, 2018, [WikimediaCommons](#), CC BY 4.0.

La posibilidad de tener direcciones ilimitadas hace que todas las direcciones sean enrutables en el núcleo de Internet, eliminando la necesidad de NAT y devolviendo la conectividad punto-a-punto.

Adicionalmente, simplifica la cabecera para reducir la complejidad operativa que arrastraba IPv4, y se proyecta de mejor manera a los requerimientos de redes avanzadas modernas como Internet de las cosas y redes 5G.

2.7.1. Paquete IPv6

El protocolo IPv6 establece una estructura de paquete mucho más simple que la definida para IPv4, mientras la cabecera IPv4 tiene un tamaño variable, la cabecera IPv6 tiene un tamaño fijo de 40 bytes y si requiere funciones adicionales usa cabeceras de extensión.

En la Figura 42, usted tiene la comparativa de ambas cabeceras.

Figura 42

Encabezado del protocolo IPv6 y su comparación con los campos para IPv4

Encabezado IPv4				Encabezado IPv6			
versión	IHL	Tipo de servicio	Longitud total	versión	Clase de tráfico	Identificador de flujo	
Identificación		Señaladores	Desplazamiento de fragmentos	Longitud de contenido		Siguiente encabezado	Límite de salto
Tiempo de existencia	Protocolo	Checksum de encabezado		Dirección de origen			
Dirección de origen		Dirección de destino		Dirección de destino			
Opciones		Relleno		Dirección de origen			
Leyenda <ul style="list-style-type: none"> Se conservan los nombres de campo de IPv4 a IPv6 No se conservan los campos en IPv6 Cambian el nombre y la posición en IPv6 Nuevo campo en IPv6 							

Nota. Tomado de *ENCABEZADO IPV6* [Ilustración], por AKRAM.ABOU, 2013, [WikimediaCommons](#), CC BY 4.0.

Los campos Versión, Dirección de origen y Dirección de destino se mantienen. Los campos Tipo de servicio, Longitud total, Tiempo de existencia y Protocolo cambian de nombre y posición a Clase de tráfico, Longitud de contenido, Límite de salto y Siguiente encabezado, respectivamente. Los campos IHL, Identificación, Señaladores, Desplazamiento de fragmentos, Checksum, Opciones y relleno de IPv4 se eliminan en IPv6. Y el campo Identificador de flujo se añade para la cabecera IPv6.

En la Tabla 25, puede encontrar la descripción y uso de todos los campos de la cabecera IPv6.

Tabla 25*Descripción de campos de la cabecera del protocolo IPv6*

Campo	Longitud	Descripción	Función
Versión	4 bits	Indica la versión del protocolo (0101 = IPv6).	Permite la coexistencia con IPv4 en la pila dual (dual-stack).
Clase de tráfico	8 bits	Establece prioridad de tráfico y ECN; reemplaza al antiguo TOS/DSCP.	Base para QoS y control de congestión extremo a extremo.
Identificado de flujo	20 bits	Identifica flujos que requieren tratamiento especial (por ejemplo, voz sobre IP).	Los routers pueden aplicar ingeniería de tráfico sin inspeccionar la capa de transporte.
Longitud de carga útil	16 bits	Longitud del contenido después de la cabecera básica (excluye los 40 bytes fijos).	Admite hasta 65 535 bytes. Si se usa la cabecera Jumbo Payload puede superar ese límite.
Siguiente encabezado	8 bits	Identifica la cabecera de extensión siguiente o bien el protocolo de capa 4 (TCP = 6, UDP = 17, etc.).	Permite una correspondencia de funciones entre capas (seguridad, routing, fragmentación).
Límite de saltos	8 bits	Equivalente al TTL de IPv4. Los routers lo decrementan en cada salto.	Elimina bucles.
Dirección origen	128 bits	Identificador del origen	Estructura jerárquica facilita agregación en las tablas de rutas.
Dirección destino	128 bits	Identificador del receptor	Encaminamiento se basa en prefijos globales /48, /56, etc.

Nota. Ludeña, P., 2025.

Reflexione, ¿qué impacto tiene el uso del campo límite de salto y la ausencia del campo suma de comprobación en la eficiencia de las redes?, analice la latencia a lo largo de una ruta de varios routers.

2.7.2. Tipos de direcciones IPv6

Las direcciones IPv6, como vimos anteriormente, se dividen en tres grandes familias por el número de destinatarios: unidifusión, multidifusión y anycast. Y en este contexto luego se tiene una subclasificación que explicaremos a continuación mediante la siguiente infografía que organiza de manera visual y jerárquica los diferentes tipos de direcciones IPv6, mostrando las relaciones entre las categorías principales y sus subdivisiones específicas.

Tipos de direcciones IPv6

Como pudo observar en el mapa mental, la clasificación de direcciones IPv6 sigue una estructura lógica que refleja tanto la funcionalidad como el alcance de cada tipo de dirección. Su comprensión de esta taxonomía le ha permitido identificar que la categoría de unidifusión se subdivide en varios tipos específicos, incluyendo direcciones globales unicast (GUA), link-local (LLA), loopback, direcciones locales únicas, y unspecified. Los dispositivos IPv6 suelen contar con al menos una GUA y una LLA, si no se asigna manualmente la dirección LLA, el sistema operativo generará una automáticamente.

La multidifusión describe direcciones que permiten que una sola transmisión sea recibida por múltiples dispositivos suscritos a un grupo, como FF02::1 para todos los nodos y FF02::2 para todos los routers, reemplazando al broadcast de IPv4. Finalmente, la categoría de anycast agrupa direcciones compartidas por múltiples dispositivos, en las que el paquete se entrega al nodo más cercano según la métrica de red, siendo muy útiles para servicios distribuidos como los servidores raíz DNS.

2.7.3. Tipos de direccionamiento para IPv6

Al igual que IPv4, el direccionamiento IPv6 puede ser configurado estáticamente y dinámicamente. En IPv6 el direccionamiento dinámico necesita la participación del router de la red local. El router anunciará

qué método de direccionamiento dinámico deben aplicar los hosts a través de la activación de banderas específicas que serán enviadas en mensajes periódicos denominados anuncios de router (RA). En la Tabla 26 puede ver los valores de banderas para cada método de direccionamiento y cómo se genera la dirección global de unidifusión para el dispositivo en cada caso. Recuerde que las interfaces en IPv6 también deben tener dirección link-local, por tanto, el sistema la autogenerará.

Tabla 26

Métodos de direccionamiento dinámico para IPv6 y uso de banderas RA

Método de direccionamiento dinámico	Banderas			Mecanismo de dirección IPv6
	A	O	M	
SLAAC	1	0	0	El dispositivo genera su propia dirección GUA con el prefijo anunciado por el router (por lo general /64). Configura los parámetros adicionales: servidor de DNS, dominio, etc. con base en lo anunciado por el router.
SLAAC+DHCPV6 sin estado	1	1	0	El dispositivo genera su propia dirección GUA con el prefijo anunciado por el router (por lo general /64). Para configurar los parámetros adicionales consulta al servidor DHCPv6.
DHCPV6 con estado	0	0	1	El dispositivo solicita todos los parámetros de direccionamiento al servidor DHCPv6. El servidor DHCPv6 luego de arrendar la dirección guarda un registro con marca de tiempo.

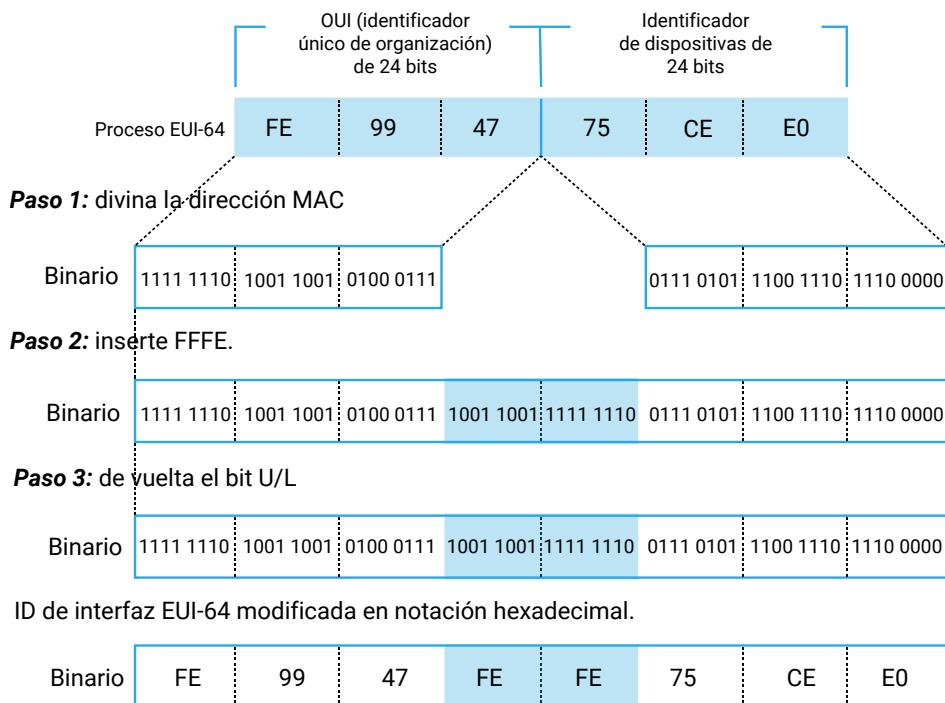
Nota. Ludeña, P., 2025.

El dispositivo tiene dos mecanismos para generar la dirección IPv6 cuando el prefijo es /64. El primero es un método obvio, simplemente generar 64 bits aleatorios para completar la porción de interfaz y adjuntarla al prefijo anunciado por el router. El segundo mecanismo, es utilizar su dirección MAC para generar una dirección única, este mecanismo es conocido como EUI-64. La dirección MAC tiene 48 bits, por tanto, se deben agregar bits hasta completar 64 bits. Para hacerlo

se divide la dirección en dos partes de 6 dígitos hexadecimales cada una y se añade los dígitos hexadecimales FFFE en el centro. Luego se invierte el séptimo bit desde la izquierda y el resultado es la porción de host. Al prefijo anunciado por el router se le añade esta porción y esa es la dirección IPv6 del dispositivo. En la Figura 43, usted puede ver un ejemplo de cómo se realiza el proceso.

Figura 43

Proceso EUI-64 para generar la porción de interfaz de una dirección IPv6



Nota. Tomado de *Direccionamiento IPv6 - Bases y Fundamentos [Ilustración]*, por Salazar, G., 2016, [CISCO](#), CC BY 4.0.

La interfaz del equipo tiene dirección MAC FC99-4775-CEE0, se divide en dos y se introducen FFFF. Luego se invierte el séptimo bit y se obtiene como resultado la dirección de interfaz FE99:47FF:FE75:CEE0.

Tipos de direcciones IP

Los protocolos IPv4 e IPv6 tienen diferentes tipos de direcciones cuya funcionalidad es variada. El objetivo de esta actividad es que usted pueda determinar las características de cada tipo para que sepa cuándo utilizar cada una de ellas en un entorno real. Para ello, diríjase a revisar el siguiente juego de emparejamiento:



Tipos de direcciones IPv4 e IPv6

Su capacidad para identificar correctamente las características de los diferentes tipos de direcciones IPv4 e IPv6 refleja un entendimiento sólido de uno de los aspectos más fundamentales del direccionamiento en redes modernas. Ha demostrado dominio sobre conceptos que van desde direcciones unicast y multicast hasta direcciones de enlace local y globales, competencias esenciales para el diseño e implementación de esquemas de direccionamiento eficientes.

Luego de desarrollar la actividad, conteste en su cuaderno de apuntes o en un documento de Word las siguientes preguntas de reflexión:



- ¿Quién asigna las direcciones APIPA?
- ¿La dirección FF02::2 describe a qué grupo multicast?
- ¿Cuáles son las direcciones IPv6 enrutables a nivel global?

¡Felicitaciones! Terminamos la novena semana. Es momento de demostrar lo aprendido a través del siguiente quiz.

Protocolos IPv4 e IPv6

Su desempeño en esta evaluación demuestra el nivel de comprensión técnica necesario para tomar decisiones fundamentadas sobre arquitecturas de direccionamiento y selección de protocolos en entornos empresariales. Ha logrado consolidar conocimientos que van desde la estructura detallada de cabeceras de paquete hasta las implicaciones operacionales de diferentes métodos de asignación de direcciones, competencias que constituyen la base técnica para el diseño, implementación y troubleshooting de infraestructuras de red robustas.



Actividad de aprendizaje recomendada

Es hora de reforzar los conocimientos adquiridos resolviendo la siguiente actividad:

Lectura de los contenidos propuestos

Ingrese a la plataforma [Netacad](#) y revise el módulo 11: Asignación de direcciones IPv4, subtemas 11.1 a 11.3, y el módulo 12: Asignación de direcciones IPv6, específicamente los subtemas 12.1 a 12.7, donde se explican los principios de los protocolos IPv4 e IPv6.

Estrategia de trabajo:

- Dedique un tiempo semanal específico a la lectura y análisis de los materiales de estudio propuestos.
- Mantenga un cuaderno de notas o un documento de Word donde pueda registrar las ideas y conceptos esenciales.
- Desarrolle la actividad sobre direcciones públicas y privadas.

- Complete todas las actividades denominadas. Verifique su comprensión para afianzar los conocimientos adquiridos.

Retroalimentación:

Luego de realizar las actividades, responda las siguientes preguntas:

- ¿La dirección 192.0.3.15 es pública o privada?
- ¿La dirección 192.168.11.5 es pública o privada?



Sem 1 Sem 2 Sem 3 Sem 4 Sem 5 Sem 6 Sem 7 Sem 8



Semana 8



Actividades finales del bimestre

¡Felicitaciones! Usted ha alcanzado el 50 % del curso.

Nos encontramos cerca de finalizar el primer bimestre de la asignatura de Introducción a las redes; es un excelente momento para repasar los contenidos abordados durante estas 7 semanas. Le animo a tomarse un tiempo para reforzar los conceptos fundamentales de la asignatura y así prepararse adecuadamente para la evaluación bimestral.

En esta semana, le invito a revisar sus apuntes, volver a ver las grabaciones de las tutorías semanales y practicar las configuraciones con las actividades propuestas. Si tiene inquietudes, no dude en compartirlas durante la tutoría de esta semana.

Además, le sugiero revisar el video titulado "[¿Cómo funciona internet? La magia de TCP/IP y redes explicadas](#)", con el objetivo de reforzar la idea de que *Internet* es una red global. Para conseguir este propósito, *Internet* opera sobre dos protocolos básicos, TCP e IP, complementando sus funcionalidades para conseguir un desplazamiento eficiente de los datos. Luego de ver el video, reflexione sobre las siguientes preguntas:

- ¿Por qué TCP/IP desplazó al modelo OSI como estándar de comunicación?
- ¿Por qué es importante que se puedan asignar dinámicamente las direcciones IP?
- ¿Por qué es importante migrar de IPv4 a IPv6?

índice

I Bimestre

II Bimestre

Solucionario

Referencias

Aproveche esta oportunidad para afianzar su aprendizaje y evidenciar todo lo que ha logrado hasta ahora. ¡Estoy seguro de que su dedicación y compromiso le permitirán obtener excelentes resultados de aprendizaje! La siguiente presentación interactiva de repaso le permitirá revisar de manera integrada los conceptos fundamentales abordados durante las primeras siete semanas del curso.

Repaso primer bimestre.

Como pudo constatar durante el repaso interactivo, los contenidos del primer bimestre forman una progresión lógica que construye sistemáticamente su comprensión de las redes de computadoras. Esta visión integral le servirá como base sólida para abordar los contenidos más avanzados del segundo bimestre.

¡Evalúe sus conocimientos sobre redes de datos!

Le invito a medir sus conocimientos resolviendo el crucigrama propuesto y encontrando la palabra escondida.



Generalidades de redes de datos.

Como pudo comprobar al resolver el crucigrama, el dominio de la terminología técnica es fundamental para la comunicación efectiva en el campo de las redes de datos. Su capacidad para identificar conceptos como aplicación, red, router, bits, broadcast, OSI, enlace, trama y hexadecimal demuestra que ha asimilado vocabulario especializado que utilizará constantemente en su práctica profesional.



Actividad de aprendizaje recomendada

Es momento de aplicar sus conocimientos a través de la actividad que se ha planteado a continuación:

¡Configuremos equipos!

Como actividad de cierre del primer bimestre de la materia Introducción a las redes, y continuando con su proceso de aprendizaje, le propongo desarrollar la implementación de una red. En esta actividad integraremos lo aprendido sobre configuración de dispositivos, con los conceptos de capa física, capa de enlace y capa de red. En este escenario, usted tendrá la visión de modo físico de Packet Tracer donde deberá armar la red solicitada, seleccionando los dispositivos y los medios cableados apropiados. Posteriormente, deberá realizar las configuraciones solicitadas para implementar la red y ejecutar las pruebas de conectividad que demuestren el pleno funcionamiento de la red.

Estrategia de trabajo:

- Revise los comandos de configuración y monitoreo revisados durante el primer bimestre.
- Tenga a mano su cuaderno de ingeniería, le será de mucha utilidad para recordar los comandos y la sintaxis apropiada de cada uno de ellos.
- Desarrolle la actividad siguiendo el guion detallado que encontrará en el archivo.

[Práctica 2.9.2 de CCNA-1: configuración básica de conmutadores y dispositivos finales- modo físico.](#)

índice

I Bimestre

II Bimestre

Solucionario

Referencias

En esta actividad usted podrá practicar lo aprendido sobre configuración en Cisco IOS y sobre las capas inferiores del modelo OSI, y desarrollar habilidades fundamentales en la gestión de redes, que es una tarea habitual en el ejercicio profesional de un ingeniero en Redes y Analítica de Datos.

Retroalimentación:

Este ejercicio en Packet Tracer le brindará una retroalimentación inmediata, mostrándole su progreso como porcentaje. Además, podrá hacer clic en la pestaña “Check Results” para ver los ítems considerados para medir su avance y verificar cuáles están pendientes o no se ejecutaron correctamente.

Una vez que haya completado la práctica en Packet Tracer, reflexione sobre su experiencia y sus resultados respondiendo las siguientes preguntas:

- Basándose en la práctica, ¿por qué cree que algunos puertos FastEthernet en los switches (como F0/1 y F0/6) estaban activos con luces verdes, mientras que otros no lo estaban o permanecieron inactivos?, ¿qué factores influyen en el estado de una interfaz de switch?
- Durante las pruebas de conectividad a través del comando ping, ¿qué posibles configuraciones o situaciones en la red podrían haber evitado que un ping se enviara correctamente entre las PC o entre una PC y un switch? Mencione al menos dos razones.
- ¿Cuál fue la importancia de utilizar el comando copy running-config startup-config en los switches?, ¿qué ocurriría si no se guardara la configuración después de realizar cambios importantes en un dispositivo de red?



¡Le deseo mucho éxito en el desarrollo de esta importante práctica que consolidará sus conocimientos sobre redes!



Segundo bimestre

Resultado de aprendizaje 2

- Analiza la comunicación entre dispositivos y aplicaciones en redes considerando el modelo de capas OSI y TCP/IP, garantizando el desempeño y la conectividad eficientes.

Para alcanzar este resultado de aprendizaje, se propone que usted consolide una visión integral de la comunicación extremo a extremo, comprendiendo cómo las funciones de las capas física, de enlace y de red se articulan con los protocolos Ethernet, IP, ARP e ICMP para garantizar la transferencia eficiente y segura de datos. Al analizar los procesos que ocurren desde que una señal abandona el dispositivo emisor hasta que la aplicación de destino recibe la información, usted podrá diagnosticar problemas comunes, interpretar capturas de tráfico y explicar, con propiedad técnica, el rol de cada capa dentro de los modelos OSI y TCP/IP.

Para lograrlo se combinarán estrategias de aprendizaje activo: laboratorios guiados en Packet Tracer, análisis colaborativo de capturas en Wireshark, ejercicios de cálculo y aplicación de configuración de routers y switches que incluyan pruebas de conectividad con ping y traceroute.

Contenidos, recursos y actividades de aprendizaje recomendadas



Sem 9

Sem 10

Sem 11

Sem 12

Sem 13

Sem 13

Sem 14

Sem 14

Sem 15

Sem 16



Semana 9

Esta semana revisaremos dos tareas muy importantes para el desarrollo de las redes modernas. La primera es la extracción de información de control y comunicación de errores en redes IP, que se realiza a través del Protocolo ICMP y ha permitido disponer de herramientas de diagnóstico como ping y traceroute. La segunda tarea es el mapeo de la relación que existe entre las direcciones lógicas y las direcciones físicas, ya que el trabajo dual que realizan hace posible que los datos lleguen desde el origen al destino. Por ello, estudiaremos el Protocolo de Resolución de Direcciones (ARP) para IPv4, comprendiendo cómo un host consulta y completa su tabla ARP, cuáles son los riesgos de difusión y suplantación, y por qué el dominio de estos conceptos es esencial para diagnosticar fallos de conectividad. Y luego, analizaremos el mecanismo equivalente en IPv6, el cual es Neighbor Discovery (ND). Este protocolo usa mensajes específicos para no solo resolver direcciones, sino también para descubrir dispositivos en redes locales.



Los conocimientos teóricos los complementaremos con la práctica mediante simulaciones guiadas en Packet Tracer, contribuyendo directamente a su perfil de egreso. ¡Le animo a seguir con entusiasmo las actividades recomendadas!

2.8. Protocolo ICMP

El Protocolo de Mensajes de Control de Internet (ICMP) en sus versiones 4 y 6, es uno de los protocolos más importantes para un administrador de red y, aunque usted no lo crea desde el inicio del semestre, ha estado trabajando con él, por eso ha llegado el momento de que estudiemos cómo trabaja. ICMP dispone de un conjunto de mensajes ligeros que los dispositivos emplean para informar eventos anómalos, verificar

Índice

I Bimestre

II Bimestre

Solucionario

Referencias

la conectividad o trazar una ruta. Aunque no transporta datos de usuario, su presencia es indispensable porque brinda retroalimentación inmediata.

2.8.1. Mensajes del protocolo ICMP

Para comprender el funcionamiento completo del protocolo IP es fundamental conocer ICMP (*Internet Control Message Protocol*), un protocolo auxiliar que proporciona mecanismos de control y diagnóstico esenciales en las redes TCP/IP. La siguiente infografía le introducirá de manera detallada a los diferentes tipos de mensajes ICMP, sus códigos específicos y sus aplicaciones prácticas en el diagnóstico de redes.

Mensajes ICMP.

Como pudo observar en el mapa mental, ICMP es un protocolo fundamental que opera de manera transparente para proporcionar información crítica sobre el estado de la comunicación en redes IP. Su exploración de los diferentes tipos de mensajes le ha mostrado que ICMP no solo reporta errores, sino que también facilita funciones esenciales como el descubrimiento de rutas, la detección de destinos inalcanzables y la notificación de problemas de fragmentación.

Ahora que comprende la importancia funcional de ICMP, examine los aspectos técnicos: los mensajes ICMPv4 viajan encapsulados en un paquete IP y constan de Tipo (8 bytes), Código (8 bytes) y Checksum (16 bytes), seguidos del cuerpo de mensaje. En la tabla 27 encontrará la descripción de los mensajes ICMPv4.

Tabla 27*Descripción de los mensajes ICMPv4*

Mensaje	Tipo	Propósito	Códigos	Significado del Código
Echo Reply	0	Responder a un mensaje de solicitud de eco (ping).	0	Respuesta de eco
Destination Unreachable	3	Indica que el destino no se puede alcanzar por alguna razón.	0–15	Varias razones como red/host/puerto inalcanzable, comunicación prohibida, etc.
Source Quench (obsoleto)	4	Solicitaba reducir la velocidad de envío de paquetes. Sustituido por mecanismos de capa 4 y ECN.	0	Control de congestión.
Redirect	5	Informa al host que utilice otra ruta para llegar al destino.	0–3	Redirección para red/host (para tráfico específico o general)
Echo Request	8	Solicita una respuesta de eco para verificar la conectividad (ping).	0	Solicitud de eco
Time Exceeded	11	Indica que el tiempo de vida (TTL) de un paquete ha expirado. Cada router que agota el TTL devuelve este mensaje al origen.	0–1	TTL expirado en tránsito o fragmentación sin ensamblar
Parameter Problem	12	Señala un problema con los parámetros del encabezado del paquete IP. Router descarta un datagrama mal formado.	0–2	Error en el puntero, campo obligatorio faltante u opción desconocida
Timestamp Request	13	Solicita la hora actual del host destino.	0	Solicitud de marca de tiempo
Timestamp Reply	14	Responde con la hora del host al mensaje de Timestamp Request.	0	Respuesta de marca de tiempo

Nota. Ludeña, P., 2025.

Por ejemplo, el mensaje Echo Reply (tipo 0) se utiliza para responder a una solicitud de eco, como en el comando ping, confirmando que el host destino es alcanzable; el mensaje Destination Unreachable (tipo 3) indica que un paquete no pudo llegar a su destino; esto puede deberse a que la red, el host o el puerto está inalcanzable, o por restricciones de acceso; y, el mensaje Time Exceeded (tipo 11) se genera cuando el TTL (Time To Live) de un paquete ha expirado, ya sea en tránsito o durante

el reensamblaje de fragmentos IP, siendo común en herramientas como traceroute.

El protocolo ICMPv6, definido en RFC 4443, reorganiza los campos Tipo y Código (ver Tabla 28) para ampliar las funcionalidades del protocolo original.

Tabla 28

Descripción de los mensajes ICMPv6

Mensaje	Tipo	Propósito	Códigos	Significado del Código
Destination Unreachable	1	Indica que el destino no es accesible.	0–7	Red/host inalcanzable, comunicación administrativamente prohibida, etc.
Packet Too Big	2	Indica que un paquete excede el MTU del siguiente salto.	0	MTU excedido
Time Exceeded	3	Límite de salto ha expirado o tiempo agotado en reensamblado.	0–1	TTL expirado en tránsito o en reensamblado
Parameter Problem	4	Problema con el encabezado del paquete.	0–2	Campo erróneo en encabezado, opción no reconocida, etc.
Echo Request	128	Solicita una respuesta para verificar conectividad (ping).	0	Solicitud de eco
Echo Reply	129	Responde al mensaje de solicitud de eco.	0	Respuesta de eco
Router Solicitation	133	Host solicita información de enrutadores.	0	Solicitud enviada por un host
Router Advertisement	134	El router anuncia su presencia e información de red.	0	Anuncio enviado por un router
Neighbor Solicitation	135	Solicita la dirección MAC de un vecino (como ARP en IPv6).	0	Solicitud de vecino

Mensaje	Tipo	Propósito	Códigos	Significado del Código
Neighbor	136	Responde con la dirección MAC del vecino.	0	Respuesta de vecino
Advertisement				

Nota. Ludeña, P., 2025.

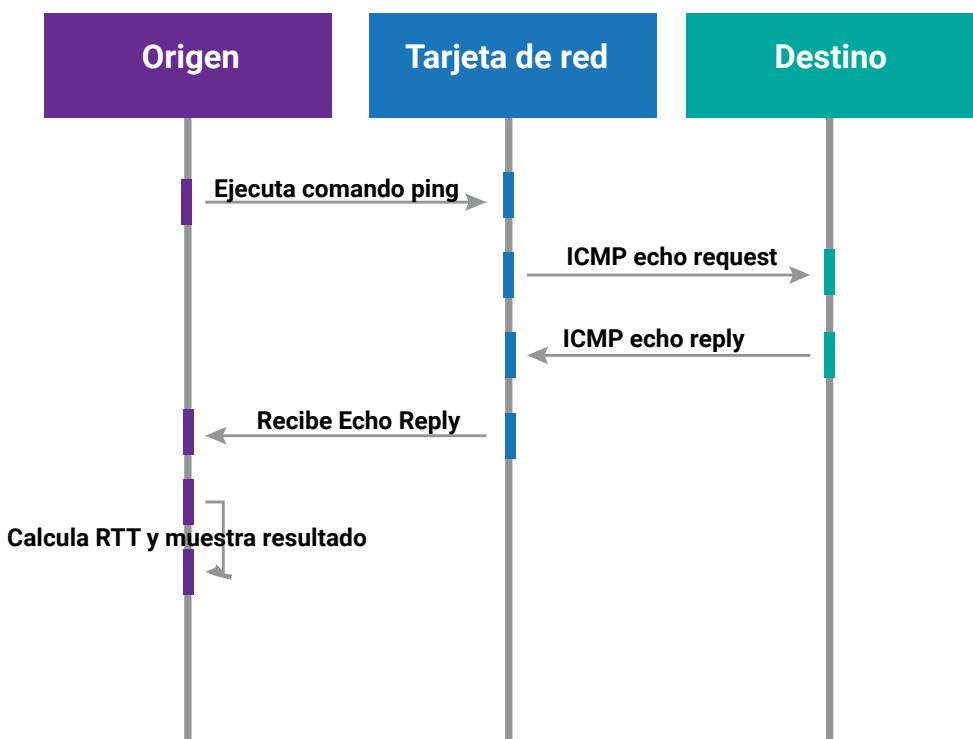
Por ejemplo, en el contexto de la autoconfiguración y descubrimiento de vecinos, Router Solicitation (tipo 133) permite que un host solicite información de enrutadores, mientras que Router Advertisement (tipo 134) es enviado por los routers para anunciar su presencia y parámetros de red. Finalmente, Neighbor Solicitation (tipo 135) y Neighbor Advertisement (tipo 136) permiten a los nodos descubrir y confirmar direcciones MAC de vecinos en la red, función que revisaremos en detalle en la Sección 2.9.2.

2.8.2. Herramienta ping

El comando ping usa los mensajes Echo de ICMP como un sonar, en la puedes ver el proceso.

Figura 44

Diagrama de secuencia del comando ping



Nota. Ludeña, P., 2025.

Cuando el origen ejecuta el comando ping, la tarjeta de red envía un Echo Request (tipo 8 en ICMPv4, 128 en ICMPv6). Cuando la solicitud llega al destino, éste responde con un Echo Reply (tipo 0 en ICMPv4, 129 en ICMPv6) con la misma carga de datos y el mismo identificador. El origen recibe el Echo Reply y puede medir el tiempo transcurrido entre la salida y la vuelta para calcular la latencia de ida y vuelta (RTT). Así mismo, al contar cuántas solicitudes no reciben respuesta se deduce la pérdida de paquetes. De este modo, cada secuencia de pings aporta información objetiva sobre disponibilidad y calidad del enlace.

2.8.3. Herramienta traceroute

El comando traceroute convierte los campos de control de IP y los mensajes ICMP en un GPS que descubre, salto a salto, qué enrutadores atraviesa un paquete hasta llegar a su destino.

El mecanismo que usa traceroute es muy sencillo e ingenioso y puede revisarlo en el [Anexo 2. Funcionamiento del Protocolo Traceroute](#).

2.9. Resolución de direcciones IP-MAC



Para comprender la importancia de la resolución de direcciones IP-MAC, imagine una empresa que tiene decenas de empleados distribuidos en varios cubículos dentro de una planta en un edificio. La paquetería física tendrá el nombre de cada empleado como destinatario, pero entre tanto empleado, el repartir los paquetes es una tarea muy difícil para el mensajero. Cuando un mensajero debe entregar un paquete, lo que realmente necesita es el número de cubículo. Para redes, el nombre sería la dirección IP y el número de cubículo es decir la ubicación física sería la dirección MAC.

Siguiendo con nuestra analogía, si el mensajero conoce el nombre del destinatario, pero no la ubicación física, una posible estrategia, sería acercarse a la recepción y pregunta en voz alta: ¿En qué cubículo se encuentra Juan Pérez? Eventualmente Juan escuchará que están preguntando por él y responderá con el número de cubículo donde se encuentra. Entonces, la próxima vez que el mensajero tenga un paquete para Juan Pérez irá directamente al cubículo, sin volver a preguntar.

Esto es una versión resumida del proceso de resolución direcciones IP a direcciones MAC, que es un proceso cotidiano en redes locales ya sea a través de ARP para IPv4 o Neighbor Discovery para IPv6. El equipo que requiera entregar un paquete envía la pregunta ¿quién tiene

esta dirección IP? a todos los dispositivos presentes en la red local y el dispositivo dueño de esa dirección responde con su MAC. El emisor guarda el par dirección IP-dirección MAC en la tabla ARP/ND y la consulta, mientras, la información siga siendo válida.

El proceso de resolución de direcciones es necesario porque, como se vio en la Sección 1.4 de esta Guía Didáctica, los paquetes de capa 3 se encapsulan en tramas de capa 2, para poder enviarse las unidades de datos deben tener todos sus campos llenos. Eso quiere decir que el paquete debe tener dirección IP de origen y destino y la trama debe tener dirección MAC de origen y destino. Si se tiene la dirección IP de destino se puede armar el paquete, pero al pasar a capa 2 la trama se retendrá hasta completar el campo de dirección MAC de destino. En primera instancia el emisor consulta su propia tabla ARP, si encuentra un par IP-MAC, la trama se completa y se envía. Si no la encuentra, se pone en marcha el método de resolución de direcciones.

Para consultar la tabla ARP de dispositivos Windows puede utilizar el comando **arp -a**. La información desplegada por el comando incluye tres columnas:

1. **Dirección Internet:** muestra la dirección IP de los dispositivos con los que el equipo ha intentado comunicarse recientemente.
2. **Dirección física:** muestra la dirección MAC correspondiente a la dirección IP del dispositivo.
3. **Tipo:** indica si la entrada es dinámica, es decir, fue aprendida automáticamente por ARP o estática si se incluyó manualmente por el usuario o el sistema y no cambia hasta que se elimina.

En la Figura 45, puede ver un ejemplo de una tabla ARP.

Figura 45

Visualización de la tabla ARP en Windows mediante el comando arp -a

```

Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Instale la versión más reciente de PowerShell para obtener nuevas
características y mejoras. https://aka.ms/PSWindows

PS C:\Users\pjludeña> arp -a

Interfaz: 192.168.1.238 --- 0x7
          Dirección de Internet      Dirección física      Tipo
 192.168.1.1           84-93-b2-57-f1-e4    dinámico
 192.168.1.222         38-e7-c0-b9-b2-66    dinámico
 192.168.1.255         ff-ff-ff-ff-ff-ff    estático
 224.0.0.22            01-00-5e-00-00-16    estático
 224.0.0.251           01-00-5e-00-00-fb    estático
 224.0.0.252           01-00-5e-00-00-fc    estático
 255.255.255.255       ff-ff-ff-ff-ff-ff    estático

```

Nota. Ludeña, P., 2025.

Usted puede ver dos entradas aprendidas a través de ARP para los equipos 192.168.1.1 y 192.168.1.222. Adicionalmente puede ver cinco entradas estáticas, que corresponden a direcciones de difusión (terminadas en 255) y multidifusión (inician con prefijo 224.0.0), al ser direcciones de propósito específico son fijadas por el sistema.

IMPORTANTE:


- Debido a que las direcciones MAC se usan para la entrega de tramas entre dispositivos dentro de la red local, las direcciones IP aprendidas de manera dinámica en una tabla ARP deben pertenecer siempre a la red local.
- Si la dirección IP destino está fuera de la red local, es decir, el destino está en una red remota, el host no busca la dirección MAC del destino final, sino la de su Gateway o puerta de enlace predeterminada. De este modo cada segmento solo maneja direcciones locales.

A continuación, revisaremos cómo se realiza el proceso tanto en IPv4 como en IPv6.

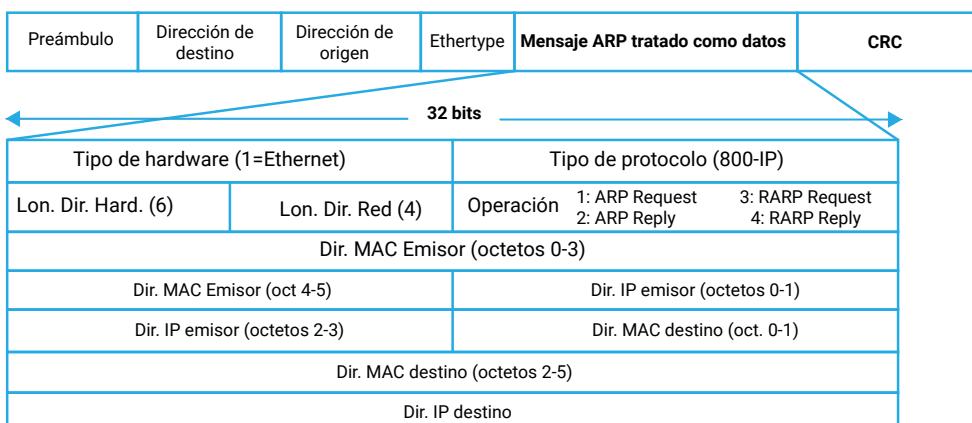
2.9.1. Dirección IPv4- dirección MAC

El protocolo ARP (*Address Resolution Protocol*) es el encargado de traducir una dirección IPv4 conocida en la dirección MAC que la capa 2 necesita para encapsular la trama, permitiendo que los dispositivos se comuniquen dentro de una red local.

Los mensajes del protocolo ARP se envían como datos dentro de la trama, en la Figura 46, puede ver la estructura del mensaje ARP en una trama Ethernet.

Figura 46

Estructura de un mensaje ARP encapsulado en una trama Ethernet



Nota. Adaptado de ARP. Redes de computadores (p. 167) [Ilustración], por Sánchez, M., 2020, Universidad de Alcalá, CC BY 4.0.

A continuación, se explicará cada uno de los campos estándar.

- **Tipo de hardware:** especifica el tipo de red física utilizada. El valor más común es 1, que representa Ethernet.

- **Tipo de protocolo:** indica el protocolo de red que se está utilizando para mapear la dirección, típicamente 0x0800 para IPv4.
- **Longitud de la dirección de hardware (MAC):** especifica el número de bytes de la dirección física. En redes Ethernet, este valor es 6.
- **Longitud de la dirección de red (IP):** indica el número de bytes de la dirección de protocolo. Para IPv4, este valor es 4.
- **Operación:** determina el tipo de mensaje ARP. Será 1 para ARP Request (solicitud), 2 para ARP Reply (respuesta), 3 para RARP Request (solicitud inversa) y 4 para RARP Reply (respuesta inversa).
- **Dirección MAC del emisor:** contiene la dirección física del dispositivo que envía el mensaje ARP.
- **Dirección IP del emisor:** indica la dirección IP del host que envía el mensaje. Es útil para que el receptor conozca cómo devolver la respuesta.
- **Dirección MAC del receptor:** en un ARP Request, este campo suele estar en ceros (00:00:00:00:00:00) porque aún no se conoce. En un ARP Reply, se completa con la dirección del destino.
- **Dirección IP del receptor:** es la dirección IP que se desea resolver o responder. En una solicitud, es la IP de destino; en una respuesta, es la IP del solicitante.

La operación del protocolo se compone de los siguientes elementos:

- a. **Solicitud ARP:** el host crea un paquete ARP de consulta (ARP Request) añadiendo como datos la dirección IP de destino, su dirección IP y su propia dirección MAC. La consulta se envía a todos los equipos en la red local, por tanto, el destino en la trama es la dirección MAC de difusión FF-FF-FF-FF-FF-FF.

- b. **Respuesta ARP:** debido a que la solicitud se envía en broadcast, todos los nodos de la red local reciben la solicitud, pero solo el dispositivo cuya dirección IPv4 coincide con la consultada envía como respuesta (ARP Reply) su dirección MAC. La respuesta se envía únicamente al host que realizó la consulta y puede incluir la asociación inversa para que el emisor también actualice su caché.
- c. **Actualización de caché:** en el proceso de solicitudes y respuestas ambos extremos pueden ir almacenando información de sus vecinos en un espacio de memoria denominado caché ARP. La funcionalidad de la caché es evitar que se realicen múltiples consultas por difusión que inyecten tráfico innecesario en la red. Cada entrada en la caché ARP se compone de un par IP-MAC correspondiente a un dispositivo con el cual se ha tenido comunicación y está asociada a un temporizador con un valor de 15 minutos, típicamente. Las entradas dentro del caché pueden caducar automáticamente con el vencimiento del temporizador o pueden eliminarse manualmente; con esta estrategia se reduce el impacto de cambios de topología y de direcciones duplicadas.

Revisemos un ejemplo práctico sobre el funcionamiento del protocolo ARP.

Suponga que en la red 192.168.10.0/24, el equipo PC-A (192.168.10.15, MAC AA:AA:AA:AA:AA:AA) necesita enviar un paquete a PC-B (192.168.10.30, MAC BB:BB:BB:BB:BB:BB).

- a. En primera instancia PC-A revisa su tabla ARP y si no encuentra una entrada para la IP 192.168.10.30, comienza el proceso de ARP.
- b. Luego, PC-A envía un ARP Request a FF-FF-FF-FF-FF-FF. ¿Quién tiene la dirección IP 192.168.10.30? Soy 192.168.10.15 con dirección MAC AA:AA:AA:AA:AA:AA.

- c. Después, PC-B responde en unicast. Yo tengo la dirección IP 192.168.10.30 y mi dirección MAC es BB:BB:BB:BB:BB:BB. Ambos equipos actualizan su caché ARP y el temporizador para esta nueva entrada ($t=15$ min).
- d. Con la información que obtuvo por ARP, PC-A encapsula el paquete IP dentro de una trama Ethernet con destino BB:BB:BB:BB:BB:BB y transmite. PC-B recibe la trama, extrae el paquete y continúa el procesamiento como corresponda a los protocolos de capas superiores que contenga.

A partir de esta transacción, todo el tráfico entre las mismas direcciones IP utilizará la MAC almacenada en la caché ARP hasta que el temporizador expire y se requiera repetir el proceso ARP. Este ciclo, es transparente para el usuario, pero es de vital para la eficiencia de la red local.

El protocolo ARP (Address Resolution Protocol) tiene varias variantes diseñadas para resolver diferentes necesidades en la comunicación de redes, en la Figura 47, encontrará los cuatro tipos de ARP que revisaremos.

Figura 47

Tipos de ARP utilizados en redes de computadoras

Tipos de ARP	
— ARP de proxy	<ul style="list-style-type: none"> - Un dispositivo responde por otro de su red - Ofrece su dirección MAC como destino
— ARP gratuito	<ul style="list-style-type: none"> - El host anuncia su dirección IP a MAC - No responde a una solicitud previa
— ARP reverso (RARP)	<ul style="list-style-type: none"> - El host detecta su propia dirección IP - Usa su dirección MAC para encontrar una IP
— ARP inverso (IARP)	<ul style="list-style-type: none"> - Usa una dirección MAC para encontrar una IP - Inverso al ARP tradicional

Nota. Ludeña, P., 2025.

El ARP de proxy permite que un dispositivo responda en nombre de otro que está fuera de la red local, usando su propia dirección MAC para redirigir el tráfico. Por otro lado, el ARP gratuito es utilizado por un host para anunciar o confirmar su propia dirección IP sin haber recibido una solicitud previa, funcionando como una actualización o verificación dentro de la red.

El ARP reverso (RARP) se emplea cuando un dispositivo conoce su dirección MAC, pero no su dirección IP, solicitando esta información a un servidor RARP. Y, por último, el ARP inverso (IARP) busca una dirección IP a partir de una dirección MAC dentro de la misma red, lo opuesto al funcionamiento del ARP tradicional. Cada tipo de ARP cumple una función específica que contribuye a la correcta resolución y gestión de direcciones en entornos de red.



Para mejorar la comprensión sobre el protocolo ARP, le invito a revisar el video titulado “[¿Cómo funciona el protocolo ARP?](#)”, en donde verá cómo trabaja el protocolo a través de la implementación de una red simple en GNS3. GNS3 es un emulador de red, es decir, que podrá revisar el comportamiento real de los equipos de red ante el despliegue de consultas ARP. La red estará compuesta de dos computadores y dos switches y se realizará una prueba de conectividad usando ping para generar tráfico y la herramienta Wireshark para capturar y evaluar los paquetes transmitidos.

Luego de ver el video, conteste en su cuaderno de apuntes o en un documento de Word las siguientes preguntas:

- ¿Cuáles son los primeros paquetes que se capturan cuando se hace la prueba de conectividad? ¿Por qué?
- ¿Cuál es la dirección MAC de destino del ARP request? ¿Por qué se pone esta dirección?
- ¿Cuál es la dirección MAC de destino del ARP response? ¿Por qué se pone esta dirección?
- ¿Qué diferencia hay entre el proceso ARP cuando el destino está en la red local y cuando el destino está en una red remota?

2.9.2. Dirección IPv6- dirección MAC

El Neighbor Discovery Protocol (NDP) reemplaza a ARP en IPv6. Los pasos que sigue este protocolo para resolver direcciones son similares a los usados por el protocolo ARP, pero usa mensajes específicos para intercambiar la información. NDP usa los mensajes ICMPv6 que estudiamos en la Sección 2.8.1 de esta guía didáctica, NS (Neighbor Solicitation) y NA (Neighbor Advertisement); y con ellos, además de resolver la dirección MAC tiene otras funciones, entre ellas puede

descubrir routers, detectar vecinos inalcanzables y evitar duplicados de dirección.

Al igual que con IPv4, cuando un dispositivo quiere enviar un paquete, primero consulta su tabla y consulta si tiene un par IPv6-MAC, en este caso, para completar la información y enviar el paquete. Si no hay una entrada coincidente se genera el proceso de resolución, el cual consta de tres pasos fundamentales:

- a. **Solicitud de vecino:** el host envía un mensaje NS a la dirección multidifusión de nodo solicitado derivada de la dirección IPv6 del destino, siguiendo el formato FF02::1:FFxx:xxxx, donde las equis serán reemplazadas por los seis últimos hexetos (24 bits) de la dirección IPv6 de destino. La dirección MAC de destino debe ser coherente con la enviada en capa de red, por tanto, se usa una dirección de multidifusión Ethernet con prefijo 33:33, siguiendo el formato 33:33:yy:yy:yy:yy donde las y representan los últimos 32 bits de la dirección multicast IPv6.
- b. **Anuncio de vecino:** el dispositivo que posee la dirección IPv6 responde con un NA unidifusión (o multidifusión si anuncia su presencia) incluyendo su dirección MAC.
- c. **Actualización de la caché de vecinos:** ambos dispositivos registran la pareja IPv6-MAC en estado *Reachable*, en una tabla similar a la caché ARP, con un temporizador (30 segundos por defecto). Si no hay actividad, el estado pasa a *Stale* y, antes de usarla, se envía un NS unicast para confirmar.

Para visualizar cómo funcionan los mensajes NS y NA en este proceso de tres pasos, revisemos un **ejemplo práctico**.

Supongamos que en una red IPv6 se tienen dos dispositivos PC-A (2001:db8:1::10, MAC AA-AA-AA-AA-AA-AA) y PC-B (2001:db8:1::20, MAC BB-BB-BB-BB-BB-BB). PC-A quiere enviar un paquete a PC-B y no tiene una entrada en su tabla de vecinos, es decir, no tiene su dirección MAC.

En primer lugar, PC-A envía un mensaje NS a la dirección IPv6 multicast de destino solicitada FF02::1:FF00:20 (últimos 24 bits de la IPv6 de destino 00:00:20) y a la dirección MAC 33:33:ff:00:00:20 (últimos 32 bits de la dirección multicast ff:00:00:20). Después, el mensaje NS se encapsula en un paquete ICMPv6 y se envía a la red local. Esta dirección multicast permite que solo el host con esa dirección IPv6, en este caso PC-B, lo escuche y responda su dirección MAC con un mensaje NA.

Luego, PC-A y PC-B guardan en su caché de vecinos el par dirección IPv6-MAC, ponen estas entradas en estado *Reachable* y actualizan el temporizador.

Con base en lo estudiado, le invito a poner a prueba sus conocimientos respondiendo en su cuaderno de apuntes o en un documento de Word las siguientes preguntas:

- ¿Qué tipo de dirección IPv6 y qué dirección MAC se utilizará al enviar un NS para descubrir la dirección MAC de un nodo con dirección GUA 2001:db8:1::15? Revise nuevamente el ejemplo práctico para calcular su respuesta.
- ¿Cuáles son las principales ventajas de NDP frente a ARP en entornos IPv6? Mencione al menos dos.

Poderosos mensajes

Esta tarea tiene como objetivo que usted identifique algunos mensajes usados por los protocolos ICMP y ARP para realizar sus funciones.

Agudice su visión y encuentre las palabras escondidas en esta sopa de letras.



Mensajes de los protocolos ICMP y ARP

Su habilidad para identificar los diferentes tipos de mensajes ICMP y ARP demuestra una comprensión sólida de los protocolos auxiliares que hacen posible el funcionamiento eficiente de las redes IP. Ha logrado reconocer elementos fundamentales que van desde mensajes de diagnóstico como Echo Request y Destination Unreachable hasta procesos de resolución de direcciones como ARP Request y ARP Reply, componentes esenciales para el troubleshooting y la operación automatizada de redes.



Luego de desarrollar la actividad, conteste en su cuaderno de apuntes o en un documento de Word las siguientes preguntas de reflexión:

- ¿Por qué es importante el protocolo ICMP?
- ¿Cómo se complementan los protocolos ICMP y ND?

Perfecto, concluimos con éxito la semana 9. Ahora pueden participar en esta quiz para consolidar su aprendizaje.

Protocolo ICMP y Resolución de Direcciones

Su desempeño en esta evaluación demuestra un dominio sólido de los protocolos auxiliares que constituyen la infraestructura invisible pero indispensable para el funcionamiento eficiente de las redes IP modernas. Ha consolidado conocimientos que van desde la interpretación de códigos de error ICMP hasta la comprensión de procesos de

autoconfiguración IPv6, competencias técnicas que son fundamentales para el troubleshooting avanzado y la optimización de rendimiento en redes empresariales.



Actividades de aprendizaje recomendadas

Continuemos con el aprendizaje mediante su participación en las actividades que se describen a continuación:

Actividad 1. Lectura de los contenidos propuestos

Ingresé a la plataforma [Netacad](#) y revise el módulo 9: Resolución de dirección y el módulo 13: ICMP. Evalúe cómo puede utilizar las herramientas de diagnóstico ping y traceroute para detectar fallos en la red y diseñar estrategias de solución. Determine, además, por qué es importante disponer de un protocolo que mapee direcciones IP a direcciones MAC para la entrega de datos en la red local. Adicionalmente, deberá analizar el proceso de resolución de direcciones que se realiza para IPv4 e IPv6, con el objetivo de marcar las diferencias entre los dos procedimientos y evaluar cómo ha evolucionado esta tarea tan fundamental en la comunicación de redes.

Estrategia de trabajo:

- Planifique un tiempo semanal para la lectura de los materiales sugeridos.
- Tenga a mano un cuaderno de apuntes o un documento Word donde pueda tomar nota de las ideas principales.
- Desarrolle las actividades. Verifique su comprensión.
- Realice las autoevaluaciones disponibles para evaluar su comprensión sobre los contenidos.

Retroalimentación:

En las autoevaluaciones, la plataforma Netacad revisará sus respuestas y señalara aquellas que sean incorrectas, lo que le ayudará a reconocer los conceptos que necesita reforzar y revisar nuevamente.

Actividad 2. ¡Exploraremos el protocolo ARP en redes locales y remotas!

En esta actividad usted aplicará sus conocimientos sobre el modelo OSI y el protocolo ARP mediante una simulación interactiva con Cisco Packet Tracer. A través de distintos escenarios de red, observará cómo se generan las solicitudes ARP, cómo se construyen las tablas de direcciones MAC en los switches, y cómo se resuelven las direcciones IP a nivel de capa de enlace. Esta experiencia le permitirá analizar el flujo de información en redes tanto locales como remotas, fortaleciendo su comprensión sobre el funcionamiento interno de las redes de computadoras.

Estrategia de trabajo:

- Repase la información sobre el protocolo ARP.
- Revise los tipos de mensajes que el protocolo ARP envía para realizar la resolución de direcciones.
- Desarrolle la actividad propuesta siguiendo el guion disponible en la misma.

[Práctica 9.2.9 de CCNA-1: examinar la tabla ARP.](#)

Este recurso le permitirá comprender el funcionamiento del protocolo ARP y su rol fundamental en la resolución de direcciones dentro de una red. A través de la simulación con Packet Tracer, podrá analizar cómo se generan y procesan las solicitudes ARP en distintos escenarios, observando los paquetes (PDU) en cada capa del modelo OSI, especialmente en las capas de enlace de datos y red.

El uso de este recurso fortalece la observación analítica de la interacción entre dispositivos y el comportamiento de los switches y routers ante la comunicación local y remota. Además, promueve el desarrollo de habilidades prácticas que son esenciales para el perfil profesional del ingeniero en Redes y Analítica de Datos, tales como la capacidad de inspeccionar tablas ARP, interpretar la información de tráfico de red, y entender el impacto de la resolución de direcciones en la conectividad de dispositivos.

Retroalimentación:

Luego de desarrollar la práctica, le invito a resolver las siguientes preguntas de reflexión:

- ¿Qué función cumple la solicitud ARP dentro de una red cuando no se conoce la dirección MAC de destino? Piense en el mecanismo de difusión que usa ARP para realizar las consultas. ¿Por qué cree que este proceso es importante antes de enviar un paquete?
- Cuando el switch recibe la solicitud ARP, ¿por qué cree que genera varias copias de la PDU? Recuerde cuando estudiamos la operación del switch en la sección 2.3.3 de esta guía didáctica. Cuando un switch recibe una trama de difusión. ¿Cómo decide a qué puertos enviarla?
- ¿Qué ocurre con las direcciones MAC de origen y destino al pasar por cada dispositivo? Recuerde que, en cada salto, los encabezados cambian. ¿Cómo se refleja esto en los niveles de la PDU que está observando?
- Al revisar la tabla MAC del switch, ¿qué puede deducir si hay dos direcciones asociadas a un solo puerto?, ¿podría deberse a un dispositivo con múltiples interfaces conectadas?, ¿o es que varios dispositivos están detrás de un mismo punto de acceso?

- En el caso de una comunicación remota, ¿por qué el dispositivo no genera una solicitud ARP para la IP de destino final? Piense en el rol del *gateway* predeterminado. ¿Qué papel juega el *router* en esta situación?, ¿cómo le ayuda esta práctica a entender mejor los procesos automáticos que ocurren cada vez que se conecta a una red?

índice

I Bimestre

II Bimestre

Solucionario

Referencias



Sem 9

Sem 10

Sem 11

Sem 12

Sem 13

Sem 13

Sem 14

Sem 15

Sem 16



Semana 10

En esta semana centraremos nuestro estudio en la configuración de dispositivos para obtener conectividad. Para ello entrenaremos tres habilidades tecnológicas fundamentales para un profesional en Redes y Analítica de Datos, primero la configuración de parámetros iniciales en un router, segundo la configuración de interfaces, tanto físicas como lógicas para habilitar conectividad; y, finalmente, el uso sistemático de comandos de monitoreo para evaluar el estado de la red y para extraer información de operación de protocolos y sistemas.

El dominio de estas tareas le permitirá desplegar redes con criterios de seguridad, diagnosticar fallos en tiempo real y recopilar métricas fiables que más adelante alimentarán procesos analíticos de rendimiento y capacidad. Para alcanzar el resultado de aprendizaje previsto, desarrollará prácticas guiadas en Cisco Packet Tracer que le permitirán aplicar las configuraciones paso a paso y verificará su éxito con comandos de monitoreo. De esta forma integrará teoría y práctica y fortalecerá su perfil profesional. Cuando lo considere necesario, puede acudir a la bibliografía básica para revisar la configuración de enrutadores, en especial para consultar en detalle la sintaxis de los comandos aquí presentados.

2.10. Configuración de enrutadores

La configuración de enrutadores constituye una de las competencias fundamentales en la formación de un ingeniero en Redes y Analítica de Datos, ya que permite comprender y gestionar el flujo de datos entre diferentes segmentos de red. Esta habilidad es la base para destrezas más avanzadas como el enrutamiento dinámico, la segmentación de redes y la aplicación de políticas de calidad de servicio. Dominar la configuración de estos dispositivos le capacitará para diseñar,

Índice

I Bimestre

II Bimestre

Solucionario

Referencias

administrar y optimizar redes, respondiendo a las necesidades actuales de interconectividad en entornos empresariales, académicos y tecnológicos.

Empecemos el estudio de este tema tan importante en su formación.

2.10.1. Configuración de parámetros iniciales

Una de las fortalezas de Cisco IOS es la compatibilidad de sintaxis entre todos los dispositivos. Aprovecharemos esta ventaja para reducir la curva de aprendizaje, puesto que los comandos que aprendimos para la configuración de parámetros iniciales para switches también se aplican a routers.

En la siguiente infografía, a manera de repaso, se describen los comandos básicos que se ejecutan al acceder por primera vez al modo de configuración global de un router Cisco IOS. Para cada instrucción se indica su propósito y cualquier aspecto de formato que convenga recordar.

Comandos de configuración inicial de un router Cisco

El dominio de estos comandos de configuración inicial representa una competencia fundamental para la administración profesional de infraestructuras de red empresariales basadas en tecnología Cisco. La comprensión de aspectos como el establecimiento de credenciales seguras, configuración de acceso remoto, sincronización temporal y persistencia de configuraciones constituye la base técnica necesaria para implementar y mantener redes robustas y seguras.

Para garantizar estas implementaciones seguras, es fundamental seguir las mejores prácticas en tres aspectos clave, tal como se presenta a continuación:

▪ **Con relación al uso de *hostname*:**

- El nombre del dispositivo debe contener solo letras, números y guiones bajos o medios, no caracteres especiales.
- Los nombres de dispositivos deberían responder a un formato homogéneo en toda la red para mejorar la gestión, por ejemplo, prefijos del tipo de equipo y sufijos que se refieran a la ubicación.

▪ **En cuanto al uso de contraseñas:**

- Establezca contraseñas con base en letras mayúsculas, minúsculas, números y símbolos.
- Evite palabras de diccionario, fechas de nacimiento, o información relacionada con usted o a la institución.
- Longitud mínima entre 10 y 12 caracteres.
- Cambie periódicamente la contraseña, recomendablemente cada 90 días.

▪ **En cuanto al uso del aviso legal:**

- Redacte un mensaje que informe claramente que el acceso está restringido solo a personal autorizado, puesto que puede servir como respaldo legal si alguien accede sin permiso.
- Use advertencias claras, formales y con lenguaje profesional.
- No use frases como "Bienvenido" u "Hola", ya que se podrían interpretar como una invitación al acceso.

- El mensaje debe informar sin comprometer la seguridad, no ponga nombres de usuarios ni información sobre la red.
- Evite errores de formato, faltas de ortografía o cortes inesperados.

La aplicación práctica de estas buenas prácticas se puede ilustrar con el siguiente escenario profesional:



Suponga que usted es un administrador de red y que está configurando el router de borde de su organización. Debe configurar el equipo de manera segura, protegiendo con contraseñas el acceso por líneas y el modo de ejecución con privilegios. Además, se debe configurar un mensaje disuasorio para el acceso no autorizado y cifrar las contraseñas que se creen con el comando *password*.

En la figura 48, se observan las configuraciones iniciales realizadas desde el modo de configuración global.

Figura 48

Ejemplo de configuración de parámetros iniciales de un router Cisco

```
R1
CLI
IOS Command Line Interface

Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1_Borde
R1_Borde(config)#enable secret R3d3s_UTPL
R1_Borde(config)#service password-encryption
R1_Borde(config)#banner motd #ACCESO RESTRINGIDO:
Solo personal autorizado#
```

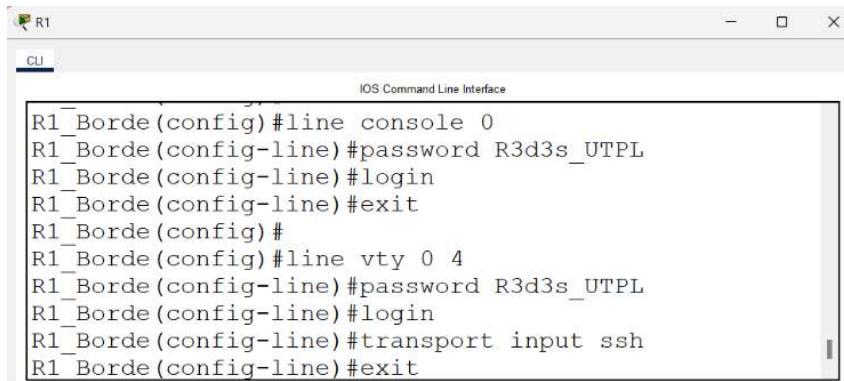
Nota. Ludeña, P., 2025.

Primero se fija el nombre del equipo que guarda el formato tipo de equipo y ubicación, en este caso es un router ubicado en el borde de la red. Se establece la contraseña cifrada R3d3s_UTPL siguiendo las recomendaciones de longitud y uso de caracteres. Se cifran todas las contraseñas con el comando service password-encryption y se añade el aviso legal de acceso no autorizado.

En la Figura 49, usted puede revisar el detalle de configuración de las líneas consola y vty, para el acceso local y remoto, respectivamente.

Figura 49

Ejemplo de configuración de líneas de acceso local por consola y SSH en un router Cisco



```
R1_Borde(config)#line console 0
R1_Borde(config-line)#password R3d3s_UTPL
R1_Borde(config-line)#login
R1_Borde(config-line)#exit
R1_Borde(config)#
R1_Borde(config)#line vty 0 4
R1_Borde(config-line)#password R3d3s_UTPL
R1_Borde(config-line)#login
R1_Borde(config-line)#transport input ssh
R1_Borde(config-line)#exit
```

Nota. Ludeña, P., 2025.

Para cada tipo de línea se configura una contraseña, por motivos didácticos se usa la misma contraseña que para el acceso al modo de ejecución con privilegios, pero lo recomendable es que sean diferentes contraseñas para cada línea.

2.10.2. Configuración de interfaces

Una de las funciones principales de la capa de red es el **direccionamiento IP**, por tanto, una de las configuraciones más importantes que se deben realizar en los routers es asignar

direcciónamiento y habilitar a sus interfaces. En la Tabla 29 tiene disponible los comandos que usará para configurar interfaces y su función.

Tabla 29

Comandos de Cisco IOS para configuración de interfaces

Comando	Función	Recomendaciones
interface <tipo-número>	Permite ingresar al contexto de la interfaz (GigabitEthernet 0/0, Serial 0/1/0) para poder aplicar parámetros específicos.	Es recomendable llevar un orden lógico al numerar y documentar las conexiones, facilitando así la administración y el mantenimiento.
description <texto>	Permite añadir una etiqueta que identifique el propósito de la interfaz.	Útil para la generación de documentación automática. Se recomienda evitar acentos y espacios excesivos.
ip address <ipv4> <máscara>	Asigna la dirección IPv4 y la máscara de subred.	Solo una IP primaria por interfaz; las secundarias usan secondary.
ipv6 address <ipv6>/<prefijo>	Asigna direcciones GUA o Link-Local (LLA) si se añade link-local.	El IOS crea automáticamente la LLA FE80::/10 si no se especifica.
no shutdown	Cambia el estado administrativo a up.	Sin este comando la interfaz permanece inactiva.
(Opcional) speed <valor>	Fija velocidad cuando la autonegociación falla.	Cuide que ambos extremos tengan la misma configuración.
(Opcional) mtu <bytes>	Ajusta la MTU cuando el enlace lo requiere.	Mantenga coherencia en ambos extremos.

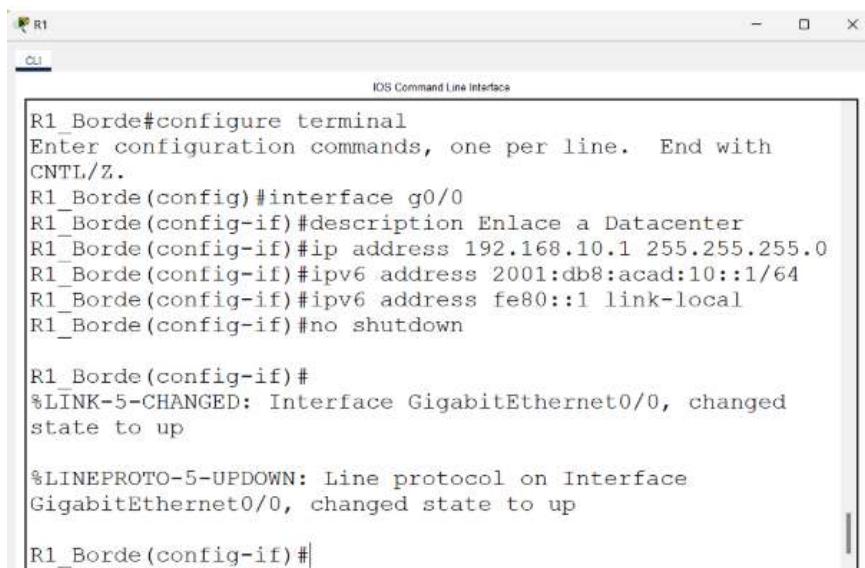
Nota. Ludeña, P., 2025.

Ejemplo:

Consideré el mismo equipo que en el ejemplo anterior y continuemos con la configuración de interfaces. El equipo usado es el router **Cisco 2911**, el cual conecta la red LAN con el data center. En la Figura 50, se detalla la configuración de la interfaz GigabitEthernet 0/0, un proceso similar se sigue para todas las interfaces

Figura 50

Configuración de la interfaz GigabitEthernet0/0 en un router Cisco



```
R1_Borde#configure terminal
Enter configuration commands, one per line. End with
CTRL-Z.
R1_Borde(config)#interface g0/0
R1_Borde(config-if)#description Enlace a Datacenter
R1_Borde(config-if)#ip address 192.168.10.1 255.255.255.0
R1_Borde(config-if)#ipv6 address 2001:db8:acad:10::1/64
R1_Borde(config-if)#ipv6 address fe80::1 link-local
R1_Borde(config-if)#no shutdown

R1_Borde(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed
state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up

R1_Borde(config-if)#[
```

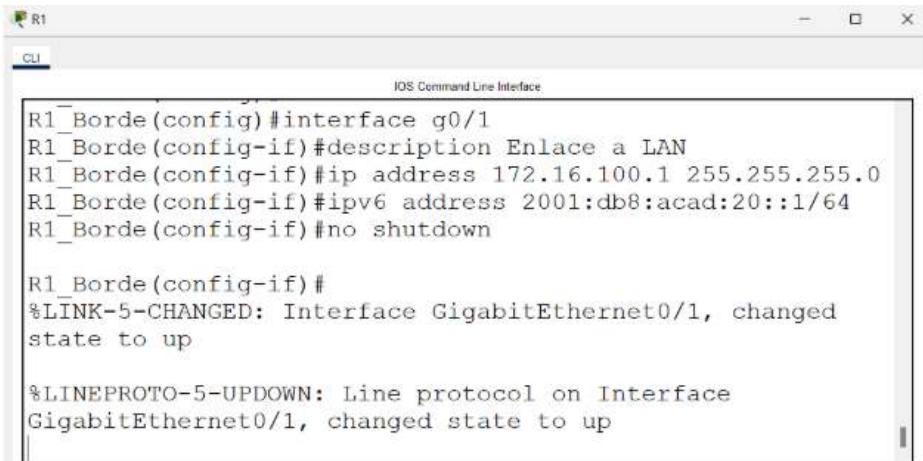
Nota. Ludeña, P., 2025.

Note que el formato de configuración de las direcciones IPv4 e IPv6 cambia, mientras para IPv4 es necesario poner la máscara de red, para IPv6 se declara la longitud de prefijo. Por otra parte, las interfaces IPv6 tienen dos direcciones, la dirección GUA y la dirección link-local. Finalmente, es necesario que se activen las interfaces a través del comando no shutdown.

En la Figura 51, se muestra la configuración para la interfaz GigabitEthernet 0/1, usando la misma secuencia de comandos que para la interfaz 0/0.

Figura 51

Configuración de la interfaz GigabitEthernet0/1 como enlace a LAN



```
R1_Borde(config)#interface g0/1
R1_Borde(config-if)#description Enlace a LAN
R1_Borde(config-if)#ip address 172.16.100.1 255.255.255.0
R1_Borde(config-if)#ipv6 address 2001:db8:acad:20::1/64
R1_Borde(config-if)#no shutdown

R1_Borde(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed
state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up
```

Nota. Ludeña, P., 2025.

Note que no se configuró la dirección link-local, sin embargo, no se presenta ningún error. Esto se debe a que, como se vio en la sección 2.7.2 de esta Guía Didáctica, si no se configura explícitamente una dirección link-local el sistema genera una para la interfaz. En la Figura 52, se puede verificar la configuración de las dos interfaces, usted puede ver que mientras la interfaz g0/0 tiene la dirección fe80::1 que se configuró, la interfaz g0/1 tiene la dirección FE80::240:BFF:FE88:8002 generada automáticamente.

Figura 52

Verificación del estado y direcciones IPv6 de las interfaces del router

```
R1_Borde#show ipv6 interface brief
GigabitEthernet0/0          [up/up]
  FE80::1
  2001:DB8:ACAD:10::1
GigabitEthernet0/1          [up/up]
  FE80::240:BFF:FE88:8002
  2001:DB8:ACAD:20::1
```

Nota. Ludeña, P., 2025.

Con esta configuración, el router ya está operativo y puede empezar a gestionar tráfico básico de sus redes directamente conectadas. Por ello, es momento de conocer los comandos de monitoreo que se pueden utilizar para monitorear el funcionamiento de la red, consolidando las habilidades operativas que exige el perfil profesional.

2.10.3. Comandos de monitoreo

Los comandos de monitoreo son herramientas muy poderosas para extraer información de los equipos de red y evaluar el estado de la misma. Con ellos se puede detectar cuellos de botella, determinar en qué capa se están produciendo fallos e identificar estrategias de solución. En la Tabla 30 se describen los comandos de uso cotidiano, la información que revelan y los fallos típicos que ayudan a descubrir, junto con la posible acción correctiva más inmediata.

Tabla 30*Comandos de monitoreo y diagnóstico en dispositivos de red Cisco*

Comando	Información que presenta	Fallas que ayuda a detectar	Solución habitual
show ip interface brief / show ipv6 interface brief	Estado up/down, dirección lógica y tipo de encapsulado de cada interfaz.	Detectar interfaces administrativamente apagadas o con errores. Interfaces con dirección IP asignada. Máscara/prefix incorrecto, Verificar qué interfaces están activas (protocolo de línea down.)	Comprobar cableado, ejecutar no shutdown, corregir dirección o VLAN.
show interfaces <tipo>	Estadísticas físicas: CRC, colisiones, input/output errors, velocidad y dúplex.	Problemas de capa física, falla de configuración de modo de operación (dúplex/halfduplex), exceso de errores, saturación.	Sustituir cable/SFP, hacer configuraciones iguales en dos extremos del enlace (velocidad, dúplex, etc) limpiar conectores, cambiar puerto.
show ip route / show ipv6 route	Tabla de rutas conectadas, estáticas y dinámicas con prefijo más largo y métrica.	Problemas de capa 3. Rutas ausentes, prefijos erróneos, métrica inadecuada, bucles.	Añadir/corregir ruta, revisar vecinos OSPF/BGP, ajustar costos o redistribución.
show arp / show ipv6 neighbors	Caché IP-MAC Tabla de vecinos (estado Reachable, Stale, etc.).	Entradas caducadas, IP duplicada, flooding ARP.	Limpiar caché (clear arp), buscar host conflictivo, habilitar protección ARP/ND.
ping / traceroute	Latencia, pérdida, ruta de saltos.	Cortes de capa 3, MTU excesivo, bucles de ruta.	Verificar interfaz o enlace caído, ajustar MTU, corregir anuncio de prefijos.
show controllers	Estado del ASIC/PHY: Fallos de hardware, clocking, framing, errores de capa física.	desalineación de reloj en enlaces WAN.	Reemplazar módulo, sincronizar CSU/DSU, abrir ticket al proveedor.
show logging	Buffer con mensajes de sistema y marcas de hora.	Inestabilidad de puertos, intentos de acceso fallidos, avisos IP SLA.	Revisar cable/SFP, reforzar contraseñas/ACL, ajustar umbrales IP SLA.
show cdp neighbors detail	Modelo, nombre y IP de equipos Cisco conectados (CDP/ LLDP).	Cableado incorrecto, topología errónea o filtrada.	Reubicar cable, actualizar documentación, desactivar CDP en zonas sensibles.

Nota. Ludeña, P., 2025.

A continuación, en el [Anexo 3. Comandos show para monitoreo en Cisco IOS](#) se mostrará la información que proporcionan los comandos de monitoreo más utilizados en la gestión de equipos de red.

Comprobador de sintaxis

En esta actividad usted deberá ordenar los comandos para realizar configuraciones y monitorear redes. La competencia técnica se verá reforzada en esta actividad puesto que la sintaxis de los comandos es básica para garantizar una buena configuración de equipos y una buena gestión de las redes.



Comandos de Configuración

Su habilidad para construir correctamente la sintaxis de comandos Cisco IOS demuestra el nivel de precisión técnica requerido para la administración efectiva de infraestructuras de red empresariales. Ha consolidado la comprensión de estructuras de comandos que van desde configuraciones básicas de interfaces hasta implementación de protocolos de enrutamiento avanzados, competencia que es fundamental para evitar errores de configuración que podrían comprometer la estabilidad operacional de la red.



Luego de desarrollar la actividad, responda en su cuaderno de apuntes o en un documento de Word el siguiente cuestionario:

- ¿Qué comando se le dificultó más reconocer?

- ¿Cuál es la principal diferencia en la configuración de interfaces IPv4 e IPv6?
- ¿Qué estrategia podría sugerir para aprender los comandos de monitoreo?

¡Enhorabuena! Hemos llegado al final de la semana 10. Aprovechen esta oportunidad para reforzar sus conocimientos con el quiz.

Configuración de Enrutadores Cisco

Su desempeño en esta evaluación demuestra el nivel de competencia técnica requerido para administrar eficientemente infraestructuras de red basadas en tecnología Cisco en entornos empresariales de producción. Ha consolidado habilidades que abarcan desde la implementación de configuraciones seguras y el establecimiento de conectividad IP hasta la utilización sistemática de herramientas de monitoreo para diagnóstico preventivo y correctivo.



Actividades de aprendizaje recomendadas

Reforcemos el aprendizaje resolviendo las siguientes actividades.

Actividad 1. Lectura de los contenidos propuestos

Ingresé a la plataforma [Netacad](#) y revise el módulo 10: Configuración de parámetros básicos de *router*, los cuales le permitirán alcanzar una competencia muy apetecida en el campo laboral en un entorno cada vez más demandante.

Estrategia de trabajo:

- Dedique un tiempo exclusivo a leer el módulo en Netacad, asegurándose de comprender a fondo cada subtema.

- Anote los conceptos más relevantes en un cuaderno o archivo digital para consolidar su aprendizaje.
- Interactúe con los recursos multimedia y actividades que ofrece la plataforma para aplicar lo aprendido, en especial con el *comprobador de sintaxis* del módulo.
- Realice las evaluaciones al final del módulo como una forma de autoverificar su progreso.

Retroalimentación:

Al acabar la evaluación, la retroalimentación de la autoevaluación le indicará con claridad cuáles temas requieren un repaso adicional.

Actividad 2. ¡Configuremos equipos!

Esta actividad tiene como objetivo consolidar su comprensión sobre la comunicación entre dispositivos de red, mediante la configuración práctica de una topología básica que incluye PC, un switch y un router. A través de la experiencia directa con comandos de Cisco IOS en Packet Tracer y la interacción con estos equipos en modo físico. Adicionalmente, usted podrá analizar cómo se establecen y validan las rutas de comunicación entre dispositivos, contextualizando estos procesos dentro de los modelos de referencia OSI y TCP/IP.

Estrategia de trabajo:

- Repase la información sobre direccionamiento y funcionamiento de switches y routers.
- Revise los parámetros de configuración de dispositivos intermediarios.
- Tenga a mano su cuaderno de ingeniería.

- Desarrolle la actividad propuesta siguiendo el guion disponible en la misma.

Práctica 10.4.4. de CCNA-1: crear una red con un switch y un router.

La actividad busca fomentar el razonamiento técnico al identificar y resolver problemas de conectividad, fortaleciendo así su competencia para interpretar la lógica de configuración y diagnóstico en redes reales.

Retroalimentación:

Luego de desarrollar la práctica, le invito a resolver las siguientes preguntas de reflexión:

- ¿Qué ocurrió cuando hizo la prueba de conectividad ping entre los dos PC antes de configurar el *router*? , ¿por qué ocurre esto?
- ¿Por qué se debe configurar una puerta de enlace predeterminada en las PC y en el switch?
- Cuando se usa el comando *show ip interface brief*, ¿cómo se identifica si una interfaz está funcionando correctamente?

Actividad 3. Es hora de medir nuestro avance

En la plataforma Netacad encontrará el Examen de punto de control: Examen de comunicación entre redes (módulos 8-10), que le propondrá cuestiones sobre las secciones 2.5 a la 2.9 de esta guía didáctica.

Le invito a dedicar tiempo a realizar la evaluación de los módulos de CCNA 1. Esta actividad es un requisito fundamental para la aprobación del módulo y, además, le permitirá aspirar a una microcertificación oficial de Cisco. Esta credencial puede representar una ventaja significativa en su formación técnica y futura carrera profesional. ¡Le animo a dar este paso con determinación!



Sem 9

Sem 10

Sem 11

Sem 12

Sem 13

Sem 13

Sem 14

Sem 14

Sem 15

Sem 16



Semana 11

En esta semana estudiaremos las técnicas de división de subredes de cada uno de los protocolos IP, cuyo objetivo es optimizar espacio de direccionamiento, aislar dominios de broadcast y diseñar topologías escalables que simplifiquen la gestión de tráfico. Analizaremos qué técnicas utilizar para evitar el desperdicio de espacio y sostener el crecimiento futuro.

Manejar con solvencia estos conceptos le convertirá en un profesional capaz de diseñar planes de direccionamiento escalables, garantizar la coexistencia de los protocolos IPv4 e IPv6 y extraer métricas fiables para analizar el tráfico, competencias que el perfil de ingeniero en Redes y Analítica de Datos exige en entornos empresariales. Para lograrlo trabajará de forma activa, esto incluirá análisis de ejemplos paso a paso sobre *subnetting* FLSM y VLSM (IPv4) y de segmentación de prefijos (IPv6), resolución de ejercicios propuestos y la configuración de escenarios en Packet Tracer donde comprobará, con ping y traceroute, el correcto funcionamiento de su esquema de direccionamiento.

2.11. División en subredes

La división en subredes o *subnetting* es el proceso de fraccionar una red IP en redes más pequeñas llamadas subredes. Para armar las subredes se toman *bits* de la porción de *host*, que se consideran *bits* de subred. Estos *bits* de subred se añaden al prefijo de la red base. Con esta estrategia, un bloque de direcciones único se convierte en varios dominios lógicos más pequeños, cada uno con su propio prefijo.

Dividir una red en subredes ofrece múltiples beneficios tanto en el rendimiento como en la gestión y seguridad de la infraestructura. En la figura 53, encontrará un mapa mental que resume de forma clara y

índice

I Bimestre

II Bimestre

Solucionario

Referencias

estructurada las principales ventajas, permitiendo visualizar cómo la segmentación mejora la eficiencia, facilita la administración y permite escalar las redes de forma más ordenada y segura.

Figura 53

Ventajas de dividir una red en subredes



Nota. Ludeña, P., 2025.

Usted se debe estar preguntando: ¿cómo debo agrupar los equipos en subredes? ¿qué debo considerar para dividir las redes? ¿cuál es el proceso para dividir la red?

Estas preguntas son muy válidas, porque antes del aspecto técnico de configuración de dispositivos está la planificación, de hecho, de una buena planificación depende en gran grado el éxito de la implementación de la red.

En primer lugar, usted debe considerar que las subredes le permitirán tener una organización de dispositivos, darle un uso práctico depende de su gestión como técnico. Se pueden tener varias formas de agrupar los dispositivos, como se muestra en la Figura 54.

Figura 54

Formas de agrupar dispositivos en subredes



Por función: ponga usuarios finales en subredes distintas de servidores o de dispositivos de gestión.



Por área geográfica: asigne un prefijo por planta o edificio para que el movimiento físico de equipos no requiera cambiarlos de red y asignarles una nueva dirección IP.



Por criticidad: separe sistemas de producción, pruebas y laboratorio para que, en caso de incidentes, no afecten a equipos críticos.



Enlaces punto-a-punto: utilice prefijos /30 (IPv4) o /127 (IPv6) exclusivos para no desperdiciar direcciones.

Nota. Ludeña, P., 2025.

Luego, se debe considerar algunos aspectos importantes a considerar antes de dividir una red.

- Requisitos de hosts y crecimiento:** calcule cuántas direcciones reales necesita la red en la actualidad y cuál es su proyección de crecimiento a futuro.
- Topología física y lógica:** identifique cuántos equipos de cada tipo tiene, por ejemplo, cuántos routers, switches, etc. Esto es

importante porque los equipos de capa 3 le permitirán tener subredes en cada una de las interfaces.

- c. **Política de seguridad y servicios:** identifique políticas en la organización y si es necesario, agrupe dispositivos con el mismo nivel de confianza o el mismo tipo de servicio (DMZ, servidores IoT, gestión).
- d. **Enrutamiento:** planee tener rutas que se puedan agregar en un único bloque para tener simplicidad en la tabla de rutas.

En las siguientes secciones abordaremos la tercera pregunta: ¿cuál es el proceso para dividir la red?, puesto que no hay un solo método de división.

A cada prefijo su máscara

En la división de red una habilidad muy importante es el cálculo de la máscara de red para cada nuevo prefijo. En esta actividad el objetivo es afianzar este conocimiento proponiendo varios prefijos para que se encuentre la máscara resultante con base en el número de bits disponibles en la porción de red.



Máscaras de subred

Su habilidad para establecer correspondencias correctas entre prefijos CIDR y máscaras de subred demuestra una competencia fundamental para el diseño e implementación de arquitecturas de direccionamiento IP eficientes. Este dominio de las relaciones entre notaciones de red le

proporciona las bases técnicas necesarias para planificar crecimientos de red escalables, implementar esquemas VLSM (Variable Length Subnet Masking) y troubleshoot problemas de enrutamiento relacionados con configuraciones incorrectas de máscaras, competencias directamente aplicables en proyectos de rediseño de red y consolidación de infraestructuras empresariales.

Luego de desarrollar la actividad, responda en su cuaderno de apuntes o en un documento de Word el siguiente cuestionario:



- ¿Para qué tipo de redes puede servir una máscara 255.255.255.252?
- ¿Por qué todas las máscaras son múltiplos de 2?
- ¿Cómo cambiarán estas máscaras para prefijos que tengan su límite en el tercer octeto?

2.11.1. División de redes IPv4 con máscara de subred de longitud fija (FLSM)

Como introducción a este tema, le invito a ver el video titulado “[Direccionamiento IPv4 y Subredes](#)”, que realiza un repaso sobre la estructura de las direcciones IP, los prefijos de red y las máscaras IP, para luego explicar de una manera muy didáctica el método de división de redes con máscara de subred de longitud fija. Repase sobre todo el tamaño de las direcciones IPv4 de 32 bits y cómo se calcula los prefijos y máscaras de red a través de los valores posicionales como se estudió en la Sección 2.5.3 de esta guía didáctica.

El Subneteo FLSM parte de la premisa de que todas las subredes tendrán exactamente la misma cantidad de hosts, por lo tanto, divide la red en una cantidad equitativa de direcciones para cada subred. El procedimiento se resume en seis pasos consecutivos que se encuentran explicados en la siguiente infografía. Note que en ella se encuentra un ejemplo didáctico para la red 192.168.0.0/24, donde se detalla cómo

aplicar cada paso para calcular bits prestados, máscara, número mágico e intervalos de subredes.

Algoritmo para dividir redes utilizando FLSM

Como pudo observar en la infografía, el proceso FLSM sigue una secuencia lógica bien definida. El dominio de esta metodología sistemática de subnetting representa una competencia fundamental para el diseño eficiente de arquitecturas de direccionamiento IP en infraestructuras empresariales complejas. La comprensión de conceptos como el cálculo de bits prestados, determinación del número mágico y generación de rangos de subredes constituye la base técnica necesaria para optimizar el uso de espacios de direcciones, implementar segmentación lógica apropiada y planificar crecimientos escalables de red.

Para aplicar correctamente esta metodología, tenga en cuenta las siguientes consideraciones técnicas fundamentales:

- El número total de subredes que se obtienen en la división de red es 2^n .
- El número total de direcciones de hosts válidas se calcula con $2^n - 2$, del rango de posibles direcciones se restan dos direcciones porque la primera dirección es la dirección de red y la última dirección es la dirección de broadcast; y, ninguna de estas dos direcciones puede ser asignada a interfaces de dispositivos.
- El incremento dado por el número mágico sólo afecta al octeto donde se encuentra el último bit prestado.
- El valor máximo por octeto es 255 en decimal, cuando con el incremento sea mayor a 255 se debe añadir una unidad al octeto de la izquierda y poner 0 en el octeto en el octeto del incremento.

- La frontera entre la porción de red y la porción de host se desplaza de izquierda a derecha, cada bit adicional duplica el número de subredes y divide a la mitad la cantidad de hosts.

Para consolidar su comprensión de estos conceptos teóricos y aplicar el algoritmo FLSM en diferentes escenarios, analicemos algunos ejemplos adicionales que enseñan variaciones comunes en el proceso de *subnetting*

1. Red original: 10.0.0.0/8

Requisito: 1000 subredes para un ISP pequeño.

Originalmente con esta red se tienen de 24 bits en la porción de host. El requerimiento es tener 1000 subredes, para conseguirlo se deben tomar prestados 10 bits ($2^{10} = 1024 \geq 1000$).

Los bits de subred se añaden al prefijo de la red original, así el nuevo prefijo es /18. Y la nueva máscara es 255.255.192.0. En la nueva porción de host quedan 14 bits, con lo cual cada red tiene $2^{14} - 2 = 16\,382$ hosts.

El bit prestado más hacia la derecha está en el segundo bit del tercer octeto, por eso el número mágico es 64.

Así las primeras 9 subredes serán: 10.0.0.0/18, 10.0.64.0/18, 10.0.128.0/18, 10.0.192.0/18, 10.1.0.0/18, 10.1.64.0/18, 10.1.128.0/18, 10.1.192.0/18, 10.2.0.0/18.

Manejo de incrementos: Note que para la quinta subred al sumar el número mágico a 192, la suma es 256. Entonces, se añade una unidad al segundo octeto y se pone 0 en el tercer octeto obteniendo la subred 10.1.0.0/18. Lo mismo ocurre para la novena subred, obteniéndose la dirección 10.2.0.0/18.

2. Red original: 192.168.1.0/24

Requisito: LAN pequeñas de hasta 16 hosts.

El prefijo de la red original es /24, lo que indica que se tienen 8 bits en la porción de host.

En este caso el Paso 2 de la técnica se resuelve por el número de direcciones válidas. Se necesitan 30 direcciones, si n es 4, $2^4 - 2 = 14$, no es suficiente, se deben añadir más bits. Si n es 5, $2^5 - 2 = 30$, con lo cual se satisface la demanda. Entonces, el número de bits prestados (m) es igual a 8 menos la nueva porción de host, que es 5, $m=3$.

El nuevo prefijo es /27 y la nueva máscara de red es 255.255.255.224 y el número mágico es 32 en el cuarto octeto.

Con $m=3$ se obtienen 8 subredes: 192.168.1.0/27, 192.168.1.32/27, 192.168.1.64/27, 192.168.1.96/27, 192.168.1.128/27, 192.168.1.160/27, 192.168.1.192/27 y 192.168.1.224/27.



Reflexión sobre el método: Como se pudo dar cuenta dividir una red IPv4 con máscara de longitud fija se parece a cortar una barra de chocolate que viene marcada en filas y columnas, basta con seguir las divisiones predeterminadas y todas las porciones salen idénticas y ordenadas. Por esta razón, FLSM es el método más sencillo y natural para dividir redes.

Sin embargo, esta simplicidad de FLSM también puede convertirse en una limitación en ciertos escenarios. En la Figura 55, usted puede encontrar desventajas de usar FLSM.

Figura 55

Desventajas del uso de FLSM en redes IP

Desventajas de FLSM	
Uso ineficiente de direcciones IP	<ul style="list-style-type: none"> - Asignación fija a todas las subredes - Desperdicio de espacio de direccionamiento
Falta de flexibilidad	<ul style="list-style-type: none"> - No se adapta al tamaño real de cada subred - Difícil personalización
Escalabilidad limitada	<ul style="list-style-type: none"> - Complicado aumentar el tamaño de una subred - Requiere rediseñar la red completa
No óptimo para redes modernas	<ul style="list-style-type: none"> - Mal ajuste en entornos heterogéneos - Dificulta la planificación eficiente
Complejidad administrativa	<ul style="list-style-type: none"> - Mas subredes de las necesarias - Dirección y mantenimiento más complicados
Tablas de enrutamiento más grandes	<ul style="list-style-type: none"> - Mas entradas por subredes pequeñas - Posible sobrecarga en el dispositivo

Nota. Ludeña, P., 2025.

Por ejemplo, con FLSM se desperdician masivamente direcciones, ya que todas las subredes resultan idénticas y cada una de ellas tiene el mismo número de direcciones, aun cuando algunas redes LAN necesiten cientos de direcciones y otras sólo un par. Otras desventajas encontradas son la rigidez en la configuración, la escalabilidad limitada y una mayor complejidad administrativa en comparación con métodos más flexibles como VLSM que analizaremos en la siguiente sección.

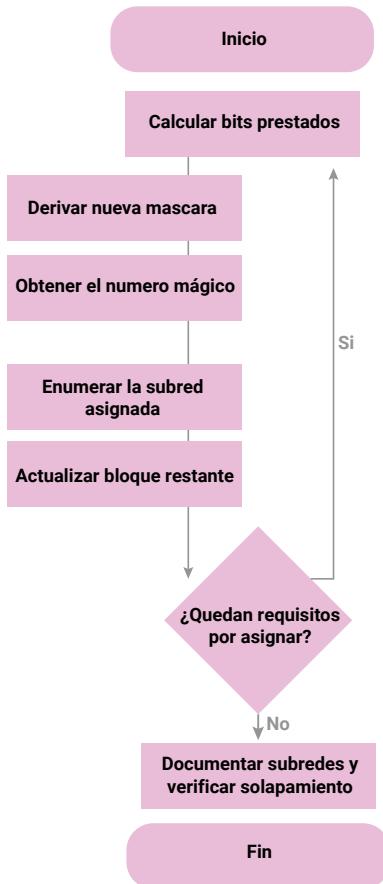
2.11.2. División de redes IPv4 con máscara de subred de longitud variable (VLSM)

La división de red con máscara de subred de longitud variable surge para resolver el desperdicio de direcciones que podría darse al usar FLSM. La técnica se basa en CIDR y permite hacer subredes de subredes tantas veces como haga falta y dar a cada segmento exactamente el prefijo que necesita. La máscara de longitud variable permite recortar o extender el prefijo tantas veces como sea necesario para que cada subred reciba solo las direcciones que realmente usará. Así se evitan derroches en enlaces punto-a-punto y se obtienen sumarios compactos que simplifican las tablas de enrutamiento.

El procedimiento VLSM es un método iterativo (puede ver el fluograma correspondiente en la Figura 56) que consta de los siguientes pasos:

Figura 56

Procedimiento para calcular subredes con máscara de longitud variable (VLSM)



Nota. Ludeña, P., 2025.

INICIO: reunir los requisitos de las subredes y ordenarlos de mayor a menor.

Paso 1. Definir la red base que hará de prefijo padre de todas las subredes derivadas.

Paso 2. Calcular los bits que se tomarán prestados de la porción de host, de la misma forma que se lo hizo para FLSM cuando el requerimiento es tener h direcciones de host por subred $2^n - 2 \geq h$.

Paso 3. Calcular la nueva máscara de red. Recuerde que el nuevo prefijo será $/ (32 - h)$.

Paso 4. Identificar el número mágico y el octeto en que se va a realizar el incremento.

Paso 5. Calcular las subredes derivadas de la división y asignar la subred.

Paso 6. Actualizar el bloque de requerimientos.

Decisión: Si faltan subredes por atender, repetir el proceso con el siguiente requisito.

FIN: cuando se terminen de atender las subredes se deberá documentar y pasar a la fase de pruebas e implementación.



Una pregunta frecuente que surge cuando se divide redes con VLSM es: ¿por qué es necesario comenzar a dividir las redes desde la subred de mayor tamaño?

La respuesta es porque las subredes más grandes requieren más espacio contiguo en el rango de direcciones, si se empezara por las subredes pequeñas, se podría fragmentar el espacio de tal forma que ya no quede suficiente espacio contiguo para alojar a las más grandes, a pesar de tener direcciones disponibles. Dividir desde la más grande garantiza que las subredes más exigentes en tamaño puedan ser atendidas sin restricciones, y luego se reutilizan los bloques más pequeños sobrantes para las subredes menores.

Para una aplicación más detallada de la técnica VLSM, consulte el [Anexo 4. Ejemplo Práctico de Subnetting VLSM](#).

Para complementar esta información teórica con una demostración práctica, le invito a revisar el video titulado “[VLSM](#)” para que, a través de un ejemplo resuelto paso a paso, repase la técnica de división de redes con máscara de longitud variable. El primer paso siempre será ordenar de mayor a menor los requisitos. Note que el método es iterativo y se debe repetir hasta cumplir con todos los requisitos.

índice

I Bimestre

II Bimestre

Solucionario

Referencias



Una vez que haya comprendido la aplicación práctica de VLSM a través del video, es momento de evaluar las diferencias entre ambas metodologías. Ahora lo invito a pensar en un ejemplo en el cual pueda realizar una división de redes con ambos esquemas FLSM y VLSM. Resuelva la asignación por ambos procedimientos y compare los resultados respondiendo las siguientes preguntas de reflexión que le ayudarán a identificar las ventajas y limitaciones de cada técnica:

- ¿Cómo cambia la asignación para cada técnica?
- ¿Con qué técnica se asigna un mayor número de direcciones del espacio total de direcciones?
- ¿Con qué método se desperdician más direcciones ¿cuántas por cada subred?
- ¿Para qué tipo de redes es aconsejable FLSM?
- ¿En qué tipo de redes se debe utilizar VLSM?

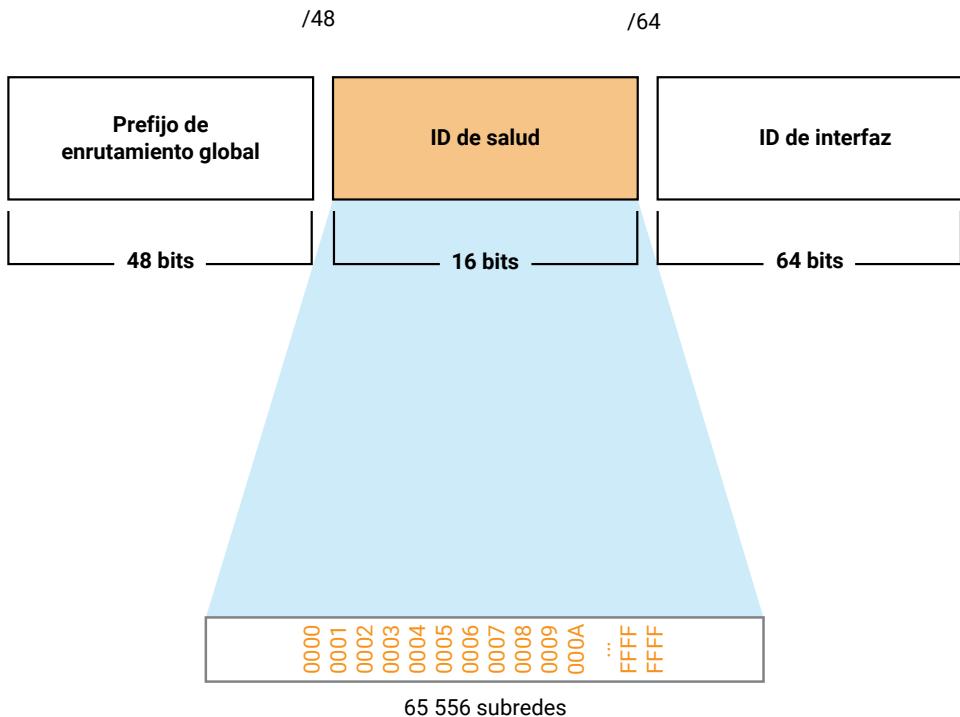
2.11.3. División de redes IPv6

La división en subredes IPv6 se realiza con un enfoque distinto al de IPv4, ya que no busca conservar direcciones, sino construir una estructura lógica y jerárquica de la red. Recordemos que la dirección IPv6 tiene 128 bits distribuidos en ocho hextetos de 16 bits. En un entorno corporativo típico el proveedor entrega un prefijo /48 (primeros 48 bits), luego el

administrador puede utilizar de 1 a 16 bits siguientes como ID de subred y los 64 bits finales constituyen el ID de interfaz, quedando la estructura que puede ver en la Figura 57.

Figura 57

Estructura de subredes en un bloque de direcciones IPv6 /48



Nota. Tomado de *División en subredes mediante la ID de subred* [Ilustración], por Cisco Networking Academy, s.f., CISCO, CC BY 4.0.

El método de **división de redes IP en el ID de subred** utiliza este espacio para generar subredes de manera fácil. Con este esquema se dispone de 16 bits para armar subredes, lo que permite crear hasta 65 536 subredes /64 sin necesidad de tomar bits de la porción de host. Cada subred /64 contiene una cantidad enorme de direcciones (alrededor de 18 trillones), por lo que no hay limitaciones en ese aspecto.

En la Tabla 31 se resumen los pasos para la asignación de subredes en IPv6.

Tabla 31

Pasos para la división de subredes en IPv6 a partir de un prefijo /48

Paso	Acción	Ejemplo
1. Reunir requisitos	Determine cuántas subredes se requieren (LAN, WLAN, DMZ o enlaces WAN)	10 LAN internas + 2 enlaces punto-a-punto.
2. Seleccionar el tamaño del campo ID de subred	Para s subredes se elige el menor número r tal que $2^r \geq s$.	12 subredes $\Rightarrow 4$ bits ($2^4 = 16$).
3. Fijar el nuevo prefijo	Sume esos bits al /48 inicial.	$/48 + 4$ bits = /52 El nuevo prefijo es /52
4. Numerar las subredes	Trabaje en grupos de 4 bits para leer fácilmente.	0000, 0001, 0002, ... 000B en el cuarto hexadeto
5. Asignar cada /64	Complete hasta 64 bits añadiendo ceros	2001:db8:acad: 0001 ::/64 (LAN 1) 2001:db8:acad: 0002 ::/64 (LAN 2)...
6. Documentar e implementar	Configure las interfaces	El router anunciará un único prefijo /52

Nota. Ludeña, P., 2025.

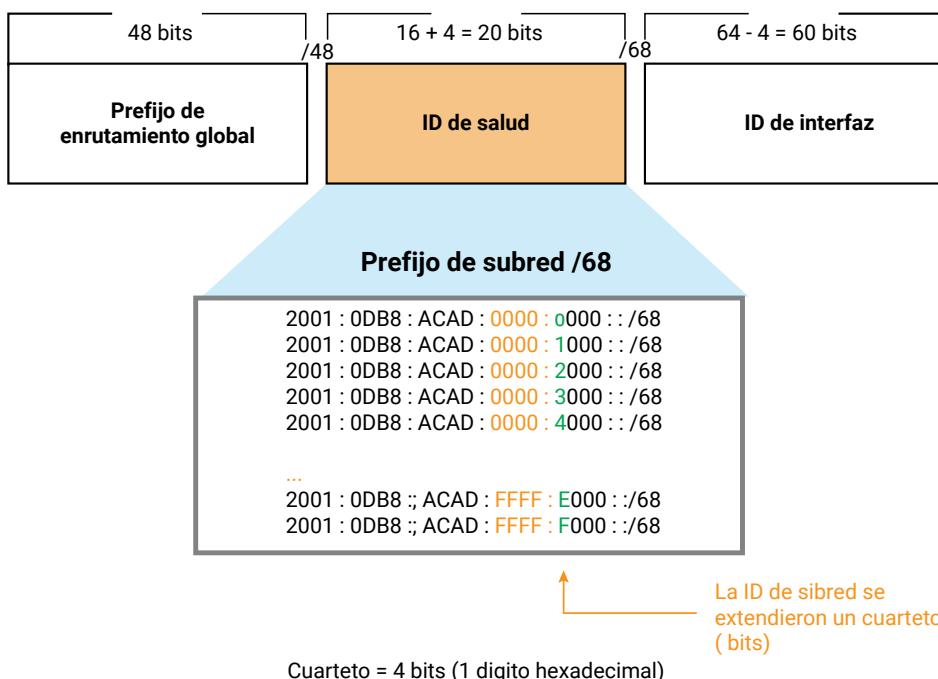
El proceso es muy sencillo pues no se requiere convertir a binario, basta con incrementar el valor hexadecimal en la ID de subred. El prefijo de enrutamiento global se mantiene igual en todas las subredes; solo varía el cuarteto que representa la ID de subred.

Otro método usado en IPv6 es la **división de subredes en la ID de interfaz**. Al igual que en IPv4 se pueden tomar bits de la porción de host para crear subredes, en IPv6 es posible tomar prestados bits de la ID de interfaz para crear más subredes, comúnmente con fines de seguridad y no necesariamente para aumentar el número de redes. Lo

recomendado es hacerlo en múltiplos de 4 bits (cuartetos), para facilitar la administración. Por ejemplo, en la Figura 58, al extender el prefijo de /64 a /68, se reducen 4 bits de la ID de interfaz de 64 a 60 bits y se obtienen nuevas subredes organizadas por valores hexadecimales, como del 00000 al FFFFF.

Figura 58

División de subredes IPv6 en límites de cuartetos con prefijo /68



Nota. Tomado de *División en subredes en la ID de interfaz [Ilustración]*, por Cisco Networking Academy, s.f., CISCO, CC BY 4.0.

Dividir en límites de cuarteto, es decir, usar prefijos como /68, /72, /76, etc. mantiene claridad en la estructura de direcciones, porque sólo se usan máscaras de subred alineadas en cuartetos. Aunque es técnicamente posible subdividir dentro de un cuarteto (como usar /66), no se recomienda, ya que complica la identificación visual del prefijo y la

interfaz, reduciendo la legibilidad y la eficiencia en la administración de redes IPv6.



Luego de haberle presentado los dos métodos. ¿Cuál cree usted que es el método más sencillo? ¿Por qué?



Actividades de aprendizaje recomendadas

Es hora de reforzar los conocimientos adquiridos resolviendo las siguientes actividades:

Actividad 1. Lectura de los contenidos propuestos

Ingresé a la plataforma [Netacad](#) y revise el módulo 11: Asignación de direcciones IPv4, secciones 11.5 a 11.8, y la sección 12.8 del módulo 12: Asignación de direcciones IPv6. En los cuales revisaremos fundamentalmente cómo organizar las redes y cómo podemos comprobar la conectividad y las rutas que siguen los paquetes para llegar desde un sitio a otro.

Estrategia de trabajo:

- Asigne un tiempo específico y libre de interrupciones para la lectura comprensiva del módulo correspondiente en la plataforma Netacad.
- Registre los contenidos más relevantes en un cuaderno físico o en un documento digital como parte de su proceso de sistematización del conocimiento.
- Participe activamente en las actividades interactivas y revise las animaciones proporcionadas, con el fin de fortalecer su comprensión conceptual.

- Realice las autoevaluaciones disponibles al finalizar el módulo, como mecanismo de verificación y consolidación de su aprendizaje.

Retroalimentación:

Luego de desarrollar la autoevaluación, revise su rendimiento. Al conocer qué respuestas fueron incorrectas, podrá enfocar su estudio en los conceptos que aún no domina por completo.

Actividad 2. ¡Direcciones para todos!

En esta actividad usted consolidará sus conocimientos y habilidades en el diseño de subredes y configuración de redes. Como futuro profesional en Redes y Analítica de Datos, es fundamental que evalúe los requerimientos de los clientes y brinde soluciones de ingeniería de calidad.

Estrategia de trabajo:

- Revise las técnicas de división de redes presentadas en esta semana.
- Repase los ejemplos dados, en especial el paso a paso para VLSM.
- Tenga a mano su cuaderno de ingeniería, ya que se le pedirá que realice configuraciones y realice pruebas de conectividad.
- Desarrolle la actividad propuesta siguiendo el guion disponible en la misma.

[Práctica 11.9.3. de CCNA-1: diseño e implementación de VLSM.](#)



En esta actividad usted dispone de tres escenarios para practicar VLSM. Se puede usar la opción *Reset Activity* para generar un nuevo conjunto de requisitos (se perderán las configuraciones realizadas).

Retroalimentación:

En esta actividad de Packet Tracer podrá ver su progreso como porcentaje, además pueden hacer clic en la pestaña *Check Results* para ver los ítems que se consideran para medir su progreso y verificar cuáles están incompletas o incorrectas. Luego de finalizar la actividad, responda las siguientes preguntas de retroalimentación:

- ¿Cómo determinó la máscara de subred adecuada para cada segmento de red según la cantidad de hosts requeridos?
- ¿Qué pasos debe seguir para asignar direcciones IP de forma eficiente utilizando VLSM en esta topología?
- ¿Cuántas direcciones tiene el rango de direcciones de su red original?, ¿cuántas direcciones disponibles tiene en los rangos de las subredes que asignó? Calcule la eficiencia de su división de redes.

Actividad 3. Es hora de medir nuestro avance

En la plataforma Netacad encontrará el Examen de punto de control: Examen de direccionamiento IP (módulos 11-13), que le propondrá cuestiones sobre las secciones 2.8 a la 2.11 de esta guía didáctica.

Esta es una excelente oportunidad para demostrar sus conocimientos y obtener una microcertificación que enriquecerá notablemente su hoja de vida. Su compromiso con este proceso no solo le permitirá aprobar el módulo, sino que también le distinguirá en el entorno laboral actual.

Actividad 4. Autoevaluación 2

Estimado estudiante, a continuación, usted tiene unas preguntas para que pueda medir su nivel de conocimiento sobre los contenidos de la unidad 2.

Estrategia de trabajo:

- Resuelva la autoevaluación sin revisar material adicional.
- Revise el solucionario disponible al final de la guía.

Una vez comprendida la actividad, realice la autoevaluación para comprobar sus conocimientos.

índice

I Bimestre

II Bimestre

Solucionario

Referencias



Autoevaluación 2

Lea cada pregunta con atención y seleccione la alternativa que considere correcta.

1. Si una interfaz en un *router* Cisco se muestra con un estado "down down" en el comando `show ip interface brief`, la causa más probable es un problema de configuración de la dirección IP que impide el establecimiento del protocolo de línea.
 - a. Verdadero.
 - b. Falso.
2. La principal ventaja del protocolo IPv6 sobre IPv4 es la simplificación de la cabecera del paquete, eliminando campos como la suma de comprobación, lo que reduce la latencia en redes con múltiples saltos.
 - a. Verdadero.
 - b. Falso.
3. Un administrador de red debe diseñar una infraestructura para un nuevo centro de datos que requiere conexiones de alta velocidad y una inmunidad total a las Interferencias Electromagnéticas (EMI). Los servidores se ubicarán a una distancia de 300 metros de los switches de acceso. ¿Qué medio de transmisión es el más adecuado para interconectar estos equipos, considerando los requisitos planteados?
 - a. Cable de par trenzado UTP Cat 6.
 - b. Cable coaxial.
 - c. Fibra óptica monomodo.
 - d. Fibra óptica multimodo.

4. Una empresa está experimentando problemas de conectividad intermitente en su red local. Al realizar una captura de tráfico con Wireshark, usted observa que se están descartando muchas tramas que son más pequeñas que el tamaño mínimo permitido por el estándar Ethernet. ¿Qué método de reenvío en los switches de la red es el más probable que esté contribuyendo a este problema de propagación de tramas corruptas?
- a. Comutación de almacenamiento y reenvío.
 - b. Comutación de corte sin fragmentos.
 - c. Comutación de corte de avance rápido.
 - d. Ninguna de las anteriores.
5. Un administrador está implementando un nuevo esquema de direccionamiento IPv4 utilizando VLSM. Se le ha asignado el bloque 192.168.1.0/24 y necesita crear una subred para el departamento de ventas que requiere al menos 60 hosts. Considerando una implementación óptima con VLSM, ¿cuál de las siguientes opciones representa la máscara de subred que mejor se ajusta al requisito de 60 hosts sin desperdiciar excesivas direcciones?
- a. Máscara: 255.255.255.192 Prefijo: /26.
 - b. Máscara: 255.255.255.224 Prefijo: /27.
 - c. Máscara: 255.255.255.128 Prefijo: /25.
 - d. Máscara: 255.255.255.0 Prefijo: /24.

6. ¿Cuáles son dos de los principales beneficios o propósitos de implementar la división en subredes (*subnetting*) en una red IP? (Elija dos opciones).
- Optimizar el espacio de direccionamiento y evitar el desperdicio de direcciones IP.
 - Aislar los dominios de *broadcast* para reducir el tráfico innecesario en la red.
 - Aumentar directamente la velocidad de transmisión de datos en el medio físico.
 - Convertir direcciones lógicas a físicas para la entrega de tramas en la capa de enlace.
7. En un entorno de red, un nuevo dispositivo se ha conectado y necesita obtener una dirección IP de forma dinámica. El *router* de la red local está configurado para anunciar qué método de direccionamiento deben aplicar los *hosts*. ¿Cuáles de las siguientes dos opciones son posibles métodos que el *router* puede indicar para que el dispositivo obtenga su dirección global de unidifusión IPv6 de forma dinámica? (Elija dos opciones).
- DHCPv6 con estado (Stateful DHCPv6).
 - Traducción de direcciones de red (NAT).
 - Autoconfiguración de direcciones sin estado (SLAAC).
 - Asignación manual (Static IPv6).

8. Usted está monitoreando un *router* Cisco y necesita identificar la dirección MAC de los dispositivos conectados directamente a sus interfaces para propósitos de resolución de problemas. ¿Cuáles de los siguientes dos comandos de monitoreo son los más adecuados para obtener información sobre las asociaciones entre direcciones IP y MAC aprendidas por el *router*? (Elija dos opciones).
- show cdp neighbors detail
 - show ip route
 - show arp
 - show ipv6 neighbors
9. Empareje cada campo de la cabecera IPv4 con su función principal.

Campo	Función
1. Tiempo de vida (TTL).	A. Gestionan la fragmentación del paquete cuando excede la MTU de un enlace, permitiendo su reensamblaje en destino.
2. Longitud de cabecera (IHL).	B. Previene bucles de enrutamiento al descartar el paquete cuando su contador llega a cero en un <i>router</i> .
3. Protocolo.	C. Determina dónde comienza la carga útil (datos) del paquete, indicando el tamaño de la cabecera.
4. Identificación, Indicador y desplazamiento de fragmentos.	D. Enlaza la capa de red con la de transporte, especificando el tipo de PDU de capa 4 que transporta (ej.: TCP, UDP, ICMP).

10. Empareje cada característica del protocolo IP de capa de red con su consecuencia en la operación de redes.

Característica IP	Consecuencia
1. Independencia de los medios.	A. Permite la interconexión de redes heterogéneas (cobre, fibra, radio) sin modificar el formato del paquete IP, ajustándose a la MTU de cada enlace.
2. Direccionamiento lógico jerárquico.	B. Delega la confiabilidad a capas superiores (ej.: TCP), manteniendo la operación de la capa de red ligera y eficiente, sin garantizar la entrega, el orden o la duplicación.
3. Servicio de mejor esfuerzo (Best-effort service).	C. Facilita la escalabilidad de las redes al permitir que los enrutadores almacenen rutas de forma compacta (prefijos), en lugar de rutas individuales para cada dispositivo.
4. Fragmentación y adaptación al tamaño de trama.	D. Permite que un paquete grande se divida en piezas más pequeñas para atravesar enlaces con MTU reducida, y se reensambla en el destino.

[Ir al solucionario](#)



Sem 9

Sem 10

Sem 11

Sem 12

Sem 13

Sem 13

Sem 14

Sem 15

Sem 16



Semana 12

Esta semana estudiaremos la Capa de transporte, se analizarán sus funciones y el papel de los números de puerto para mapear cada paquete con la aplicación correspondiente. Luego, nos enfocaremos en describir las características y el funcionamiento de los protocolos UDP y TCP para establecer las diferencias que permiten que aplicaciones de diferente naturaleza puedan enviar sus datos.

El dominio de estos conceptos fortalecerá su perfil como ingeniero en Redes y Analítica de Datos, pues le permitirá seleccionar el protocolo de transporte más conveniente para sus aplicaciones, automatizar la clasificación de flujos y detectar anomalías. Para afianzar sus conocimientos como actividad recomendada, le propongo una práctica en Packet Tracer donde podrá analizar en detalle el proceso de comunicación de UDP y TCP. Finalmente, le sugiero revisar el video introductorio que presenta una visión integral de los contenidos que abordaremos en la [unidad 3](#).

Como pudo identificar en el video, la capa de transporte actúa como el “puente” entre las aplicaciones y la infraestructura de red. La diferencia entre UDP y TCP que se presentó demuestra cómo las aplicaciones pueden elegir entre velocidad o confiabilidad según sus necesidades específicas, algo que experimentamos a diario sin darnos cuenta.

Unidad 3. Comunicación entre aplicaciones

3.1. Capa de transporte

Imagine que usted contrata a una empresa de mensajería para enviar varios paquetes a diferentes apartamentos de un mismo edificio. La empresa no solo recoge cada paquete, lo rotula con la dirección y el

Índice

I Bimestre

II Bimestre

Solucionario

Referencias

número del apartamento (puertos), sino que también le permite decidir si entregará el envío con acuse de recibo (TCP) o lo dejará en el buzón de correo sin firma de recepción (UDP). De la misma manera, la capa de transporte actúa como ese operador logístico entre procesos, toma los datos de la capa de aplicación, los divide en segmentos, les asigna números de puerto de origen y destino, coordina la entrega ordenada o rápida según la conveniencia de la aplicación, y mapea los datos de extremo a extremo.



Reflexione, ¿en qué escenarios sugeriría usar el esquema de entrega certificada y en qué escenarios le bastaría con que dejen los paquetes rápidamente?, ¿por qué?

3.1.1. Funciones de la capa de transporte

La capa de transporte tiene dos protocolos UDP y TCP, con características muy definidas y que se usan para objetivos distintos. Sin embargo, la capa de transporte tiene funciones generales que tienen un objetivo técnico clave en la estructura de capas.

- Multiplexación y demultiplexación:** permite que varios procesos de aplicación utilicen simultáneamente la red sobre un mismo host, identificando cada flujo con números de puerto. De esta forma, los datos que llegan al equipo se entregan únicamente al proceso correspondiente.
- Segmentación y reensamblaje:** se encarga de fraccionar los datos recibidos de la capa de aplicación en unidades de tamaño adecuado denominados segmentos, para que la capa de red los transporte eficientemente, y, si fuera el caso, reensamblarlos en destino utilizando números de secuencia para preservar la integridad del mensaje original.
- Verificación de integridad (checksum):** permite detectar alteraciones accidentales de los datos durante la transmisión.

Tanto TCP como UDP incluyen un campo de *checksum* que cubre la cabecera y la carga útil.

- 4. Identificación de aplicaciones:** la capa de aplicación usa números de puerto para identificar aplicaciones o servicios que requieren acceder a la red.



Después de analizar estas cuatro funciones esenciales de la capa de transporte, reflexione sobre su importancia relativa: ¿cuál cree usted que es la función más importante de la capa de transporte?, ¿hay alguna función que ya se haya visto en otra capa?

3.1.2. Números de puerto

El número de puerto es un identificador numérico asociado a una aplicación específica. El puerto se representa mediante un número entero de 16 bits, por lo que su valor numérico está en un rango entre 0 y 65535.

Para facilitar la administración de los servicios de red para aplicaciones, la IANA (*Internet Assigned Numbers Authority*), organiza los números de puerto en grupos. En la tabla 32 puede encontrar esta clasificación y su propósito específico.

Tabla 32

Clasificación de números de puerto en la capa de transporte

Grupo	Rango	Propósito principal	Ejemplos de servicios (TCP/UDP)
Puertos bien conocidos	0 – 1023	Reservados y estandarizados por IANA para protocolos básicos del sistema y de Internet.	20/21 FTP, 22 SSH, 53 DNS, 80 HTTP, 123 NTP, 443 HTTPS

Grupo	Rango	Propósito principal	Ejemplos de servicios (TCP/UDP)
Puertos registrados	1024 – 49151	Asignados por IANA a aplicaciones comerciales o de código abierto para evitar colisiones.	1521 Oracle DB, 3306 MySQL, 5432 PostgreSQL, 8080 HTTP alternativo
Puertos privados /	49152 – 65535	Seleccionados de forma temporal por el SO para que el cliente inicie una conexión; se liberan al cerrarse la sesión.	52000-62000 conexiones web salientes, puertos efímeros en VoIP, RPC dinámico
Puertos dinámicos / Efímeros			

Nota. Ludeña, P., 2025.

El primer rango corresponde a los puertos bien conocidos, que abarcan del 0 al 1023. Estos están reservados para servicios fundamentales del sistema y de Internet. Debido a su importancia, estos puertos requieren privilegios de administrador en la mayoría de los sistemas operativos para poder ser utilizados. El segundo grupo incluye los puertos registrados, que van del 1024 al 49151. Estos son asignados por la IANA a pedido de fabricantes, empresas de software, etc. para registrar sus aplicaciones y así evitar colisiones. Aunque no requieren privilegios elevados para su uso, están regulados para mantener orden en la asignación. Por último, los puertos dinámicos o efímeros van del 49152 al 65535 y son seleccionados automáticamente por el sistema operativo cuando un cliente inicia una conexión. Estos puertos se liberan cuando la sesión termina.

3.2. Protocolo UDP

UDP (*User Datagram Protocol*) es un protocolo de la capa de transporte que permite enviar datos de forma rápida y sin conexión entre dispositivos en una red. UDP incorpora apenas la información imprescindible para llegar al destino y no requiere confirmación de entrega. Todo esto reduce la sobrecarga de procesamiento y latencia,

cualidades imprescindibles para aplicaciones que toleran cierta pérdida de datos, pero no demoras, como voz sobre IP, streaming en tiempo real, DNS o telemetría IoT.

3.2.1. Cabecera UDP

La cabecera de UDP consta únicamente de 8 bytes (64 bits) y contiene cuatro campos que proporcionan la mínima información necesaria para transportar datos entre procesos, como se ve en la Figura 59.

Figura 59

Estructura de cabecera UDP

Punto de origen	Puerto de destino
Longitud	Suma de control (Checksum)
34 Bitd (4bytes)	

Nota. Tomado de *Protocolo UDP [Ilustración]*, por Marcelo, 2019, [CCNA Desde Cero](#), CC BY 4.0.

Para comprender el funcionamiento del protocolo UDP, es fundamental analizar la estructura de su cabecera. En la Tabla 33 puede ver la descripción de cada uno de estos campos.

Tabla 33

Campos y funciones de la cabecera UDP

Campo	Longitud	Propósito técnico
Puerto de origen	16 bits	Identificar el proceso emisor en el host origen; puede ser cero cuando no se requiera respuesta.
Puerto de destino	16 bits	Identificar el proceso receptor en el host destino.
Longitud	16 bits	Indicar el tamaño total (cabecera + datos) en bytes
Checksum	16 bits	Verificar la integridad del datagrama y parte de la cabecera IP

Nota. Ludeña, P., 2025.

El campo de puerto de origen identifica el número de puerto del proceso que envía el segmento, mientras que el de puerto de destino señala el proceso que debe recibirla. El campo de longitud indica el tamaño total del segmento UDP, incluyendo los datos, para que el receptor pueda procesarlo correctamente. Por último, el campo de checksum garantiza la integridad del segmento, evitando la entrega de información con errores.

índice

I Bimestre

II Bimestre

Solucionario

Referencias

Ahora que comprende la estructura y función de cada campo, analice las implicaciones de esta simplicidad:
Reflexione sobre la estructura de la cabecera UDP:



- ¿Por qué no se tienen campos para identificar cada uno de los segmentos que se envían? ¿Cree usted que esto puede traer problemas al rearmar los datos?
- ¿Por qué es necesario tener el campo Checksum o suma de verificación?

3.2.2. Características de UDP

UDP proporciona un servicio de transporte sin conexión, de mejor esfuerzo, que sacrifica la fiabilidad para minimizar la latencia y la sobrecarga. En la siguiente infografía, se detallan las características de UDP y qué ventaja aporta a las aplicaciones que usan este protocolo en capa de aplicación.

Características del protocolo UDP

Como pudo observar en la infografía, su análisis de las características de UDP demuestra una comprensión sólida de cómo los diferentes protocolos de transporte se adaptan a necesidades específicas de aplicación, optimizando el rendimiento según los requerimientos operacionales. El protocolo UDP es un protocolo no orientado a la conexión, no tiene entrega garantizada, ni ordenada y no tiene control de congestión. Adicionalmente, es un protocolo ligero que tiene

una cabecera de sólo 8 bytes, lo que lo hace simple en operación y funcionamiento.

Ahora que ya hemos visto las características de UDP, podemos pensar en las aplicaciones que podrían usar UDP. En la Tabla 34 se presentan ejemplos actuales de aplicaciones y servicios que suelen usar UDP porque necesitan una estructura ligera y la ausencia de conexión que caracteriza a UDP. Para cada caso se indica el motivo técnico que justifica su elección.

Tabla 34

Ejemplos de aplicaciones que utilizan UDP

Protocolo de aplicación	Puertos típicos	Motivo para usar UDP
DNS (Domain Name System)	53	Consultas breves de pocos cientos de bytes.
		La reducción de latencia pesa más que la fiabilidad absoluta. TCP solo se emplea cuando el mensaje supera 512 bytes o para transferencias zonales.
DHCP (Dynamic Host Configuration Protocol)	67/68	Mensajes broadcast en redes locales durante el arranque.
		UDP simplifica la entrega a hosts sin IP configurada.
RTP/RTCP en VoIP y videoconferencia	Dinámicos (≥ 16384)	Flujo continuo donde el retardo es crítico. Pequeñas pérdidas son preferibles a retrasos por retransmisión.
HTTP/3 (QUIC)	443	QUIC encapsula multiplexación y control de congestión sobre UDP, evitando interferir con middleboxes que filtran nuevos protocolos sobre TCP.
Video en vivo (HLS Low-Latency, SRT, WebRTC)	Variados	Requiere entrega casi instantánea y adaptación rápida al ancho de banda disponible.

Protocolo de aplicación	Puertos típicos	Motivo para usar UDP
Juegos en línea (FPS, MMO)	3074, 27015, etc.	Sincronización de estado en tiempo real; la corrección de paquetes perdidos se hace mediante predicción del cliente para no detener la acción.
SNMP Traps	162	Notificaciones de eventos críticos con volumen reducido.
Syslog UDP	514	Registro ligero donde algunas pérdidas son aceptables frente a la sobrecarga de confirmaciones.
Telemetría IoT (CoAP, MQTT-SN)	5683, 1883/UDP	Dispositivos con recursos limitados y enlaces de alta latencia.

Nota. Ludeña, P., 2025.

Por ejemplo, para aplicaciones en tiempo real que usan los protocolos RTP y RTCP se usan puertos dinámicos en UDP debido a que se requiere rapidez en el envío de datos, ya que este tipo de aplicaciones no son tolerantes a fallos.



Para profundizar en el tema, mencione otras aplicaciones que, según su criterio, podría beneficiarse del uso de UDP y justifique su respuesta en su cuaderno de apuntes o en un documento de Word. Además, responda: ¿Qué consideraciones de seguridad debería prever al usar UDP para servicios que van hacia Internet?

3.3. Protocolo TCP

En 1974, Vint Cerf y Bob Kahn presentaron una propuesta denominada *Transmission Control Program* que unificaba comutación de paquetes y control de errores para la naciente ARPANET. La especificación maduró hasta el RFC 793 (1981), que fijó el estándar de *Transmission Control Protocol* (TCP), pieza angular de la suite TCP/IP. Desde entonces TCP

se ha perfeccionado (RFC 1122, RFC 6298, entre otras) para responder a los retos de bandas anchas, enlaces inalámbricos y aplicaciones interactivas.

3.3.1. Cabecera TCP

La cabecera del protocolo TCP es una estructura compleja diseñada para garantizar una transmisión confiable, ordenada y eficiente entre procesos finales. En la Figura 60, puede ver la disposición de los campos dentro de la cabecera y en la Tabla 35 encontrará la longitud y descripción de cada campo.

Figura 60

Estructura de cabecera TCP

Punto de origen		Puerto de destino			
Número de secuencia					
Número de reconocimiento					
Offset	Reservado	Bits de bandera (Flag)	Ventana		
Suma de control (Checksum)		Urgente			
34 Bitd (4bytes)					

Nota. Tomado de *Protocolo UDP [Ilustración]*, por Marcelo, 2019, CCNADesdeCero, CC BY 4.0.

Tabla 35

Estructura de la cabecera TCP y función de sus campos

Campo	Longitud	Propósito técnico
Puerto de origen	16 bits	Identifica el proceso emisor en el host de origen.
Puerto de destino	16 bits	Identifica el proceso receptor en el host de destino.
Número de secuencia	32 bits	Marca el primer byte de datos transmitidos; permite el reensamblaje ordenado.

Campo	Longitud	Propósito técnico
Número de acuse de recibo (ACK)	32 bits	Indica el siguiente byte esperado; confirma la recepción correcta.
Longitud de cabecera (Data Offset)	4 bits	Especifica el tamaño de la cabecera en múltiplos de 32 bits.
Bits de control (flags)	9 bits	Controlan el estado de la conexión: SYN, ACK, FIN, RST, PSH, URG, etc.
Ventana de recepción	16 bits	Define cuántos bytes puede recibir el receptor sin desbordarse.
Checksum	16 bits	Verifica la integridad de la cabecera y los datos.
Puntero urgente	16 bits	Señala la posición de datos urgentes si se establece la bandera URG.
Opciones (variable)	Variable (hasta 40 bytes)	Mejora la funcionalidad: escalado de ventana, timestamp, SACK.
Relleno (padding)	Variable	Alinea la cabecera a múltiplos de 32 bits.

Nota. Ludeña, P., 2025.

El puerto de origen y el puerto de destino (16 bits cada uno), identifican los procesos de comunicación en los extremos. También posee un número de secuencia y un número de acuse de recibo, utilizados para ordenar y confirmar la entrega de datos, respectivamente. El campo de bits de control o flags (como SYN, ACK, FIN) gestiona el establecimiento y cierre de la conexión. Además, contiene campos para el tamaño de ventana, checksum para verificación de integridad, y opciones adicionales como escalado de ventana. Esta cabecera permite controlar el flujo de datos, garantizar la entrega correcta y ordenar los segmentos transmitidos.

3.3.2. Características de TCP

TCP brinda un servicio orientado a conexión, confiable y seguro. En la siguiente imagen interactiva, se detallan las características de TCP y cómo estas aportan robustez a las aplicaciones que lo usan.

[Características del protocolo TCP](#)

Como pudo observar, existen múltiples características interconectadas que trabajan de manera coordinada para asegurar una comunicación efectiva. Cada uno de estos elementos - desde el establecimiento de conexión hasta la verificación de errores - cumple un papel fundamental en mantener la integridad y confiabilidad de los datos transmitidos a través de la red. Esta robustez es particularmente importante en aplicaciones críticas como los servicios financieros.



Reflexione: ¿Cuál de estas características considera más crítica para garantizar la integridad de una transacción bancaria y por qué?

Identificadas las características de TCP y su aporte a los procesos, podemos pensar en aplicaciones que usan este protocolo. En la Tabla 36 encontrará algunos ejemplos de aplicaciones el número de puerto en el que operan y la razón para usar TCP.

Tabla 36

Ejemplos de aplicaciones que utilizan TCP

Protocolo de aplicación	Puertos típicos	Motivo para usar TCP
HTTP	80	Requiere entrega confiable y ordenada para cargar correctamente páginas web.
FTP (File Transfer Protocol)	21 (control), 20 (datos)	Transfiere archivos completos; necesita asegurar integridad y reenvío en caso de errores.
SMTP (Email envío)	25	El correo electrónico necesita que los mensajes lleguen completos y en orden.
IMAP / POP3	143 / 110	Permite a los usuarios acceder a su correo sin pérdida ni corrupción de datos.
SSH (Secure Shell)	22	Proporciona acceso remoto seguro; requiere autenticación y cifrado confiables.
Telnet	23	Comunicación remota en texto plano; necesita mantener una sesión continua y ordenada.

Protocolo de aplicación	Puertos típicos	Motivo para usar TCP
HTTPS (HTTP seguro)	443	Asegura la integridad y confidencialidad del tráfico web mediante cifrado TLS sobre TCP.
MySQL	3306	Bases de datos requieren conexiones estables y sin pérdida de datos para mantener la consistencia.
RDP (Remote Desktop Protocol)	3389	Acceso remoto a escritorios necesita transmisión fluida y precisa de eventos de teclado, ratón y pantalla.

Nota. Ludeña, P., 2025.

Por ejemplo, para el envío de correo electrónico se usa el protocolo SMTP que usa el puerto TCP 25 para enviar los datos de correo al servidor, se comprueba que todos los datos lleguen ya que esta aplicación es tolerante al retardo, pero no a la pérdida de paquetes.

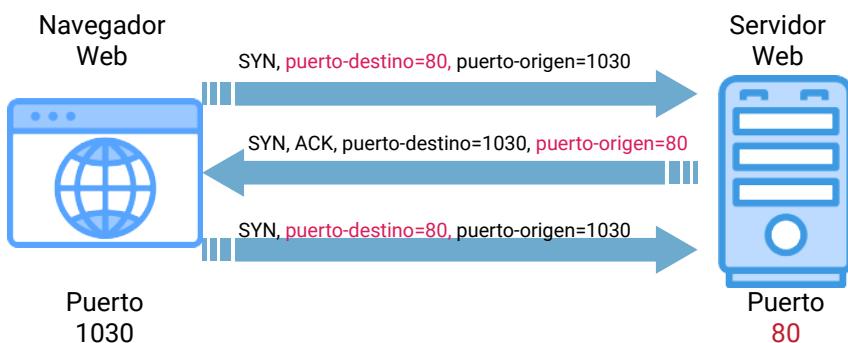
Considerando las características de TCP que hemos estudiado, ¿qué otras aplicaciones usted puede analizar?

3.3.3. Conexión en TCP

El establecimiento de conexión en TCP se realiza mediante un proceso llamado three-way handshake o saludo de tres vías. Este mecanismo asegura que ambos extremos estén sincronizados, acuerden los parámetros iniciales y estén listos para intercambiar datos de manera confiable. En la Figura 61, se ve el proceso que consta de tres pasos.

Figura 61

Proceso de establecimiento de conexión TCP (Three-Way Handshake)



Nota. Tomado de *Protocolo UDP [Ilustración]*, por Marcelo, 2019, CCNADesdeCero, CC BY 4.0.

A continuación, se describe cada uno de los pasos:

Paso 1: SYN. El cliente envía un segmento TCP con la bandera SYN activada. Este segmento contiene un número de secuencia inicial que servirá para rastrear los datos que se envíen desde el cliente al servidor y tiene especificado un número de puerto origen y un número de puerto destino que permanecerán sin modificación a lo largo de la conexión.

Paso 2: SYN-ACK. El servidor, al recibir el SYN, responde con un segmento que tiene activadas las banderas SYN y ACK. En ese segmento, el servidor selecciona su propio número de secuencia.

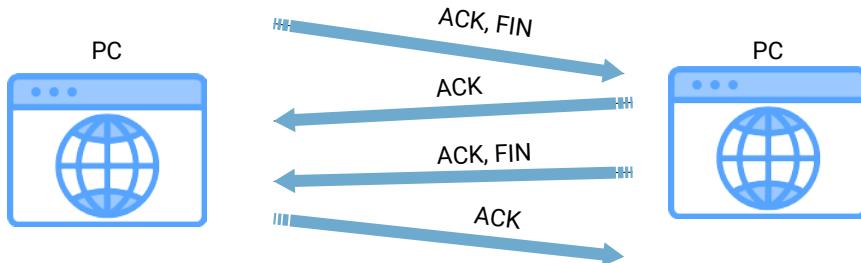
Paso 3: ACK. Finalmente, el cliente responde con un tercer segmento que tiene la bandera ACK activa, confirmando el número de secuencia del servidor. Una vez que el servidor recibe este ACK, ambos extremos consideran que la conexión está establecida y pueden comenzar a intercambiar datos.

La finalización de una conexión TCP se lleva a cabo mediante un proceso ordenado y controlado, conocido como el four-way handshake

(ver Figura 62). Este mecanismo permite que ambos extremos cierren la conexión de forma independiente, asegurando que todos los datos pendientes hayan sido recibidos antes de liberar los recursos.

Figura 62

Proceso de finalización de una conexión TCP



Nota. Tomado de *Protocolo UDP [Ilustración]*, por Marcelo, 2019, [CCNADesdeCero](#), CC BY 4.0.

Analice la descripción de cada uno de los pasos de este proceso:

Paso 1: FIN. Cuando un extremo desea cerrar la conexión (por ejemplo, el cliente), envía un segmento TCP con la bandera FIN activada. Esto indica que ya no tiene más datos que enviar.

Paso 2: ACK. El otro extremo (por ejemplo, el servidor) responde con un segmento que tiene ACK activado, confirmando la recepción del FIN. Aunque ya se ha cerrado un sentido de la conexión (del cliente al servidor), el otro aún puede seguir enviando datos temporalmente.

Paso 3: FIN. Este paso corresponde al cierre del otro extremo. Por ejemplo, una vez que el servidor ha terminado de enviar sus propios datos, también envía un segmento con la bandera FIN activada, indicando que desea cerrar la conexión en sentido inverso.

Paso 4: ACK. Finalmente, el cliente responde con un segmento con ACK, confirmando la recepción del FIN del servidor. En este punto, el

servidor puede liberar la conexión. Luego, la conexión se considera completamente cerrada.

3.3.4. Confiabilidad

Una de las propiedades más distintivas del protocolo TCP es su capacidad para garantizar una comunicación confiable, libre de pérdidas y en orden, incluso sobre redes no confiables. Esta confiabilidad se basa principalmente en dos mecanismos coordinados: los números de secuencia y los acuses de recibo (ACK).

- **Números de secuencia:** TCP no numera segmentos, sino bytes. Cada byte del flujo de datos tiene asignado un número secuencial. El número de secuencia del segmento corresponde al primer byte útil que transporta.
 - **Ejemplo:** si el número de secuencia es 1000 y el segmento tiene 500 bytes de datos, el siguiente segmento debería comenzar con número de secuencia 1501.
- **Acuses de recibo (ACK):** el receptor confirma la recepción del último byte consecutivo que ha recibido correctamente. Este valor se coloca en el campo de ACK del siguiente segmento. El ACK no es por paquete, sino por flujo y siempre indica el byte que espera recibir en el siguiente envío.
 - **Ejemplo:** si el receptor recibió un paquete con número de secuencia 1000 y el segmento tiene 1000 bytes de datos. El ACK tendrá marcado 2001.

Si un segmento no llega o llega dañado, el receptor no avanza su ACK, lo que alerta al emisor.



Con los números de secuencia TCP puede detectar que está recibiendo segmentos en desorden. Si eso ocurre los mantiene en una cola hasta que todos los segmentos lleguen

y pueda reensamblarlos. TCP garantiza la entrega ordenada y completa de segmentos a la capa de aplicación.

Con el mecanismo de confirmación de segmentos, TCP puede detectar segmentos que no han llegado a su destino. El protocolo emplea temporizadores (timeout) para cada segmento enviado. Si no recibe confirmación antes de que expire, retransmite el segmento.

3.3.5. Control de flujo

El control de flujo es una función esencial del protocolo TCP que evita que un emisor rápido abrume a un receptor más lento. Aunque ambos dispositivos estén conectados a la misma red, sus capacidades internas (memoria, procesamiento, velocidad de lectura) pueden ser muy distintas. TCP incorpora un mecanismo adaptativo que asegura que los datos enviados no excedan lo que el receptor puede almacenar y procesar de forma segura.

Imagine que usted vierte agua desde una jarra a una botella usando un embudo. Si vierte demasiado rápido, el embudo se desborda, y parte del agua se pierde. De forma similar, si un emisor envía datos más rápido de lo que el receptor puede procesar, los datos se pierden o deben ser descartados. El control de flujo es como un medidor que regula la velocidad con la que se vierte el agua, de acuerdo con la capacidad del embudo en cada momento.

El control de flujo en TCP se realiza con el **método de ventana deslizante**. Este mecanismo regula la cantidad máxima de datos (en bytes) que el emisor puede enviar sin recibir una confirmación (ACK). Al confirmar la recepción de datos, el receptor puede ajustar la ventana si ha liberado espacio. El receptor anuncia constantemente el tamaño de su ventana, basado en la capacidad disponible de su buffer. La ventana varía a medida que el receptor procesa datos y libera espacio.

Para ilustrar de manera práctica cómo opera el mecanismo de control de flujo TCP, el [Anexo 5. Control de flujo TCP: ejemplo práctico](#), presenta un escenario detallado que muestra la interacción entre cliente y servidor, incluyendo el manejo de la ventana deslizante, el procesamiento de datos en el buffer y las respuestas del servidor según su capacidad disponible. Este ejemplo paso a paso permite visualizar cómo se ajusta dinámicamente el flujo de datos para evitar la saturación del receptor.

¡Perfecto! Finalizamos la semana 12. ¿Curiosos por saber qué sorpresa les tengo? ¡Una actividad súper divertida!

Para cada aplicación un protocolo de transporte

En esta actividad se le presentarán algunas aplicaciones para que usted seleccione cuál protocolo de capa de transporte debería utilizar cada una de ellas. El objetivo es que pueda relacionar las características y bondades de UDP y TCP para que puedan brindar servicios a las aplicaciones de acuerdo con sus requerimientos.



Reconocimiento de protocolo de transporte

Como pudo comprobar durante la actividad, cada protocolo de aplicación tiene características específicas que determinan qué protocolo de transporte es más adecuado para su funcionamiento. Algunos requieren la confiabilidad y control de errores, mientras que otros priorizan la velocidad y eficiencia en la transmisión, lo que explica por qué ciertos protocolos pueden utilizar ambos tipos de transporte según el contexto.

Luego de desarrollar la actividad, responda en su cuaderno de apuntes o documento de Word las siguientes preguntas de reflexión:



- ¿Qué protocolo utilizan las aplicaciones de tiempo real?
- ¿Los accesos remotos a los equipos de red en qué protocolo se realizan? ¿Por qué?
- ¿Por qué hay aplicaciones que pueden usar los dos protocolos?



Actividad de aprendizaje recomendada

Es momento de aplicar sus conocimientos a través de las actividades que se han planteado a continuación:

Actividad 1. Lectura de los contenidos propuestos

Ingresé a la plataforma [Netacad](#) y revise el módulo 14: Capa de transporte. Revise las funciones esenciales de esta capa y los protocolos que operan en la misma, estos son TCP y UDP. Con estos protocolos podemos transportar la gran variedad de protocolos de capa de aplicación.

Estrategia de trabajo:

- Dedique un momento tranquilo para leer el módulo en Netacad, y aproveche esta oportunidad para aprender algo nuevo que fortalecerá su formación profesional.
- Tome apuntes de los conceptos más importantes, ya sea en un cuaderno o en formato digital, y cree su propio material de consulta.

- Disfrute las actividades interactivas y animaciones, que hacen más dinámico el aprendizaje y le ayudan a comprender mejor cada tema.
- Ponga a prueba lo que ha aprendido con las autoevaluaciones, y si se equivoca, ¡No se preocupe! Es parte del proceso de aprender y crecer.

Retroalimentación:

Gracias a los resultados de la autoevaluación, sabrá exactamente qué partes del material necesita revisar para afianzar su comprensión.



Sem 9

Sem 10

Sem 11

Sem 12

Sem 13

Sem 13

Sem 14

Sem 15

Sem 16



Semana 13

Esta semana estará centrada en las capas superiores del modelo OSI, las cuales son sesión, presentación y aplicación. Estas capas representan la parte más cercana al usuario final y son esenciales para garantizar una comunicación efectiva, segura y significativa entre aplicaciones distribuidas en la red. Su estudio permite comprender cómo se gestionan los diálogos entre dispositivos (capa de sesión), cómo se preparan los datos para ser interpretados correctamente (capa de presentación) y cómo se ofrecen los servicios de red directamente a las aplicaciones de usuario (capa de aplicación). Dominar estas capas resulta clave en la asignatura, ya que fortalece las bases para diseñar, analizar y dar soporte a los sistemas de red orientados a la experiencia del usuario, interoperabilidad y estandarización.

El análisis y comprensión de estas capas contribuye directamente a los resultados de aprendizaje del perfil profesional, ya que desarrollan habilidades para identificar y aplicar protocolos y servicios según los requerimientos funcionales de la red. Instrumentos como mapas mentales y videos explicativos serán las herramientas que se usarán para interiorizar los conocimientos sobre estas capas.

3.4. Capas superiores

Las capas superiores del modelo OSI actúan como el puente entre el usuario y la red, y pueden entenderse como los niveles donde la comunicación se vuelve humana. Estas capas son importantes porque hacen posible que distintos sistemas y programas se comuniquen de forma clara, segura y sin errores, independientemente de las diferencias internas de cada dispositivo. Son responsables de que se pueda acceder a una página web, recibir correos electrónicos o tener una

índice

I Bimestre

II Bimestre

Solucionario

Referencias

videollamada con calidad y consistencia. Sin ellas, los datos podrían llegar, pero no tendrían sentido para el usuario final.

Para comprender mejor cómo funcionan estas capas y su importancia en nuestra comunicación digital cotidiana, le invitamos a escuchar el siguiente pódcast donde se explican mediante ejemplos prácticos y analogías cotidianas:

[Capas superiores del modelo OSI.](#)

Como pudo escuchar en el pódcast, cada una de estas capas superiores tiene un rol específico y complementario en el proceso de comunicación digital. La explicación mediante analogías – como la llamada telefónica para la capa de sesión o el traductor universal para presentación – demuestra cómo estos conceptos técnicos se relacionan directamente con situaciones familiares, haciendo evidente que estas capas son fundamentales para que nuestras aplicaciones diarias funcionen de manera transparente y eficiente.

A continuación, se describirán a detalle cada una de las capas superiores:

3.4.1. Capa de sesión

Para entender cómo trabaja la capa de sesión, imagine una llamada telefónica entre dos personas. No solo es importante establecer la conexión, como lo hace TCP, sino también saber cuándo hablar, cuándo pausar y cómo retomar la conversación si la llamada se interrumpe. Ahora, le invito a revisar el video titulado "[Capa de sesión del modelo OSI](#)", donde se explica cómo esta capa se encarga de establecer sesiones entre aplicaciones con un ejemplo de paquetería. Es de especial interés analizar que la capa de sesión en el modelo OSI se encarga de establecer, coordinar, mantener activas y finalizar sesiones de comunicación entre dos aplicaciones, asegurando que puedan intercambiar información de forma ordenada y coherente. Esta

capa también puede incluir puntos de restauración (*checkpoints*) en transmisiones largas, lo que permite reanudar una sesión sin tener que empezar desde cero.

Las principales funciones de la capa de sesión son:

- **Establecimiento, mantenimiento y terminación de sesiones:** establece los canales de comunicación entre aplicaciones en distintos sistemas y los mantiene abiertos mientras son necesarios.
- **Sincronización:** coloca puntos de control (*checkpoints*) durante la transmisión de datos. Esto permite reanudar una transferencia desde el último punto conocido en caso de una interrupción, sin necesidad de reiniciar todo el proceso.
- **Control de diálogo:** administra el modo en que se comunica cada parte (por turnos o simultáneamente), gestionando el flujo bidireccional de datos.
- **Recuperación de sesión:** si se detecta una falla, la capa puede negociar la reanudación de la sesión desde el último estado coherente conocido.



Un **ejemplo** práctico de su aplicación es en una videollamada, pues esta capa asegura que ambos usuarios estén conectados correctamente, manteniendo activa la sesión durante la conversación y cerrándola cuando alguno cuelga.

3.4.2. Capa de presentación

Imagine que dos personas quieren conversar por teléfono, pero hablan distintos idiomas, ambas necesitarán contar con un traductor personal. En efecto, pese a que ya tengan establecida la llamada telefónica (capas inferiores), no podrán entender el mensaje si este no se traduce.

La capa de presentación se encarga de esta tarea en el modelo OSI, actúa como un traductor universal que garantiza que los datos enviados desde una aplicación en un sistema puedan ser entendidos por la aplicación receptora en otro sistema.



Antes de continuar, revise el video denominado "[Capa de presentación del modelo OSI](#)", donde encontrará una interesante introducción a los conceptos más importantes de esta capa. Como verá, esta capa se encarga de la conversión de formatos de datos, la compresión para hacer más eficiente el transporte, y el cifrado/descifrado para mantener la seguridad de la información transmitida.

Las funciones principales de la capa de presentación son:

- **Traducción de formatos de datos:** convierte los datos del formato utilizado por la aplicación del remitente al formato que entiende la aplicación del receptor. Por ejemplo, transforma un archivo de texto ASCII a EBCDIC si el sistema destino lo requiere.
- **Compresión de datos:** reduce el tamaño de los datos para optimizar el uso del ancho de banda y acelerar las transmisiones.
- **Cifrado y descifrado:** aplica algoritmos de seguridad para proteger la confidencialidad de los datos durante la transmisión. Esta función puede incluir el uso de algoritmos como AES, RSA o TLS a nivel de contenido.
- **Conversión de estructuras de datos:** alinea y adapta las estructuras de datos complejas (como gráficos, tablas o archivos multimedia) para que se interpreten correctamente entre diferentes plataformas.

Como **ejemplo** práctico se puede citar que, cuando se envía un archivo PDF por correo electrónico, esta capa se asegura de que el archivo

llegue intacto y pueda visualizarse correctamente, independientemente del sistema operativo del receptor.

3.4.3. Capa de aplicación

Imagine que usted quiere enviar una carta. La logística para enviar la carta ya existe (capas inferiores), pero usted requiere de alguien que redacte la carta y se encargue de enviarla a su nombre. La capa de aplicación hace las veces de esa persona, puesto que es la encargada de interactuar con el usuario final y actuar en su nombre para proporcionar las instrucciones necesarias al sistema operativo para iniciar la comunicación.



Para una mejor comprensión del funcionamiento de esta capa, le invito a revisar el video titulado "[Capa de aplicación del modelo OSI](#)", donde se presentan algunos ejemplos cotidianos de uso. En el video se explica que la capa debe proveer servicios de red a las aplicaciones que usamos diariamente, como navegadores, clientes de correo electrónico o plataformas de mensajería. Esta capa interactúa directamente con el software del usuario y permite acceder a funciones como enviar correos, consultar páginas web o subir archivos a la nube.

La capa de aplicación se encarga de:

- **Proporcionar servicios de red a las aplicaciones del usuario:** permite que programas como navegadores web, clientes de correo electrónico o plataformas de transferencia de archivos puedan comunicarse a través de la red.
- **Gestión de autenticación y autorización:** muchos protocolos de esta capa manejan procesos de identificación de usuarios (*login*) y permisos de acceso a recursos.

- **Identificación de recursos y sesiones:** define a qué servicio se está accediendo (por ejemplo, una página web o un archivo FTP) y gestiona la conexión con él.
- **Interfaz directa con el usuario:** aunque esta capa no es la interfaz gráfica en sí, es donde se inician o terminan los procesos de red de las aplicaciones que usan los usuarios.

Por **ejemplo**, cuando se usa un navegador para entrar a una página web, esta capa es la responsable de iniciar la solicitud HTTP y recibir la respuesta del servidor web.

Ya que hemos repasado las capas superiores y sus principales funciones, responda en su cuaderno de apuntes o en un documento de Word las siguientes preguntas de reflexión:



- ¿Por qué cree que muchas funciones de la capa de presentación no se implementan como una capa independiente en redes modernas como en TCP/IP, sino que se integran en las aplicaciones?
- ¿Qué consecuencias tendría una falla en la capa de sesión durante una transferencia de archivos entre dos sistemas?, ¿cómo afectaría al usuario?
- En su experiencia diaria con *Internet* (navegar, enviar correos, usar apps), ¿puede identificar ejemplos concretos en los que interactúa con cada una de estas tres capas?

¿Para qué sirven las capas superiores?

En este quiz usted afianzará su conocimiento sobre las capas superiores. La finalidad de esta tarea es que usted pueda diferenciar las funciones de las capas de sesión, presentación y aplicación para que pueda determinar. El conocimiento de dichas funciones le permitirá detectar

fallos en la ejecución de servicios y proponer soluciones en su ejercicio profesional.



Capas superiores.

Como pudo comprobar durante el *quiz*, las capas superiores del modelo OSI tienen funciones claramente diferenciadas que trabajan de manera complementaria para facilitar la comunicación de aplicaciones. Su desempeño refleja qué tan bien comprende que la capa de sesión gestiona el diálogo y la sincronización. La capa de presentación actúa como traductor manejando formato, compresión y cifrado, mientras que la capa de aplicación proporciona la interfaz directa con el usuario y los servicios de red.

Luego de desarrollar la actividad, responda en su cuaderno de apuntes o en un documento de Word las siguientes interrogantes:



- ¿Qué capa se encarga del cifrado de datos?
- ¿Qué capa determina la gestión de autenticación?
- ¿Qué capa puede recuperar la sesión en caso de requerirlo?

3.4.4. Aplicaciones de red

La diversidad de servicios que usamos en *Internet* está respaldada por una amplia variedad de aplicaciones de red. Cada una de ellas responde a necesidades distintas, por ejemplo, algunas priorizan la

rapidez, otras la seguridad, otras el acceso continuo o la transferencia de grandes volúmenes de información. Por ello, existen protocolos especializados para cada tipo de servicio, y todos ellos se comunican mediante los mecanismos de la capa de transporte, principalmente TCP y UDP.

En la figura 63, se describen algunas de las aplicaciones de red más representativas, su propósito, el protocolo de transporte que utilizan, los tipos de mensajes que gestionan y cómo se estructuran las solicitudes y respuestas.

Figura 63

Principales aplicaciones de red

Aplicaciones comunes en redes y computadoras	
Servicios web {HTTP Y HTTPS}	<ul style="list-style-type: none"> - Propósito: Acceso a páginas web y recursos online - Protocolo de transporte: TCP - Protocolos: HTTP (sin cifrado), HTTPS (con TLS/SSL) - Mensajes comunes: GET, POST, PUT, DELETE, HEAD - Gestión: Cliente solicita recursos, servidor responde cifrado en HTTPS
Servicios de intercambio de archivos {FTP / SFTP}	<ul style="list-style-type: none"> - Propósito: Transferencia de archivos - Protocolo de transporte: TCP - Protocolos: FTP (puertos 20, 21), SFTP (sobre SSH) - Mensajes comunes: USER, PASS, STOR, RETR, QUIT - Gestión: Sesión de control, FTP con dos canales, SFTP cifrado y único canal
Servicio de correo electrónico {SMTP, POP3, IMAP}	<ul style="list-style-type: none"> - Propósito: Envío, recepción y gestión de correos - Protocolo de transporte: TCP - Protocolos: SMTP, POP3, IMAP - Mensajes comunes: HELLO, MAIL, FROM, RCPT TO, DATA, QUIT, USER, PASS, LIST, RETR, FETCH - Gestión: SMTP para envío: POP3 descarga y elimina: IMAP sincroniza con el servidor
Servicio de direccionamiento {DHCP Y DNS}	<ul style="list-style-type: none"> - Propósito: DHCP asigna IPs, DNS traduce dominios a IPs - Protocolo de transporte: DHCP (UDP 67/68), DNS (UDP 53, a veces TCP) - Mensajes comunes: DHCP: DISCOVER, OFFER, REQUEST, ACK; DNS: QUERY, RESPONDE - Gestión: DHCP asigna IPs dinámicamente: DNS responde con la IP del dominio solicitud

Nota. Ludeña, P., 2025.

A continuación, se describirán una a una estas aplicaciones:

Servicio de direccionamiento

El protocolo DHCP (*Dynamic Host Configuration Protocol*) permite asignar automáticamente direcciones IP, máscara de subred, puerta de enlace y otros parámetros a dispositivos al conectarse a una red. Utiliza UDP (puertos 67 y 68), y su intercambio típico incluye:

1. **DHCP Discover:** mensaje enviado por el cliente en difusión para buscar servidores disponibles.
2. **DHCP Offer:** el servidor propone una configuración.
3. **DHCP Request:** el cliente responde con este mensaje solicitando una de las ofertas.
4. **DHCP ACK:** el servidor confirma la asignación del direccionamiento.

Este protocolo es vital para redes grandes o redes que no tienen usuarios frecuentes y en consecuencia asignar direcciones IP manualmente sería poco práctico.

Servicio de traducción de nombres de dominio

DNS (*Domain Name System*) traduce nombres de dominio (como www.utpl.edu.ec) en direcciones IP. También usa UDP (puerto 53) para consultas simples, aunque puede usar TCP para respuestas más grandes o transferencias de zona. Un cliente realiza una consulta del tipo ¿Cuál es la IP de www.example.com? y el servidor DNS responde con la dirección correspondiente. Este proceso es invisible para el usuario, pero es fundamental para que la navegación funcione.

Navegación Web

El protocolo HTTP (*HyperText Transfer Protocol*) permite que los navegadores soliciten páginas web desde servidores. Cada vez que usted ingresa una URL, el navegador genera una solicitud HTTP

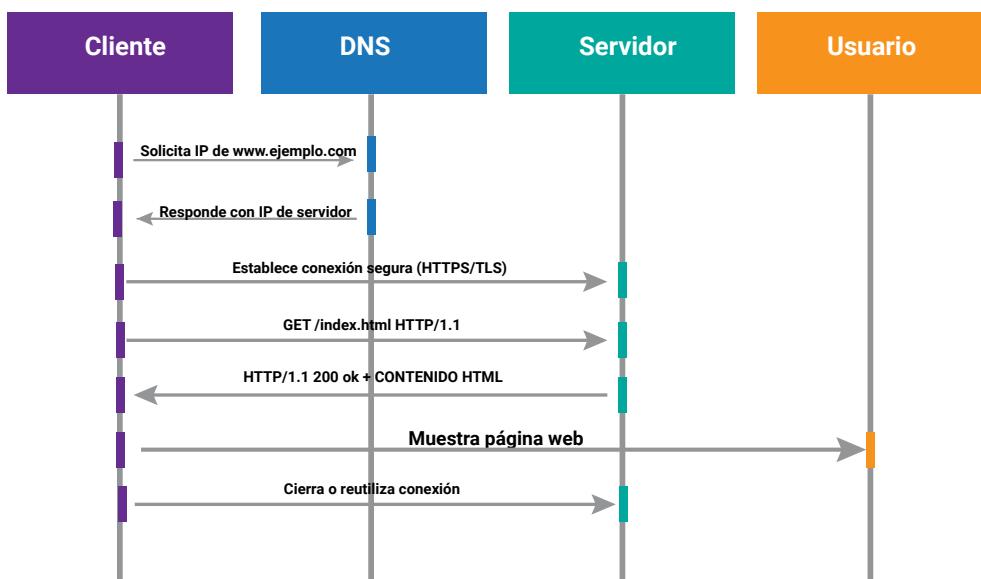
(usualmente GET o POST) que viaja por la red hasta llegar al servidor correspondiente, el cual responde con el contenido solicitado: texto, imágenes, scripts, etc.

HTTP opera sobre TCP (puerto 80), lo que garantiza una entrega confiable y ordenada. Cuando la seguridad es prioritaria se emplea HTTPS, que encapsula HTTP dentro de un canal cifrado TLS, utilizando el puerto 443.

En la Figura 64, se puede ver el diagrama de secuencia para cargar una página web con HTTP.

Figura 64

Diagrama de secuencia de funcionamiento de HTTP



Nota. Ludeña, P., 2025.

EL URL que se escribe en el navegador es resuelto por el servidor DNS, quien devuelve la dirección IP del servidor. A través de TCP el cliente establece la conexión con el servidor usando el saludo de tres vías. El cliente inicia el protocolo HTTP con el método GET y el servidor responde

con el mensaje 200 OK. El servidor envía los datos. Cuando se terminan de enviar los datos se da el proceso de cierre de conexión en ambos extremos.

Transferencia de archivos

Cuando se requiere intercambiar archivos entre equipos remotos, se utilizan protocolos especializados como FTP (File Transfer Protocol). FTP permite la autenticación de usuarios, listado de directorios y transferencia de archivos en ambos sentidos.

FTP utiliza dos canales TCP, el canal de control (puerto 21) para enviar comandos como USER, PASS, LIST, RETR (descargar), STOR (subir); y, el canal de datos (puerto 20) para transferir los archivos como tal.

Sin embargo, FTP no cifra ni la contraseña ni los datos, por lo que en entornos modernos se prefiere SFTP (Secure FTP), que encapsula toda la sesión dentro de SSH. A diferencia de FTP, SFTP usa solo un canal seguro (puerto 22), lo que lo hace más seguro y eficiente.

En ambos casos, el cliente inicia sesión, explora el sistema de archivos remoto y realiza operaciones de lectura o escritura, recibiendo respuestas que confirman cada acción.

Correo electrónico

El correo electrónico combina varios protocolos que trabajan de forma complementaria. SMTP (Simple Mail Transfer Protocol) se encarga del envío de correos, mientras que POP3 e IMAP permiten recibirlós.

SMTP utiliza TCP (puerto 25, o 587 para envío autenticado), y es utilizado tanto entre servidores de correo como por clientes que envían mensajes. Los comandos típicos son HELO/EHLO, MAIL FROM, RCPT TO, DATA, que inician el saludo, definen remitente y destinatario, y transmiten el contenido.

Para la descarga de correos, existen dos enfoques. El primero es POP3 (*Post Office Protocol v3*) que descarga los mensajes al dispositivo y los borra del servidor, ideal para acceder desde un solo equipo. Usa TCP puerto 110 (o 995 cifrado). Y el segundo es IMAP (*Internet Message Access Protocol*) que permite acceder y gestionar los mensajes directamente en el servidor, ideal para múltiples dispositivos. Usa TCP puerto 143 (o 993 seguro). Ambos protocolos permiten al cliente recuperar cabeceras, consultar el estado de los mensajes y sincronizar carpetas, aunque IMAP es más flexible para operaciones remotas y acceso parcial.

Ahora que ya conoce algunas aplicaciones de uso cotidiano, conteste en su cuaderno de apuntes o en un documento de Word las siguientes preguntas de reflexión:

- ¿Cómo facilita el protocolo DNS la navegación en internet y qué riesgos podrían surgir si este servicio es comprometido?
- ¿Por qué es crucial el protocolo DHCP en redes grandes y qué consecuencias tendría su mal funcionamiento en una red corporativa?
- En el contexto del protocolo HTTP, ¿cómo influye la seguridad (HTTPS) en la confianza del usuario y la integridad de la información transmitida?
- ¿En qué escenarios actuales sigue siendo útil el uso del protocolo FTP y qué alternativas más seguras existen hoy en día?
- ¿Cuál es la importancia del protocolo SMTP en el funcionamiento del correo electrónico y qué mecanismos se pueden aplicar para prevenir el envío de correos maliciosos o spam?



Actividades de aprendizaje recomendadas

Continuemos con el aprendizaje mediante su participación en las actividades que se describen a continuación:

Actividad 1. Lectura de los contenidos propuestos

Ingrese a la plataforma [Netacad](#) y revise el módulo 15: Capa de aplicación, en el cual usted abordará el estudio de las capas de sesión, presentación y aplicación.

Estrategia de trabajo:

- Aproveche el tiempo para sumergirse en la lectura del módulo, visualizando cómo cada nuevo concepto se conecta con su futuro profesional.
- Construya su propio resumen de aprendizajes, anotando en un cuaderno o en formato digital lo esencial para convertir la teoría en conocimiento útil y duradero.
- Interactúe con cada recurso que ofrece la plataforma, como animaciones y ejercicios, para transformar la teoría en experiencia práctica.
- Evalúe su avance con las autoevaluaciones, celebrando los aciertos y aprendiendo de cada desafío como parte de su crecimiento.

Retroalimentación:

El sistema le mostrará en qué áreas ha cometido errores, permitiéndole volver al módulo y reforzar esos contenidos.

índice

I Bimestre

II Bimestre

Solucionario

Referencias

Actividad 2. Es hora de medir nuestro avance

En la plataforma Netacad encontrará el Examen de punto de control: Examen de comunicaciones de aplicaciones de red (módulos 14-15), que le propondrá cuestiones sobre la unidad 3.

Al completar esta actividad, no solo estará cumpliendo un requisito académico, sino que también estará más cerca de obtener una valiosa microcertificación. Esta credencial técnica puede ser un gran impulso para su desarrollo profesional y una señal clara de compromiso y excelencia.

Actividad 3. Autoevaluación 3

Estimado estudiante, a continuación, usted tiene unas preguntas para que pueda medir su nivel de conocimiento sobre los contenidos de la unidad 3.

Estrategia de trabajo:

- La estrategia sugerida es resolver la autoevaluación sin revisar material adicional.
- Revise el solucionario disponible al final de la guía.

Una vez comprendida la actividad, realice la autoevaluación para comprobar sus conocimientos.



Autoevaluación 3

Lea cada pregunta con atención y seleccione la alternativa que considere correcta.

1. La principal razón por la que el protocolo UDP no incluye campos para identificar cada segmento enviado con un número de secuencia es para reducir la complejidad de su cabecera y minimizar la latencia, lo que lo hace ideal para aplicaciones donde la velocidad es más crítica que la fiabilidad total, como el *streaming* de video.
 - a. Verdadero.
 - b. Falso.
2. El método *three-way handshake* en TCP garantiza que la sesión se cierre de forma ordenada al finalizar la comunicación.
 - a. Verdadero.
 - b. Falso.
3. Considere una aplicación que requiere enviar notificaciones de eventos críticos de bajo volumen y donde la sobrecarga de confirmaciones es inaceptable, aunque se puedan tolerar algunas pérdidas ocasionales. Según las características de los protocolos de transporte, ¿cuál de los siguientes protocolos sería el más apropiado para esta tarea?
 - a. TCP, debido a su fiabilidad y garantía de entrega ordenada.
 - b. HTTP/3 (QUIC), porque es una aplicación de capa de aplicación veloz.
 - c. FTP, ya que maneja la transferencia de archivos completos con reenvío en caso de errores.
 - d. UDP, porque su diseño sin conexión y de baja sobrecarga se adapta a la tolerancia de pérdidas a cambio de rapidez.

4. Un administrador de red está diagnosticando un problema donde los datos de una aplicación se reciben por partes y fuera de orden en el destino, a pesar de que la conexión está establecida. Considerando las funciones de la capa de transporte, ¿qué mecanismo del protocolo TCP es fundamental para resolver este problema y asegurar que la aplicación reciba el mensaje original completo y correctamente secuenciado?
- a. La multiplexación y demultiplexación por números de puerto.
 - b. El control de flujo mediante la ventana deslizante.
 - c. Los números de secuencia.
 - d. La verificación de integridad (*checksum*).
5. Según el modelo OSI, ¿cuál es la implicación principal de que la capa de presentación actúe como un traductor universal para los datos en la comunicación entre aplicaciones?
- a. Permite que varias aplicaciones utilicen simultáneamente la red sobre un mismo host.
 - b. Garantiza que el tráfico de difusión se limite a una subred específica.
 - c. Asegura que los datos enviados desde una aplicación en un sistema sean entendidos por la aplicación receptora en otro sistema, independientemente de sus formatos internos.
 - d. Define cuántos bytes puede recibir el receptor sin desbordarse para controlar el flujo.

6. Un desarrollador está creando una aplicación de mensajería instantánea que requiere establecer y mantener una conversación fluida, pero también necesita garantizar que los mensajes extensos no se pierdan o lleguen incompletos, y que la comunicación pueda reanudarse si hay una interrupción temporal de la red. ¿Cuáles dos funciones de las capas superiores del modelo OSI serían fundamentales para esta aplicación? (Elija dos opciones).
- a. La sincronización y recuperación de sesión de la capa de sesión.
 - b. La gestión de autenticación y autorización de la capa de aplicación.
 - c. La traducción de formatos de datos y el cifrado/descifrado de la capa de presentación.
 - d. La segmentación y reensamblaje de la capa de transporte.
7. Un ingeniero de redes está diseñando una infraestructura para una plataforma de telemetría IoT, donde miles de dispositivos con recursos limitados envían constantemente pequeños volúmenes de datos. Para optimizar el rendimiento y el uso de recursos, ¿cuáles dos características del protocolo de transporte serían más beneficiosas para esta aplicación? (Elija dos opciones).
- a. La operación sin conexión para reducir la sobrecarga de establecimiento y cierre.
 - b. La minimización de la latencia, incluso a costa de una posible pérdida de datos.
 - c. La garantía de entrega ordenada de todos los datos mediante acuses de recibo.
 - d. El mecanismo de ventana deslizante para control de flujo adaptativo.

8. En el contexto de la carga de una página web a través de HTTP sobre TCP, ¿cuáles dos de las siguientes afirmaciones describen correctamente un aspecto de la interacción entre estos protocolos y las capas involucradas? (Elija dos opciones).
- a. La solicitud HTTP inicial (GET) se encapsula directamente en una trama Ethernet antes de cualquier establecimiento de conexión TCP.
 - b. El servidor DNS se encarga de traducir el nombre de dominio de la URL a una dirección IP antes de que el cliente intente establecer la conexión TCP con el servidor web.
 - c. El saludo de tres vías de TCP debe completarse exitosamente antes de que la solicitud HTTP (GET) pueda ser enviada al servidor web.
 - d. El cierre de la conexión TCP se produce inmediatamente después de que el servidor envía el mensaje 200 OK, sin ningún paso adicional.

9. Empareje cada función de la capa de transporte con su propósito técnico fundamental:

Función de capa de transporte	Propósito
1. Multiplexación y demultiplexación.	A. Fraccionar datos de la capa de aplicación y reensamblarlos en destino.
2. Segmentación y reensamblaje.	B. Identificar aplicaciones o servicios que requieren acceso a la red.
3. Verificación de integridad (checksum).	C. Permitir que varios procesos de aplicación utilicen la red simultáneamente sobre un mismo host.
4. Identificación de aplicaciones.	D. Detectar alteraciones accidentales de los datos durante la transmisión.

10. Empareje cada protocolo de la capa de aplicación con su protocolo de transporte típico y el motivo principal de su elección:

Protocolo de aplicación	Protocolo de transporte/Puerto
1. HTTP.	A. UDP/53.
2. RTP/RTCP (VoIP).	B. TCP/80-443.
3. DNS.	C. UDP/67-68.
4. DHCP.	D. UDP/puertos dinámicos.

[Ir al solucionario](#)

Resultado de aprendizaje 3

- Implementa redes LAN y medidas de seguridad en la configuración y gestión de infraestructuras de telecomunicaciones con el fin de garantizar una conectividad eficiente, segura y sostenible.

Para alcanzar el resultado de aprendizaje, se ha diseñado un recorrido que integra de manera progresiva la teoría, la práctica y el análisis crítico de los elementos clave que componen una red local y su entorno seguro. Comenzaremos por explorar los fundamentos de la seguridad en redes, entendiendo las vulnerabilidades más comunes que pueden afectar los sistemas y dispositivos de comunicación, los tipos de ataques que se presentan con mayor frecuencia (como malware, ataques de acceso o de denegación de servicio) y las estrategias básicas de mitigación que todo profesional debe dominar. Posteriormente, nos enfocaremos en la implementación técnica de una red LAN. Se estudiarán los dispositivos esenciales y se abordarán aspectos prácticos de configuración, conexión física y lógica, direccionamiento IP y verificación de la conectividad. Además, se introducirán técnicas de resolución de problemas comunes, indispensables para mantener la operatividad de una red real.

El estudio de estos contenidos irá acompañado por recursos interactivos y simulaciones en Packet Tracer, análisis de casos reales, mapas conceptuales y evaluaciones que promuevan la reflexión sobre la sostenibilidad y la calidad del servicio. Todo ello le permitirá a usted no solo adquirir destrezas técnicas, sino también comprender el impacto que tiene el diseño seguro y eficiente de una red LAN en el entorno empresarial y social actual.

Contenidos, recursos y actividades de aprendizaje recomendadas



Sem 9

Sem 10

Sem 11

Sem 12

Sem 13

Sem 13

Sem 14

Sem 15

Sem 16



Semana 14

En el transcurso de esta semana, nos adentraremos en el estudio de los Fundamentos de seguridad, ya que la seguridad es un componente esencial para su formación como futuro ingeniero en Redes y Analítica de Datos. Los temas clave que incluirán vulnerabilidades, ataques y estrategias de mitigación que podrán ser ampliados en la bibliografía básica.

Como estrategias de aprendizaje, se le presentará la información teórica a través de mapas mentales, videos explicativos y lecturas orientadas. Usted aplicará los conocimientos adquiridos para construir entornos de red local robustos, implementando medidas básicas de seguridad que permitan proteger tanto la infraestructura física como lógica en un escenario de red simulado. Para complementar estas estrategias de aprendizaje, puede consultar el video introductorio que sintetiza los conceptos centrales de la [unidad 4](#).

Como pudo constatar en la introducción, la seguridad no es un añadido opcional, sino un componente integral desde el diseño de la red. Lo que observó sobre las vulnerabilidades y medidas de protección refleja la realidad actual, donde cada dispositivo conectado representa tanto una oportunidad como un riesgo potencial que debe gestionarse proactivamente.

Unidad 4. Fundamentos de seguridad e implementación

Índice

I Bimestre

II Bimestre

Solucionario

Referencias

4.1. Fundamentos de seguridad

La seguridad en redes de computadoras es fundamental para cualquier organización que dependa de la conectividad para operar. A medida que las infraestructuras digitales crecen en complejidad y alcance,

también lo hacen las amenazas que las rodean. Un fallo de seguridad en la red no solo compromete la confidencialidad y la integridad de los datos, sino que puede paralizar por completo los procesos operativos de una empresa. Basta con considerar que, según el informe *Cybersecurity Ventures 2024* (Morgan, 2024), se estima que el costo global del cibercrimen alcanzará los 10.5 billones de dólares anuales para el año 2025. Este impacto económico se traduce en pérdidas de productividad, fuga de información crítica, daños reputacionales y, en muchos casos, interrupciones totales del servicio.

Con esto en mente, reflexione sobre las siguientes preguntas:

- ¿Qué consecuencias económicas y operativas cree usted que podría enfrentar una empresa si su red es comprometida durante 24 horas?
- ¿Ha considerado que una mala configuración en un router o switch puede abrir puertas invisibles a intrusos?
- ¿Qué tan preparado se siente para identificar un ataque en su fase temprana?

La criticidad de la seguridad en redes abre una oportunidad laboral para usted como futuro ingeniero en Redes y Analítica de Datos. En el mismo reporte se prevé 3.5 millones de puestos vacantes en áreas relacionadas con ciberseguridad. En esta sección usted aprenderá a identificar las vulnerabilidades comunes presentes en redes, a reconocer los tipos de ataques más frecuentes y a comprender las estrategias básicas de mitigación, sentando las bases para abrirse camino a esta interesante área técnica.

4.1.1. Introducción a la seguridad en redes

En los orígenes de las redes de computadoras, su diseño se enfocó en lograr una conectividad eficaz entre dispositivos, con usuarios considerados confiables y entornos controlados. La seguridad era una preocupación secundaria. Este enfoque optimista se justificaba en

redes académicas o militares de acceso restringido, donde el riesgo de intrusiones maliciosas era muy bajo. Sin embargo, con el crecimiento exponencial de *Internet*, la incorporación de millones de usuarios anónimos y el uso generalizado de redes para fines comerciales, gubernamentales y personales, surgieron nuevas amenazas.



Le invito a ver el video denominado "[¡ASÍ fue el PRIMER VIRUS que AMENAZÓ todo INTERNET!](#)", donde se explica el contexto en el cual se desarrolló el primer ataque masivo, mismo que fue realizado por el gusano de Morris (1988), y afectó al 10 % del total de máquinas conectadas a *Internet* en ese momento. A partir de este hecho, se popularizan otras técnicas de ataque que aprovechaban vulnerabilidades de las redes para causar daños a los sistemas.

Los objetivos fundamentales de la seguridad de redes se resumen en la tríada CIA:

1. **Confidencialidad:** garantiza que la información solo sea accesible para las personas, procesos o sistemas autorizados. Su violación implica que datos sensibles puedan ser leídos, interceptados o divulgados por terceros no autorizados.

La confidencialidad es esencial en aplicaciones como la banca en línea, comunicaciones empresariales o información médica, donde una filtración puede tener consecuencias legales, económicas y sociales graves.

2. **Integridad:** se refiere a la protección de los datos frente a modificaciones no autorizadas, durante la transmisión o almacenamiento, ya sea por error o manipulación maliciosa. Un sistema con buena integridad asegura que la información permanece exacta, coherente y completa durante su ciclo de vida. Se utilizan firmas digitales, sumas de verificación y controles de acceso para protegerla.

Preservar la integridad es vital para aplicaciones como el comercio electrónico, los sistemas de control industrial, o los historiales clínicos, donde cualquier alteración puede ser crítica.

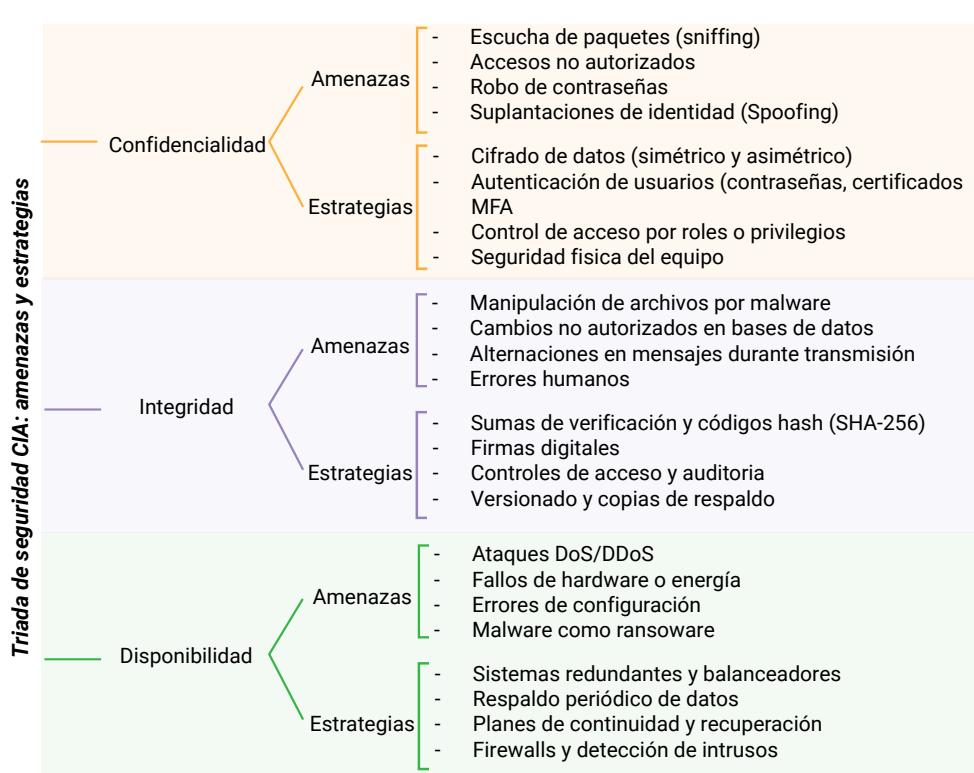
3. **Disponibilidad:** busca que los recursos, sistemas, servicios y datos de red estén accesibles y operativos cuando se necesiten. Es decir, que los usuarios autorizados puedan acceder a la información y los recursos sin interrupciones indebidas. Esto implica protección contra ataques de denegación de servicio, fallos de *hardware*, y errores de configuración.

La disponibilidad es esencial en sectores donde la interrupción del servicio puede significar una pérdida económica o poner en riesgo la vida humana, como en hospitales, bancos, aeropuertos o servicios públicos.

Para complementar esta información, en la figura 65, podrá encontrar la información sobre las amenazas que van en contra de cada uno de estos objetivos y las estrategias que se pueden implementar para lograr confiabilidad, integridad y disponibilidad.

Figura 65

Principales estrategias usadas por triada CIA para prevenir amenazas



Nota. Ludeña, P., 2025.

Por ejemplo, las principales amenazas contra la Integridad son la manipulación de archivos por software maliciosos, los cambios no autorizados, la modificación en transmisión y los errores humanos. Dichas amenazas se pueden atacar a través del uso de la suma de verificación, firmas digitales, controles de acceso y copias de respaldo. Analice en detalle las amenazas para los otros aspectos de la triada.

En la actualidad, se han definido algunos objetivos complementarios, como:

- **Autenticación:** consiste en verificar la identidad de usuarios y dispositivos que acceden a los dispositivos y a la red.
- **No repudio:** trata de impedir que un emisor legítimo niegue su participación en un proceso.
- **Auditoría:** registrar eventos para identificar ataques o actividades sospechosas a través de logs del sistema. Esto aporta información relevante en actividades de análisis post-ataques para prevención.



Para afianzar sus conocimientos, le invito a visualizar el video titulado "[Qué es la TRIADA CIA para la seguridad informática en la ISO 27001](#)", el cual le explicará cómo la triada CIA se aplica a empresas a través de la norma ISO 27001. Estos conceptos son fundamentales para su formación en seguridad en redes, por lo que ponga atención en los ejemplos descriptivos que se presentan en el recurso.

Luego de revisar el video, en su cuaderno de apuntes o en documento de Word, escriba 5 estrategias que se recomiendan para implementar la triada CIA en una organización.

4.1.2. Vulnerabilidades de seguridad

En el contexto de las redes de computadoras, una vulnerabilidad se define como una debilidad o fallo en el diseño, implementación, configuración o administración de un sistema que puede ser aprovechado por un atacante para comprometer la seguridad de la red.

Esta condición puede estar presente en hardware, software, protocolos de comunicación, o incluso en las políticas operativas y de gestión de una organización. Por esta razón, identificar y mitigar vulnerabilidades es un paso crucial para mantener la integridad, confidencialidad y disponibilidad de la información.

Para ampliar su conocimiento sobre estas vulnerabilidades, le invito a escuchar atentamente el siguiente podcast:

[Vulnerabilidades en Seguridad de Redes](#)

Después de analizar el contenido del podcast, habrá notado que la seguridad efectiva en infraestructuras tecnológicas requiere un enfoque integral que va más allá de las soluciones técnicas. Es importante comprender cómo las vulnerabilidades tecnológicas, de configuración y de política se interrelacionan y pueden amplificar los riesgos operacionales.

Ahora bien, conocer los tipos de vulnerabilidades es importante, pero más importante aún es ir ejercitando la habilidad para reconocerlas en el entorno operativo real y evaluar su severidad. Detectar puntos débiles en infraestructuras de red y corregirlos proactivamente es una habilidad que se va consiguiendo con el tiempo y el monitoreo constante.

Evalúe su actitud frente a la detección de vulnerabilidades contestando en su cuaderno de apuntes o en un documento de Word las siguientes preguntas:

- ¿Ha evaluado alguna vez si sus propias redes o dispositivos personales presentan alguna de estas vulnerabilidades? Este puede ser un buen momento para empezar a observar con mirada crítica su entorno digital.
- ¿Qué tipo de vulnerabilidad considera usted que representa un mayor riesgo en una red pequeña, una tecnológica, una de configuración o una de política de seguridad? Justifique su respuesta con ejemplos.
- Si se encuentra administrando una red empresarial y descubre que muchos dispositivos aún tienen contraseñas por defecto, ¿cuál sería su plan de acción inmediato? ¿Cómo podría prevenir que esto vuelva a ocurrir?

- ¿Qué consecuencias podría tener una política de seguridad mal definida o inexistente en una organización que maneja datos sensibles de clientes?

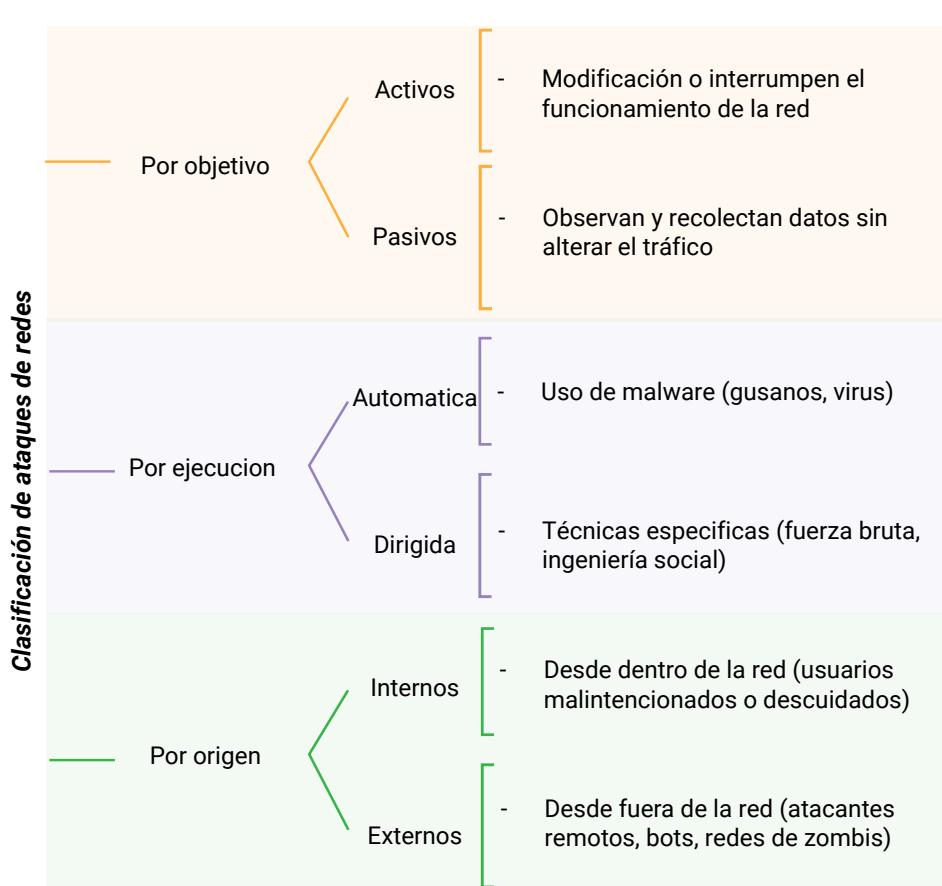
4.1.3. Ataques de red

Un ataque de red es cualquier acción maliciosa diseñada para comprometer, interrumpir o acceder sin autorización a sistemas, datos o servicios a través de una red. Estos ataques son ejecutados por actores de amenaza que, mediante técnicas y herramientas especializadas, buscan explotar vulnerabilidades previamente identificadas. Los objetivos pueden ser diversos, entre los más frecuentes: robo de información, daño a la infraestructura, espionaje, manipulación de datos, interrupción del servicio, o incluso el simple acto de demostrar poder técnico.

En la Figura 66, se presenta un mapa mental con la clasificación de los ataques por objetivo si son activos o pasivos, por ejecución si son automáticos o dirigidos y por origen de pendiendo desde donde se produce el ataque ya sea premeditado o involuntario.

Figura 66

Clasificación de ataques a redes



Nota. Ludeña, P., 2025.

Analice los tipos de ataques y los ejemplos dados para que identifique si ha escuchado anteriormente sobre alguno de ellos.

En la Tabla 37 se detalla algunos tipos de ataques dependiendo del daño que ocasionan a la red.

Tabla 37

Clasificación de ataques de red según el tipo de daño ocasionado

Tipo de ataque	Descripción	Ejemplo real
Malware	<p>El malware se infiltra en los sistemas para causar daño o extraer información sin el consentimiento del usuario. Incluye virus, gusanos, troyanos y ransomware.</p> <p>Efecto: daño al sistema, cifrado de datos, pérdida de información.</p>	<p>El gusano WannaCry (2017) afectó a más de 200,000 computadoras en 150 países, cifrando archivos y pidiendo rescate en bitcoins. Entre los afectados estuvo el sistema de salud del Reino Unido.</p>
Reconocimiento	<p>Estos ataques recopilan información sobre la red y sus dispositivos antes de lanzar un ataque más específico. Herramientas como ping sweep, traceroute o whois son usadas para mapear la red.</p> <p>Efecto: riesgo de ataques posteriores, filtración de topologías</p>	<p>Un atacante puede usar Nmap para escanear puertos de una empresa y determinar qué servicios están activos, preparando así un ataque más sofisticado.</p>
Acceso no autorizado	<p>Buscan eludir los mecanismos de autenticación para tomar el control de sistemas o datos. Se valen de técnicas como fuerza bruta, explotación de contraseñas débiles o redireccionamiento de puertos.</p> <p>Efecto: robo de datos, suplantación, control de sistemas</p>	<p>El ataque a Yahoo! (2013–2014), donde se comprometieron más de 3 mil millones de cuentas, fue posible por robo de credenciales y acceso a cuentas de alto privilegio.</p>

Tipo de ataque	Descripción	Ejemplo real
Denegación de servicio (DoS/ DDoS)	Consisten en saturar un servidor o red con tráfico excesivo hasta que el servicio colapsa. Los ataques distribuidos (DDoS) son coordinados desde múltiples fuentes.	El ataque DDoS a DynDNS en 2016 , ejecutado por la botnet Mirai, dejó sin acceso a servicios como Twitter, Netflix y Spotify en gran parte de Estados Unidos y Europa. Efecto: interrupción total del servicio, caída de infraestructura
Man-in-the-Middle (MitM)	El atacante intercepta o modifica las comunicaciones entre dos partes sin que estas lo perciban.	Un ataque MitM podría ocurrir en una red Wi-Fi pública no segura, donde el atacante capturará datos, por ejemplo, credenciales que un usuario envía a un sitio web. Efecto: intercepción de credenciales, alteración de datos
Phishing / Ingeniería social	Suplantación de identidad, robo de credenciales	Campañas de phishing por correo falso

Nota. Ludeña, P., 2025.

Para comprender la magnitud y naturaleza del impacto que estos ataques pueden tener sobre la disponibilidad, integridad y confidencialidad de los sistemas se menciona un incidente real para los ataques más críticos. Le recomiendo ingresar en cada enlace para ampliar la información sobre cada ataque y evaluar el daño provocado a la red, en algunos casos se encuentran los datos de las pérdidas monetarias y las técnicas de recuperación usadas.

En el entorno profesional de redes, identificar los ataques por su nivel de daño permite priorizar defensas y establecer políticas de mitigación eficaces. Como futuro ingeniero, usted deberá ser capaz de diagnosticar incidentes con agudeza y aplicar medidas que no solo solucionen el problema, sino que lo prevengan desde su origen.

Conceptos fundamentales de seguridad de redes

Le invito a poner a prueba su conocimiento sobre seguridad informática mediante esta sopa de letras interactiva. Esta tarea tiene como objetivos identificar y relacionar conceptos esenciales de seguridad de la información, mediante una actividad de reconocimiento visual, que estimule el aprendizaje activo y la retención de términos técnicos clave.



Seguridad de Redes

Como pudo comprobar durante la búsqueda, estos conceptos forman un ecosistema integral de seguridad digital. Cada término que encontró representa una pieza fundamental: desde los principios básicos como confidencialidad e integridad, hasta las amenazas como troyanos, y las medidas preventivas como autenticación. La familiarización con esta terminología es el primer paso para comprender cómo se construye una estrategia de seguridad robusta y efectiva.

Luego de desarrollar la actividad, conteste en su cuaderno de apuntes o en un documento de Word las siguientes preguntas de reflexión:



- ¿Cuál es la diferencia entre confidencialidad e integridad de la información?
- ¿Por qué es importante la autenticación en un sistema seguro?
- ¿Qué tipo de amenazas representan mayor riesgo para la disponibilidad de un sistema?

4.1.4. Estrategias básicas de seguridad

Proteger una red informática no se limita a la instalación de software antivirus o la configuración de contraseñas, además, implica un enfoque estructurado y continuo que combine políticas, buenas prácticas, y herramientas técnicas. Las estrategias básicas de seguridad tienen como objetivo minimizar la exposición a riesgos, dificultar el acceso no autorizado y permitir una respuesta eficaz ante incidentes. Estas estrategias son la primera línea de defensa que todo ingeniero en Redes y Analítica de Datos debe comprender, implementar y mantener actualizada en cualquier entorno tecnológico.

En la Figura 67, se presenta la clasificación de las estrategias de seguridad en redes informáticas en función del tipo de actor involucrado: usuario final, administrador de red, responsables de la empresa y organismos reguladores. Cada grupo tiene responsabilidades específicas que, en conjunto, fortalecen la protección integral de los sistemas y los datos.

Figura 67

Estrategias de seguridad en redes según el rol del actor

Estrategias de seguridad según el actor	
Usuario final	<ul style="list-style-type: none"> - Usar contraseñas seguras y no compartidas - No instalar software no autorizado - Identificar correos o enlaces sospechoso (phishing) - Cerrar sesiones al terminar
Administrador de red	<ul style="list-style-type: none"> - Implementar VLANs, ACLs, firewalls y segmentación - Configurar autenticación multifactor (MFA) - Actualizar sistemas y aplicar parches - Monitorizar logs y alertas - Respaldar configuraciones y datos
Dueños o responsables de la red / empresa	<ul style="list-style-type: none"> - Establecer políticas y normas de seguridad claras - Definir roles y accesos - Invertir en infraestructura segura - Fomentar la cultura de seguridad
Organismos de regulación y normativas externas	<ul style="list-style-type: none"> - Establecer estándares obligatorios (ISO 27001, NIST, GDPR) - Exigir auditoria de cumplimiento - Definir lineamientos para protección de datos personales y ciberseguridad

Nota. Ludeña, P., 2025.

Una de las primeras acciones consiste en aplicar el principio de defensa en profundidad, el cual implica implementar múltiples capas de protección para dificultar al atacante el acceso a recursos sensibles. Esta defensa se complementa con el uso de contraseñas seguras y autenticación multifactor, lo cual reduce el riesgo de acceso indebido, incluso si las credenciales de un usuario son comprometidas.

La actualización constante de software y firmware es otra práctica esencial. Muchos ataques exitosos explotan vulnerabilidades conocidas que ya han sido corregidas por los fabricantes, pero que no han sido aplicadas en los sistemas. Por ello, contar con una política clara de

gestión de parches es clave para cerrar brechas antes de que puedan ser aprovechadas.

Asimismo, es importante realizar copias de seguridad periódicas, almacenadas en lugares seguros y con procedimientos de restauración ya probados. Estas copias no solo protegen contra pérdidas accidentales, sino que también permiten la recuperación ante incidentes como ataques de ransomware. Estas prácticas deben ir acompañadas de una política de seguridad formal, que defina roles, responsabilidades, normas de acceso y manejo de incidentes.

Desde el punto de vista físico, proteger el acceso a los equipos, a las salas de servidores y al cableado de red evita que se vulneren dispositivos directamente. La seguridad física es frecuentemente subestimada, pero es crítica, especialmente en redes pequeñas o medianas donde no existen sistemas automáticos de vigilancia.

Por último, la educación y concienciación de los usuarios es tan importante como las medidas técnicas. Muchos ataques, como el phishing o el uso de malware a través de correos engañosos, tienen éxito por errores humanos. La capacitación periódica del personal en temas de ciberseguridad fortalece el componente humano como parte de la defensa de la red.

Estas estrategias forman una base indispensable sobre la cual usted, como futuro profesional, deberá construir soluciones seguras, robustas y sostenibles. La seguridad no es un estado estático, sino un proceso que requiere vigilancia, adaptación y mejora continua.

Luego de revisar el mapa mental de las estrategias de seguridad, conteste en su cuaderno de apuntes o en un documento de Word las siguientes preguntas de reflexión:



- ¿Qué tipo de estrategias de seguridad básicas ha aplicado usted alguna vez en sus propios dispositivos?
- ¿Considera que una red pequeña o doméstica necesita aplicar estas mismas estrategias que una red empresarial?
- ¿Qué pasaría si una organización no tuviera ninguna política formal de seguridad? ¿Cómo afectaría esto la respuesta ante un incidente?

¡Fantástico progreso! Completamos la semana 14. Ahora puede validar su comprensión participando en este quiz.

Fundamentos de Seguridad en Redes

Como pudo comprobar a través de esta evaluación, la seguridad en redes requiere un enfoque integral que combine conocimientos técnicos con estrategias organizacionales. Los conceptos evaluados - desde la confidencialidad, integridad y disponibilidad hasta las diferentes categorías de vulnerabilidades y ataques - son interdependientes y forman la base para construir defensas robustas. Su desempeño en este quiz refleja su preparación para identificar amenazas, evaluar riesgos y proponer soluciones de seguridad apropiadas para diferentes contextos de red.



Actividades de aprendizaje recomendadas

Reforcemos el aprendizaje resolviendo las siguientes actividades.

Actividad 1. Lectura de los contenidos propuestos

Ingresé a la plataforma [Netacad](#) y revise el módulo 16: Fundamentos de seguridad de la red. La seguridad de la información es un pilar fundamental en el mundo digital actual y es necesario que usted, como profesional en Redes y Analítica de Datos, maneje conceptos básicos sobre seguridad de redes.

Estrategia de trabajo:

- Lea detenidamente el módulo en Netacad, dedicando al menos 45 minutos a comprender los conceptos clave.
- Registre las ideas más importantes en un cuaderno o documento digital mientras avanza en la lectura.
- Realice todas las actividades interactivas y revise las animaciones disponibles en la plataforma para reforzar su aprendizaje.
- Complete las autoevaluaciones del módulo para verificar su nivel de comprensión y detectar aspectos que necesita repasar.

Retroalimentación:

Después de leer los temas recomendados, reflexione sobre lo siguiente:

- ¿Cómo cree que será el panorama de seguridad en redes en los próximos 5 años?
- ¿Conoce sobre políticas públicas en torno a la seguridad de redes y de la información en su país?

Actividad 2. ¡Configuremos redes seguras!

En esta actividad usted aplicará medidas fundamentales de seguridad en dispositivos de red dentro de una infraestructura LAN, mediante la configuración de un *router* y un *switch* en Cisco Packet Tracer. A través de esta experiencia, usted complementará su conocimiento teórico con la práctica y reforzará su competencia técnica en el uso del sistema operativo IOS. Con ello, se alinea el aprendizaje a una visión sostenible de la gestión de redes, atendiendo tanto a la disponibilidad del servicio como a la integridad y confidencialidad de los recursos de red.

Estrategia de trabajo:

- Revise los conceptos fundamentales de seguridad de redes.
- Revise los comandos para configuración de dispositivos intermediarios, como accesos seguros, contraseñas robustas, cifrado, bloqueo de sesiones, SSH y desactivación de puertos no usados.
- Tenga a mano su cuaderno de ingeniería.
- Desarrolle la actividad propuesta siguiendo el guion disponible en la misma.

[Práctica 16.5.1. de CCNA-1: dispositivos de red seguros.](#)

Retroalimentación:

En esta actividad de Packet Tracer, se mostrará su avance en forma de porcentaje. También pueden acceder a la pestaña *Check Results* para consultar los elementos evaluados, identificar cuáles ya se han completado correctamente y cuáles aún están pendientes o presentan errores.

Finalizada la actividad, con base en lo aprendido, conteste las siguientes preguntas de reflexión:

- ¿Por qué es importante que el *router* y el *switch* usen SSH en lugar de Telnet? En una red real, ¿qué consecuencias podría tener dejar Telnet habilitado?
- ¿Qué función cumple el comando *login block-for* en la protección del dispositivo?, ¿cómo ayuda esto a detener ataques por fuerza bruta?
- ¿Qué beneficios ofrece deshabilitar los puertos del *switch* que no están en uso?
- ¿Por qué es importante usar contraseñas complejas y cifradas para los accesos al dispositivo?
- ¿Cuál opción es mejor para crear contraseñas *enable secret* o *enable password*? Justifique su respuesta.



Sem 9

Sem 10

Sem 11

Sem 12

Sem 13

Sem 13

Sem 14

Sem 14

Sem 15

Sem 16



Semana 15

En esta semana, estudiaremos la implementación práctica de redes LAN, desde la identificación y configuración de dispositivos hasta la resolución de problemas técnicos, que constituye un ámbito esencial en su formación como futuro ingeniero en Redes y Analítica de Datos.

Los conocimientos se abordarán combinando recursos didácticos, técnicos y prácticos, para pasar de la teoría a la práctica. Se explicarán los elementos esenciales para tener en cuenta en la implementación de redes y una metodología de resolución de problemas en la red. Para ejercitarse la aplicación de la metodología, se propondrán algunos estudios de caso y para fortalecer las competencias prácticas, se desarrollarán actividades de configuración en el simulador Packet Tracer.



Si requiere ampliar la información proporcionada en esta semana, puede acudir a la bibliografía básica recomendada.

4.2. Implementación de redes LAN

La implementación de redes es el proceso de diseñar, configurar y poner en funcionamiento una infraestructura de comunicación que permita la interconexión eficiente de dispositivos dentro de una organización. Una red mal implementada puede convertirse rápidamente en un cuello de botella para la productividad, generar vulnerabilidades de seguridad, dificultar la administración y elevar innecesariamente los costos.

La implementación de redes requiere de planificación de manera metódica, incluyendo fases de diseño estructurado y selección adecuada de dispositivos que respondan a los requerimientos técnicos, operativos y de crecimiento de la organización.

Índice

I Bimestre

II Bimestre

Solucionario

Referencias



En esta sección abordaremos la implementación de redes LAN, que son redes pequeñas y brindan un entorno controlado y manejable para desarrollar habilidades prácticas esenciales, como son: selección de equipos, direccionamiento IP, asignación de dispositivos finales, configuración de servicios y verificación de conectividad. Estas experiencias, aunque parezcan sencillas, permiten establecer las bases para escalar a redes más complejas con múltiples segmentos, políticas de seguridad, Calidad de Servicio (QoS) y alta disponibilidad.

A través de este enfoque progresivo, usted desarrollará no solo capacidades técnicas para conectar dispositivos, sino también una visión estratégica que le permitirá diseñar e implementar redes LAN sostenibles, resilientes y preparadas para los desafíos actuales del entorno digital.

4.2.1. Componentes de una red LAN

Antes de comenzar a revisar cada componente de una red LAN, le invito a visualizar el siguiente video:

[Construyendo una red local.](#)

Como pudo observar en el video, la analogía de la ciudad digital transforma conceptos técnicos abstractos en elementos tangibles y comprensibles. La comparación entre dispositivos finales con edificios, switches con glorietas, y protocolos con reglas de tránsito demuestra que el diseño de redes requiere la misma planificación estratégica que el urbanismo. Esta perspectiva refuerza la importancia de considerar no solo las necesidades actuales, sino también proyectar el crecimiento futuro, convirtiendo cada decisión técnica en una inversión a largo plazo para la infraestructura digital.

Al diseñar e implementar una red LAN, es fundamental tener claridad sobre qué dispositivos, protocolos y aplicaciones se necesitan, y cómo

estos deben integrarse de forma coherente y funcional. Cada uno de estos elementos juega un papel determinante en el rendimiento, la seguridad y la capacidad de la red para cumplir los objetivos del entorno donde se despliega.

Para comprender estos elementos, revise la descripción de cada uno:

1. Dispositivos para redes LAN: recordemos que los dispositivos pueden ser dispositivos finales y dispositivos intermedios.

- Los **dispositivos finales** son los que utilizan los usuarios para acceder a los recursos de red. En redes LAN, estas pueden incluir: computadoras, impresoras, teléfonos IP, cámaras de seguridad y servidores. Por ejemplo, en una oficina, las estaciones de trabajo de los empleados, la impresora compartida y el servidor de archivos son dispositivos finales.
- Los **dispositivos intermedios** son los que permiten la conectividad entre los dispositivos finales, gestionando el flujo de datos. En un entorno LAN tendremos, por ejemplo, un switch de 12/24 puertos puede interconectar todas las computadoras de una pequeña oficina, enrutadores que hagan las veces de servidor DHCP y con funciones de firewall básico; y, también podríamos tener Puntos de Acceso inalámbrico (AP) para conectar los dispositivos como *laptops*, *tablets* o teléfonos móviles.

2. Protocolos de red: una red funciona gracias a un conjunto de protocolos que definen cómo se comunican los dispositivos entre sí. A lo largo de las unidades estudiadas hemos revisado varios de estos protocolos, entre los más importantes se encuentran: IP, Ethernet, ARP, DHCP, DNS e ICMP.

3. Servicios de capa de aplicación o aplicaciones en redes LAN: las aplicaciones que se implementan en una LAN varían según

el entorno (hogar, oficina, industria), pero suelen incluir: Correo electrónico interno mediante servidores de correo local, telefonía IP, videovigilancia, servicios de impresión compartida, servicio web.



Con estos elementos en mente, reflexione sobre lo siguiente:

- ¿Qué pasaría si todos los dispositivos de una oficina se conectaran directamente entre sí sin un switch central?
- ¿Cómo afectaría el desempeño de una red LAN si no se implementa un servidor DHCP y las direcciones IP se asignan manualmente?
- ¿Qué tipo de aplicaciones en su entorno (hogar, universidad o trabajo) considera que dependen de una red LAN bien configurada?

La selección de los componentes de la red dependerá de varios factores. No se trata solo de adquirir dispositivos funcionales, instalar protocolos y aplicaciones, sino de alinear la tecnología con las necesidades reales del entorno, proyectando también su evolución futura. A continuación, en el módulo didáctico se detallan los principales factores que deben considerarse al momento de seleccionar dispositivos de red, medios de transmisión y tecnologías asociadas.

Factores para la selección de dispositivos de red.

Como pudo observar en la infografía, la selección de equipos de red requiere un análisis integral que va más allá del costo inicial. Cada criterio, desde el equilibrio costo-funcionalidad hasta las capacidades del sistema operativo, interactúa con los demás para determinar el éxito a largo plazo de la infraestructura. Los ejemplos presentados demuestran que las decisiones técnicas aparentemente simples pueden tener impactos significativos en la escalabilidad, rendimiento y

capacidad de gestión futura de la red, validando la importancia de una planificación estratégica integral.

Con base en lo estudiado, reflexione sobre las siguientes preguntas:

- ¿Cree usted que es más conveniente ahorrar en costos iniciales o invertir en dispositivos con proyección a futuro?
- ¿Qué consecuencias podría tener elegir un switch sin capacidad PoE en una red que requerirá cámaras IP?
- ¿Ha considerado cómo influye la experiencia del personal técnico en la elección del sistema operativo de los equipos?

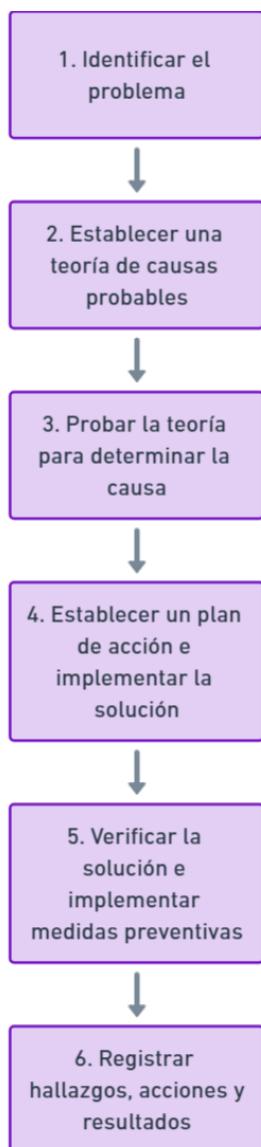


4.2.2. Técnicas de resolución de problemas

A futuro, en su ejercicio profesional, sobre todo en la administración de redes, se encontrará con una variedad de problemas técnicos. Los problemas pueden ser de diferente naturaleza y gravedad, por ejemplo, pérdida de conectividad, lentitud en el servicio, errores de configuración, entre otros. Ya que evitar los problemas es imposible, lo recomendable es establecer una metodología de resolución eficiente. En esta sección le presentaré una metodología de 6 pasos propuesta por Cisco Networking Academy (ver figura 68), la cual está basada en el método científico y que usted podrá hacer suya y adaptarla a su forma de trabajo. La clave es aplicar un enfoque estructurado que permita detectar, analizar y corregir fallos de forma lógica y documentada.

Figura 68

Guía paso a paso para la solución de problemas en redes de datos



Nota. Ludeña, P., 2025.

A continuación, revisaremos en detalle cada uno de los pasos que compone la metodología para la solución de problemas básicos.

Paso 1: Identificar el problema

Este es el paso inicial y consiste en reconocer y definir claramente el síntoma del problema. Puede implicar la recopilación de información mediante herramientas como ping, tracert, ipconfig o mediante una simple conversación con el usuario afectado, se puede extraer mucha información con base en la experiencia del usuario, así que no se debe menospreciar lo que el usuario puede aportar.

Recomendaciones:

- Escuche con atención la descripción del problema por parte del usuario.
- Pregunte desde cuándo ocurre y si ha cambiado algo en la red recientemente.
- Use herramientas de diagnóstico para verificar si el problema es de conectividad, velocidad, DNS, etc.

Paso 2: Establecer una teoría de causas probables

Una vez identificado el problema, el siguiente paso es formular una o varias hipótesis sobre lo que podría estar fallando. Esta teoría debe basarse en experiencia, conocimientos técnicos y síntomas observados. Mientras más trabaje con redes podrá hacer mejores conjeturas y podrá presumir de mejor manera las causas del problema,

Recomendaciones:

- Considere causas comunes antes de asumir errores complejos.
- Consulte la documentación de la red o registros de cambios recientes.

- Revise si el problema pudiera estar vinculado a una configuración, un cable dañado o una política mal aplicada.

Paso 3: Poner a prueba la teoría para determinar la causa

En este punto se deben realizar pruebas específicas para confirmar si la teoría propuesta explica efectivamente el problema. Recuerde siempre ir de lo más simple a lo más complejo. Se pueden modificar configuraciones, cambiar cables o sustituir dispositivos temporalmente.

Recomendaciones:

- Haga un cambio a la vez para poder identificar el efecto específico.
- No realice modificaciones permanentes sin confirmar que esa es la causa real.
- Documente los cambios que realiza para poder revertirlos si es necesario.

Paso 4: Establecer un plan de acción e implementar la solución

Con la causa confirmada, se debe diseñar un plan de solución, especificando qué se va a cambiar, cómo se hará y cuándo, sobre todo si el problema afecta a más de un dispositivo o a más de un sector de la red. La implementación debe hacerse de forma controlada y, si es posible, fuera del horario crítico.

Recomendaciones:

- Priorice soluciones sostenibles y alineadas con las políticas de la organización.
- Si es un entorno sensible, realice una copia de seguridad antes de modificar configuraciones.

- Informe al usuario o al equipo sobre la intervención.

Paso 5: Verificar la solución e implementar medidas preventivas

Una vez aplicada la solución, es indispensable verificar que el problema se haya resuelto completamente. Además, se deben aplicar medidas para prevenir que el mismo fallo vuelva a ocurrir.

Recomendaciones:

- Revise la conectividad, el rendimiento y el comportamiento del sistema.
- Aplique actualizaciones o cambios de configuración que refuercen la estabilidad.
- Considere automatizar tareas repetitivas o generar alertas tempranas.

Paso 6: Registrar hallazgos, acciones y resultados

El último paso es documentar todo lo realizado y aprendido durante el proceso. Este paso suele ser omitido, pero va ligado a prevenir problemas, llevar un histórico de la operación de la red y servir como guía para futuras incidencias similares.

Recomendaciones:

- Use formatos estandarizados para registrar el problema, la causa, la solución y las pruebas realizadas.
- Comparta el registro con el equipo técnico.
- Archive los cambios de configuración o scripts aplicados.

Ahora es momento de aplicar la metodología a un ejemplo práctico donde definiremos un escenario de un problema frecuente en una red.

Escenario: Un usuario informa que no puede acceder a Internet desde su estación de trabajo con sistema operativo Windows.

Paso 1. Identificación del problema: se confirma que solo ese equipo está afectado, y no puede hacer ping al gateway de la red. Se conversa con el usuario y se anota la hora en qué se dio cuenta del fallo y otros detalles.

¿Qué preguntas adicionales puede realizar al usuario para recolectar información sobre el problema?

Paso 2. Teoría de causa probable: puede tener dirección IP mal asignada o el cable desconectado.

¿Qué otras teorías usted puede generar sobre las causas del problema?

Paso 3. Prueba de la teoría: se verifica con ipconfig y se detecta que el equipo tiene una IP APIPA (169.x.x.x). Se revisa en la parte posterior del equipo si los leds titilan como indicativo de conectividad. Se comprueba que el cable está desconectado.

¿Cuáles estrategias podrían llevar a comprobar sus teorías sobre las causas del problema?

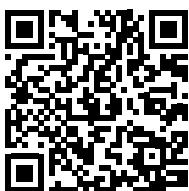
Paso 4. Plan de acción: conectar el cable correctamente y forzar renovación de IP dinámica a través de línea de comando en el terminal, usando los comandos: ipconfig /renew.

Paso 5. Verificación: el equipo recibe una IP del rango correcto y recupera la conectividad a Internet.

Paso 6. Registro: se documenta que el problema fue causado por un cable suelto y se recomienda revisar puntos de red semanalmente.

Paso a paso llegamos a la solución

Le invito a poner en práctica su comprensión sobre metodologías sistemáticas de troubleshooting mediante este ejercicio de emparejamiento. En esta actividad usted interiorizará los seis pasos que componen la metodología de resolución de problemas de red. El objetivo es que recuerde qué debe realizar en cada fase para que, con práctica, se convierta en un proceso natural en el desarrollo de sus actividades técnicas en el ámbito profesional.



Metodología de Resolución de Problemas de Red

Como pudo comprobar durante el emparejamiento, la resolución de problemas de red sigue una metodología lógica y secuencial que va desde la identificación inicial hasta la documentación final. Cada paso tiene un propósito específico y se conecta con el siguiente de manera coherente, demostrando que el troubleshooting efectivo no es casualidad sino el resultado de aplicar un proceso sistemático que minimiza errores y maximiza la eficiencia en la resolución de incidencias técnicas.

Luego de desarrollar la actividad, responda en su cuaderno de apuntes o en un documento de Word la siguiente cuestión: ¿en qué paso de la metodología hubiera hecho modificaciones/adaptaciones?, ¿por qué?

Ahora que ya conoce la metodología, reflexione sobre las fortalezas que aporta seguir una metodología para la resolución de problemas.

4.2.3. Casos de estudio para resolución de problemas

En esta sección se le presentarán cuatro casos de estudio para que usted aplique la metodología de seis pasos estudiada.

Caso 1

Escenario:

Una pequeña empresa ha instalado recientemente un nuevo switch para ampliar su red. Uno de los usuarios reporta que su conexión es extremadamente lenta, especialmente al transferir archivos a un servidor local. El problema no afecta a otros equipos.

Paso 1. Identificación del problema

El administrador verifica que el problema ocurre solo con un equipo conectado al nuevo switch. La transferencia de archivos es muy lenta, aunque no hay pérdida total de conectividad.

Paso 2. Teoría de causa probable

Podría ser una mala configuración del cable, un puerto defectuoso o un desajuste de velocidad/dúplex.

Paso 3. Prueba de la teoría

Se ejecuta el comando en el switch: show interfaces fa0/1.

La salida muestra errores de colisión y que el puerto está configurado como *full dúplex*, mientras que la tarjeta del equipo cliente fue configurada manualmente en *half duplex*.

Paso 4. Plan de acción

Cambiar la configuración en el equipo cliente para que use autonegociación o igualar los modos dúplex en ambos extremos.

Paso 5. Verificación

Se vuelve a probar la transferencia de archivos y se eliminan las colisiones. Se establece una política de estandarizar la autonegociación en toda la red.

Paso 6. Registro

Se registra el error y la solución aplicada en el historial de incidencias del equipo, recomendando revisar parámetros de velocidad y dúplex en futuras instalaciones.

Retroalimentación:

¿Cuál fue la causa concreta del problema en el caso 1?

¿Qué otras pruebas se pudieron haber realizado?

Caso 2

Escenario:

Una institución educativa conecta nuevos equipos en un laboratorio. Algunos estudiantes pueden acceder a Internet, pero otros no, a pesar de tener direcciones IP válidas.

Paso 1. Identificación del problema

Un estudiante informa que no puede navegar. El administrador verifica con ipconfig que el equipo tiene una dirección IP válida dentro de la red, pero no puede hacer ping al gateway.

Paso 2. Teoría de causa probable

El gateway predeterminado puede estar mal configurado o fuera del rango de red del host.

Paso 3. Prueba de la teoría

Se observa la configuración IP del equipo:

IPv4 Address: 192.168.10.25

Gateway predeterminado: 192.168.1.1

Claramente, el gateway no corresponde a la subred 192.168.10.0/24

Paso 4. Plan de acción

Modificar manualmente el gateway o reconfigurar el servidor DHCP para que asigne correctamente la puerta de enlace predeterminada.

Paso 5. Verificación

Una vez corregido a 192.168.10.1, el estudiante puede navegar correctamente. Se verifica la conectividad con ping y navegación en el navegador.

Paso 6. Registro

Se registra la mala configuración en el laboratorio y se revisan todos los scopes de DHCP activos para evitar conflictos.

Retroalimentación:

¿Qué otras teorías sobre las causas podría usted generar?

¿Cómo puede saber cuál es el gateway correcto para configurarlo manualmente?

Caso 3

Escenario:

Un colaborador nuevo conecta su *laptop* a la red y no logra acceder a ningún recurso. No tiene acceso a *Internet* ni al servidor compartido.

Paso 1. Identificación del problema

El usuario muestra su configuración IP. El equipo tiene una dirección 169.254.x.x, asignada automáticamente por Windows (APIPA).

Paso 2. Teoría de causa probable

El servidor DHCP puede estar inactivo, fuera de alcance o sin direcciones disponibles.

Paso 3. Prueba de la teoría

En el switch, se usa:

```
show ip dhcp binding
```

```
show ip dhcp pool
```

No se ve el registro del nuevo host.

Además, se intenta renovar manualmente la IP en el equipo:

```
ipconfig /release
```

```
ipconfig /renew
```

Sin éxito.

Paso 4. Plan de acción

Se detecta que el puerto del switch donde se conecta el equipo está deshabilitado.

Se corrige con:

interface fa0/5

no shutdown

Paso 5. Verificación

El equipo obtiene una dirección IP válida de DHCP y accede a los recursos de red.

Paso 6. Registro

Se documenta la configuración de los puertos y se etiqueta correctamente cada puerto del switch.

Retroalimentación:

¿Qué comando se usa para determinar que la interfaz del switch está desactivada?

Caso 4

Escenario:

Un equipo dentro del área administrativa puede hacer ping a direcciones IP externas (por ejemplo, 8.8.8.8), pero no puede navegar en ninguna página web usando nombres de dominio.

Paso 1. Identificación del problema

El usuario informa que "no tiene Internet", pero las pruebas muestran que puede hacer ping a servidores IP externos, lo que indica conectividad funcional.

Paso 2. Teoría de causa probable

Puede tratarse de un problema con la resolución de nombres: fallo del servidor DNS.

Paso 3. Prueba de la teoría

Desde el equipo afectado: nslookup www.google.com

La respuesta indica que el servidor DNS no responde.

Paso 4. Plan de acción

El administrador reemplaza la dirección DNS por una válida (por ejemplo, 8.8.8.8) en la configuración IP del host.

Paso 5. Verificación

El equipo ahora puede resolver nombres de dominio y navegar normalmente. Se prueba con múltiples páginas.

Paso 6. Registro

Se revisa la configuración DHCP para asegurar que entregue servidores DNS válidos. Se documenta el incidente y se actualiza la plantilla de configuración.

Retroalimentación:

Identifique otras posibles teorías sobre la causa del problema.

¿Qué otras pruebas se pueden plantear para identificar la causa real del problema?



Actividades de aprendizaje recomendadas

Es momento de aplicar sus conocimientos a través de las actividades que se han planteado a continuación:

Actividad 1. Lectura de los contenidos propuestos

Ingresé a la plataforma [Netacad](#) y revise el módulo 17; crea una red pequeña, en la cual se ven los conceptos esenciales para la planificación de una red LAN. Adicionalmente, se presenta la metodología de resolución de problemas que hemos estudiado ampliamente durante esta semana.

Estrategia de trabajo:

- Reserve un momento tranquilo para estudiar el módulo en Netacad y aproveche esta ocasión para adquirir conocimientos que fortalecerán su formación profesional.
- Registre los conceptos clave en un cuaderno o en un archivo digital, elaborando así su propio material de referencia.
- Participe en las actividades interactivas y visualice las animaciones, que hacen el aprendizaje más atractivo y facilitan la comprensión de cada tema.
- Evalúe su comprensión realizando las autoevaluaciones, y si comete algún error, no se preocupe; es una parte natural del proceso de aprendizaje y mejora continua.

Retroalimentación:

La plataforma le ayudará a reconocer las secciones del módulo que requieren una revisión más detallada antes de avanzar.

Actividad 2. ¡Solucionemos problemas de conectividad!

En esta actividad tendrá la oportunidad de desarrollar habilidades de diagnóstico, análisis y solución de problemas de conectividad en redes LAN reales, fortaleciendo su capacidad para implementar y mantener infraestructuras de telecomunicaciones eficientes, seguras y sostenibles. A través del uso de Packet Tracer en modo físico, usted aplicará sus conocimientos técnicos y procedimentales para identificar fallos, probar hipótesis, corregir configuraciones y documentar cambios, simulando entornos laborales en donde pueda aplicar la metodología estudiada esta semana.

Estrategia de trabajo:

- Revise la teoría sobre las redes LAN y la metodología de solución de problemas de red.
- Repase los comandos de configuración de dispositivos intermedios y finales.
- Repase el uso de las herramientas de diagnóstico.
- Consulte su cuaderno de ingeniería.
- Desarrolle la actividad propuesta siguiendo el guion disponible en la misma.

Práctica 17.7.7. de CCNA-1: solucione problemas de conectividad.

En esta actividad usted podrá hacer un proceso reflexivo de evaluación de causas probables para los problemas de conectividad presentados, a través de las herramientas de evaluación de conectividad.

Retroalimentación:

En esta actividad de Packet Tracer podrá ver su progreso como porcentaje, además pueden hacer clic en la pestaña *Check Results* para ver los ítems que se consideran para medir su progreso y verificar cuáles están pendientes o no están correctamente ejecutados.

Cuando acabe la práctica simulada, conteste las siguientes preguntas de reflexión:

- ¿Qué hizo primero cuando notó que no había acceso al servidor externo?, ¿qué herramienta le ayudó a validar la conectividad interna?
- ¿Qué comando fue más útil para descubrir qué interfaz tenía el problema?, ¿cómo verificó que los cambios que realizó resolvieron los problemas de conectividad?
- ¿Por qué es importante documentar los problemas encontrados y las acciones tomadas?

Actividad 3. Es hora de medir nuestro avance

En la plataforma Netacad encontrará el Examen de punto de control: Examen de creación y protección de redes pequeñas (módulos 16-17), que le propondrá cuestiones sobre la unidad 4. La evaluación puede ser realizada varias veces para medir su avance en la interiorización de conceptos fundamentales de redes.

Tiene la oportunidad de realizar la evaluación correspondiente a los módulos del CCNA 1 en Cisco Netacad. Esta actividad forma parte de los requisitos esenciales para la aprobación del curso y le permitirá, si cumple con los criterios establecidos, acceder a una microcertificación oficial. Esta distinción puede mejorar significativamente su perfil laboral. Le animo a asumir este desafío con entusiasmo y confianza.

Actividad 4. Autoevaluación 4

Estimado estudiante, a continuación, usted tiene unas preguntas para que pueda medir su nivel de conocimiento sobre los contenidos de la unidad 4.

Estrategia de trabajo

- Resolver la autoevaluación sin revisar material adicional.
- Revisar el solucionario disponible al final de la guía.

Una vez comprendida la actividad, realice la autoevaluación para comprobar sus conocimientos.



Autoevaluación 4

Lea cada pregunta con atención y seleccione la alternativa que considere correcta.

1. Una mala configuración en un *router* o *switch*, como dejar contraseñas predeterminadas o habilitar servicios innecesarios, es una vulnerabilidad de configuración que puede abrir puertas a intrusos, comprometiendo la confidencialidad y la integridad de la red.
 - a. Verdadero.
 - b. Falso.
2. Los ataques de Denegación de Servicio (DoS/DDoS) se enfocan principalmente en comprometer la integridad de los datos, alterando la información durante la transmisión o el almacenamiento.
 - a. Verdadero.
 - b. Falso.

3. Un usuario informa que no puede acceder a *Internet* desde su estación de trabajo con sistema operativo Windows. Después de la identificación del problema, se verifica con ipconfig que el equipo tiene una IP APIPA (169.254.x.x) y, al revisar físicamente, se comprueba que el cable de red está desconectado. Siguiendo la metodología de resolución de problemas, ¿cuál sería el siguiente paso lógico después de determinar la causa del problema?
- Registrar los hallazgos y las acciones realizadas en un documento oficial.
 - Establecer un plan de acción para conectar el cable y renovar la dirección IP.
 - Establecer una nueva teoría de causas probables, como un servidor DHCP inactivo.
 - Verificar la solución e implementar medidas preventivas para evitar el mismo fallo en el futuro.
4. Una pequeña empresa con diez empleados está planificando la expansión de su red. Actualmente, sus necesidades son básicas, pero prevén un crecimiento futuro y la incorporación de servicios críticos que requerirán mayores capacidades de administración, seguridad y monitoreo. Basándose en los factores de selección de componentes de red, ¿qué tipo de *switch* sería el más adecuado para esta empresa, considerando una visión sostenible y a futuro?
- Un *switch* no gestionable, priorizando un bajo costo inicial sin considerar la escalabilidad.
 - Un *switch* de 12 puertos Fast Ethernet, ya que es suficiente para el número actual de empleados.
 - Un *switch* gestionable con soporte para Gigabit Ethernet y funciones avanzadas, invirtiendo en escalabilidad y capacidad.
 - Un *switch* de 8 puertos con red inalámbrica.

5. En la configuración de dispositivos intermediarios como routers y switches, se recomienda el uso de SSH en lugar de Telnet para los accesos seguros. ¿Cuál es la principal ventaja de SSH sobre Telnet en términos de seguridad?
- a. SSH es más fácil de configurar para los administradores de red.
 - b. SSH consume menos recursos del dispositivo, mejorando el rendimiento.
 - c. SSH cifra las credenciales y los datos de la sesión, protegiéndolos de intercepciones no autorizadas.
 - d. Telnet ofrece mayor compatibilidad con dispositivos de red antiguos, lo que lo hace más versátil.
6. La seguridad de redes se basa en la tríada CIA (Confidencialidad, Integridad y Disponibilidad). Sin embargo, en la actualidad, se han definido algunos objetivos complementarios para fortalecer la protección. ¿Cuáles de los siguientes son considerados objetivos adicionales de la seguridad en redes? (Seleccione dos opciones correctas).
- a. QoS (Quality of Service).
 - b. No repudio.
 - c. Escalabilidad.
 - d. Autenticación.

7. Un ingeniero de redes está realizando una auditoría y descubre que varios routers de la organización tienen *firmware* obsoleto con fallos de seguridad conocidos. Además, se da cuenta de que la política de la empresa sobre el cambio de contraseñas es deficiente, y muchos dispositivos aún tienen contraseñas predeterminadas de fábrica. ¿Qué categorías de vulnerabilidades se están manifestando en este escenario? (Seleccione dos opciones correctas).
- Vulnerabilidades de política de seguridad.
 - Vulnerabilidades de configuración.
 - Vulnerabilidades físicas.
 - Vulnerabilidades tecnológicas.
8. Si una red empresarial fuera comprometida durante 24 horas debido a un ataque de seguridad, ¿cuáles de las siguientes consecuencias son las más probables que enfrente la empresa, basándose en el análisis del impacto de un fallo de seguridad? (Seleccione dos opciones correctas).
- Un aumento significativo en la productividad de los empleados.
 - Pérdidas de productividad y posibles daños reputacionales.
 - Fuga de información crítica e interrupciones totales del servicio.
 - Una reducción en los costos operativos de TI debido a la simplicidad de la red.

9. Empareje cada tipo de ataque de red con su descripción o efecto principal, según la clasificación de ataques por tipo de daño ocasionado.

Ataque	Descripción
1. Malware.	A. Se refiere a la intercepción o modificación de las comunicaciones entre dos partes sin que estas lo perciban.
2. Acceso no autorizado.	B. Infiltración en los sistemas para causar daño o extraer información sin el consentimiento del usuario.
3. Denegación de Servicio (DoS/DDoS).	C. Consiste en saturar un servidor o red con tráfico excesivo hasta que el servicio colapsa.
4. Man-in-the-Middle (MitM).	D. Buscan eludir los mecanismos de autenticación para tomar el control de sistemas o datos.

10. Relacione cada acción o propósito con el paso correspondiente de la metodología de seis pasos para la resolución de problemas en redes de datos.

Pasos de la metodología	Propósito
1. Paso 1. Identificar el problema.	A. Documentar todo lo realizado y aprendido durante el proceso para servir como guía y prevenir problemas futuros.
2. Paso 3. Poner a prueba la teoría para determinar la causa.	B. Recopilar información detallada sobre el síntoma del problema, a menudo mediante conversación con el usuario y herramientas de diagnóstico.
3. Paso 5. Verificar la solución e implementar medidas preventivas.	C. Realizar pruebas específicas, como modificar configuraciones o cambiar componentes, haciendo un solo cambio a la vez.
4. Paso 6. Registrar hallazgos, acciones y resultados.	D. Confirmar que el problema se ha resuelto completamente y aplicar actualizaciones o cambios para reforzar la estabilidad.

[Ir al solucionario](#)



Sem 9

Sem 10

Sem 11

Sem 12

Sem 13

Sem 13

Sem 14

Sem 15

Sem 16



Semana 16



Actividades finales del bimestre

Para consolidar los conocimientos adquiridos durante las semanas 9 a la 15, lo invito a revisar la siguiente presentación interactiva que resume los contenidos estudiados.

[Raposo de segundo bimestre.](#)

Como pudo constatar a través de esta presentación, el segundo bimestre construyó una progresión lógica desde los mecanismos básicos de comunicación hasta la implementación práctica de redes completas. La integración de conceptos, desde ICMP y resolución de direcciones hasta TCP/UDP, capas superiores y seguridad, demuestra cómo cada elemento técnico se interconecta para formar sistemas de red funcionales y seguros. Esta visión panorámica confirma que domina tanto los fundamentos teóricos como su aplicación práctica en el diseño e implementación de infraestructuras de red robustas.

Falta poco para finalizar el segundo bimestre, por esta razón estamos en un momento clave para repasar y consolidar los conocimientos adquiridos durante estas siete semanas de trabajo. Le animo cordialmente a tomarse un tiempo para reforzar los protocolos, técnicas y herramientas que hemos estudiado, con el fin de prepararse de manera sólida para la evaluación bimestral. Además, una comprensión clara de estos contenidos le brindará una base firme para avanzar con éxito en el resto de la carrera.

Durante esta semana, le invito a revisar sus apuntes y su cuaderno de ingeniería, repasar las grabaciones de las tutorías semanales y practicar las configuraciones utilizando las actividades sugeridas.

[Índice](#)[I Bimestre](#)[II Bimestre](#)[Solucionario](#)[Referencias](#)

Estas acciones le permitirán afianzar su aprendizaje y detectar posibles dudas. Recuerde que estoy disponible para acompañarle en este proceso, por lo que le animo a compartir cualquier inquietud o consulta durante la próxima sesión de tutoría. Aproveche este espacio como una oportunidad para fortalecer su preparación.

¡Felicitaciones! Ha terminado con éxito las unidades de la asignatura Introducción a las redes.

Confío plenamente en que su esfuerzo y constancia se reflejarán en logros académicos significativos.



Actividades de aprendizaje recomendadas

Es hora de reforzar los conocimientos adquiridos resolviendo las siguientes actividades:

Actividad 1. ¡Desafío de habilidades!

Como actividad de cierre del segundo bimestre de la materia de Introducción a las redes, y con la finalidad de integrar de forma práctica los conocimientos adquiridos sobre direccionamiento, configuración y seguridad de redes LAN, le propongo implementar una red funcional en Packet Tracer. La red incluye múltiples subredes, dispositivos de red configurados con IPv4 e IPv6, y políticas básicas de protección de acceso. Al finalizar la actividad, usted habrá puesto a prueba sus habilidades para garantizar una infraestructura de telecomunicaciones eficiente, segura y sostenible, alineada a los estándares del entorno profesional.

Estrategia de trabajo:

- Revise la teoría sobre direccionamiento, subredes y medidas de seguridad LAN.

- Revise los procesos y comandos de configuración de dispositivos intermedios y finales.
- Tenga a mano su cuaderno de ingeniería, le será de mucha utilidad para recordar los comandos y la sintaxis apropiada de cada uno de ellos.
- Desarrolle la actividad siguiendo el guion detallado que encontrará en el archivo.

[Práctica 17.8.2. de CCNA-1: desafío de integración de habilidades.](#)

Retroalimentación:

Esta actividad en Packet Tracer le brindará una retroalimentación inmediata, mostrándole su progreso como porcentaje. Además, podrá hacer clic en la pestaña “Check Results”, para ver los ítems considerados para medir su avance y verificar cuáles están pendientes o no se ejecutaron correctamente.

Al terminar la actividad, conteste las siguientes preguntas de retroalimentación:

- ¿Cómo decidió la forma de dividir la red 192.168.0.0/24 para los distintos departamentos?
- ¿Qué importancia tiene no desperdiciar direcciones IP?
- ¿Por qué es importante configurar tanto las direcciones IPv4 como IPv6 en los dispositivos?
- ¿Cree usted que IPv6 ya es necesario en las redes actuales?, ¿cómo afecta esto la escalabilidad de la red?
- ¿Qué ventajas aporta usar SSH y usuarios con niveles de privilegio definidos?

- ¿Cómo un administrador de red sabe que la red está correctamente implementada?



4. Solucionario

Autoevaluación 1		
Pregunta	Respuesta	Retroalimentación
1	F	<p>Internet se caracteriza por tener una administración distribuida, lo que significa que no pertenece a un solo dueño ni es controlada por una única entidad, sino que su funcionamiento se basa en el cumplimiento de estándares y tecnologías homogéneas por parte de múltiples organizaciones y proveedores de servicios.</p>
2	F	<p>Las contraseñas configuradas con el comando <code>password</code> se almacenan en texto plano en el archivo de configuración. Para cifrar estas credenciales y protegerlas de lecturas no autorizadas, es necesario añadir el comando <code>service password-encryption</code>.</p>
3	b	<p>La Calidad de Servicio (QoS) se refiere a la capacidad de una red para priorizar el tráfico de datos, como el de voz y video en tiempo real, sobre otros tipos de tráfico menos críticos. Esto es fundamental para asegurar que los servicios esenciales mantengan la velocidad y disponibilidad requeridas, especialmente en entornos de red congestionados, mejorando la experiencia del usuario y la productividad.</p>
4	c	<p>La capa de sesión (capa 5) del modelo OSI es la encargada de establecer, administrar y finalizar las sesiones o diálogos entre las aplicaciones de diferentes hosts. Además, se ocupa de la sincronización de la comunicación y la gestión de puntos de restauración para asegurar la fluidez del intercambio de datos.</p>

Autoevaluación 1

Pregunta	Respuesta	Retroalimentación
5	c	Para agilizar la navegación en la estructura jerárquica de Cisco IOS, los comandos <i>end</i> o la combinación de teclas Ctrl + Z son atajos muy útiles que permiten salir de cualquier modo de subconfiguración y volver directamente al modo EXEC privilegiado (#), sin necesidad de usar <i>exit</i> múltiples veces.
6	a	La integridad es uno de los tres requisitos fundamentales de la seguridad de la información. Su propósito es asegurar que los datos no sean alterados o manipulados en su viaje a través de la red, garantizando que lo que se envía es exactamente lo que se recibe. La confidencialidad se refiere a que solo los usuarios autorizados puedan acceder a la información, y la disponibilidad asegura que la información y los servicios estén accesibles cuando se necesiten. La autenticidad es un concepto relacionado con la verificación de la identidad, pero no es uno de los tres requisitos fundamentales mencionados explícitamente en el contexto de la protección de las estructuras de datos durante el tránsito.
7	a y c	La elección del medio de interconexión (cableado o inalámbrico) es un paso crítico en el diseño de redes. Los factores clave a considerar incluyen la distancia máxima o alcance que se necesita cubrir, el ambiente donde se desplegará la red, la capacidad de transmisión de datos o velocidad requerida, y el costo total (del medio y la instalación). El sistema operativo del dispositivo final y los modelos de madurez de sistemas no son factores directos para la selección del medio físico.



Autoevaluación 1		
Pregunta	Respuesta	Retroalimentación
8	a y d	<p>SSH es el protocolo preferido para el acceso remoto en entornos de producción debido a su robusta seguridad. Ofrece cifrado completo de todo el tráfico (incluyendo credenciales) utilizando algoritmos como AES, protegiendo contra espionaje y manipulación. Además, integra funcionalidades para la copia segura de archivos como SCP/SFTP, lo que no está disponible en Telnet, el cual transmite en texto plano y carece de dichas funciones. Aunque SSH puede tener una mayor complejidad en la gestión de claves y un uso ligeramente mayor de CPU debido al cifrado, sus beneficios de seguridad son superiores.</p>
9	1-B 2-C 3-A 4-D	<p>La clasificación de las redes según su alcance geográfico es un principio fundamental para comprender la infraestructura de telecomunicaciones. Desde las Redes de Área Personal (PAN) que cubren unos pocos metros, hasta las Redes de Área Global (GAN) con cobertura mundial, cada tipo de red está diseñada para necesidades y escalas específicas, influenciando el diseño y las tecnologías empleadas.</p>
10	1-B 2-C 3-A	<p>Comprender la arquitectura de los dispositivos de red es esencial para su configuración y gestión. El <i>hardware</i> es la base física. El Kernel es el sistema operativo central que gestiona los recursos y el reenvío de datos, y el <i>Shell</i> (a través de la CLI o GUI), es la interfaz que permite a los administradores interactuar y configurar el dispositivo.</p>

[Ir a la autoevaluación](#)

Autoevaluación 2

Pregunta	Respuesta	Retroalimentación
1	F	Una interfaz en estado "down down" indica que la capa física no está operativa y, por lo tanto, el protocolo de línea tampoco se ha podido establecer. Las causas más comunes para un estado "down down" son la ausencia de un cable, un cable dañado, una discrepancia de velocidad o dúplex entre los dispositivos conectados, o que la interfaz esté administrativamente apagada (lo que se corrige con el comando <code>no shutdown</code>). Un problema de configuración de la dirección IP (como una máscara incorrecta o una IP duplicada), generalmente ocasionaría un estado "up down" (físicamente activa, pero con un problema de protocolo de línea).
2	V	El protocolo IPv6 fue diseñado con una cabecera más simple y de tamaño fijo (40 bytes) en comparación con la cabecera variable de IPv4. La eliminación de campos como la suma de comprobación (<code>checksum</code>), que en IPv4 debe recalcularse en cada router por el decremento del TTL, y la ausencia de campos de opciones variables, reduce la carga de procesamiento en los routers intermedios. Esto, a su vez, contribuye a una menor latencia y un mayor rendimiento general en redes con múltiples saltos, lo cual es una ventaja significativa en el diseño de redes modernas.
3	d	La fibra óptica multimodo proporciona alta velocidad (1-100 Gbps) y total inmunidad a EMI, siendo ideal para distancias de hasta 550 m. Esta opción se ajusta perfectamente a los 300 m y a los requisitos de rendimiento de un centro de datos, siendo la solución más eficiente y rentable. El cable UTP tiene distancia de hasta 100 m, el cable coaxial tiene menos velocidad y la fibra monomodo está diseñada para distancias mayores.

Autoevaluación 2

Pregunta	Respuesta	Retroalimentación
4	c	El problema se centra en el descarte de tramas más pequeñas que el tamaño mínimo permitido y la propagación de tramas corruptas que se da cuando se utiliza el método de commutación de corte y avance rápido, ya que el switch comienza a reenviar la trama tan pronto como ha leído la dirección MAC de destino (los primeros 6 bytes), sin esperar el resto de la trama ni realizar ninguna verificación de errores.
5	a	El número de hosts válidos se calcula con la fórmula $2^n - 2$, donde n es el número de bits dedicados a la porción de host. Un prefijo /26 significa que 26 bits son para la red, dejando $32 - 26 = 6$ bits para la porción de host (n=6). Esto resulta en $2^6 - 2 = 64 - 2 = 62$ hosts válidos. Esta opción cumple el requisito de 60 hosts y es la más eficiente en el uso de direcciones.
6	a y b	Las subredes permiten ajustar el tamaño de redes a los requerimientos de cada red, reduciendo el dominio de broadcast y evitando el desperdicio de direcciones, sobre todo en el método VLSM.
7	a y c	El router puede indicar DHCPv6 con estado, indica al host que debe obtener su dirección global de unidifusión y otros parámetros de configuración de un servidor DHCPv6; y, también puede anunciar Autoconfiguración de direcciones sin estado (SLAAC) donde el dispositivo debe generar automáticamente su dirección global de unidifusión IPv6 combinando el prefijo de red anunciado por el router con su propio ID de interfaz.
8	c y d	El comando show arp muestra las asociaciones entre direcciones IPv4 y sus correspondientes direcciones MAC aprendidas por ARP, mientras que show ipv6 neighbors muestra la caché de vecinos para IPv6, aprendidas por NDP.

Autoevaluación 2		
Pregunta	Respuesta	Retroalimentación
9	1-B	El campo TTL es un contador que se decrementa en cada salto. Si llega a 0, el router descarta el paquete para evitar bucles. La longitud de cabecera indica dónde termina la cabecera y dónde comienzan los datos. El campo protocolo identifica el protocolo de la capa de transporte al que se entregará la carga útil del paquete una vez que este llegue a su destino. Los campos Identificación, Indicador y Desplazamiento de fragmentos trabajan en conjunto para manejar la fragmentación de paquetes IPv4.
	2-C	
	3-D	
	4-A	
10	1-A	El protocolo IP opera de manera independiente del tipo de medio físico subyacente, por lo que el mismo paquete puede viajar a través de diversas tecnologías. El direccionamiento lógico jerárquico permite que los routers almacenen rutas para bloques enteros de redes (prefijos) en sus tablas de enrutamiento, en lugar de rutas individuales para cada host. El protocolo IP no establece circuitos virtuales previos, no garantiza la entrega de paquetes, su orden de llegada, ni evita la duplicación. La fragmentación asegura que el paquete pueda atravesar enlaces con diferentes límites de MTU.
	2-C	
	3-B	
	4-D	

[Ir a la autoevaluación](#)

Autoevaluación 3

Pregunta	Respuesta	Retroalimentación
1	V	El protocolo UDP está diseñado para ser ligero y rápido, sacrificando la fiabilidad y el control de orden para minimizar la sobrecarga y la latencia. La ausencia de números de secuencia específicos por segmento (a diferencia de TCP), contribuye a esta ligereza, haciendo que UDP sea adecuado para aplicaciones que pueden tolerar cierta pérdida de datos o reordenamiento, pero no demoras, como el <i>streaming</i> en tiempo real o la voz sobre IP.
2	F	El método <i>three-way handshake</i> establece la conexión TCP y asegura que ambos extremos estén sincronizados y listos para intercambiar datos de manera confiable. Sin embargo, la finalización ordenada de una conexión TCP se realiza mediante un proceso separado conocido como el <i>four-way handshake</i> . Por lo tanto, el establecimiento no garantiza el cierre ordenado.
3	d	El protocolo UDP es la elección más adecuada para escenarios donde la velocidad y la baja latencia son prioritarias sobre la fiabilidad absoluta. Su diseño sin conexión y la mínima sobrecarga de cabecera lo hacen eficiente para el envío de notificaciones de bajo volumen.
4	c	Los números de secuencia en TCP son críticos para garantizar la entrega ordenada de los datos. TCP numera cada byte del flujo de datos, permitiendo al receptor detectar segmentos fuera de orden y mantenerlos en cola hasta que todos los segmentos lleguen y puedan reensamblarse correctamente, asegurando la integridad y el orden del mensaje original para la capa de aplicación. La multiplexación/demultiplexación gestiona qué proceso recibe los datos, el control de flujo previene el desbordamiento del receptor, y el <i>checksum</i> detecta alteraciones, pero solo los números de secuencia y el reensamblaje resuelven el problema del orden y la completitud del mensaje a partir de segmentos desordenados.

Autoevaluación 3

Pregunta	Respuesta	Retroalimentación
5	c	<p>La capa de presentación se encarga de la conversión de formatos de datos, compresión y cifrado/descifrado para garantizar que los datos sean interpretables entre sistemas con diferentes representaciones internas.</p> <p>Las otras opciones describen funciones de la capa de transporte (multiplexación, control de flujo), o conceptos de la capa de red/enlace (aislamiento de dominios de broadcast), no de la capa de presentación.</p>
6	a y c	<p>Para una aplicación de mensajería instantánea, las funciones clave serían la sincronización y la recuperación de sesión de la capa de sesión para reanudar la comunicación desde el último punto conocido sin perder el hilo de la conversación o los datos, especialmente en mensajes extensos. Y la traducción de formatos de datos y el cifrado/descifrado de la capa de presentación para asegurar que los mensajes sean legibles entre diferentes sistemas y que la información transmitida mantenga su confidencialidad.</p>
7	a y b	<p>Para dispositivos IoT con recursos limitados y el envío constante de pequeños volúmenes de datos, el protocolo UDP es el más adecuado debido a sus características operación sin conexión, lo que reduce significativamente la sobrecarga de procesamiento y los recursos necesarios en dispositivos con limitaciones, haciéndolo más eficiente para envíos rápidos y breves; y, la minimización de latencia y sobrecarga lo que es crucial para la telemetría.</p>
8	b y c	<p>El diagrama de secuencia para cargar una página web con HTTP muestra claramente que el URL que se escribe en el navegador es resuelto por el servidor DNS, quien devuelve la dirección IP del servidor. Esta resolución es un paso previo y necesario antes de que el cliente pueda iniciar una conexión TCP con el servidor web usando su dirección IP. Luego, a través de TCP, el cliente establece la conexión con el servidor usando el saludo de tres vías. El cliente inicia el protocolo HTTP con el método GET.</p>

Autoevaluación 3

Pregunta	Respuesta	Retroalimentación
9	1-C	La multiplexación y demultiplexación permite que múltiples aplicaciones comparten la misma conexión de red, identificando cada flujo con números de puerto. La segmentación y reensamblaje se encarga de dividir los datos grandes en segmentos más pequeños para un transporte eficiente y de volver a unirlos en el destino.
	2-A	La verificación de integridad (<i>checksum</i>) proporciona un mecanismo para detectar si los datos han sido corrompidos durante la transmisión. Y la identificación de aplicaciones utiliza números de puerto para dirigir los datos a la aplicación o servicio correcto en el host de destino.
	3-D	
	4-B	
10	1-B	HTTP utiliza TCP puerto 80 y 443 para HTTPS para garantizar la entrega confiable y ordenada de una página web. RTP/RTCP (en VoIP) utiliza UDP con puertos dinámicos porque en el tráfico de voz y video en tiempo real, el retardo es crítico. El DNS mayoritariamente utiliza UDP en el puerto 53. DHCP utiliza UDP en los puertos 67 y 68 para asignar automáticamente direcciones IP.
	2-D	
	3-A	
	4-C	

[Ir a la autoevaluación](#)

Autoevaluación 4

Pregunta	Respuesta	Retroalimentación
1	V	Dejar contraseñas por defecto, servicios innecesarios habilitados, puertos abiertos o permisos excesivos, son errores de configuración comunes que facilitan el acceso no autorizado desde la red local o incluso desde Internet.
2	F	Los ataques de Denegación de Servicio (DoS/DDoS) tienen como objetivo la interrupción total del servicio comprometiendo la disponibilidad de la red o los servicios, no la integridad de los datos.
3	b	El escenario describe la culminación del paso 3: poner a prueba la teoría para determinar la causa, donde se ha confirmado que el cable está desconectado. El siguiente paso en la metodología es el paso 4: establecer un plan de acción e implementar la solución. Conectar el cable y forzar la renovación de la IP dinámica son acciones directas de este plan.
4	c	Un switch gestionable ofrece mayores capacidades de administración, seguridad y monitoreo. Además, la velocidad (Gigabit Ethernet en lugar de Fast Ethernet) es crucial para el tráfico de archivos pesados o video, y la capacidad de expansión es fundamental para el crecimiento futuro, evitando la necesidad de reemplazar equipos en poco tiempo. La opción A no considera el crecimiento, la B no es adecuada para servicios críticos o crecimiento, y la D es incorrecta, porque no satisface la demanda actual.
5	c	La seguridad en redes es fundamental y un pilar para la formación del ingeniero, y el cifrado es una estrategia clave contra amenazas. Telnet, al transmitir información en texto plano, es vulnerable a la intercepción, mientras que SSH garantiza la confidencialidad de las comunicaciones.
6	b y d	Además de la tríada CIA, se han definido objetivos complementarios como la autenticación, que consiste en verificar la identidad de usuarios y dispositivos, y el No repudio, que trata de impedir que un emisor legítimo niegue su participación en un proceso. También auditoría, pero no era una opción en la pregunta.

Autoevaluación 4		
Pregunta	Respuesta	Retroalimentación
7	b y d	<p>El <i>firmware</i> obsoleto con fallos conocidos se clasifica como una vulnerabilidad tecnológica, ya que se deriva directamente de la naturaleza del <i>software</i> y la falta de actualizaciones. La presencia de contraseñas predeterminadas de fábrica en los dispositivos es un claro ejemplo de vulnerabilidad de configuración, resultado de no ajustar los valores por defecto para un entorno de producción.</p>
8	b y c	<p>Un fallo de seguridad puede paralizar por completo los procesos operativos de una empresa, y que el impacto económico se traduce en pérdidas de productividad, fuga de información crítica, daños reputacionales y, en muchos casos, interrupciones totales del servicio.</p>
9	1-B 2-D 3-C	<p>El <i>malware</i> se describe como <i>software</i> que se infiltra para causar daño o extraer información. El acceso no autorizado busca evadir la autenticación para tomar control. La Denegación de Servicio satura la red hasta que colapsa. Y el <i>Man-in-the-Middle</i> intercepta o modifica comunicaciones.</p>
10	4-A 1-B 2-C 3-D 4-A	<p>Cada emparejamiento corresponde a la descripción detallada de cada paso en la metodología propuesta por Cisco Networking Academy. El paso 1 se enfoca en la identificación y recopilación de información. El paso 3 se centra en las pruebas controladas para confirmar la causa. El paso 5 se dedica a la verificación y la prevención de recurrencias. Finalmente, el paso 6 es crucial para documentar y aprender de la experiencia.</p>

Ir a la autoevaluación



5. Glosario

- Anycast: técnica donde un paquete se envía a múltiples destinos, pero solo el más cercano responde.
- ARP (*Address Resolution Protocol*): Protocolo que traduce direcciones IP a direcciones MAC.
- Broadcast: envío de paquetes a todos los dispositivos de una red.
- CIDR (*Classless Inter-Domain Routing*): método para asignación flexible de direcciones IP.
- DHCP (*Dynamic Host Configuration Protocol*): asigna direcciones IP dinámicamente a dispositivos en red.
- DNS (*Domain Name System*): sistema que traduce nombres de dominio a direcciones IP.
- Ethernet: tecnología de red de área local (LAN) que opera en la capa de enlace.
- Firewall: sistema que filtra el tráfico de red según reglas de seguridad.
- FTP (*File Transfer Protocol*): Protocolo para la transferencia de archivos.
- HTTP (*HyperText Transfer Protocol*): Protocolo de la capa de aplicación utilizado en la web.

- HTTPS (*HTTP Secure*): variante segura de HTTP que utiliza cifrado TLS/SSL.
- ICMP (*Internet Control Message Protocol*): Protocolo de mensajes de control de la red; usado en diagnósticos como ping.
- IP (*Internet Protocol*): Protocolo de la capa de red que direcciona y envía paquetes.
- IPv4: versión del protocolo IP con direcciones de 32 bits.
- IPv6: nueva versión del protocolo IP con direcciones de 128 bits.
- MAC (*Media Access Control*): dirección física única de una interfaz de red.
- MTU (*Maximum Transmission Unit*): tamaño máximo de paquete que puede transmitirse sin fragmentación.
- Multicast: envío de un solo paquete a un grupo específico de dispositivos.
- NAT (*Network Address Translation*): traduce direcciones IP privadas a públicas para acceder a *Internet*.
- OSI: modelo de referencia con siete capas que guía el diseño de redes y protocolos.
- QoS (*Quality of Service*): conjunto de tecnologías que garantizan una calidad mínima de transmisión.
- Router: dispositivo de capa de red que enruta paquetes entre redes.
- SMTP (*Simple Mail Transfer Protocol*): Protocolo de envío de correo electrónico.

- *Subnetting*: técnica para dividir una red IP en subredes más pequeñas.
- *Switch*: dispositivo de capa de enlace que filtra y reenvía tramas dentro de una red LAN.
- *TCP (Transmission Control Protocol)*: Protocolo de transporte orientado a la conexión y confiable.
- *TCP/IP*: conjunto de protocolos fundamentales para el funcionamiento de *Internet*.
- *TTL (Time To Live)*: valor que limita el número de saltos que un paquete puede dar.
- *UDP (User Datagram Protocol)*: Protocolo de transporte sin conexión y con menor sobrecarga.



6. Referencias bibliográficas

Ariganello, E. (2020). *Redes Cisco: guía de estudio para la certificación CCNA 200-301* (1st ed.). RA-MA Editorial. <https://elibro.net/es/ereader/bibliotecaupl/222695>

CCNA-1. (2020). CCNA v7.0: Introducción a las Redes. In *Cisco Certified Network Associate*. Cisco Network Academy. <https://www.netacad.com/es/dashboard>

Cisco. (2025). *Networking Software (IOS & NX-OS) - Cisco IOS*. <Https://Www.Cisco.Com/c/En/Us/Products/Ios-Nx-Os-Software/Ios-Software-Releases-Listing.Html>.

DARPA, P. (1981). RFC 791_ Internet Protocol. In <https://www.rfc-es.org/rfc/rfc0791-es.txt>.

Fernández, R. (2024). *El uso de Internet a nivel mundial – Datos estadísticos*. <Https://Es.Statista.Com/Temas/9795/El-Uso-de-Internet-En-El-Mundo/#editorsPicks>.

Hays. (2025). *10 empleos tecnológicos que se prevé que surjan hasta 2030*. <Https://Www.Hays.Cl/Consejos-de-Carrera/Articulo/10-Empleos-Tecnologicos-Que-Se-Preve-Que-Surjan-Hasta-2030>.

IEEE. (2022). *IEEE Standard for Ethernet*. IEEE. <https://doi.org/10.1109/IEEESTD.2022.9844436>

IETF. (1989). RFC 1122: Requirements for Internet Hosts – Communication Layers. In <https://datatracker.ietf.org/doc/html/rfc1122#page-8>.

- Institut Sa Palomera. (2020). *Introducción a redes*. <Https://Www.Sapalomera.Cat/Moodlecf/RS/1/Index.Html>.
- ISO. (1994). ISO/IEC 7498-1:1994. In <https://www.iso.org/es/contents/data/standard/02/02/20269.html?browse=tc>.
- Kurose, J. F., & Ross, K. (2022). *Computer networking: a top-down approach* (8th ed.). Pearson.
- Liberatori, M. C. (2016). *Redes de datos y sus protocolos*. Editorial de la Universidad Nacional de Mar del Plata.
- Morgan, S. (2024, February 5). *Top 10 Cybersecurity Predictions and Statistics For 2024*. <Https://Cybersecurityventures.Com/Top-5-Cybersecurity-Facts-Figures-Predictions-and-Statistics-for-2021-to-2025/>.
- Sánchez Rubio, M. (2020). *Redes de computadoras*. Alcalá de Henares: Universidad de Alcalá, Servicio de Publicaciones. <https://elibro.net/es/ereader/bibliotecaupl/131606>
- Statista. (2025). Número de usuarios de Internet por país en América Latina en febrero de 2025. <Https://Es.Statista.Com/Estadisticas/1073677/Usuarios-Internet-Pais-America-Latina/>.
- Tanenbaum, A., & Wetherall, D. (2021). *Computer Networks, Global Edition* (6a ed.). Pearson.
- WEForum. (2025). The Future of Jobs Report 2025. In <https://www.weforum.org/publications/the-future-of-jobs-report-2025/>.



7. Anexos

Anexo 1. Cómo crear una cuenta en academia NETACAD

¡Inicie su aprendizaje en redes con Cisco Packet Tracer!

Para comenzar a trabajar con esta poderosa herramienta de simulación de redes, necesitará crear una cuenta en la academia NETCAD de Cisco y descargar el software Packet Tracer. Además, podrá acceder a cursos gratuitos que le otorgarán certificaciones digitales.

A continuación, se detallan los pasos necesarios para configurar su entorno de aprendizaje:

1. Acceda a la academia NETACAD

Instrucciones:

- a. Acceda a la página web: www.netacad.com/es/
- b. Seleccione la esquina superior izquierda, en la opción: **Iniciar Sesión**
- c. Luego para crear la cuenta, seleccione la opción: **Inscríbase**

Figura 1
Interfaz de NETACAD



Nota. Ludeña, P., 2025.

2. Cree su cuenta en la academia NETACAD

Instrucciones:

- Llene la información personal solicitada y coloque **Continuar**.

Figura 2

Interfaz para inscribirse en NETACAD – datos demográficos

The screenshot shows a registration form titled "Inscríbase". At the top right is a language selection "Español (Spanish) ▾". Below it is a "Volver" button with a left arrow icon. The main title "Inscríbase" is underlined. A sub-instruction "Podrá comenzar las clases tan pronto como se registre." is displayed. Below this, there's a "Registrese con" section with a "Google" button. The "Crear nueva cuenta" section is highlighted with a red border. It contains two dropdown menus: "Su país o región de residencia" (Ecuador) and "Estado" (Loja). Another pair of dropdown menus shows "Año de nacimiento" (2000) and "Mes de nacimiento" (Mayo). At the bottom is a blue "Continuar" button.

Nota. Ludeña, P., 2025.

- b. Para llenar la información personal solicitada, use su correo institucional, cree una contraseña segura de acuerdo con las indicaciones de la plataforma y coloque **Crear Cuenta**.

Figura 3

Interfaz para inscribirse en NETACAD – datos del nuevo usuario

Inscribase

Podrá comenzar las clases tan pronto como se registre.

Regístrate con



Crear nueva cuenta

Nombre: Juan	Apellido: Perez
Correo electrónico: jperez@utpl.edu.ec	
Contraseña: <input type="password"/>	
<input type="checkbox"/> Requisitos de la contraseña.	
Confirmar contraseña: <input type="password"/>	

Crear cuenta

Nota. Ludeña, P., 2025.

- c. Acepte los términos y condiciones, y haga clic en **Aceptar y continuar**, como se indica en la figura.
- d. Con esto ya ha creado su cuenta y puede empezar a revisar la información de la página de la academia.

Figura 4

Términos y condiciones



Nota. Ludeña, P., 2025.

3. Descargue e instale Packet Tracer

Instrucciones:

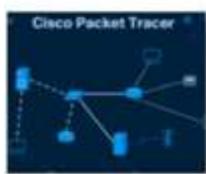
- a. Acceda a la página web: <https://www.netacad.com/resources/lab-downloads?courseLang=es-XL>
- b. Aquí accederá al **Centro de recursos** donde podrá descargar

Packet Tracer y encontrará las instrucciones de instalación.

Figura 5

Cisco Packet Tracer

Recursos de aprendizaje



Cisco Packet Tracer

Cisco Packet Tracer, una innovadora herramienta de simulación de configuración de redes, lo ayuda a perfeccionar sus habilidades de configuración de redes desde su escritorio. Use Packet Tracer para experimentar mientras construye, administra y asegura infraestructuras.

Para obtener e instalar su copia de Cisco Packet Tracer, siga estos sencillos pasos:

Paso 1. Descargue la versión de Packet Tracer que necesita

[Packet Tracer 8.3.2 Mac OS X 64Bit](#)
[Packet Tracer 8.3.2 Ubuntu 64Bit](#)
[Packet Tracer 8.3.2 Windows 64Bit](#)

Paso 2. Inicie el programa de instalación de Packet Tracer.

Paso 3. Inicie Cisco Packet Tracer seleccionando el ícono apropiado.

Paso 4. Cuando se le solicite, haga clic en el botón verde Sígueme. ¡Listo!

Paso 5. Se iniciará Cisco Packet Tracer y estará listo para explorar sus funciones.

Si necesita más orientación, siga las [Instrucciones de descarga e instalación de Cisco Packet Tracer](#).

Nota. Ludeña, P., 2025.

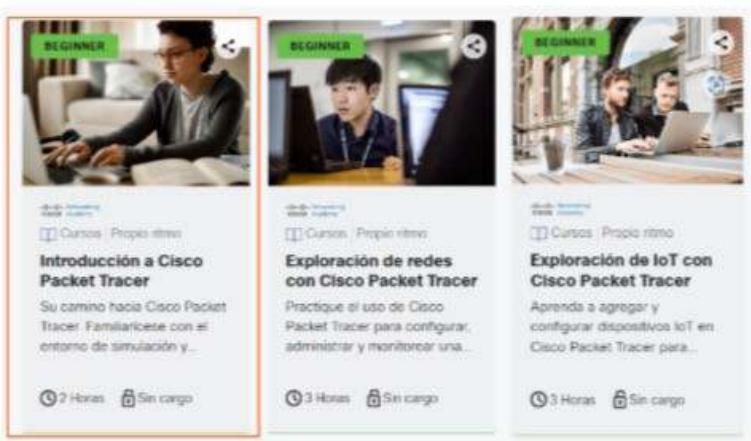
Es importante que lo instale para realizar las actividades.

4. Explore cursos de Packet Tracer

Instrucciones:

- a. Acceda a la página web: <https://www.netacad.com/es/cisco-packet-tracer>
- b. Aquí accederá a toda la información disponible de la Herramienta.
- c. Seleccione el curso: Introducción a Packet Tracer.

Figura 6
Cursos de Cisco Packet Tracer



Nota. Ludeña, P., 2025.

- Inscríbase en el curso, aquí encontrará toda la información necesaria para manejar la herramienta.

Figura 7
Introducción a Cisco Packet Tracer.

This screenshot shows the landing page for the 'Introducción a Cisco Packet Tracer' course. It includes a brief description, language options, and a prominent 'Comience con Self-Pace' button.

Introducción a Cisco Packet Tracer

Este curso es parte de Colecciones de aprendizaje - Cisco Packet Tracer

Su camino hacia Cisco Packet Tracer. Familiarícese con el entorno de simulación y descargue la última versión.

Autoguiado en línea
Aprende en línea a su propio ritmo

Español (Spanish) Comience con Self-Pace 2.412.198 ya inscritos

IDIOMAS DISPONIBLES: English, Español, Français, Português, Українська

Nota. Ludeña, P., 2025.

Al finalizar el curso obtendrá una insignia digital.

Anexo 2. Funcionamiento del Protocolo Traceroute

Funcionamiento del Protocolo Traceroute

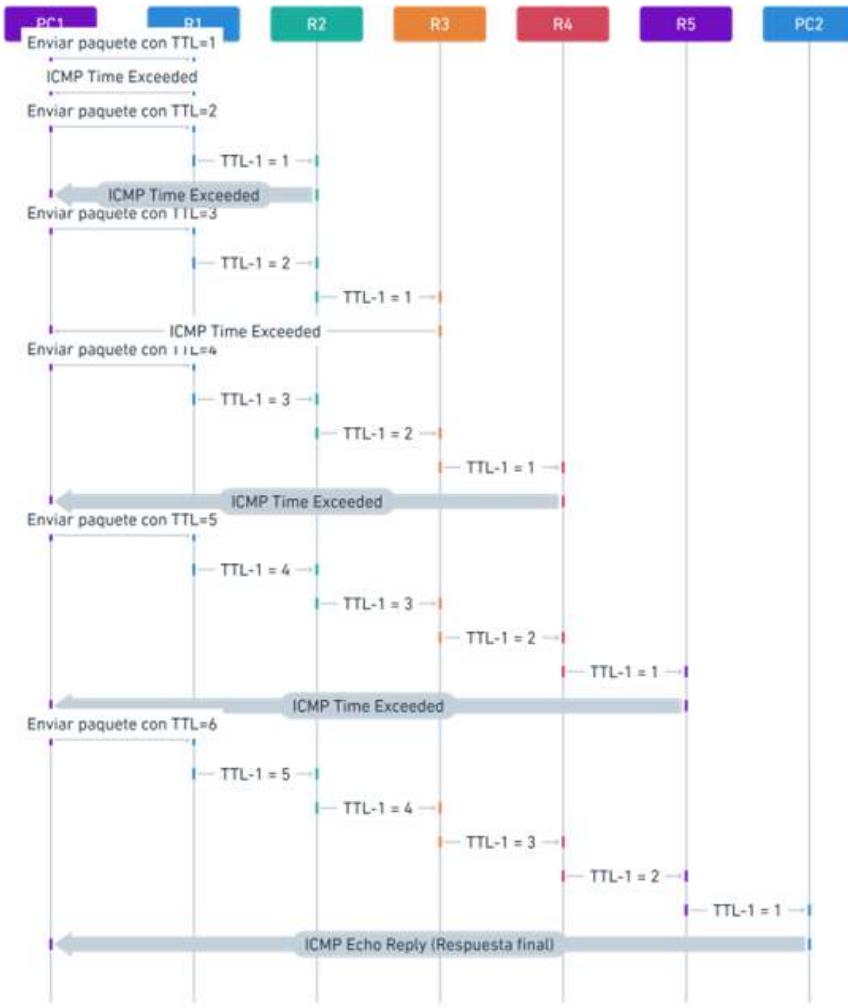
Para que usted pueda comprender mejor el mecanismo interno del comando traceroute, a continuación, se presenta un diagrama de secuencia que ilustra paso a paso cómo este protocolo descubre la ruta que siguen los paquetes a través de la red hasta llegar a su destino.

La figura muestra el intercambio de mensajes ICMP entre el host origen y cada router intermedio, evidenciando cómo el incremento progresivo del campo TTL (Time To Live) permite identificar cada salto en la ruta de comunicación.

Observe usted atentamente la secuencia temporal y el comportamiento de cada dispositivo de red en el proceso de descubrimiento de ruta:

Figura 1

Funcionamiento de Traceroute con mensajes ICMP y valores TTL



Made with Whimsical

Nota. Ludeña, P., 2025.

El origen envía un primer paquete con TTL = 1 (IPv4) o Hop Limit = 1 (IPv6). Al llegar al primer router R1, el TTL se decrementa una unidad y llega a 0, por lo cual el router descarta el paquete y genera un mensaje ICMP Time Exceeded (Tipo 11 en IPv4, Tipo 3 código 0 en IPv6). El mensaje de error llega a PC1, quien anota la dirección de R1 como primera marca.

El proceso se repite incrementando el valor del campo TTL/Hop Limit una unidad cada vez que se arme un nuevo paquete de prueba en el origen. Cada router de tránsito decrementa una unidad el contador y en cada prueba, eventualmente, el campo llegará a 0 y se descartará el paquete, generando un mensaje ICMP Time Exceeded (Tipo 11 en IPv4, Tipo 3 código 0 en IPv6). Con este mensaje de error el origen descubrirá la identidad de un router, anotando la dirección IP del router y la latencia; y, así construirá la ruta seguida por los paquetes hasta llegar al destino.

El proceso finaliza el origen recibe un mensaje ICMP Destination Unreachable – Port Unreachable (Tipo 3 código 3) o un mensaje ICMP Echo Reply, señal de que el paquete de prueba llegó al destino.

Anexo 3. Comandos show para monitoreo en Cisco IOS

Comandos básicos de diagnóstico y verificación

Comencemos con los comandos **show ip interface brief / show ipv6 interface brief**, los cuales sirven para ver un resumen rápido del estado de las interfaces del router o switch, tanto para IPv4 como para IPv6, respectivamente. En la figura 1 puede ver un ejemplo, donde se muestra una lista de todas las interfaces y su información ordenada en las siguientes columnas: interfaz, dirección IPv4 asignada, YES si se reconoce como configuración válida, cómo se asignó la dirección IP, estado físico (up/down), estado del protocolo de la interfaz.

Figura 1

Visualización del estado de interfaces con el comando *show ip interface brief* en Cisco IOS

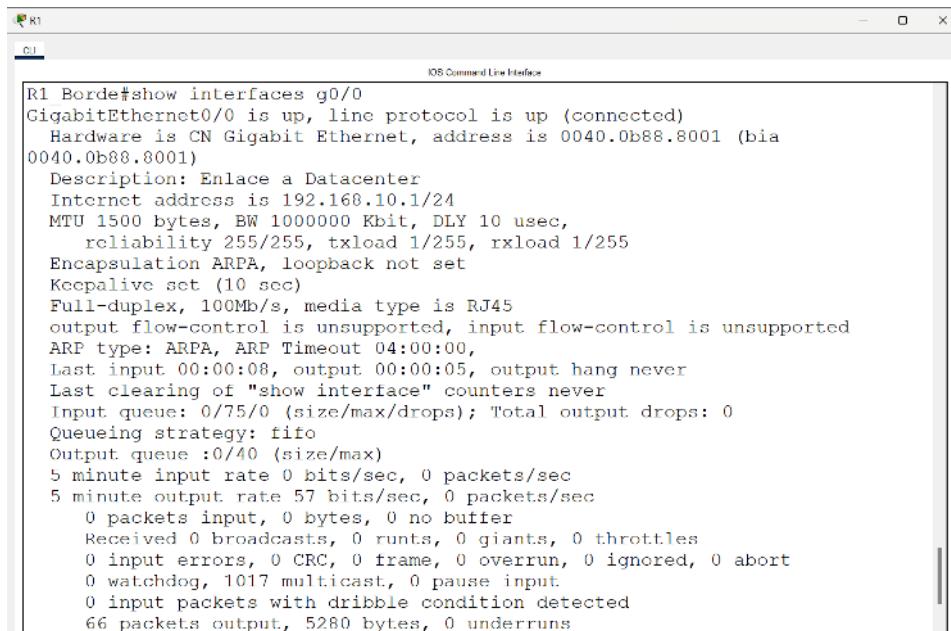
```
R1_Borde#show ip interface brief
Interface          IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0    192.168.10.1   YES manual up
GigabitEthernet0/1    172.16.100.1  YES manual up
GigabitEthernet0/2    unassigned      YES unset administratively down down
Serial0/0/0           unassigned      YES unset administratively down down
Serial0/0/1           172.16.1.2    YES manual up
Vlan1                unassigned      YES unset administratively down down
R1_Borde#
```

Nota. Ludeña, P., 2025.

El comando **show interfaces <tipo>** sirve para mostrar información detallada sobre una interfaz específica, por ejemplo, en la figura 2, se puede ver la información para la interfaz GigabitEthernet0/0.

Figura 2

Visualización del estado y estadísticas de operación de una interfaz con el comando *show interfaces* en Cisco IOS



```
R1#show interfaces g0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
  Hardware is CN Gigabit Ethernet, address is 0040.0b88.8001 (bia
  0040.0b88.8001)
    Description: Enlace a Datacenter
    Internet address is 192.168.10.1/24
    MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
      reliability 255/255, txload 1/255, rxload 1/255
    Encapsulation ARPA, loopback not set
    Keepalive set (10 sec)
    Full-duplex, 100Mb/s, media type is RJ45
    output flow-control is unsupported, input flow-control is unsupported
    ARP type: ARPA, ARP Timeout 04:00:00,
    Last input 00:00:08, output 00:00:05, output hang never
    Last clearing of "show interface" counters never
    Input queue: 0/75/0 (size/max/drops); Total output drops: 0
    Queueing strategy: fifo
    Output queue :0/40 (size/max)
    5 minute input rate 0 bits/sec, 0 packets/sec
    5 minute output rate 57 bits/sec, 0 packets/sec
      0 packets input, 0 bytes, 0 no buffer
      Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      0 watchdog, 1017 multicast, 0 pause input
      0 input packets with dribble condition detected
      66 packets output, 5280 bytes, 0 underruns
```

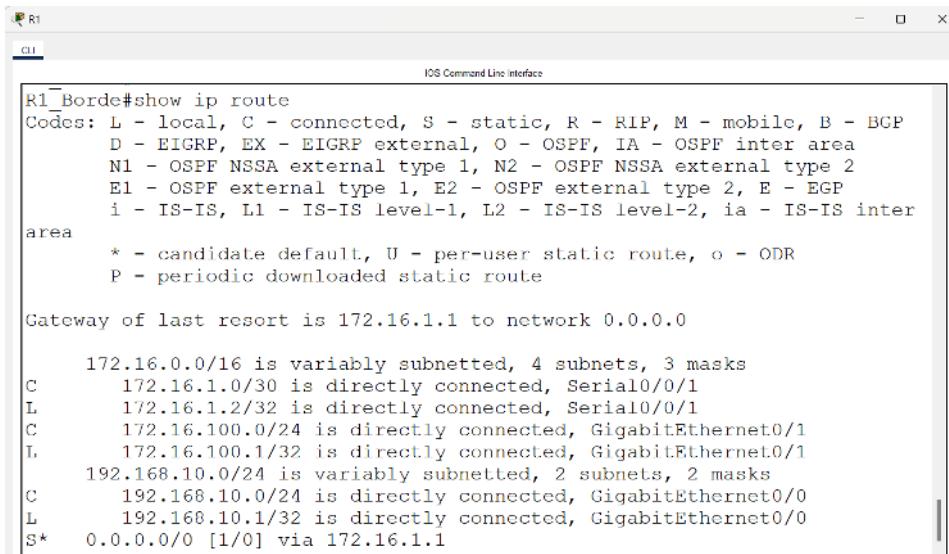
Nota. Ludeña, P., 2025.

El comando proporciona datos técnicos como estado físico y lógico de la interfaz, dirección MAC, velocidad y dúplex, estadísticas de tráfico, errores (CRC, colisiones), uso de colas, tipo de encapsulación, y configuración de ARP. Esta información es clave para diagnosticar problemas de conectividad, verificar el rendimiento de la interfaz y detectar fallos en la capa física o de enlace de datos.

El comando **show ip route / show ipv6 route** se utiliza para visualizar la tabla de enrutamiento IPv4 e IPv6, respectivamente. La tabla de enrutamiento contiene todas las rutas conocidas e incluye la información del origen de la ruta (rutas estáticas, dinámicas y locales), los detalles de la dirección IP de destino, el siguiente salto y la interfaz de salida, como se puede observar en la figura 3.

Figura 3

Visualización de la tabla de enrutamiento IPv4 con el comando `show ip route` en Cisco IOS



```
R1_Borde#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is 172.16.1.1 to network 0.0.0.0

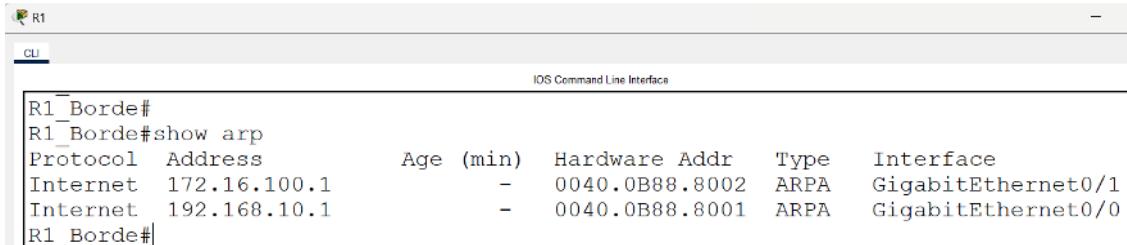
      172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
C        172.16.1.0/30 is directly connected, Serial0/0/1
L        172.16.1.2/32 is directly connected, Serial0/0/1
C        172.16.100.0/24 is directly connected, GigabitEthernet0/0/1
L        172.16.100.1/32 is directly connected, GigabitEthernet0/0/1
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet0/0/0
L        192.168.10.1/32 is directly connected, GigabitEthernet0/0/0
S*    0.0.0.0/0 [1/0] via 172.16.1.1
```

Nota. Ludeña, P., 2025.

El comando **show arp** se utiliza para mostrar la tabla ARP (Address Resolution Protocol) de un dispositivo de red, como se puede ver en la figura 4.

Figura 4

Visualización de la tabla ARP con el comando `show arp` en Cisco IOS



```
R1_Borde#
R1_Borde#show arp
Protocol Address          Age (min)  Hardware Addr   Type     Interface
Internet 172.16.100.1           -  0040.0B88.8002  ARPA    GigabitEthernet0/1
Internet 192.168.10.1           -  0040.0B88.8001  ARPA    GigabitEthernet0/0
R1_Borde#
```

Nota. Ludeña, P., 2025.

La tabla ARP contiene la asociación entre las direcciones IP y las direcciones MAC, en el ejemplo, el equipo con dirección IP 172.16.100.1 tiene dirección MAC 0040.0B88.8002. El comando ayuda a diagnosticar problemas de conectividad y a verificar que las traducciones ARP se están realizando adecuadamente.

El comando **show cdp neighbors detail** se utiliza para obtener información completa y detallada sobre los dispositivos vecinos descubiertos mediante el protocolo Cisco Discovery Protocol (CDP). Como se puede visualizar en la figura 5, este comando proporciona datos como el nombre del dispositivo vecino, su dirección IP, el tipo de dispositivo, la plataforma, la interfaz local y remota conectada, y otra información relevante que facilita la identificación y diagnóstico de la topología de red. Es útil para entender cómo están interconectados los dispositivos Cisco y para solucionar problemas de conectividad y configuración.

Figura 5

Visualización de información de dispositivos vecinos con el comando `show cdp neighbors detail` en Cisco IOS

R1_Borde#show cdp neighbors detail

```
Device ID: Central
Entry address(es):
  IP address : 172.16.1.1
Platform: cisco C1900, Capabilities: Router
Interface: Serial0/0/1, Port ID (outgoing port): Serial0/0/1
Holdtime: 124

Version :
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thurs 5-Jan-12 15:41 by pt_team

advertisement version: 2
Duplex: full
-----
Device ID: Switch
Entry address(es):
Platform: cisco 2960, Capabilities: Switch
Interface: GigabitEthernet0/0, Port ID (outgoing port): GigabitEthernet0/1
Holdtime: 147
```

Nota. Ludeña, P., 2025.

Anexo 4. Ejemplo Práctico de Subnetting VLSM

Diseño de subredes de longitud variable para una red empresarial

Ahora revisaremos un **ejemplo** de cómo se aplican estos pasos para resolver un escenario práctico.

Suponga que usted administra la red de una empresa que recibe la dirección 192.168.0.0/24 y necesita cinco subredes para asignar direcciones en su topología con los siguientes requisitos: LAN 1: 100 hosts, LAN 2: 10 hosts, LAN 3: 8 hosts, LAN 4: 40 hosts y un enlace punto a punto.

La red base es 192.168.0.0/24.

Los requisitos se ordenan de mayor a menor son: 100, 40, 10, 8 y 2.

Entonces primero debemos atender los requerimientos de la LAN 1: 100 hosts. Se requieren 7 bits en la porción de host para esta primera división ya que $2^7 - 2 = 126$ ($h=7$), entonces el nuevo prefijo es /25 y la máscara de subred es 255.255.255.128. El número mágico es 128 en el cuarto octeto.

El número de subredes es 2^m , $m=1$ porque sólo se ha pedido un bit de la porción de host, en consecuencia, con esta primera división sólo se obtienen 2 subredes.

- Subred 192.168.0.0/25 se asigna a LAN 1
- Subred 192.168.0.128/25

En la primera división se han obtenido dos subredes, la primera subred se asigna a la red con mayor demanda de requisitos, en este caso LAN 1 y la subred restante puede ser usada para divisiones sucesivas con el objetivo de satisfacer los requisitos de las otras redes.

El bloque 192.168.0.128/25, entonces, será la nueva base. La siguiente subred requiere 40 direcciones. Para tener el número de direcciones necesitado basta con 6 bits en la porción de red, entonces el nuevo

prefijo es /26 y la máscara de subred es 255.255.255.192. El número mágico es 64 en el cuarto octeto. Con esta división se tienen 2 subredes:

- Subred 192.168.0.128/26 se asigna a LAN 4
- Subred 192.168.0.192/26

El bloque libre es 192.168.0.192/26.

Ahora es el turno de la subred que requiere 10 direcciones. Para 10 direcciones h debe ser 4, así el nuevo prefijo es /28 y la máscara de subred es 255.255.255.240. El número mágico está en el cuarto octeto y tiene valor 16. El prefijo de la base para esta división es 26 y el nuevo prefijo es 28, por tanto, valor de m es 2, por lo que se deduce que en esta división se extraen cuatro subredes. La siguiente subred, LAN 3, tiene un requerimiento de 8 direcciones que puede ser atendido con los bloques de direcciones que se trajeron en la división anterior.

- Subred 192.168.0.192/28 se asigna a LAN 2
- Subred 192.168.0.208/28 se asigna a LAN 3
- Subred 192.168.0.224/28
- Subred 192.168.0.240/28

Finalmente, se atiende el requerimiento de dos direcciones para el enlace. Con la nueva base 192.168.0.224/28, se calcula que h es igual a dos y el prefijo es /30 para una máscara 255.255.255.252. El número mágico es 4 en el cuarto octeto y las posibles subredes son 4.

- 192.168.0.224/30 se asigna a enlace
- 192.168.0.228/30
- 192.168.0.232/30
- 192.168.0.236/30

Al finalizar, todas las subredes caben en el /24 original y sobran las siguientes direcciones: 192.168.0.240/28, 192.168.0.228/30, 192.168.0.232/30 y 192.168.0.236/30 para futuros requerimientos. En la tabla 1 se resume

para cada subred la máscara, prefijo, dirección de red, rangos de direcciones válidas y la dirección de broadcast.

Tabla 1

Resumen de subredes VLSM para el escenario de la dirección 192.168.0.0/24

Red	Máscara de red	Prefijo	Dirección de red	Primera dirección válida	Última dirección válida	Dirección de broadcast
LAN 1	255.255.255.128	/25	192.168.0.0	192.168.0.1	192.168.0.126	192.168.0.127
LAN 4	255.255.255.192	/26	192.168.0.128	192.168.0.129	192.168.0.190	192.168.0.191
LAN 2	255.255.255.240	/28	192.168.0.192	192.168.0.193	192.168.0.206	192.168.0.207
LAN 3	255.255.255.240	/28	192.168.0.208	192.168.0.209	192.168.0.222	192.168.0.223
Enlace	255.255.255.252	/30	192.168.0.224	192.168.0.225	192.168.0.226	192.168.0.227

Nota. Ludeña, P, 2025.



Analice cómo se asignan subredes de distintos tamaños según las necesidades de cada segmento y cómo varían los prefijos para ajustarse a los requerimientos sin desperdiciar direcciones. En el caso del ejemplo la dirección base permite asignar 254 direcciones, los requisitos son 160 direcciones y el número de direcciones de hosts que se tienen disponibles con la división es 218, dando un 86% de direcciones usables. Se tienen 20 direcciones válidas en los rangos sobrantes que constituyen un 8% de reserva.

Anexo 5. Control de flujo TCP: ejemplo práctico

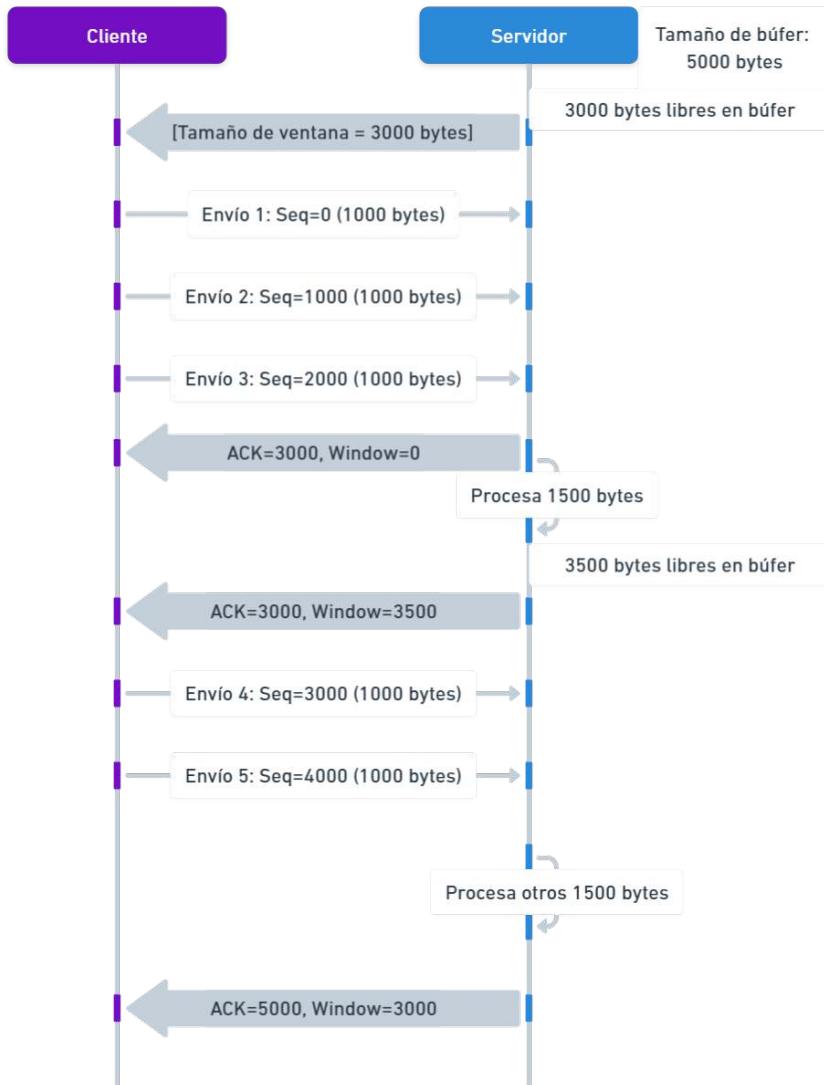
Ejemplo

Supongamos que hay una conexión entre dos dispositivos. El cliente envía datos al servidor. El tamaño del buffer del servidor es 5000 bytes, el tamaño inicial de ventana de recepción anunciada por el servidor es 3000 bytes, el tamaño de segmento de cada envío es de 1000 bytes. El servidor lee datos de su buffer en bloques de 1500 bytes.

En la figura 1, puede seguir el proceso descrito.

Figura 1

Ejemplo de control de flujo TCP con ventana deslizante



Made with Whimsical

Nota. Ludeña, P., 2025.

A continuación, se explicará paso a paso para comprender el diagrama de la figura.

Paso 1: conexión establecida

El servidor anuncia el tamaño de su ventana 3000 bytes. Por lo tanto, el cliente puede enviar hasta 3000 bytes sin esperar ACK.

Paso 2: el cliente envía tres segmentos

Envío 1: Seq = 0, 1000 bytes, Envío 2: Seq = 1000, 1000 bytes y Envío 3: Seq = 2000, 1000 bytes

Total en vuelo: 3000 bytes

La ventana del cliente se cierra temporalmente hasta recibir ACK.

Paso 3: el servidor envía como tamaño de ventana 0. Con lo cual se bloquean los envíos.

Paso 4: el servidor pasa 1500 bytes a su aplicación

Libera espacio en su buffer (ahora hay 3500 bytes libres).

Envía ACK = 3000 y Window = 2000 (quedan 2000 bytes disponibles).

El cliente puede enviar 2000 bytes más.

Paso 5: cliente envía dos nuevos segmentos

Envío 4: Seq = 3000, 1000 bytes y Envío 5: Seq = 4000, 1000 bytes

Total enviado = 5000 bytes (cumple con el límite del buffer del servidor).

Paso 6: el Servidor procesa otros 1500 bytes

Pasa datos a la aplicación. En total ya ha procesado 3000 bytes.

Su buffer vuelve a tener espacio ($5000 - 2000$ restantes = 3000 libres).

Envía ACK = 5000 y Window = 3000

La ventana desliza y permite continuar con nuevos envíos.

Observe que el cliente se va adaptando a la ventana que le comunica el servidor. Este mecanismo de adaptación es fundamental para el correcto funcionamiento de las redes TCP/IP, lo que nos lleva a considerar algunas reflexiones sobre las siguientes preguntas:



- ¿Cómo podría afectar a la red la falta de un sistema de control de flujo?
- ¿Cómo afectaría el rendimiento de la red si todos los receptores enviaran ventanas de tamaño cero?