Compás
capacitación e investigación

2025

Fundamentos de enrutamiento en redes de computadoras

Rodrigo Fernando Morocho Román

Fundamentos de enrutamiento en redes de computadoras

Rodrigo Fernando Morocho Román

ISBN: 978-9942-53-058-5 DOI: http://doi.org/10.48190/9789942530585

Compás
capacitación e investigación

https://orcid.org/0000-0003-0194-5033
Univesidad Técnica de Machala

Primera edición, 2025-10-27

ISBN: 978-9942-53-058-5
DOI: http://doi.org/10.48190/9789942530585
Distribución online
Acceso abierto

Cita
Morocho, R. (2025) Fundamentos de enrutamiento en redes de computadoras. Editorial Grupo Compás

Este libro es parte de la colección de la Univesidad Técnica de Machala y ha sido debidamente examinado y valorado en la modalidad doble par ciego con fin de garantizar la calidad de la publicación.

TABLA DE CONTENIDOS

Capítulo 1: Fundamentos del Funcionamiento de los Routers y Cisco IOS 7

1.1. ¿Qué es un Router y cuál es su función? 9

1.2. Arquitectura Interna de un Router Cisco 11

1.3. Cisco IOS y Modos de Operación 14

1.4. Proceso de Arranque del Router 16

1.5. Administración de Configuraciones 18

1.6. Buenas Prácticas Operativas 19

1.7. Práctica Guiada: Configuración Básica de un Router Cisco en Packet Tracer 22

Capítulo 2: Fundamentos de Enrutamiento y Configuración de Rutas 30

2.1. Subredes Conectadas Directamente 31

2.2. Rutas Estáticas y Rutas Predeterminadas 32

2.3. Convergencia en Enrutamiento 34

2.4. Métricas de Enrutamiento 35

2.5. Distancia Administrativa 37

2.6. Protocolos de Enrutamiento: IGP y EGP 38

2.7. Algoritmos: Vector de Distancia y Estado de Enlace 41

2.8. Configuración y Verificación de RIP v2 43

2.9. Práctica Guiada: Configuración de Rutas Estáticas en Cisco Packet Tracer 45

2.10. Práctica Guiada: Configuración de RIPv2 en Cisco Packet Tracer 48

2.11. Evaluación del capítulo 51

Capítulo 3: VLSM y Diseño de Subredes Eficientes 55

3.1. ¿Qué es VLSM y para qué se utiliza? 57

3.2. Diseño eficiente de subredes con VLSM 59

3.3. Subredes solapadas y no solapadas 63

3.4. Resumen de Rutas (Route Summarization) 65

3.5. Práctica Guiada: Diseño y Configuración de Subredes con VLSM 70

3.6. Evaluación del capítulo 74

Capítulo 4: Enrutamiento con IPv6 78

4.1. Fundamentos de IPv6 80

4.2. Tipos de Direcciones IPv6 83

4.3. Representación y Abreviación de Direcciones IPv6 87

4.4. Subredes IPv6 88

4.5. Direccionamiento Especial en IPv6 90

4.6. Configuración Básica de IPv6 en Routers Cisco 93

4.7. Enrutamiento Estático en IPv6 95

4.8. Enrutamiento Dinámico con RIPng 97

4.9. Métodos de Transición IPv4 – IPv6 100

4.10. Práctica Guiada: Configuración de Enrutamiento IPv6 en Cisco Packet Tracer 104

4.11. Evaluación del Capítulo.....109

ÍNDICE DE ILUSTRACIONES

Ilustración 1. Proceso de arranque de un router Cisco 16
Ilustración 2. Topología de red propuesta para la práctica en Cisco Packet Tracer 22
Ilustración 3. Salida de una tabla de enrutamiento 32
Ilustración 4. Interconexión de Sistemas Autónomos 39
Ilustración 5. Verificación de protocolo de enrutamiento activo.....40
Ilustración 6. Verificación de tabla de enrutamiento con rutas RIP 45
Ilustración 7. Topología de red propuesta para la práctica de configuración de rutas estáticas en Cisco Packet Tracer 45
Ilustración 8. Topología de red propuesta para la práctica de configuración de RIPv2 en Cisco Packet Tracer 48
Ilustración 9. Topología de red propuesta para la práctica 71

ÍNDICE DE TABLAS

Tabla 1. Tipos de memoria en routers Cisco.....11

Tabla 2. Comandos de gestión de configuración en Cisco IOS.....18

Tabla 3. Ejemplo de Distancias Administrativas 37

Tabla 4. Comparación de Algoritmos 42

Tabla 5. Ejemplo de comparación entre subneteo tradicional y VLSM..... 58

Tabla 6. Asignación de subredes con VLSM 62

Tabla 7. Ejemplo de subredes no solapadas correctamente asignadas..... 65

Tabla 8. Conversión de decimal a binario 67

Tabla 9. Comparación bit a bit para el resumen de rutas 68

Tabla 10. Diseño VLSM propuesto 72

Tabla 11. Comparación entre IPv4 e IPv6..... 82

Tabla 12. Tipos de direcciones IPv6..... 86

Tabla 13. Comparación de los mecanismos de transición a IPv6..... 103

Prefacio

La enseñanza de redes de computadoras enfrenta el desafío de equilibrar teoría sólida con aplicación práctica, en un entorno tecnológico que evoluciona constantemente. Este libro, titulado Fundamentos de Enrutamiento en Redes de Computadoras, nace como un texto guía para apoyar la asignatura "Tecnologías de Conmutación II", con un enfoque integral que combina explicaciones conceptuales claras, comandos aplicados, topologías realistas y prácticas guiadas.

El contenido ha sido cuidadosamente estructurado para atender las necesidades de estudiantes universitarios que se enfrentan por primera vez al mundo del enrutamiento, brindando recursos que promuevan la comprensión y desarrollo de habilidades técnicas. Cada capítulo ha sido revisado para garantizar rigurosidad académica, relevancia práctica y coherencia pedagógica.

Este esfuerzo busca no solo preparar a los estudiantes para los retos de aprobar asignaturas del área de redes de computadoras, sino también fomentar el pensamiento crítico y la capacidad de diseño eficiente de redes en la vida profesional. Esperamos que esta obra sea una herramienta útil tanto en el aula como en el autoaprendizaje.

Objetivo general del libro

Aplicar los fundamentos del enrutamiento en redes de computadoras, mediante el análisis conceptual, la configuración práctica de routers y la simulación de topologías reales, con el fin de desarrollar competencias técnicas para el diseño, implementación y gestión eficiente de redes IPv4 e IPv6.

Capítulo 1: Fundamentos del Funcionamiento de los Routers y Cisco IOS

Introducción

En la era digital actual, las redes de comunicación constituyen la infraestructura fundamental sobre la que se asientan todas las interacciones, desde el intercambio de información personal hasta las operaciones críticas de las empresas y los gobiernos. En el corazón de esta vasta infraestructura se encuentran los routers, dispositivos inteligentes que actúan como directores de tráfico, guiando los paquetes de datos a través de intrincadas rutas para asegurar que lleguen a su destino final (Kurose & Ross, 2021). Su función es análoga a la de los controladores de tráfico aéreo en un aeropuerto, garantizando que cada "avión" (paquete de datos) tome la "pista" (ruta) correcta para alcanzar su "ciudad" (dispositivo) de destino.

La omnipresencia de los routers se manifiesta en diversos escenarios. En el ámbito doméstico, un router conecta múltiples dispositivos (computadoras, teléfonos inteligentes, tabletas, dispositivos IoT) a la vasta red de Internet, permitiendo la navegación web, la transmisión de contenido y la comunicación global. Para las empresas, los routers son esenciales para interconectar diferentes segmentos de la red (departamentos, sucursales, centros de datos), facilitar la comunicación interna y externa, y proporcionar acceso seguro a recursos críticos. Los proveedores de servicios de Internet (ISP) dependen de routers de alta capacidad y rendimiento para construir sus redes troncales (backbones), gestionando el tráfico masivo que fluye a través de

Internet y conectando a millones de usuarios y organizaciones (Cisco Networking Academy, 2024).

La relevancia de los routers ha evolucionado significativamente con el avance tecnológico. Con la proliferación de la virtualización de redes (Network Functions Virtualization - NFV) y la creciente adopción de la computación en la nube, los routers ya no son exclusivamente dispositivos físicos. Los routers virtuales y las funciones de enrutamiento basadas en software permiten una mayor flexibilidad, escalabilidad y eficiencia en la gestión de las redes, facilitando la creación de infraestructuras más ágiles y resilientes. Este capítulo proporciona una base sólida para comprender el rol crucial de los routers, su arquitectura interna, el sistema operativo que los gobierna (Cisco IOS) y las prácticas esenciales para su configuración y administración. Se busca integrar tanto una base conceptual robusta como aplicaciones prácticas para preparar al lector en el entorno profesional de las redes.

Objetivos del Capítulo

- Identificar las funciones principales de un router en una red, para comprender su papel en el direccionamiento de datos entre dispositivos, mediante el análisis de sus características operativas y funciones en el modelo OSI.
- Describir la arquitectura interna de un router Cisco, con el fin de reconocer sus componentes clave de hardware y su relación con la funcionalidad del equipo, a través del estudio estructurado de sus memorias, CPU e interfaces.
- Explicar el funcionamiento y jerarquía de modos del sistema operativo Cisco IOS, para administrar de manera eficiente un router,

mediante la ejecución de comandos en la interfaz CLI.

- Analizar el proceso de arranque de un router, con el propósito de diagnosticar problemas comunes y validar el inicio correcto del sistema, mediante la interpretación de fases como POST, bootstrap e inicio de configuraciones.
- Aplicar comandos de configuración básicos en routers Cisco, para establecer redes funcionales y seguras, a través de la simulación de escenarios reales en Packet Tracer con acceso al modo privilegiado y configuración global.

1.1. ¿Qué es un Router y cuál es su función?

Un router es un dispositivo que opera en la capa 3 del modelo OSI (capa de red), cuyo principal propósito es seleccionar la mejor ruta para que los datos IP lleguen a su destino a través de redes interconectadas. A diferencia de los switches, que operan dentro de una misma red, los routers interconectan diferentes subredes o redes completas. Esta función de encaminamiento permite establecer la lógica de tráfico entre múltiples redes, y es esencial para el funcionamiento de Internet (Kurose & Ross, 2021).

La selección de la "mejor ruta" por parte de un router implica la evaluación de múltiples factores. Los routers utilizan métricas, que son valores que se asignan a las rutas en función de características como la distancia, el ancho de banda, la carga y el retardo. Los protocolos de enrutamiento, como RIP (Routing Information Protocol) y OSPF (Open Shortest Path First), permiten a los routers intercambiar información sobre las redes y las rutas disponibles, lo que les permite actualizar dinámicamente sus tablas de

enrutamiento y adaptarse a los cambios en la topología de la red.

Además de su función principal de enrutamiento, los routers ofrecen una variedad de funcionalidades adicionales que son cruciales para el funcionamiento y la seguridad de las redes modernas:

- **Traducción de direcciones (NAT):** NAT permite que múltiples dispositivos en una red privada compartan una única dirección IP pública para acceder a Internet. Esto es importante porque ayuda a conservar las direcciones IP (que son un recurso limitado) y también proporciona una capa de seguridad al ocultar las direcciones IP privadas de los dispositivos de la red interna.
- **Listas de control de acceso (ACL):** Las ACLs son reglas que permiten controlar el tráfico que entra y sale de una red o de una interfaz del router. Se utilizan para implementar políticas de seguridad, como bloquear el acceso a determinados servicios o redes, o permitir el acceso solo a usuarios autorizados.
- **Calidad de servicio (QoS):** QoS permite priorizar el tráfico de red en función de su importancia. Esto es esencial para garantizar que las aplicaciones críticas, como la voz y el video en tiempo real, reciban el ancho de banda y el retardo adecuados, incluso cuando la red está congestionada.
- **Conectividad remota y VPN (Virtual Private Network):** Los routers pueden proporcionar conectividad remota segura a través de VPNs. Una VPN crea

un túnel cifrado a través de una red pública (como Internet), lo que permite a los usuarios remotos acceder a los recursos de la red corporativa de forma segura (Cisco Networking Academy, 2024).

1.2. Arquitectura Interna de un Router Cisco

Un router Cisco, al igual que una computadora, está compuesto por varios componentes de hardware y software que trabajan en conjunto para llevar a cabo su función principal de enrutamiento. Comprender la función de cada uno de estos componentes es crucial para diagnosticar problemas, optimizar el rendimiento y configurar el dispositivo de manera efectiva (Cisco Networking Academy, 2024; Leinwand & Pinsky, 1998).

Memoria

La memoria en un router Cisco se organiza en varios tipos, cada uno con un propósito específico.

Tabla 1. Tipos de memoria en routers Cisco

Tipo de memoria	Función	Volatilidad	Contenido típico
ROM	Arranque inicial, POST, Bootstrap	No volátil	Software básico de arranque
RAM	Operaciones activas	Volátil	running-config, tablas de enrutamiento
NVRAM	Configuración de inicio	No volátil	startup-config
FLASH	Almacenamiento del IOS	No volátil	Imagen del sistema operativo

Fuente: Cisco Networking Academy, 2024; Leinwand & Pinsky, 1998.

CPU (Central Processing Unit)

La CPU es el "cerebro" del router. Es responsable de ejecutar las instrucciones del sistema operativo, procesar los paquetes de datos y tomar las decisiones de enrutamiento. La velocidad y la capacidad de procesamiento de la CPU afectan directamente al rendimiento del router. Una CPU más potente puede manejar más tráfico y ejecutar tareas más complejas de manera más eficiente.

Interfaces

Las interfaces son los puertos físicos del router que se utilizan para conectar el router a otras redes. Existen diferentes tipos de interfaces, cada una diseñada para un tipo específico de conexión. Cada interfaz tiene una velocidad y un estándar específico. Por ejemplo, las interfaces Ethernet pueden ser Fast Ethernet (100 Mbps), Gigabit Ethernet (1 Gbps) o 10 Gigabit Ethernet (10 Gbps).

- **Ethernet:** Se utiliza para conectar el router a redes de área local (LAN). La evolución de Ethernet en los routers ha pasado de 10 Mbps a 100 Mbps (Fast Ethernet), 1 Gbps (Gigabit Ethernet), 10 Gbps (Ten Gigabit Ethernet) y más allá. Es crucial para conectar segmentos de red, switches, servidores y estaciones de trabajo (Cisco Networking Academy, 2024).
- **Serial:** Se utiliza para conectar el router a redes de área amplia (WAN). Aunque menos comunes en las redes LAN modernas, siguen siendo relevantes para la interconexión de sitios geográficamente dispersos a través de servicios de WAN tradicionales como líneas dedicadas, Frame Relay o ATM. Utilizan protocolos de encapsulación como HDLC (High-Level Data Link Control) o PPP (Point-to-Point Protocol) (Odom, 2013).
- **Console:** Se utiliza para acceder al router localmente a través de una conexión directa. Es el puerto de acceso directo al router, ideal para la configuración inicial, la recuperación de contraseñas y la resolución de problemas cuando la red no está operativa. Requiere un cable de consola RJ-45 a DB-9 (o USB-A a Mini-USB, dependiendo del modelo) y un emulador de terminal (como PuTTY o Tera Term) en una computadora (Boney, 2005).

- **Auxiliary (AUX):** Se utiliza para la administración remota del router (menos común en la actualidad). Originalmente diseñado para conectividad de módem para acceso remoto de respaldo. Su uso ha disminuido drásticamente con la prevalencia de SSH sobre Internet para la gestión remota (Brown et al., 2002).
- **Módulos de Interfaces y Slots Vacíos**

Muchos routers Cisco son modulares, lo que significa que se pueden agregar o intercambiar módulos de interfaces para satisfacer las necesidades cambiantes de la red. Esto permite a las empresas invertir en un chasis de router y luego expandirlo según sea necesario, agregando más puertos Ethernet, puertos seriales o incluso interfaces inalámbricas.

- **Slots Vacíos:** Los *slots* vacíos en un router modular son espacios donde se pueden insertar módulos de interfaz adicionales. Estos módulos pueden ser de diferentes tipos (Ethernet, serial, fibra óptica) y velocidades. Esta modularidad es un factor clave en la escalabilidad de la red (Cisco Networking Academy, 2024).

Comprender la arquitectura interna de un router Cisco es fundamental para poder configurarlo, administrarlo y solucionar problemas de manera efectiva. Los diferentes componentes trabajan en conjunto para garantizar que los datos se enruten de manera eficiente y segura a través de la red.

1.3. Cisco IOS y Modos de Operación

El sistema operativo Cisco IOS (Internetwork Operating System) permite administrar el router

mediante una interfaz de línea de comandos (CLI). Presenta una estructura jerárquica de modos operativos:

- **Modo usuario (Router>):** Permite la visualización de información básica del router y la ejecución de algunos comandos de diagnóstico. Es el modo de acceso inicial y tiene privilegios limitados.
- **Modo privilegiado (Router#)**: Permite la ejecución de comandos avanzados para la configuración, administración y resolución de problemas del router (se accede con el comando enable).
- **Modo configuración global (Router(config)#)**: Permite realizar cambios en la configuración general del router que afectan a todas las interfaces y funciones (se accede con el comando configure terminal).
- **Modos específicos**: Permiten configurar parámetros específicos de interfaces, protocolos de enrutamiento, etc.

Los accesos al IOS se pueden realizar localmente a través de la consola, que es una conexión directa al puerto de consola del router, o remotamente a través de protocolos como SSH (Secure Shell) y Telnet (Telecommunication Network) (Brown et al., 2002). SSH proporciona una conexión cifrada, lo que garantiza la seguridad de la comunicación, mientras que Telnet transmite los datos en texto plano, lo que lo hace vulnerable a la interceptación.

Para navegar entre los modos, se utilizan comandos como exit y end. El comando show ? proporciona ayuda contextual sobre los comandos disponibles en cada modo (Boney, 2005).

La seguridad en el acceso a los modos del IOS es fundamental. Se deben configurar contraseñas seguras para proteger el acceso no autorizado al router y a su configuración. El modo privilegiado es especialmente crítico, ya que permite realizar cambios que pueden afectar gravemente el funcionamiento de la red.

1.4. Proceso de Arranque del Router

Cuando un router Cisco se enciende, sigue una serie de pasos secuenciales para inicializar el hardware y cargar el sistema operativo IOS (Figura 1).

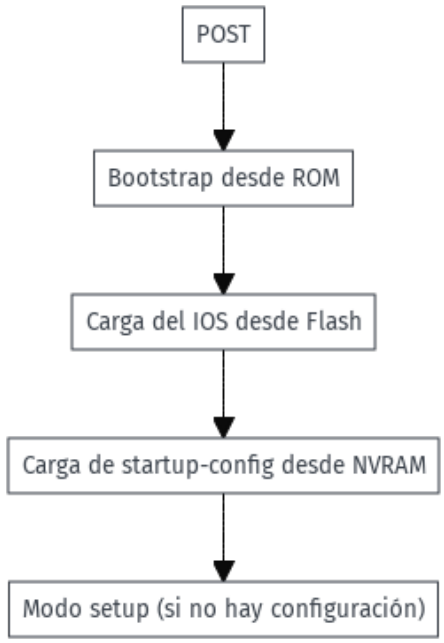

Ilustración 1. Proceso de arranque de un router Cisco

Fuente: Cisco Networking Academy, 2024.

El proceso de arranque consta de las siguientes etapas:

1. **POST (Power-On Self Test):** Es una serie de pruebas que el router realiza automáticamente al encenderse para verificar el funcionamiento correcto de sus componentes de hardware, como la CPU, la memoria y las interfaces. Si se detecta algún problema, el router mostrará un mensaje de error.
2. **Bootstrap desde ROM:** El bootstrap es un pequeño programa almacenado en la ROM que se ejecuta inmediatamente después del POST. Su función es inicializar el hardware básico y cargar el sistema operativo IOS desde la memoria Flash.
3. **Carga del IOS desde Flash:** El IOS, que es el sistema operativo del router, se carga desde la memoria Flash a la RAM. La RAM proporciona un acceso más rápido al IOS, lo que mejora el rendimiento del router.
4. **Carga de startup-config desde NVRAM:** La startup-config, que es la configuración guardada del router, se carga desde la NVRAM a la RAM. Esta configuración define los parámetros de funcionamiento del router, como las direcciones IP, los protocolos de enrutamiento y las contraseñas.
5. **Modo setup (si no hay configuración):** Si no hay una startup-config guardada en la NVRAM, el router entra en el modo setup, que es un asistente de configuración inicial que guía al usuario a través de los pasos básicos para configurar el router.

El comando show version es una herramienta de diagnóstico esencial durante el proceso de arranque y la operación normal del router (Leinwand & Pinsky, 1998). Proporciona información valiosa sobre el modelo del router, la versión del IOS, la cantidad de memoria, la configuración y el tiempo de actividad

(uptime) del sistema. Esta información es útil para verificar que el router se ha iniciado correctamente, diagnosticar problemas y planificar actualizaciones.

1.5. Administración de Configuraciones

La administración adecuada de las configuraciones del router es crucial para garantizar la estabilidad, la seguridad y la capacidad de recuperación de la red. Cisco IOS proporciona varios comandos para gestionar las configuraciones (Tabla 2).

Tabla 2. Comandos de gestión de configuración en Cisco IOS

Comando	Descripción	Modo
show running-config	Muestra la configuración activa	Privilegiado
show startup-config	Muestra la configuración almacenada	Privilegiado
copy running-config startup-config	Guarda la configuración activa de forma permanente	Privilegiado
copy tftp flash	Copia una imagen de IOS desde un servidor TFTP	Privilegiado

Fuente: Cisco Networking Academy, 2024.

Es importante implementar buenas prácticas para la gestión de archivos de configuración, como:

- Documentar los cambios realizados en la configuración.
- Realizar copias de seguridad periódicas de la configuración.
- Utilizar un servidor TFTP seguro para almacenar las copias de seguridad.
- Controlar el acceso a los archivos de configuración.

1.6. Buenas Prácticas Operativas

La implementación de buenas prácticas operativas es esencial para garantizar la seguridad, la estabilidad y la facilidad de administración de los routers y la red (Cisco Networking Academy, 2024). Algunas de las prácticas más importantes incluyen:

- **Asignar nombres claros al router con hostname:** Asignar nombres descriptivos a los routers facilita su identificación y administración, especialmente en redes grandes con múltiples dispositivos. En lugar de utilizar nombres genéricos como "Router1" o "Router2", se recomienda utilizar nombres que reflejen la ubicación, la función o el departamento del router, como "SedePrincipal-RTR" o "Servidor-Acceso-RTR".
- **Aplicar contraseñas cifradas con enable secret:** La seguridad es un aspecto crítico en la administración de redes. Es fundamental proteger el acceso al router y a su configuración

mediante el uso de contraseñas seguras. El comando enable secret permite cifrar la contraseña de acceso al modo privilegiado, lo que la hace mucho más difícil de descifrar que la contraseña configurada con el comando enable password.

- **Utilizar show ip interface brief para verificar interfaces activas:** Este comando proporciona una visión general del estado de las interfaces del router, incluyendo su estado (up o down), la dirección IP asignada y el protocolo de línea. Es una herramienta útil para verificar rápidamente la conectividad y solucionar problemas de interfaz.

Además de estas prácticas, se recomienda:

- **Documentar la red:** Mantener una documentación actualizada de la topología de la red, las direcciones IP, las configuraciones de los dispositivos y los procedimientos de administración es esencial para facilitar la resolución de problemas, la planificación de la capacidad y la gestión de cambios.
- **Implementar un sistema de gestión de contraseñas:** Utilizar un sistema seguro para almacenar y gestionar las contraseñas de los dispositivos de red ayuda a prevenir el acceso no autorizado y facilita la rotación periódica de contraseñas.
- **Mantener el IOS actualizado:** Las actualizaciones del IOS suelen incluir correcciones de errores, mejoras de seguridad y nuevas funcionalidades. Es

importante mantener el IOS actualizado para garantizar la estabilidad y la seguridad de la red.

- **Implementar copias de seguridad de la configuración:** Realizar copias de seguridad periódicas de la configuración del router permite restaurar rápidamente el dispositivo en caso de fallos o errores de configuración.
- **Utilizar SSH en lugar de Telnet:** SSH proporciona una conexión cifrada, lo que garantiza la seguridad de la comunicación, mientras que Telnet transmite los datos en texto plano, lo que lo hace vulnerable a la interceptación. SSH es la opción recomendada para la administración remota de routers.
- **Registrar eventos y mensajes del sistema (Syslog):** Configurar el router para enviar los mensajes del sistema a un servidor Syslog permite centralizar el registro de eventos y facilitar la resolución de problemas y la detección de incidentes de seguridad.
- **Implementar un sistema de monitoreo de red:** Utilizar herramientas de monitoreo de red permite supervisar el rendimiento del router y la red, detectar problemas de forma proactiva y planificar la capacidad de la red.

Siguiendo estas buenas prácticas, los administradores de red pueden mejorar significativamente la seguridad, la estabilidad y la facilidad de administración de los routers y la red (Cisco Networking Academy, 2024).

1.7. Práctica Guiada: Configuración Básica de un Router Cisco en Packet Tracer

Objetivo: Configurar un router Cisco desde cero para establecer conectividad entre dos redes LAN.

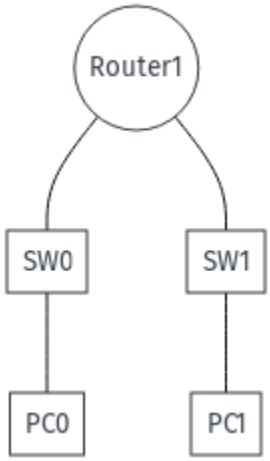

Ilustración 2. Topología de red propuesta para la práctica en Cisco Packet Tracer

Fuente: Elaboración propia.

Materiales requeridos:

Cisco Packet Tracer (v8.2 o superior)

Dispositivos: 1 router (Cisco 2901), 2 switches, 2 PCs

Topología sugerida:

Conexiones:

PC0 ↔ SW0 ↔ Router1 (Gig0/0)

PC1 ↔ SW1 ↔ Router1 (Gig0/1)

Configuraciones de red:

PC0: IP 192.168.10.2 /24, Gateway: 192.168.10.1

PC1: IP 192.168.20.2 /24, Gateway: 192.168.20.1

Pasos para la configuración:

1. Acceso inicial y nombramiento del dispositivo:

   enable

   configure terminal

   hostname Router1

   enable secret cisco123

2. Configuración de interfaces:

   interface gig0/0

   ip address 192.168.10.1 255.255.255.0

   no shutdown

   exit

   interface gig0/1

   ip address 192.168.20.1 255.255.255.0

   no shutdown

   exit

3. Verificación del estado de interfaces:

   show ip interface brief

show running-config

4. Guardar la configuración:

   copy running-config startup-config

5. Verificación de la conectividad:

   Configurar las direcciones IP y las puertas de enlace predeterminadas en las PCs según la tabla de configuraciones de red.

   Utilizar el comando ping en las PCs para verificar la conectividad entre ellas y con las interfaces del router.

   Abrir la ventana de comandos de cada PC.

   Ejecutar el comando ping para verificar la conectividad con la otra PC y con las interfaces del router. Por ejemplo:

   ping 192.168.10.1

   ping 192.168.20.2

Preguntas de reflexión:

1. **¿Por qué es necesario usar no shutdown en las interfaces del router?**

Las interfaces del router están desactivadas por defecto. El comando no shutdown es necesario para activarlas y permitir el tráfico de red.

2. **¿Qué sucede si las direcciones IP de gateway de las PCs no coinciden con las del router?**

Si las direcciones IP de gateway de las PCs no coinciden con las direcciones IP de las interfaces del router, las PCs no podrán comunicarse con otras redes, ya que no sabrán a dónde enviar el tráfico destinado a esas redes.

3. **¿Qué información proporciona el comando show ip interface brief?**

El comando show ip interface brief proporciona un resumen del estado de las interfaces del router, incluyendo su estado (up o down), la dirección IP asignada y el protocolo de línea.

4. **¿Cuál es la diferencia entre el comando enable password y el comando enable secret?**

El comando enable password configura una contraseña para acceder al modo privilegiado, pero la contraseña se almacena en texto plano en la configuración. El comando enable secret también configura una contraseña para acceder al modo privilegiado, pero la contraseña se cifra, lo que la hace mucho más segura.

1.8. Evaluación del Capítulo

1. ¿Qué memoria contiene la imagen del IOS?

a) NVRAM

b) ROM

c) Flash ✅

d) RAM

2. El comando copy running-config startup-config sirve para:

a) Reiniciar el router

b) Guardar la configuración actual ✅

c) Verificar el IOS

d) Cargar la configuración anterior

3. ¿Cuál es la función del modo privilegiado en IOS?

a) Establecer contraseñas

b) Ingresar comandos de configuración

c) Consultar y ejecutar comandos avanzados ✅

d) Cargar la configuración predeterminada

4. ¿Qué comando permite conocer la versión del IOS?

a) show config

b) show version ✅

c) show interface

d) show ip route

5. ¿Qué tipo de memoria se utiliza para almacenar la configuración de inicio?

a) RAM

b) ROM

c) Flash

d) NVRAM ✅

6. ¿Cuál de los siguientes protocolos se utiliza para la administración remota segura de un router?

a) Telnet

b) FTP

c) SSH ✅

d) HTTP

7. ¿Qué paso del proceso de arranque verifica el hardware del router?

a) Bootstrap

b) Carga del IOS

c) POST ✅

d) Carga de la configuración

8. ¿Cuál de las siguientes afirmaciones describe mejor la función de un router?

a) Conecta dispositivos dentro de la misma red.

b) Dirige el tráfico entre diferentes redes. ✅

c) Amplifica la señal de la red.

d) Proporciona conectividad inalámbrica.

Referencias Bibliográficas

Boney, J. (2005). *Cisco IOS in a Nutshell*. O'Reilly Media. ISBN: 9780596008697

Brown, S., Browne, B., Chen, N., et al. (2002). *Introduction to the Cisco IOS*. Cisco Press. ISBN: 9781587050411

Cisco Networking Academy. (2024). *Introduction to Networks*. Cisco Systems. https://www.netacad.com/ ISBN: 9781587134265

Kurose, J. F., & Ross, K. W. (2021). *Computer Networking: A Top-Down Approach* (8th ed.). Pearson. ISBN: 9780136681557

Leinwand, A., & Pinsky, B. (1998). *Cisco Router Configuration*. Cisco Press. ISBN: 9781578700224

Odom, W. (2013). *CCNA Routing and Switching Official Cert Guide, Volume 1* (Associate Level). Cisco Press. ISBN: 9781587205477

Capítulo 2: Fundamentos de Enrutamiento y Configuración de Rutas

---

Introducción

El enrutamiento es el proceso fundamental de determinar el camino más eficiente para que un paquete de datos viaje desde su origen hasta su destino a través de una red (Kurose & Ross, 2021). Es una función crucial que permite la comunicación no solo dentro de redes locales (LAN) o áreas metropolitanas (MAN), sino también a escala global a través de Internet. La correcta configuración de rutas influye directamente en la eficiencia, confiabilidad, seguridad y escalabilidad de las comunicaciones, siendo un pilar para la infraestructura de red moderna (Odom, 2013). Sin un enrutamiento eficaz, los paquetes de datos se perderían o tomarían caminos subóptimos, lo que resultaría en un rendimiento deficiente de la red y una experiencia de usuario frustrante. Este capítulo profundiza en los mecanismos por los cuales los routers toman estas decisiones de reenvío, desde las rutas directamente conectadas hasta el uso de protocolos de enrutamiento dinámico.

Objetivos del Capítulo

- Comprender qué es el enrutamiento y para qué sirve en una red, mediante el análisis de los conceptos de subredes y rutas.
- Identificar cómo se configuran rutas estáticas y predeterminadas para garantizar conectividad entre diferentes redes.
- Explicar qué son los protocolos de enrutamiento y cómo funcionan mediante

algoritmos de vector de distancia y estado de enlace.

- Analizar cómo se aplica el direccionamiento IP y subnetting en el diseño de redes, para optimizar el uso del espacio de direcciones.
- Configurar y verificar rutas y protocolos de enrutamiento dinámico en entornos de simulación usando Cisco Packet Tracer.

2.1. Subredes Conectadas Directamente

Una subred conectada directamente es aquella que está directamente accesible a través de una de las interfaces físicas del router, la cual ha sido configurada con una dirección IP que pertenece a esa misma subred (Cisco Networking Academy, 2024). Cuando una interfaz del router se activa (*up*) y se le asigna una dirección IP, el IOS de Cisco automáticamente agrega dos entradas a la tabla de enrutamiento para esa interfaz:

- **Una entrada de red conectada:** Indica la red a la que pertenece la interfaz.
- **Una entrada de interfaz local:** Representa la dirección IP de la interfaz misma, lo que permite que el router se procese a sí mismo como destino para ciertos tipos de tráfico o para funciones de gestión (Odom, 2013).

Esta conexión se registra automáticamente en la tabla de enrutamiento con una Distancia Administrativa (AD) de 0, lo que la convierte en la fuente de información de enrutamiento más confiable (Forouzan, 2007).

Verificación de rutas conectadas: show ip route

El comando show ip route permite visualizar la tabla de enrutamiento completa, identificando rutas conectadas (C), estáticas (S) y dinámicas (D, R) (Cisco Networking Academy, 2024).

Ejemplo de salida

```
Router# show ip route
Codes: 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
       i - IS-IS, su - IS-IS summary, 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 not set

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.0.0.0/24 is directly connected, GigabitEthernet0/0
L       10.0.0.1/32 is directly connected, GigabitEthernet0/0
C    192.168.1.0/24 is directly connected, GigabitEthernet0/1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/1
```

Ilustración 3. Salida de una tabla de enrutamiento

Fuente: Elaboración propia.

En este ejemplo, 10.0.0.0/24 y 192.168.1.0/24 son redes directamente conectadas a las interfaces GigabitEthernet0/0 y GigabitEthernet0/1 respectivamente. Las entradas con "L" representan las direcciones IP locales de las interfaces.

2.2. Rutas Estáticas y Rutas Predeterminadas

Las rutas estáticas permiten al administrador definir manualmente caminos específicos para el tráfico de datos, brindando un control granular y seguridad sobre el flujo de información (Forouzan, 2007). Son particularmente útiles en redes pequeñas, redes stub (aquellas con una única salida), o cuando se requiere

una política de enrutamiento muy específica que no es fácilmente lograda por protocolos dinámicos.

Configuración de ruta estática:

El comando ip route permite crear rutas estáticas especificando la red destino, la máscara de subred y el siguiente salto o interfaz de salida.

ip route [red_destino] [máscara_subred] [next-hop | interfaz_salida]

Consideraciones para Rutas Estáticas:

- **Siguiente Salto (Next-hop IP address):** Especificar la dirección IP del router vecino al que se deben enviar los paquetes. Esto es generalmente recomendado para enlaces multi-acceso como Ethernet, ya que reduce la dependencia de la resolución ARP para cada paquete. **Ejemplo:** ip route 192.168.3.0 255.255.255.0 10.0.0.2 (Los paquetes para 192.168.3.0/24 se enviarán al router con IP 10.0.0.2).
- **Interfaz de Salida:** Especificar la interfaz local del router a través de la cual los paquetes deben salir. Esto es común en enlaces punto a punto (como enlaces seriales). Para enlaces multi-acceso, el router debe realizar una búsqueda recursiva para resolver la dirección IP del siguiente salto a una interfaz de salida, lo que puede causar problemas si la interfaz no está *up* o si la dirección del siguiente salto es inaccesible (Cisco Networking Academy, 2024). **Ejemplo:** ip route 192.168.3.0 255.255.255.0 GigabitEthernet0/1 (Los paquetes para

192.168.3.0/24 saldrán por la interfaz Gig0/1 de este router).

- **Ruta Estática Flotante:** Una ruta estática puede configurarse con una distancia administrativa más alta que la predeterminada para actuar como una ruta de respaldo. Si la ruta principal (con AD más baja, por ejemplo, aprendida dinámicamente) falla, la ruta estática flotante tomará su lugar (Cisco Networking Academy, 2024).

La ruta predeterminada (tambien llamada "ruta por defecto") dirige el tráfico hacia un destino cuando no existe una ruta específica en la tabla de enrutamiento (Kurose & Ross, 2021).

Configuración de ruta predeterminada:

ip route 0.0.0.0 0.0.0.0 [next-hop]

Ejemplo: ip route 0.0.0.0 0.0.0.0 203.0.113.1

(Todo el tráfico para destinos no específicos se enviará a la dirección IP 203.0.113.1).

2.3. Convergencia en Enrutamiento

La convergencia en redes de enrutamiento se refiere al proceso mediante el cual todos los routers en una red logran un estado de consistencia en sus tablas de enrutamiento, reflejando rutas actualizadas y precisas después de un cambio topológico (Kurose & Ross, 2021). Cuando ocurre un cambio en la topología de la red (por ejemplo, un enlace cae, un router se apaga, o se añade una nueva red), los routers deben

descubrir este cambio y actualizar sus tablas de enrutamiento para reflejar la nueva realidad.

Un estado convergente significa que todos los routers tienen una visión coherente de la red, han acordado las mejores rutas y la red está lista para reenviar paquetes de manera eficiente. Una red altamente convergente minimiza tiempos de interrupción (*downtime*) y garantiza una comunicación fiable y predecible. Los protocolos de enrutamiento dinámico están diseñados para lograr y mantener la convergencia de manera automática (Odom, 2013).

Factores que Afectan la Convergencia:

- **Tipo de Algoritmo de Enrutamiento:** Los algoritmos de estado de enlace (como OSPF) suelen converger más rápido que los de vector de distancia (como RIP) debido a la forma en que comparten la información de la topología.
- **Tamaño de la Red:** Redes más grandes con más routers y enlaces pueden tardar más en converger.
- **Estabilidad del Enlace:** Enlaces inestables que caen y se levantan repetidamente pueden dificultar la convergencia.
- **Diseño de la Red:** Un diseño de red jerárquico y bien segmentado puede mejorar los tiempos de convergencia.
- ---

2.4. Métricas de Enrutamiento

Las métricas son valores numéricos utilizados por los protocolos de enrutamiento para determinar la "mejor" ruta hacia un destino cuando existen múltiples caminos posibles (Cisco Networking Academy, 2024). Cada protocolo de enrutamiento tiene su propia forma de calcular y utilizar estas métricas. El protocolo siempre selecciona la ruta con el valor de métrica más

bajo, ya que un valor más bajo generalmente indica un "costo" o "distancia" menor para alcanzar el destino.

Estas métricas pueden incluir:

- **Saltos (*Hops*):** Utilizado por RIP. Simplemente cuenta el número de routers por los que debe pasar un paquete para llegar a su destino. Una ruta con menos saltos se considera mejor.
- **Ancho de Banda (*Bandwidth*):** Utilizado por OSPF y EIGRP. Representa la capacidad de un enlace de red (por ejemplo, 100 Mbps, 1 Gbps). Una mayor capacidad de ancho de banda generalmente se traduce en un menor costo o una métrica más baja.
- **Retardo (*Delay*):** Utilizado por EIGRP y OSPF (como parte del costo). Mide el tiempo que tarda un paquete en viajar a través de un enlace. Un retardo menor es preferible.
- **Carga (*Load*):** Utilizado por EIGRP. Refleja la cantidad de tráfico que pasa por un enlace. Un enlace con menor carga es más deseable.
- **Confiabilidad (*Reliability*):** Utilizado por EIGRP. Indica la probabilidad de que un enlace permanezca activo o libre de errores. Un enlace más confiable es preferible.

La combinación y ponderación de estas métricas varían entre los protocolos, lo que influye en su idoneidad para diferentes tipos de redes (Doyle & Carroll, 2005).

2.5. Distancia Administrativa

La distancia administrativa (AD) es un valor que indica la confiabilidad de una fuente de información de enrutamiento (Forouzan, 2007). Cuando existen múltiples rutas hacia un mismo destino aprendidas por diferentes métodos, el router utiliza la ruta con menor AD.

Tabla 3. Ejemplo de Distancias Administrativas

Fuente: Cisco Networking Academy, 2024.

Origen de la Ruta	Distancia Administrativa
Conectada Directamente	0
Estática	1
EIGRP	90
OSPF	110
RIP	120

Ejemplo de Aplicación de AD:

Supongamos que un router tiene dos rutas para alcanzar la red 192.168.50.0/24:

- Una ruta aprendida por OSPF (AD = 110).
- Una ruta aprendida por RIP (AD = 120).

El router instalará la ruta aprendida por OSPF en su tabla de enrutamiento, ya que tiene una AD menor

(110 es menor que 120), indicando que es una fuente de información más fiable para el router.

2.6. Protocolos de Enrutamiento: IGP y EGP

Los **protocolos de enrutamiento** son un conjunto de reglas y especificaciones que permiten a los routers comunicarse entre sí para intercambiar información sobre la topología de la red y las rutas disponibles (Forouzan, 2007). Esta información se utiliza para construir y mantener las tablas de enrutamiento, que a su vez permiten a los routers tomar decisiones informadas sobre cómo reenviar los paquetes de datos. Los protocolos de enrutamiento automatizan el proceso de descubrir redes y determinar las mejores rutas, reduciendo la necesidad de configuración manual y permitiendo que las redes se adapten dinámicamente a los cambios (Odom, 2013).

Los protocolos de enrutamiento se pueden clasificar en dos categorías principales, basadas en el concepto de Sistema Autónomo (AS):

- **IGP (Interior Gateway Protocol):** Estos protocolos se utilizan dentro de un único sistema autónomo (AS). Un sistema autónomo es una colección de redes bajo una administración común, como la red de una empresa o una organización. Ejemplos comunes de IGP incluyen RIP (Routing Information Protocol), OSPF (Open Shortest Path First) y EIGRP (Enhanced Interior Gateway Routing Protocol) (Forouzan, 2007).
- **EGP (Exterior Gateway Protocol):** Estos protocolos se utilizan para intercambiar información de

enrutamiento entre diferentes sistemas autónomos. El ejemplo principal de un EGP es BGP (Border Gateway Protocol), que se utiliza para el enrutamiento en Internet (Forouzan, 2007).

Diagrama:

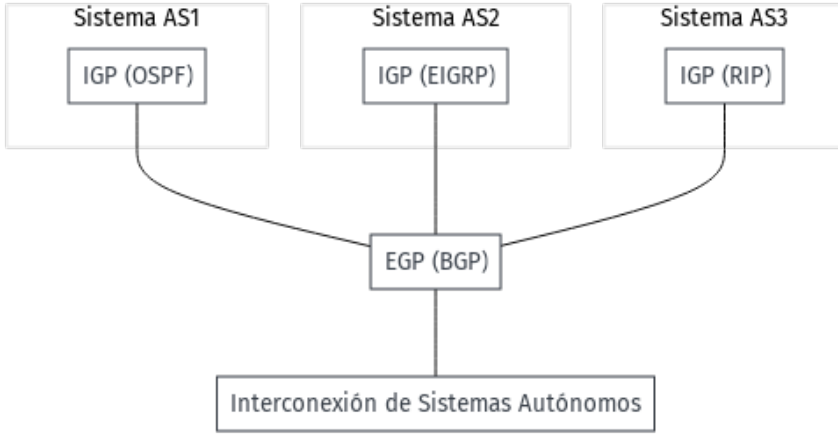

Ilustración 4. Interconexión de Sistemas Autónomos

Fuente: Elaboración propia.

Verificación de protocolos de enrutamiento:

El comando show ip protocols es una herramienta valiosa para verificar qué protocolos de enrutamiento están activos en un router y para examinar sus parámetros de configuración. Este comando proporciona información detallada sobre los protocolos de enrutamiento que se están ejecutando, incluyendo:

- **Protocolo de enrutamiento:** Indica qué protocolo (por ejemplo, RIP, OSPF, EIGRP) está configurado y activo.

- **Tiempos de actualización:** Muestra los intervalos en los que el protocolo envía actualizaciones de enrutamiento (ej., 30 segundos para RIP).
- **Redes anunciadas:** Lista las redes que el router está anunciando a otros routers.
- **Distancia Administrativa:** Muestra la distancia administrativa del protocolo, que es el valor predeterminado que utiliza el router para elegir entre rutas aprendidas de diferentes protocolos.
- **Métricas:** Indica las métricas que el protocolo está utilizando para calcular las rutas y los valores máximos permitidos (ej., máximo de 15 saltos para RIP).
- **Vecinos:** En algunos protocolos (como OSPF o EIGRP), muestra los vecinos con los que el router ha establecido adyacencias.

Ejemplo:

```
Router#show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 2 seconds
  Invalid after 180 seconds, hold down 180 seconds, flushed after 240 seconds
  Outgoing update filter list:
  Incoming update filter list:
  Redistributing: rip
  Default version control: send version 2, receive version 2
    Send packets of version 2
  Invalid after 180 seconds, hold down 180 seconds, flushed after 240 seconds
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    192.168.1.0
    192.168.2.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.2.2           120      00:00:16
  Distance: (120)
```

Ilustración 5. Verificación de protocolo de enrutamiento activo

Fuente: Elaboración propia.

Este resultado muestra que el protocolo de enrutamiento RIP está activo, con sus temporizadores, redes anunciadas y otra información relevante. En este caso, se confirma que RIP v2 está en ejecución, publicando las redes 192.168.1.0 y 192.168.2.0, y con su distancia administrativa por defecto de 120.

2.7. Algoritmos: Vector de Distancia y Estado de Enlace

Un algoritmo de enrutamiento es un procedimiento que un router utiliza para determinar la mejor ruta para reenviar un paquete de datos a través de una red. Los algoritmos de enrutamiento son la base de los protocolos de enrutamiento y dictan cómo los routers recopilan, comparten y procesan la información de enrutamiento (Kurose & Ross, 2021).

- **Algoritmos de Vector de Distancia:** En los algoritmos de vector de distancia, cada router mantiene una tabla que contiene las distancias (en términos de una métrica, como el número de saltos) a todas las demás redes en el sistema. Los routers comparten esta información con sus vecinos directos, y cada router actualiza su tabla basándose en la información recibida. Los algoritmos de vector de distancia son simples de implementar, pero pueden sufrir de problemas como los bucles de enrutamiento y la convergencia lenta. RIP es un ejemplo de un protocolo que utiliza un algoritmo de vector de distancia (Kurose & Ross, 2021).
- **Algoritmos de Estado de Enlace:** En los algoritmos de estado de enlace, cada router construye un mapa completo de la topología de la red. Esto se logra intercambiando

información sobre los enlaces directamente conectados con todos los demás routers en el sistema. Una vez que un router tiene el mapa completo, puede calcular la mejor ruta a cualquier destino utilizando un algoritmo de camino más corto, como el algoritmo de Dijkstra. Los algoritmos de estado de enlace son más complejos que los algoritmos de vector de distancia, pero convergen más rápido y son menos propensos a los bucles de enrutamiento. OSPF es un ejemplo de un protocolo que utiliza un algoritmo de estado de enlace (Kurose & Ross, 2021).

Tabla 4. Comparación de Algoritmos

Criterio	**Vector de Distancia**	**Estado de Enlace**
Velocidad de convergencia	Lenta	Rápida
Escalabilidad	Limitada	Alta
Complejidad	Baja	Alta
Información de red	Información de vecinos	Mapa completo de la topología
Recursos del router	Menos	Más
Ejemplo	RIP	OSPF

Fuente: Elaboración propia basada en Kurose & Ross, 2021; Forouzan, 2007.

2.8. Configuración y Verificación de RIP v2

RIP versión 2 (RIPv2) es una versión mejorada del protocolo de enrutamiento RIP. RIPv2 resuelve algunas de las limitaciones de la versión original, como la falta de soporte para VLSM (Variable Length Subnet Masking) y la autenticación. RIPv2 es un protocolo de vector de distancia que utiliza el conteo de saltos como su métrica. Es simple de configurar, pero no es muy escalable y converge lentamente, lo que lo hace inadecuado para redes grandes y complejas (Cisco Networking Academy, 2024).

Configuración básica de RIP v2

Para configurar RIPv2 en un router Cisco, se utilizan los siguientes comandos en el modo de configuración global:

router rip: Permite ingresar al modo de configuración de RIP, habilitando su funcionamiento en el router para la distribución de información de enrutamiento (Cisco Networking Academy, 2024).

version 2: Indica explícitamente al router que utilice la versión 2 del protocolo, soportando enrutamiento sin clases y autenticación (Forouzan, 2007).

network [red]: Informa al router qué redes deben ser anunciadas mediante RIP. No especifica subredes, sino redes principales cuyos prefijos serán anunciados (Cisco Networking Academy, 2024).

no auto-summary: Desactiva el resumen automático de rutas en RIP v2, permitiendo

anunciar subredes específicas, especialmente en redes que utilizan VLSM (Forouzan, 2007).

Ejemplo de configuración básica:

```
Router> enable

Router# configure terminal

Router(config)# router rip

Router(config-router)# version 2

Router(config-router)# network 192.168.1.0

Router(config-router)# network 192.168.2.0

Router(config-router)# no auto-summary
```

En este ejemplo, el router está configurado para ejecutar RIPv2 y anunciar las redes 192.168.1.0/24 y 192.168.2.0/24 (asumiendo que las interfaces del router pertenecen a estas subredes). La deshabilitación del resumen automático asegura que las subredes se anuncien con sus máscaras originales.

Verificación de la operación de RIP v2

Para verificar el correcto funcionamiento y las rutas aprendidas por RIPv2, se utilizan varios comandos:

show ip protocols: Muestra información sobre los protocolos de enrutamiento activos, incluyendo redes anunciadas, temporizadores de actualización y detalles de configuración.

show ip route rip: Permite visualizar las rutas aprendidas por RIP en la tabla de enrutamiento.

debug ip rip: Muestra en tiempo real los procesos de intercambio de información de

RIP, útil para diagnóstico de problemas (Cisco Networking Academy, 2024).

Ejemplo de verificación:

```
Router#show ip route rip
192.168.3.0/24 [120/1] via 192.168.2.2, 00:00:16, GigabitEthernet0/1
```

Ilustración 6. Verificación de tabla de enrutamiento con rutas RIP

Fuente: Elaboración propia.

Este resultado indica que el router ha aprendido la ruta a la red 192.168.3.0/24 a través de RIP, con una distancia administrativa de 120 (por defecto para RIP) y una métrica de 1 salto (lo que significa que la red está a un router de distancia), a través del vecino 192.168.2.2 (la dirección IP del siguiente salto). La indicación [120/1] se interpreta como [Distancia Administrativa / Métrica].

2.9. Práctica Guiada: Configuración de Rutas Estáticas en Cisco Packet Tracer

Objetivo: Configurar rutas estáticas en una red compuesta por tres routers interconectados, para garantizar la conectividad de extremo a extremo entre dos PCs.

Ilustración 7. Topología de red propuesta para la práctica de configuración de rutas estáticas en Cisco Packet Tracer

Fuente: Elaboración propia

Materiales requeridos:

Software Cisco Packet Tracer (versión 8.0 o superior)

3 routers Cisco (serie 2901 sugerido)

2 switches

2 PCs (usuario final)

Cables de conexión adecuados (cable directo y cruzado)

Topología sugerida:

Conexiones:

PC0 ↔ SW0 ↔ R1 (Gig0/0)

R1 (Gig0/1) ↔ R2 (Gig0/0)

R2 (Gig0/1) ↔ R3 (Gig0/1)

R3 (Gig0/0) ↔ SW1 ↔ PC1

Pasos para la configuración:

1. Asignación de direcciones IP:

   Cada red entre dispositivos debe pertenecer a subredes distintas.

2. Configuración básica de routers:

   Asignar nombre al dispositivo (hostname).

3. Configurar las interfaces GigabitEthernet con IP y activarlas (no shutdown).

4. Configuración de rutas estáticas:

   En R1: agregar ruta hacia redes detrás de R3.

En R3: agregar ruta hacia redes detrás de R1.

En R2: Agregar las rutas estáticas necesarias.

5. Configuración de IP en PCs: Asegurar que PC0 y PC1 tengan sus direcciones IP y puertas de enlace predeterminadas configuradas correctamente, apuntando a la interfaz de su router directamente conectado.

Resultados esperados:

Comunicación exitosa entre PC0 y PC1.

RIP v2 correctamente anunciado en R2.

Tablas de enrutamiento de R1, R2 y R3 actualizadas y optimizadas.

Preguntas de reflexión:

1. ¿Qué ventajas ofrece el uso de rutas estáticas en una red?

Las rutas estáticas ofrecen control total sobre las rutas de tráfico, lo que puede mejorar la seguridad y la eficiencia en redes pequeñas o con topologías predecibles.

2. ¿En qué situaciones sería más apropiado utilizar rutas estáticas en lugar de protocolos de enrutamiento dinámico?

Las rutas estáticas son más apropiadas en redes stub (con una única salida), redes pequeñas con pocos cambios o cuando se requiere un control estricto del tráfico.

3. ¿Cómo afectaría un cambio en la topología de la red a la configuración de las rutas estáticas?

Cualquier cambio en la topología requeriría una reconfiguración manual de las rutas estáticas, lo que puede ser una desventaja en redes dinámicas.

4. ¿Cuál es la importancia de la ruta predeterminada en una red con rutas estáticas?

La ruta predeterminada asegura que el tráfico con destinos desconocidos tenga una ruta de salida, permitiendo la conectividad a redes externas.

2.10. Práctica Guiada: Configuración de RIPv2 en Cisco Packet Tracer

Objetivo: Configurar el protocolo de enrutamiento dinámico RIP versión 2 en una red compuesta por tres routers interconectados, para garantizar la actualización automática de rutas entre routers.

Ilustración 8. Topología de red propuesta para la práctica de configuración de RIPv2 en Cisco Packet Tracer

Fuente: Elaboración propia

Materiales requeridos:

Software Cisco Packet Tracer (versión 8.0 o superior)

3 routers Cisco

2 switches

2 PCs (usuario final)

Cables de conexión adecuados

Topología sugerida:

Conexiones:

PC0 ↔ SW0 ↔ R1 (Gig0/0)

R1 (Gig0/1) ↔ R2 (Gig0/0)

R2 (Gig0/1) ↔ R3 (Gig0/1)

R3 (Gig0/0) ↔ SW1 ↔ PC1

Pasos para la configuración:

1. **Configuración básica de interfaces:** Ingresar a la configuración de cada router y configurar las interfaces (GigabitEthernet) con sus respectivas direcciones IP y máscaras de subred, y activarlas con el comando no shutdown. (Asegúrate de que las interfaces PC0-SW0-R1 y PC1-SW1-R3 también tengan direcciones IP configuradas).
2. **Activar RIP versión 2:** En cada router, ingresar al modo de configuración de enrutamiento y especificar la versión 2.
3. **Publicar las redes directamente conectadas:** Usar el comando network [dirección_de_red_de_clase] para cada red directamente conectada a las interfaces del router. Esto le indica a RIP qué redes debe incluir en sus actualizaciones y por qué interfaces debe enviar actualizaciones.
4. **Desactivar el resumen automático:** En cada router, usar no auto-summary para asegurar que las subredes sean anunciadas con sus máscaras completas, esencial para VLSM y subredes discontinuas.

5. **Guardar la configuración.**
6. **Verificar el funcionamiento:** Utilizar los comandos show ip protocols, show ip route rip, y debug ip rip (con precaución) para observar el intercambio de rutas y el estado de la tabla de enrutamiento.

Resultados esperados:

Actualización automática de las tablas de enrutamiento entre los routers.

Conectividad de extremo a extremo validada por pings exitosos.

Preguntas de reflexión:

1. **¿Cómo simplifica RIPv2 la administración de la red en comparación con las rutas estáticas?**

RIPv2 automatiza el descubrimiento de rutas y la adaptación a los cambios en la red, reduciendo la necesidad de configuración manual.

2. **¿Cuáles son las limitaciones de RIPv2 en términos de escalabilidad y convergencia?**

RIPv2 tiene limitaciones en redes grandes debido a su lenta convergencia y alta carga de tráfico por las actualizaciones periódicas.

3. **¿Por qué es importante desactivar la sumarización automática en RIPv2?**

Desactivar la sumarización automática permite el soporte de VLSM y el enrutamiento entre subredes no contiguas.

4. ¿Qué información proporciona el comando show ip protocols sobre el funcionamiento de RIPv2?

El comando muestra los parámetros de configuración de RIPv2, como las redes anunciadas, los temporizadores y los vecinos.

2.11. Evaluación del capítulo

1. El comando para configurar una ruta estática es:

a) router rip

b) ip route ✅

c) show ip route

d) enable

2. ¿Qué protocolo es de vector de distancia?

a) OSPF

b) RIP ✅

c) EIGRP

d) BGP

3. En la tabla de enrutamiento, ¿qué letra indica una ruta conectada directamente?

a) S

b) D

c) C ✅

d) R

4. Una dirección de red con prefijo /26 tiene cuántas direcciones IP utilizables?

a) 30

b) 62 ✅

c) 126

d) 254

5. ¿Cuál es la función principal de un protocolo de enrutamiento?

a) Asignar direcciones IP a los dispositivos de la red.

b) Permitir la comunicación entre diferentes protocolos de red.

c) Determinar la mejor ruta para enviar paquetes de datos a través de la red. ✅

d) Proporcionar seguridad a la red mediante el cifrado de datos.

6. ¿Qué tipo de algoritmo utiliza el protocolo OSPF?

a) Vector de distancia.

b) Estado de enlace. ✅

c) Híbrido.

d) Basado en políticas.

7. ¿Cuál de las siguientes métricas no se utiliza comúnmente en los protocolos de enrutamiento?

a) Ancho de banda.

b) Retardo.

c) Costo.

d) Nombre de dominio. ✅

8. ¿Qué valor de distancia administrativa tiene una ruta estática?

a) 0

b) 1 ✅

c) 90

d) 110

Referencias Bibliográficas

Cisco Networking Academy. (2024). *Introduction to Networks*. Cisco Systems. ISBN: 9781587134265

Doyle, J., & Carroll, J. (2005). *Routing TCP/IP, Volume I* (2nd ed.). Cisco Press. ISBN: 9781587052026

Forouzan, B. A. (2007). *Data Communications and Networking*. McGraw-Hill. ISBN: 9780072967753

Kurose, J. F., & Ross, K. W. (2021). *Computer Networking: A Top-Down Approach* (8th ed.). Pearson. ISBN: 9780136681557

Odom, W. (2013). *CCNA Routing and Switching Official Cert Guide, Volume 1* (Associate Level). Cisco Press. ISBN: 9781587205477

Capítulo 3: VLSM y Diseño de Subredes Eficientes

Introducción

El vertiginoso crecimiento de las redes de computadoras y la constante demanda de conectividad han puesto de manifiesto la necesidad imperante de utilizar técnicas que optimicen el escaso y valioso espacio de direccionamiento IP. Particularmente en IPv4, donde la cantidad de direcciones es finita, el uso tradicional de subredes de tamaño fijo, aunque conceptualmente sencillo, genera un alto desperdicio de direcciones. Este derroche se hace más evidente cuando se conectan segmentos de red con requisitos de tamaño muy dispares, como una oficina principal con cientos de dispositivos y una sucursal pequeña con solo unos pocos.

Para solventar esta ineficiencia, la industria de redes adoptó el concepto de VLSM (Variable Length Subnet Masking). VLSM es una técnica de subneteo que rompe con la rigidez del enfoque tradicional, permitiendo asignar máscaras de subred de diferentes longitudes (o prefijos CIDR variables) dentro de una misma red principal. Esto posibilita adaptar cada subred al número real de dispositivos que requiere soporte, maximizando la utilización de las direcciones IP disponibles y haciendo más sostenible el diseño de redes (Odom, 2013).

A medida que una red crece y se interconectan múltiples subredes de diversos tamaños —especialmente aquellas creadas con VLSM—, la complejidad de las tablas de enrutamiento puede aumentar exponencialmente. Aquí es donde entra en

juego el concepto de Resumen de Rutas (*Route Summarization*) o Agregación de Rutas (*Route Aggregation*). Esta poderosa técnica permite agrupar múltiples rutas específicas y contiguas en una sola entrada más general en la tabla de enrutamiento. Al consolidar la información de enrutamiento, se simplifican drásticamente las tablas de enrutamiento, se disminuye la carga de procesamiento en los *routers*, se reduce el tráfico de actualizaciones de enrutamiento, y se acelera significativamente la convergencia de la red tras un cambio topológico (Doyle & Carroll, 2005).

Este capítulo desarrolla estos dos conceptos fundamentales del diseño de redes, VLSM y Resumen de Rutas, integrando teoría y práctica mediante simulaciones en Cisco Packet Tracer. Estas prácticas guiadas permitirán al lector aplicar de forma progresiva lo aprendido en el diseño eficiente de subredes y en la implementación de un enrutamiento escalable, sentando bases sólidas para redes modernas y resilientes.

Objetivos del Capítulo

- Identificar los fundamentos de VLSM y las causas de subredes solapadas, mediante el análisis de máscaras de subred y rangos IP, para prevenir errores comunes en el diseño de direccionamiento.
- Explicar el funcionamiento del resumen de rutas manual y automático, mediante ejercicios de cálculo y esquemas de red, para comprender cómo influye en la tabla de enrutamiento.
- Detectar los efectos del autoresumen en protocolos de enrutamiento como RIP, mediante simulaciones y observación del comportamiento

de rutas, para evitar la pérdida de conectividad entre redes.

- Aplicar el diseño eficiente de subredes con VLSM, mediante la asignación progresiva de máscaras según la cantidad de hosts, para optimizar el espacio de direcciones IP en redes heterogéneas.
- Implementar configuraciones de VLSM y resumen de rutas en routers Cisco, mediante prácticas guiadas en Cisco Packet Tracer, para desarrollar habilidades técnicas en el diseño y administración de redes.

3.1. ¿Qué es VLSM y para qué se utiliza?

VLSM (Variable Length Subnet Masking), o enmascaramiento de subred de longitud variable, es una técnica de diseño de redes que permite utilizar diferentes longitudes de máscara de subred (o prefijos CIDR) dentro de una misma red principal (Cisco Networking Academy, 2024). A diferencia del subneteo tradicional (o Classful Addressing), que divide una red en subredes de tamaño fijo e igual, VLSM permite crear subredes con tamaños que se ajustan con precisión a las necesidades reales de cada segmento de red, optimizando significativamente el uso del espacio de direcciones IPv4 (Forouzan, 2007).

Este enfoque flexible permite asignar el número exacto (o el bloque más cercano y eficiente) de direcciones IP necesarias para cada subred, reduciendo drásticamente el desperdicio de direcciones IP. Esto es especialmente útil en organizaciones donde coexisten redes de diferentes escalas, como grandes departamentos administrativos (que pueden requerir un gran número de direcciones) y enlaces punto a punto entre *routers*

(que solo necesitan dos direcciones utilizables) (Odom, 2013).

Tabla 5. Ejemplo de comparación entre subneteo tradicional y VLSM

Técnica	**Subredes creadas**	**Ejemplo de máscara**	**Direcciones desperdiciadas**
Subneteo tradicional	4 iguales	/26, /26, /26, /26	Alta (si las redes son desiguales)
VLSM	4 de distinto tamaño	/26, /27, /28, /30	Mínima (ajustada a la necesidad)

Fuente: Elaboración propia basada en Cisco Networking Academy (2024).

En términos prácticos, VLSM mejora la eficiencia de las redes IPv4 al permitir la reutilización inteligente de espacios IP. Por ejemplo, si se toma una red /24 y se necesita un enlace punto a punto (requiere 2 direcciones), con subneteo tradicional se podría asignar una /28 (14 *hosts* utilizables), desperdiciando 12 direcciones. Con VLSM, se puede asignar una /30 (2 *hosts* utilizables), desperdiciando cero direcciones adicionales y preservando el espacio para otras subredes (Kurose & Ross, 2021).

Esta técnica se apoya en cálculos binarios similares a los del subneteo tradicional, pero con mayor flexibilidad en la asignación de bits de *host* y de subred. Además, requiere especial atención al orden de diseño: es crucial comenzar siempre por la subred que requiere el mayor número de *hosts* y descender progresivamente hasta la que necesita menos. Este ordenamiento es vital para evitar el solapamiento de subredes y garantizar que los bloques de direcciones no se superpongan (Forouzan, 2007).

3.2. Diseño eficiente de subredes con VLSM

Para implementar un esquema de direccionamiento eficiente con VLSM, es fundamental planificar la asignación de direcciones considerando la cantidad real de *hosts* requeridos por cada subred. A diferencia del enfoque de subneteo tradicional, con VLSM no se desperdician direcciones al asignar bloques de tamaño fijo a necesidades variables. El procedimiento recomendado, basado en las mejores prácticas de diseño de redes, consiste en (Odom, 2013; Cisco Networking Academy, 2024):

1. **Determinar cuántas subredes se necesitan y cuántos *hosts* requiere cada una.** Esto implica un análisis exhaustivo de los requisitos actuales y futuros de cada segmento de red (ej., departamentos, enlaces entre *routers*, zonas de servidores). Es importante considerar un pequeño margen de crecimiento.
2. **Ordenar las subredes de mayor a menor número de *hosts* requeridos.** Este es un paso crítico para evitar solapamientos y maximizar la eficiencia del espacio IP. Al asignar primero los bloques más grandes, se garantiza que queden

suficientes direcciones contiguas para acomodar los bloques más pequeños.

3. Asignar a cada subred el bloque de direcciones más pequeño que satisfaga su necesidad. Para calcular esto, se utiliza la fórmula $2^n - 2$ donde 'n' es el número de bits de *host* (y por lo tanto, la longitud de la máscara CIDR). Siempre se selecciona la potencia de 2 más pequeña que sea igual o mayor al número de *hosts* más 2 (dirección de red y dirección de *broadcast*).

4. Calcular los rangos de direcciones de red, *broadcast* y direcciones utilizables para cada subred. Es esencial documentar estos rangos para verificar que no haya solapamientos y para futuras configuraciones. Cada bloque debe iniciarse en una dirección que sea múltiplo del tamaño del bloque asignado (ej., una subred /26 debe empezar en un múltiplo de 64, una /27 en un múltiplo de 32, etc.).

Ejemplo práctico: Una empresa requiere direccionar los siguientes departamentos:

- Administración: 50 hosts
- Ventas: 30 hosts
- Soporte técnico: 14 hosts
- Dirección general: 6 hosts
- Enlace R1-R2: 2 hosts
- Enlace R2-R3: 2 hosts

Resolución paso a paso del ejercicio VLSM:

1. Ordenar por número de hosts (de mayor a menor):

- Administración: 50 hosts
- Ventas: 30 hosts
- Soporte Técnico: 14 hosts
- Dirección General: 6 hosts

- Enlace R1-R2: 2 hosts
- Enlace R2-R3: 2 hosts

2. Análisis de necesidades:

- Administración → necesita 50 hosts reales → se requiere un bloque de 64 direcciones (2^6 = 64), es decir, una máscara /26.
- Ventas → necesita 30 hosts reales → se requiere un bloque de 32 direcciones (2^5 = 32), máscara /27.
- Soporte técnico → necesita 14 hosts reales → requiere un bloque de 16 direcciones (2^4 = 16), máscara /28.
- Dirección general → necesita 6 hosts reales → requiere un bloque de 8 direcciones (2^3 = 8), máscara /29.
- Enlaces R1-R2 y R2-R3 → necesita 2 hosts reales → se requiere un bloque de 4 direcciones (2^2 = 4), es decir, una máscara /30.

3. Asignación ordenada desde una red mayor: Supongamos que partimos de la red 192.168.10.0/24.

Bloques asignados:

Tabla 6. Asignación de subredes con VLSM

Departamento	**Hosts necesarios**	**Máscara CIDR**	**Rango de direcciones**
Administración	50	/26	192.168.10.0 – 192.168.10.63
Ventas	30	/27	192.168.10.64 – 192.168.10.95
Soporte técnico	14	/28	192.168.10.96 – 192.168.10.111
Dirección general	6	/29	192.168.10.112 – 192.168.10.119
Enlace R1-R2	2	/30	192.168.10.120 – 192.168.10.123
Enlace R2-R3	2	/30	192.168.10.1 192.168.10 .127

Fuente: Elaboración propia con base en Cisco Networking Academy (2024).

4. Validación del diseño:

Como se observa en la tabla, todos los bloques de subredes son contiguos y no se traslapan, garantizando un direccionamiento lógico y sin conflictos. Además, el diseño ha utilizado de manera eficiente solo 128 direcciones de la red principal /24 (desde 192.168.10.0 hasta 192.168.10.127). Queda

un espacio disponible considerable para futuras asignaciones dentro del rango 192.168.10.128 – 192.168.10.255, lo que demuestra la flexibilidad y eficiencia de VLSM.

Este tipo de diseño minimiza el desperdicio de direcciones IP, facilita el crecimiento de la red de manera organizada y permite implementar técnicas complementarias como el resumen de rutas, haciendo la red más escalable. Para la asignación de subredes, puede emplearse una calculadora de subredes o realizarse manualmente aplicando lógica binaria, considerando el número de bits necesarios para cubrir la cantidad de *hosts* solicitados (Kurose & Ross, 2021).

3.3. Subredes solapadas y no solapadas

Un error crítico en el diseño de direccionamiento IP es la creación de subredes solapadas (o superpuestas). Una subred solapada ocurre cuando dos o más rangos de direcciones IP asignadas a diferentes interfaces de *routers* o segmentos de red tienen intersecciones, es decir, comparten una o más direcciones dentro de sus rangos válidos (Odom, 2013). Este tipo de conflicto en el diseño genera problemas severos e impredecibles en la red, como conflictos de direcciones IP, enrutamiento ineficaz (paquetes dirigidos a la interfaz incorrecta), pérdida de conectividad, y errores en la propagación de rutas, lo que a menudo resulta en redes inestables e imposibles de diagnosticar eficientemente.

Ejemplo de solapamiento:

Consideremos el siguiente escenario erróneo:

- Subred A: 192.168.10.0/25 → Rangos: 192.168.10.0 – 192.168.10.127
- Subred B: 192.168.10.64/26 → Rangos: 192.168.10.64 – 192.168.10.127

Como se observa, la Subred B (192.168.10.64/26) está completamente contenida dentro de la Subred A (192.168.10.0/25). Ambas subredes contienen direcciones comunes entre 192.168.10.64 y 192.168.10.127, lo que provoca ambigüedad al momento de enrutar paquetes. Un *router* conectado a ambas subredes no sabría a qué interfaz enviar un paquete destinado a, por ejemplo, 192.168.10.70.

Prevención del solapamiento:

La clave para evitar subredes solapadas radica en una planificación meticulosa y el uso correcto de VLSM:

- **Utilizar VLSM con planificación lógica:** Aplicar los principios de VLSM, asignando el tamaño de bloque exacto.
- **Asignar subredes en orden decreciente de tamaño:** Como se demostró en la sección 3.2, empezar con las subredes más grandes y luego asignar las más pequeñas garantiza que los bloques de direcciones no se superpongan.
- **Verificar que los bloques no se crucen en sus rangos de direcciones:** Utilizar calculadoras de IP o el cálculo manual para confirmar que la dirección de *broadcast* de una subred no sea igual o mayor que la dirección de red de la siguiente subred (Forouzan, 2007).

Tabla 7. Ejemplo de subredes no solapadas correctamente asignadas

Subred	Máscara	Rango IP
Subred A	/26	192.168.10.0 – 192.168.10.63
Subred B	/27	192.168.10.64 – 192.168.10.95
Subred C	/28	192.168.10.96 – 192.168.10.111

Fuente: Elaboración propia

En este caso, cada subred tiene un rango de direcciones único y separado, eliminando cualquier posibilidad de conflicto. Esta buena práctica de diseño asegura que los routers puedan operar con tablas de enrutamiento claras y sin ambigüedades (Forouzan, 2007).

3.4. Resumen de Rutas (Route Summarization)

El resumen de rutas es una técnica utilizada en enrutamiento para agrupar varias rutas específicas en una sola, lo que reduce la cantidad de entradas en la tabla de enrutamiento. Esta simplificación mejora la eficiencia de los routers y facilita la escalabilidad en redes complejas (Cisco Networking Academy, 2024).

Beneficios del Resumen de Rutas:

La implementación del resumen de rutas ofrece ventajas significativas (Doyle & Carroll, 2005; Odom, 2013):

- **Disminuye la sobrecarga de procesamiento de la CPU:** Los *routers*

tienen menos entradas que procesar en sus tablas de enrutamiento al realizar búsquedas de rutas, lo que libera recursos de CPU.

- **Reduce el tamaño de la tabla de enrutamiento:** Al reemplazar múltiples entradas con una única ruta resumen, se consume menos memoria RAM en los *routers*.
- **Acelera la convergencia de la red:** Cuando ocurre un cambio en una subred específica que está cubierta por una ruta resumen, la ruta resumen no necesita ser actualizada o re-anunciada, a menos que todas las subredes dentro de ella fallen. Esto reduce la cantidad de actualizaciones de enrutamiento que deben procesarse y, por ende, el tiempo que tarda la red en estabilizarse.
- **Reduce el tráfico de actualizaciones de enrutamiento:** Se envían menos actualizaciones a través de la red, conservando el ancho de banda, especialmente en enlaces WAN.
- **Proporciona estabilidad:** Las fallas dentro del bloque de direcciones resumido no se propagan fuera del área de resumen, lo que mejora la estabilidad de la red global.

Tipos de resumen:

- **Manual:** Es configurado explícitamente por el administrador de red en interfaces específicas de los *routers*. Este método ofrece el mayor control y precisión sobre qué rutas se resumen y dónde.
- **Automático (*Autosummarization*):** Realizado por algunos protocolos de

enrutamiento (como RIPv1 y EIGRP por defecto) al anunciar redes de clase por defecto (A, B, C) a través de un límite de red de clase principal. Este proceso puede ser útil en redes *classful*, pero puede causar problemas de enrutamiento en redes con VLSM o diseños discontinuos, por lo que a menudo se desactiva.

Ejemplo práctico de resumen manual paso a paso:

Supongamos que un router conoce las siguientes rutas:

- 192.168.32.0/24
- 192.168.33.0/24
- 192.168.34.0/24
- 192.168.35.0/24

Paso 1: Convertir a binario las direcciones de red

Tabla 8. Conversión de decimal a binario

Fuente: Elaboración propia

Red	Dirección binaria
192.168.32.0	11000000.10101000.00100000.00000000
192.168.33.0	11000000.10101000.00100001.00000000
192.168.34.0	11000000.10101000.00100010.00000000
192.168.35.0	11000000.10101000.00100011.00000000

Paso 2: Comparar bit a bit los valores binarios

Los 22 primeros bits son iguales:

11000000.10101000.001000 → común entre todas las redes

Tabla 9. Comparación bit a bit para el resumen de rutas

Fuente: Elaboración propia

Dirección de Red	**Binario (24 bits)**
192.168.32.0	11000000.10101000.00100000
192.168.33.0	11000000.10101000.00100001
192.168.34.0	11000000.10101000.00100010
192.168.35.0	11000000.10101000.00100011

Los primeros 22 bits son comunes, lo que permite aplicar un resumen con máscara /22.

Resultado del resumen:

Dirección de resumen: 192.168.32.0

Máscara resumen: /22 (255.255.252.0)

Paso 3: Verificación del rango cubierto por el resumen

Rango de redes cubiertas por 192.168.32.0/22:

192.168.32.0 - 192.168.35.255 → cubre todas las redes originales

Ventaja:

Una sola entrada puede reemplazar cuatro, reduciendo la tabla de enrutamiento.

Configuración de Resumen de Rutas en RIP (Manual):

En Cisco IOS, el resumen manual para protocolos como RIP (en la interfaz por donde se anunciará el resumen) se configura de la siguiente manera:

Router(config-if)# ip summary-address rip 192.168.32.0 255.255.248.0

Importancia del resumen:

- Disminuye la sobrecarga de procesamiento.
- Acelera la convergencia de la red.
- Facilita la lectura de la tabla de enrutamiento.

Autoresumen y sus riesgos:

Como se mencionó, los protocolos de enrutamiento basados en clases (como RIPv1) y algunos protocolos de enrutamiento sin clases (como RIPv2 y EIGRP) realizan resumen automático al límite de clase de red por defecto. Esto significa que si un *router* tiene subredes que pertenecen a la misma red principal (*classful*) pero están en diferentes interfaces y necesita anunciarlas a través de un límite de red de clase, las

resumirá a la dirección de red de clase principal (ej., 192.168.1.0/24 y 192.168.2.0/24 serían resumidas a 192.168.0.0/16 si se cruza un *router* con una interfaz 10.x.x.x).

Este comportamiento puede causar problemas graves, especialmente en redes discontinuas (donde las subredes de una misma red principal no son contiguas o están separadas por otra red de clase diferente), ya que puede generar rutas incorrectas o pérdida de conectividad a subredes específicas (Forouzan, 2007). Por esta razón, en RIPv2 (y en EIGRP), se suele desactivar el resumen automático con el comando:

```
Router(config-router)# no auto-summary
```

Deshabilitar el autoresumen permite que los *routers* anuncien las subredes con sus máscaras VLSM completas, preservando la información de la topología exacta y evitando conflictos de enrutamiento.

3.5. Práctica Guiada: Diseño y Configuración de Subredes con VLSM

Objetivo: Diseñar e implementar una red empresarial que utilice VLSM y Resumen de Rutas para optimizar el espacio de direcciones IP y simplificar la tabla de enrutamiento.

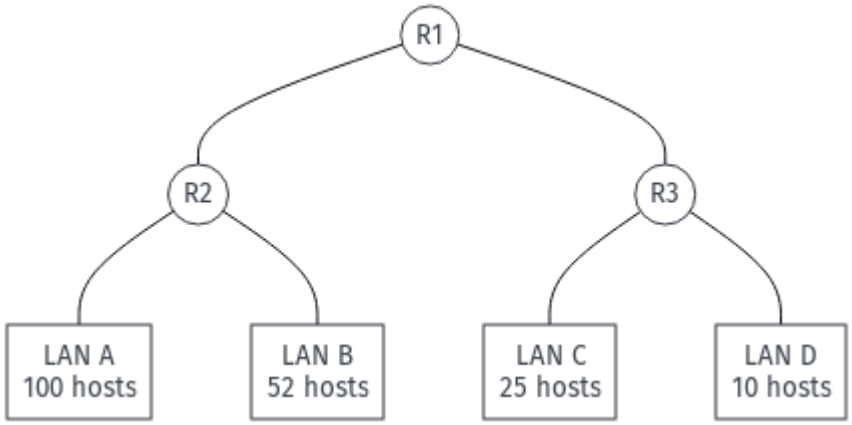

Ilustración 9. Topología de red propuesta para la práctica

Fuente: Elaboración propia.

Materiales requeridos:

Cisco Packet Tracer (v8.2 o superior)

Dispositivos: 3 routers (Cisco 2901), 2 switches

Topología sugerida:

Conexiones:

R1 conecta con R2 y R3, que a su vez conectan a LANs de diferentes tamaños:

LAN A (100 hosts), LAN B (52 hosts), LAN C (25 hosts), LAN D (10 hosts)

Considerar enlaces entre Routers.

Red principal a usar:

172.16.0.0/22 (con una máscara de red 255.255.252.0)

Diseño VLSM:

Tabla 10. Diseño VLSM propuesto

Fuente: Elaboración propia

Segmento	Hosts Necesarios	Máscara CIDR	Red Asignada
LAN-A	100	/25	172.16.0.0/25
LAN-B	50	/26	172.16.0.128/26
LAN-C	25	/27	172.16.0.192/27
LAN-D	10	/28	172.16.0.224/28
Enlace R1-R2	2	/30	172.16.0.240/30
Enlace R1-R3	2	/30	172.16.0.244/30

Pasos para la configuración:

1. Acceso inicial y configuración de hostnames

   enable

   configure terminal

   hostname R1

(Repetir para R2 y R3)

2. Configurar todas las interfaces de los *routers* con las direcciones IP y máscaras de subred calculadas en el diseño VLSM, y activarlas con no shutdown.
3. Activación de RIP v2 y desactivación del autoresumen en todos los *routers* (R1, R2, R3).

   router rip

   version 2

no auto-summary

4. Publicación de redes en RIP. En R1, R2 y R3

   network 172.16.0.0

5. Configuración de direcciones IP en PCs.

   Asegurarse de que cada PC tenga su dirección IP, máscara de subred (según VLSM) y *gateway* predeterminado correctamente configurado, apuntando a la interfaz del *router* de su propia subred.

6. Verificación del estado de interfaces y conectividad

   show ip interface brief

   show ip route

   ping [dirección IP de otra LAN]

Preguntas de reflexión:

1. ¿Por qué se inicia la asignación de direcciones con la subred que requiere más hosts?

Porque al asignar primero el bloque más grande se evita que las subredes más pequeñas interfieran en rangos de direcciones más extensos, previniendo solapamientos.

2. ¿Qué impacto tiene no configurar no auto-summary en una red discontigua?

El router podría aplicar resumen automático incorrecto al límite de clase, generando pérdida de rutas y problemas de conectividad.

3. ¿Qué ventajas ofrece configurar un resumen de rutas en el router principal?

Reduce la cantidad de rutas en la tabla de enrutamiento, mejora el rendimiento del router y acelera la convergencia.

4. ¿Qué comando permite verificar si el resumen de rutas fue aplicado correctamente?

El comando show ip route permite visualizar si se ha agregado una única entrada resumen en lugar de múltiples rutas específicas.

3.6. Evaluación del capítulo

1. ¿Qué permite hacer VLSM en el diseño de subredes?

a) Asignar máscaras iguales a todas las redes

b) Reducir el número de routers

c) Aplicar diferentes longitudes de máscara según necesidad ✅

d) Generar subredes de clase A

2. ¿Qué comando evita la pérdida de rutas por autoresumen en RIPv2?

a) network

b) version 2

c) ip route

d) no auto-summary ✅

3. ¿Cuál es una ventaja principal del resumen de rutas?

a) Aumenta la complejidad de la tabla

b) Reduce el número de entradas en la tabla ✅

c) Disminuye la eficiencia del router

d) Aumenta el tráfico de broadcast

4. ¿Qué acción evita el solapamiento de subredes al usar VLSM?

a) Aplicar autoresumen

b) Asignar bloques en orden descendente de tamaño ✅

c) Usar direcciones privadas

d) Configurar NAT

5. ¿Qué permite observar el comando show ip route?

a) Solo las direcciones MAC

b) El tráfico de broadcast

c) La tabla de enrutamiento actual ✅

d) Las contraseñas del router

6. ¿Qué se logra con la configuración ip summary-address rip?

a) Activar NAT

b) Generar resumen manual de rutas ✅

c) Reiniciar la interfaz

d) Configurar RIP versión 1

7. ¿Qué representa una máscara /29?

a) 64 direcciones disponibles

b) 30 hosts válidos

c) 8 direcciones totales ✅

d) 254 hosts posibles

8. ¿Cuál es el primer paso para aplicar VLSM correctamente?

a) Configurar DNS

b) Ordenar las subredes por tamaño ✅

c) Activar el protocolo EIGRP

d) Usar DHCP para todas las interfaces

Referencias Bibliográficas

Cisco Networking Academy. (2024). *Introduction to Networks*. Cisco Systems. ISBN: 9781587134265

Doyle, J., & Carroll, J. (2005). *Routing TCP/IP, Volume I* (2nd ed.). Cisco Press. ISBN: 9781587052026

Forouzan, B. A. (2007). *Data Communications and Networking*. McGraw-Hill. ISBN: 9780072967753

Kurose, J. F., & Ross, K. W. (2021). *Computer Networking: A Top-Down Approach* (8th ed.). Pearson. ISBN: 9780136681557

Odom, W. (2013). *CCNA Routing and Switching Official Cert Guide, Volume 1* (Associate Level). Cisco Press. ISBN: 9781587205477

Capítulo 4: Enrutamiento con IPv6

Introducción

El crecimiento acelerado de la conectividad global, impulsado por la expansión de dispositivos móviles, la computación en la nube y el auge del Internet de las Cosas (IoT), ha llevado a un aumento exponencial en la cantidad de dispositivos conectados a Internet. Esta expansión ha agotado el espacio de direcciones IPv4, originalmente limitado a aproximadamente 4.3 mil millones de direcciones únicas. Para dar respuesta a esta limitación crítica y a las crecientes demandas de la infraestructura de red, se desarrolló IPv6 (Internet Protocol Version 6). Este protocolo de red de nueva generación ofrece una capacidad de direccionamiento prácticamente ilimitada, gracias a su estructura de 128 bits, lo cual representa aproximadamente 3.4 × 10^38 direcciones posibles (Hagen, 2006; Kurose & Ross, 2021).

Más allá de la expansión del espacio de direcciones, IPv6 introduce beneficios arquitectónicos y funcionales clave. Su diseño incluye encabezados simplificados para un procesamiento más eficiente por parte de los *routers*, mecanismos robustos de autoconfiguración (como SLAAC) que reducen la necesidad de configuración manual, y mejoras integradas de seguridad mediante IPsec, que pasa de ser una característica opcional en IPv4 a una obligatoria en IPv6 (Hagen, 2006). Su concepción considera explícitamente las necesidades de las redes actuales y futuras, siendo particularmente relevante en ambientes de IoT, redes móviles (5G) y servicios en la nube, donde la escalabilidad y la eficiencia en la gestión de direcciones son primordiales (Cisco Networking Academy, 2024).

Este capítulo proporciona una visión integral del funcionamiento de IPv6, desde sus conceptos básicos y la estructura de sus direcciones, hasta su implementación práctica en *routers* Cisco. Exploraremos tanto el enrutamiento estático como el enrutamiento dinámico con RIPng, y analizaremos las estrategias de transición desde IPv4, herramientas esenciales para una coexistencia y migración exitosa en entornos híbridos.

Objetivos del Capítulo

- Reconocer las principales características y ventajas de IPv6 frente a IPv4, mediante la comparación estructural de protocolos y análisis de requerimientos actuales, para comprender la necesidad de adopción del nuevo protocolo.
- Identificar los diferentes tipos de direcciones IPv6 y sus formatos, mediante ejemplos y clasificación operativa, para emplearlas correctamente en el diseño y segmentación de redes.
- Explicar el proceso de creación de subredes IPv6, mediante ejercicios de segmentación utilizando prefijos variables, para implementar planes de direccionamiento escalables.
- Aplicar la configuración básica de interfaces y rutas IPv6 en routers Cisco, mediante comandos apropiados y pruebas de conectividad, para habilitar la comunicación en redes basadas en IPv6.
- Implementar enrutamiento estático y dinámico con RIPng, mediante simulaciones en Cisco Packet Tracer, para garantizar la correcta propagación de prefijos IPv6.
- Analizar los métodos de transición de IPv4 a IPv6, mediante esquemas comparativos y

evaluación de técnicas, para seleccionar la estrategia más adecuada en entornos híbridos.

4.1. Fundamentos de IPv6

El protocolo IPv6 (Internet Protocol version 6) fue diseñado por la IETF (Internet Engineering Task Force) como una evolución indispensable de IPv4, impulsada principalmente por el inminente agotamiento del espacio de direcciones de este último (Kurose & Ross, 2021). Mientras que IPv4 utiliza direcciones de 32 bits, ofreciendo aproximadamente 4.3 x 10^9 direcciones, IPv6 emplea direcciones de 128 bits. Esta vasta expansión del espacio de direccionamiento permite una cantidad teóricamente casi ilimitada de direcciones únicas, aproximadamente 3.4 x 10^38 (Hagen, 2006). Para ponerlo en perspectiva, esto significa que hay suficientes direcciones IPv6 para asignar una a cada átomo de la superficie de la Tierra, y aún sobrarían miles de millones.

IPv6 no solo aborda el problema del espacio de direcciones, sino que también introduce funcionalidades clave y mejoras en la arquitectura del protocolo (Hagen, 2006; Cisco Networking Academy, 2024):

- **Eliminación de NAT en redes punto a punto:** La abundancia de direcciones IPv6 hace que la Traducción de Direcciones de Red (NAT), una solución temporal para la escasez de IPv4, sea innecesaria para la conectividad de extremo a extremo. Esto simplifica la conectividad, mejora el rendimiento de aplicaciones peer-to-peer y restaura el principio original de Internet de comunicación directa entre *hosts*.

- **Autoconfiguración automática mediante SLAAC (Stateless Address Autoconfiguration):** IPv6 permite que los dispositivos se autoconfiguren con una dirección IPv6 global única y enrutable sin la necesidad de un servidor DHCPv6. Los *routers* envían mensajes de anuncio de *router* (RA) que contienen el prefijo de red, y los *hosts* utilizan este prefijo junto con su ID de interfaz (derivado comúnmente de su dirección MAC a través del formato EUI-64 modificado) para generar su dirección IP completa. Esto simplifica enormemente la gestión de direcciones en grandes redes (Kurose & Ross, 2021).
- **Seguridad obligatoria a través de IPsec:** IPsec (Internet Protocol Security) es un conjunto de protocolos que proporciona seguridad a nivel de capa de red. En IPv6, la compatibilidad con IPsec es una característica obligatoria, aunque su implementación y uso pueden ser opcionales. Esto facilita la encriptación y autenticación del tráfico, mejorando la seguridad general de la red sin necesidad de soluciones adicionales de terceros.
- **Eficiencia en el procesamiento de encabezados:** El encabezado IPv6 es más simple y fijo en longitud (40 bytes), a diferencia del encabezado IPv4 que puede variar en longitud y contener campos opcionales. La eliminación de campos como la suma de verificación y la fragmentación por parte de los *routers* intermedios (la fragmentación solo la realiza el *host* emisor) permite un procesamiento más rápido y eficiente de los paquetes por parte de los *routers*, mejorando el rendimiento general.

- **Mejor soporte para calidad de servicio (QoS):** IPv6 incluye campos en su encabezado (Traffic Class y Flow Label) diseñados para una mejor identificación y manejo del tráfico, facilitando la implementación de políticas de QoS para aplicaciones sensibles al retardo, como voz y video.
- **Descubrimiento de Vecinos (Neighbor Discovery Protocol - NDP):** IPv6 reemplaza el ARP (Address Resolution Protocol) y el ICMP Router Discovery de IPv4 con el NDP, que utiliza mensajes ICMPv6 para realizar funciones como resolución de direcciones a nivel de enlace (reemplazando ARP), detección de *routers* y *hosts* en el mismo enlace, detección de direcciones duplicadas (DAD), y autoconfiguración (Kurose & Ross, 2021).

Comparación entre IPv4 e IPv6:

Tabla 11. Comparación entre IPv4 e IPv6

Característica	IPv4	IPv6
Longitud de dirección	32 bits	128 bits
Notación	Decimal (192.168.1.1)	Hexadecimal (2001:db8::1)
Direcciones posibles	~4,300 millones	~3.4 × 10^38
Fragmentación	Por el emisor y routers	Solo por el emisor

Seguridad	Opcional	Obligatoria (IPsec)
Autoconfiguración	Limitada (DHCP)	Sí (SLAAC)

Fuente: Elaboración propia con base en Hagen (2006) y Cisco Networking Academy (2024).

4.2. Tipos de Direcciones IPv6

IPv6 admite diferentes tipos de direcciones que definen el comportamiento del tráfico de red y cómo se enrutan los paquetes. Estas direcciones son esenciales para entender la comunicación en distintos contextos y son fundamentales para el diseño y operación de redes IPv6. A diferencia de IPv4, donde predominan las direcciones unicast y el *broadcast*, en IPv6 el *broadcast* ha sido reemplazado por la funcionalidad de *multicast*, y las direcciones *anycast* adquieren una relevancia estratégica (RFC 4291).

- **Unicast:** Representa una única interfaz de red. Los paquetes enviados a una dirección unicast son entregados exclusivamente a esa interfaz. Son las direcciones más comunes y se utilizan para la comunicación uno a uno entre *hosts*. Dentro de este tipo, se encuentran (RFC 4291):
    - **Global Unicast Address (GUA):** Equivalente a las direcciones IP públicas en IPv4. Son direcciones globalmente únicas y enrutables a través de Internet. Actualmente, la mayoría de las GUA asignadas comienzan típicamente con el prefijo 2000::/3, aunque en la práctica los prefijos asignados a organizaciones

suelen ser /48 o /32 (ej., 2001:db8::/32 es un rango reservado para documentación y ejemplos).

- **Estructura:** Se componen de un **prefijo de enrutamiento global** (los primeros bits asignados por los ISP), un **ID de subred** (utilizado por las organizaciones para segmentar su red interna), y un **ID de interfaz** (que identifica un *host* específico dentro de la subred).
- **Ejemplo:** 2001:0DB8:ABCD:0001::1/64

- **Link-Local Address (LLA):** Utilizadas para la comunicación únicamente dentro del mismo enlace (red local). No son enrutables fuera del segmento de red al que pertenecen. Se generan automáticamente por los dispositivos al activar una interfaz IPv6, comenzando con el prefijo fe80::/10. Son esenciales para el funcionamiento de protocolos de descubrimiento de vecinos (NDP) y protocolos de enrutamiento como OSPFv3 o RIPng, que las utilizan para comunicarse con *routers* vecinos en el mismo enlace.
  - **Ejemplo:** fe80::20c:29ff:fe15:f0e4
- **Unique Local Address (ULA):** Equivalente a direcciones privadas en IPv4 (ej., 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16). Comienzan con fc00::/7 (en la práctica, fd00::/8 es el más utilizado ya que incluye un bit aleatorio) y están destinadas para redes internas donde se desea privacidad o

independencia del proveedor de servicios de Internet. Aunque son únicas dentro de la organización, no están garantizadas para ser globalmente únicas y no deben enrutarse en la Internet pública (RFC 4193).

- **Ejemplo:**
  fd00:abcd:ef12:3::1

- **Loopback Address:** La dirección ::1 (equivalente a 127.0.0.1 en IPv4) se utiliza para realizar pruebas internas de conectividad en el dispositivo local.
- **Unspecified Address:** La dirección :: (todos ceros) indica la ausencia de dirección y se utiliza como dirección de origen por un *host* que aún no tiene una dirección válida (ej., durante el proceso de DAD - Duplicate Address Detection).

- **Multicast:** Identifican a un **grupo de interfaces**, típicamente en diferentes *hosts* o *routers*. Un paquete enviado a una dirección *multicast* es entregado a **todas las interfaces que pertenezcan a ese grupo** (RFC 4291). IPv6 no tiene direcciones de *broadcast*; su funcionalidad ha sido reemplazada por *multicast*. Estas direcciones comienzan con ff00::/8.
  - **Ejemplos de direcciones *multicast* reservadas importantes (RFC 4291):**
    - ff02::1: Grupo "Todos los Nodos" en el enlace local. Todos los dispositivos IPv6 lo escuchan.
    - ff02::2: Grupo "Todos los Routers" en el enlace local. Todos los *routers* IPv6 lo escuchan.

    - ff02::5: Grupo OSPFv3 "All OSPF Routers"
    - ff02::6: Grupo OSPFv3 "All DR/BDR Routers"
    - ff02::9: Grupo RIPng "All RIP Routers"
    - ff05::1:3: Grupo "Todos los servidores DHCPv6" a nivel de sitio.
- **Anycast:** Un conjunto de interfaces (generalmente en diferentes *routers* o servidores) comparten la misma dirección *anycast*. Cuando un paquete es enviado a una dirección *anycast*, es entregado a la "más cercana" de las interfaces que tienen esa dirección, según la métrica del protocolo de enrutamiento (RFC 2526). Se utiliza para proporcionar servicios distribuidos y redundantes, como servidores DNS o *gateways* a Internet, donde el cliente se conecta automáticamente a la instancia del servicio más cercana geográficamente o topológicamente. Las direcciones *anycast* se asignan desde el espacio de direcciones *unicast* global.

Tabla 12. Tipos de direcciones IPv6

Tipo	Prefijo	Alcance	Ejemplo
Unicast	2000::/3, fe80::/10	Global, local	2001:db8::1
Multicast	ff00::/8	Red, grupo, sistema	ff02::1 (todos los nodos)
Anycast	Variable	Según configuración	(misma dirección en múltiples interfaces)

Fuente: RFC 4291; Cisco Networking Academy (2024).

4.3. Representación y Abreviación de Direcciones IPv6

Las direcciones IPv6 constan de 128 bits, y se representan como ocho grupos de 4 dígitos hexadecimales separados por dos puntos (:). Por ejemplo:

2001:0db8:0000:0000:0000:0000:0000:0001

Para facilitar su lectura, escritura y reducir la probabilidad de errores en la configuración, se utilizan las siguientes reglas de abreviación, tal como lo define el RFC 5952:

1. **Omisión de ceros iniciales en cada bloque:**

   2001:db8:0:0:0:0:0:1

2. **Reemplazo de grupos consecutivos de ceros por ::**

   2001:db8::1

   (Sólo puede usarse una vez por dirección).

Ejemplo completo: Dirección original:

2001:0db8:0000:0000:0000:0000:0000:0001

Abreviada paso 1 (ceros iniciales): **2001:db8:0:0:0:0:0:1**

Abreviada final: **2001:db8::1**

Este mecanismo de compresión permite representar direcciones extensas de manera más legible, lo cual es crucial en configuraciones manuales o documentación técnica (Hagen, 2006).

4.4. Subredes IPv6

La segmentación de redes en IPv6 se realiza mediante el uso de prefijos, los cuales definen la porción de la dirección correspondiente a la red, de manera análoga a la máscara de subred en IPv4. A diferencia de IPv4, donde la longitud de la máscara varía ampliamente para optimizar el uso del espacio (VLSM), en IPv6 el estándar y la práctica común es utilizar un prefijo /64 para redes LAN que conectan a *hosts* finales (Kurose & Ross, 2021).

Este prefijo /64 para las LAN no es arbitrario. Deja 64 bits para el ID de interfaz, lo que proporciona un número virtualmente ilimitado de *hosts* en una sola subred (264 dispositivos). Este tamaño estándar facilita el uso de SLAAC (Stateless Address Autoconfiguration) para la autoconfiguración de direcciones por parte de los dispositivos finales, ya que la mayoría de las tecnologías de Capa 2 (como Ethernet) pueden derivar un ID de interfaz de 64 bits a partir de su dirección MAC de 48 bits, utilizando el formato EUI-64 modificado (Cisco Networking Academy, 2024).

Cuando una organización obtiene una asignación de prefijo mayor de un ISP (por ejemplo, un prefijo /48 para un sitio), puede subdividirlo en múltiples subredes /64. Los bits entre el prefijo asignado (ej., /48) y el prefijo /64 de la subred se utilizan como ID de subred.

Cálculo de subredes IPv6:

Para dividir un bloque de direcciones IPv6 (ej., un /48) en subredes /64:

- **Prefijo asignado:** 2001:db8::/48
- **Prefijo deseado para subredes:** /64
- **Diferencia de longitud:** 64−48=16 bits disponibles para el ID de subred.
- **Total de subredes que se pueden crear:** 216=65,536 subredes de tamaño /64.

Ejemplo de subredes /64 a partir de un /48:

Si a una organización se le asigna el prefijo 2001:db8::/48, el tercer hexteto y los primeros 16 bits del cuarto hexteto son parte del prefijo de

enrutamiento global. Los 16 bits restantes del cuarto hexteto se utilizan para el ID de subred.

- **Prefijo base:** 2001:db8:0000::/48
- **Primeras subredes /64 posibles (variando el cuarto hexteto, que es el ID de subred):**
  - 2001:db8:0:0::/64 (donde 0 es el ID de subred)
  - 2001:db8:0:1::/64 (donde 1 es el ID de subred)
  - 2001:db8:0:2::/64 (donde 2 es el ID de subred)
  - ...
  - 2001:db8:0:FFFF::/64 (la última de las 65,536 subredes)

Esta abundancia de direcciones permite a las organizaciones segmentar redes sin necesidad de preocuparse por la escasez, facilitando enormemente la administración lógica, la separación por departamentos o zonas geográficas, y la aplicación de políticas de seguridad granulares. También proporciona un amplio espacio para el crecimiento futuro y la asignación de prefijos a subredes de centros de datos, redes inalámbricas, o incluso segmentos de IoT con miles de millones de dispositivos.

4.5. Direccionamiento Especial en IPv6

IPv6 incorpora varios tipos de direcciones reservadas para propósitos específicos, que permiten funciones esenciales en redes modernas y facilitan el descubrimiento y la comunicación entre dispositivos sin intervención manual del administrador. Estas

direcciones son cruciales para el funcionamiento interno del protocolo (Hagen, 2006; RFC 4291):

1. **Link-Local Address (LLA) (fe80::/10):**
    - **Generación:** Son direcciones que se generan automáticamente por los dispositivos IPv6 en cada interfaz activa, tan pronto como la interfaz se habilita para IPv6. Se forman combinando el prefijo fe80::/64 con un ID de interfaz de 64 bits (comúnmente derivado de la dirección MAC de la interfaz utilizando el formato EUI-64 modificado).
    - **Propósito:** Son estrictamente para la comunicación dentro del mismo enlace físico (red local). No son enrutables fuera de ese segmento de red.
    - **Funcionalidad:** Son fundamentales para el funcionamiento de protocolos de descubrimiento de vecinos (NDP), que permite a los *hosts* y *routers* en el mismo enlace descubrir las direcciones de Capa 2 de sus vecinos y sus roles. Además, son las direcciones de origen y destino utilizadas por los protocolos de enrutamiento IPv6 (como OSPFv3 y RIPng) para establecer adyacencias y comunicarse con sus vecinos directamente conectados.
    - **Ejemplo:** fe80::20c:29ff:fe15:f0e4%Ethernet0/0 (el %Ethernet0/0 es el *scope ID* que especifica la interfaz, requerido en algunos sistemas operativos).
2. **Loopback Address (::1):**
    - **Propósito:** Es equivalente a 127.0.0.1 en IPv4. Esta dirección se utiliza para realizar pruebas internas de conectividad de la pila TCP/IP en el dispositivo local, sin enviar tráfico a la red.

- **Formato:** Es una dirección de 128 bits con todos los bits a cero excepto el último, que es un uno.

3. **Unspecified Address (::):**
   - **Propósito:** Es una dirección de 128 bits con todos los bits a cero. Indica la ausencia de dirección o que la dirección de origen es desconocida.
   - **Uso:** Se utiliza como dirección de origen por un *host* que aún no tiene una dirección válida, por ejemplo, durante el proceso de DAD (Detección de Dirección Duplicada) cuando el *host* está probando la unicidad de una dirección generada por SLAAC antes de asignársela definitivamente. Nunca se utiliza como dirección de destino.

4. **Multicast Reservadas:** Las direcciones *multicast* son ampliamente utilizadas en IPv6 para reemplazar la funcionalidad de *broadcast* de IPv4 y para permitir que los grupos de dispositivos se comuniquen de manera eficiente. Algunas *multicast* reservadas son especialmente importantes para el funcionamiento básico de IPv6:
   - ff02::1 (Todos los nodos en el enlace local): Los *hosts* se unen a este grupo para recibir mensajes de *multicast* destinados a todos los dispositivos en el segmento de red, incluyendo los mensajes de Solicitud de Vecino (NS) y Anuncio de *Router* (RA).
   - ff02::2 (Todos los *routers* del enlace local): Los *routers* IPv6 se unen a este grupo para recibir mensajes de *multicast* destinados específicamente a *routers*, como los mensajes de Solicitud de *Router* (RS) de los *hosts*.
   - ff02::5: *Multicast* OSPFv3 "All OSPF Routers".

- ff02::6: *Multicast* OSPFv3 "All DR/BDR Routers".
- ff02::9: *Multicast* RIPng "All RIP Routers".

La importancia de estas direcciones especiales reside en su papel fundamental para las funciones internas del protocolo, permitiendo que los dispositivos se descubran, autoconfiguren y comuniquen de manera eficiente sin intervención explícita del usuario o del administrador de red. Son la base para la automatización y simplicidad que IPv6 busca ofrecer.

4.6. Configuración Básica de IPv6 en Routers Cisco

La implementación de IPv6 en *routers* Cisco requiere una serie de comandos que permiten activar el protocolo a nivel global, configurar direcciones en las interfaces y verificar el estado de la configuración. A diferencia de IPv4, donde el enrutamiento se habilita con ip routing, en IPv6 se debe activar explícitamente el enrutamiento *unicast* (Cisco Networking Academy, 2024).

Pasos para la configuración:

1. **Activar el enrutamiento IPv6 *unicast* global:** Este comando habilita la capacidad del *router* para reenviar paquetes IPv6.

   Router(config)# ipv6 unicast-routing

2. **Asignar una dirección IPv6 Global Unicast a la interfaz:** Entrar en el modo de configuración de interfaz y asignar la dirección IPv6 con su prefijo.

Router(config)# interface g0/0

Router(config-if)# ipv6 address 2001:db8:1::1/64

Router(config-if)# no shutdown

Cuando se asigna una dirección IPv6 global a una interfaz, el *router* automáticamente genera una dirección *link-local* para esa interfaz, derivada de su dirección MAC utilizando el formato EUI-64 modificado (RFC 4291). También es posible configurarla manualmente si se desea, pero generalmente la autogenerada es suficiente.

- **Configuración de EUI-64 modificado:** Para que el ID de interfaz se derive de la MAC de la interfaz.

Router(config-if)# ipv6 address 2001:db8:1::/64 eui-64

Esto es útil para generar IDs de interfaz únicos automáticamente, aunque menos predecible para la documentación.

3. Verificar el estado de las interfaces:

Router# show ipv6 interface brief

Este comando mostrará las direcciones IPv6 (global y *link-local*) asignadas a cada interfaz, así como su estado de línea y protocolo.

4. Verificar configuración general de IPv6 y los protocolos:

Router# show running-config | section ipv6

Router# show ipv6 protocols

Estos comandos permiten revisar la configuración de IPv6 en el archivo de configuración en ejecución y los protocolos de enrutamiento IPv6 activos.

Cada interfaz activa con una dirección IPv6 también obtiene automáticamente una dirección *link-local*, utilizada para protocolos internos como el Descubrimiento de Vecinos (NDP) y para que los *routers* puedan establecer adyacencias y comunicarse con otros *routers* directamente conectados en el mismo segmento de red (Cisco Networking Academy, 2024).

4.7. Enrutamiento Estático en IPv6

El enrutamiento estático en IPv6 funciona de forma similar a IPv4, aunque con una sintaxis adaptada a las direcciones de 128 bits. Se utiliza para definir rutas fijas y permanentes hacia redes remotas cuando la red es pequeña, la topología es estable o se requiere un control granular sobre el flujo de tráfico (Forouzan, 2012). No requiere procesamiento adicional por parte del *router* para descubrir rutas y es ideal en entornos controlados, como redes *stub* o para definir una ruta predeterminada hacia Internet.

Sintaxis del comando:

La sintaxis del comando ipv6 route permite especificar la red de destino y la forma de alcanzarla, ya sea a través de una interfaz de salida o la dirección del siguiente salto:

Router(config)# ipv6 route [RED_DESTINO/PREFIJO] [INTERFAZ_SALIDA | IP_NEXT_HOP]

- **[RED_DESTINO/PREFIJO]:** La red IPv6 de destino con su longitud de prefijo.
- **[INTERFAZ_SALIDA]:** La interfaz local del *router* por donde se deben enviar los paquetes para alcanzar la red destino.
- **[IP_NEXT_HOP]:** La dirección IPv6 del siguiente *router* en la ruta hacia la red destino. Para IPv6, se recomienda usar la dirección *link-local* del siguiente salto cuando se especifica la interfaz de salida, para evitar la resolución recursiva.

Ejemplo práctico:

Consideremos un *router* que necesita una ruta estática hacia una red remota:

- Red local: 2001:db8:1::/64
- Red remota: 2001:db8:2::/64
- Interfaz de salida en este *router*: GigabitEthernet0/1
- Dirección *link-local* del *router* vecino en GigabitEthernet0/1: fe80::2

Configuración usando solo la interfaz de salida:

```
Router(config)# ipv6 route 2001:db8:2::/64 GigabitEthernet0/1
```

Configuración usando la dirección *link-local* del próximo salto (recomendado):

```
Router(config)# ipv6 route 2001:db8:2::/64 GigabitEthernet0/1 fe80::2
```

Esta última opción es más robusta porque especifica exactamente el siguiente salto, incluso si hay múltiples dispositivos en el segmento de red.

Verificación:

- **Verificar la tabla de enrutamiento IPv6:**

  Router# show ipv6 route

  Las rutas estáticas aparecerán con el código S.

- **Verificar conectividad:**
  Router# ping 2001:db8:2::1

Las rutas estáticas permiten controlar con precisión el flujo de tráfico de red, pero su principal desventaja es que requieren mantenimiento manual. Cualquier cambio en la topología de la red (como la adición o eliminación de una red, o la falla de un enlace) obliga al administrador a actualizar manualmente las rutas estáticas en todos los *routers* afectados, lo que puede ser propenso a errores y poco escalable en redes en crecimiento o dinámicas (Forouzan, 2012).

4.8. Enrutamiento Dinámico con RIPng

RIPng (Routing Information Protocol Next Generation) es una versión mejorada del protocolo RIP diseñada específicamente para operar con IPv6. Hereda el mismo algoritmo de vector de distancia y las limitaciones de su predecesor IPv4, como un máximo de 15 saltos (un destino a 16 saltos o más se considera inalcanzable) y una convergencia relativamente lenta (intervalos de actualización de 30 segundos). Sin embargo, a diferencia de RIPv2 para IPv4, RIPng es compatible únicamente con direcciones IPv6 y requiere configuración a nivel de interfaz en lugar de global (Cisco Networking Academy, 2024).

RIPng es una opción adecuada para redes pequeñas y sencillas, o para fines educativos y de laboratorio, debido a su facilidad de implementación. Para redes más grandes y complejas, se recomiendan protocolos de enrutamiento de estado de enlace como OSPFv3 o protocolos avanzados de vector de distancia como EIGRP para IPv6, que ofrecen mejor escalabilidad y tiempos de convergencia más rápidos (Doyle & Carroll, 2005).

Pasos para configurar RIPng:

1. **Activar el enrutamiento IPv6 global:** (Si no se ha hecho ya)

   Router(config)# ipv6 unicast-routing

2. **Crear la instancia del proceso RIPng:** Este comando crea un proceso de RIPng con un nombre específico (ej., "RED"). Este nombre es local al *router* y permite identificar el proceso.

   Router(config)# ipv6 router rip RED

   (No se especifica network en el modo router rip como en IPv4).

3. **Habilitar RIPng en cada interfaz que participará en el proceso:** Para que RIPng envíe y reciba actualizaciones en una interfaz, debe habilitarse explícitamente en el modo de configuración de esa interfaz.

   Router(config)# interface g0/0

   Router(config-if)# ipv6 rip RED enable

Verificación del funcionamiento de RIPng:

- **Router# show ipv6 protocols**: Muestra información sobre los protocolos de enrutamiento IPv6 activos, incluyendo las interfaces donde se está ejecutando RIPng, la distancia administrativa, y los temporizadores.
- **Router# show ipv6 rip database**: Muestra la base de datos de rutas de RIPng, incluyendo las redes que está anunciando y las que ha aprendido de sus vecinos.
- **Router# show ipv6 route rip**: Filtra la tabla de enrutamiento IPv6 para mostrar solo las rutas aprendidas a través de RIPng.
- **Router# debug ipv6 rip**: Muestra en tiempo real los procesos de envío y recepción de actualizaciones de RIPng. **¡Advertencia!** Utilizar debug puede consumir muchos recursos del *router*; se debe usar con precaución y desactivarlo con undebug all cuando se haya finalizado.

Ventajas de RIPng:

- **Fácil de implementar:** Su configuración es relativamente sencilla, lo que lo hace ideal para principiantes o redes muy pequeñas.
- **Útil en redes pequeñas o en laboratorios educativos:** Proporciona una forma rápida de establecer enrutamiento dinámico IPv6.

Limitaciones:

- **No es escalable para redes grandes:** Debido a su límite de 15 saltos y a la propagación periódica de la tabla completa de enrutamiento, no es adecuado para topologías complejas o redes extensas.
- **Convergencia lenta:** En comparación con protocolos como OSPFv3 o EIGRP para IPv6, RIPng tarda más en adaptarse a los cambios de la red, lo que puede causar interrupciones temporales en la conectividad.

4.9. Métodos de Transición IPv4 – IPv6

Durante el período de adopción gradual de IPv6, es indispensable coexistir con la infraestructura IPv4 existente. Para lograrlo, se emplean diversas técnicas de transición que permiten la interoperabilidad temporal y la comunicación entre *hosts* y redes que operan con uno u otro protocolo (RFC 4213, 2005). Estas técnicas son claves para una migración ordenada y para garantizar la continuidad del servicio.

Las principales estrategias de transición son:

1. **Dual Stack (*Doble Pila*):**
    - **Descripción:** Permite que los dispositivos (hosts y *routers*) ejecuten simultáneamente los protocolos IPv4 e IPv6 en sus interfaces de red. Esto significa que un dispositivo tiene direcciones IPv4 y IPv6, y puede procesar y enviar paquetes usando cualquiera de los dos protocolos.

- **Ventaja:** Proporciona una operación nativa y paralela para ambos protocolos. Los dispositivos pueden acceder a recursos IPv4 usando IPv4 y a recursos IPv6 usando IPv6 sin necesidad de traducción o encapsulación. Es la estrategia preferida cuando es posible implementar IPv6 de extremo a extremo.
- **Desventaja:** Requiere la configuración y gestión de dos pilas de protocolos y dos esquemas de direccionamiento, lo que duplica la carga administrativa en ciertos aspectos. Consume más recursos del dispositivo (memoria y CPU) que una implementación de un solo protocolo.
- **Aplicación:** Ideal en redes modernas donde los sistemas operativos y el hardware tienen soporte completo para IPv6.

2. **Túneles (*Tunneling*):**
    - **Descripción:** Los túneles encapsulan paquetes IPv6 dentro de paquetes IPv4 para permitir que el tráfico IPv6 atraviese una infraestructura IPv4 existente que no soporta IPv6, o viceversa. El paquete IPv6 original se convierte en la "carga útil" de un paquete IPv4.
    - **Funcionamiento:** En un extremo del túnel (punto de entrada), el paquete IPv6 se encapsula en un encabezado IPv4. En el otro extremo (punto de salida), el encabezado IPv4 se elimina y el paquete IPv6 original se reenvía a su destino.
    - **Ventaja:** No requiere la modificación o actualización de la infraestructura IPv4 subyacente para transportar tráfico IPv6. Permite que *hosts* o redes IPv6 dispersas

se comuniquen a través de una "nube" IPv4.

- **Desventaja:** Añade sobrecarga (*overhead*) al paquete (debido al encabezado adicional) y puede introducir latencia. La gestión de los puntos finales del túnel puede ser compleja.
- **Ejemplos comunes:**

GRE (Generic Routing Encapsulation): Un protocolo de túnel flexible que puede encapsular múltiples protocolos de capa de red.

6to4: Un mecanismo de túnel automático que utiliza direcciones IPv4 para construir dinámicamente direcciones IPv6 de *gateway*. No requiere configuración manual de túneles punto a punto.

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol): Permite a *hosts* y *routers* IPv6 dentro de un sitio encapsular tráfico IPv6 sobre una red IPv4 interna.

DS-Lite (Dual-Stack Lite): Un enfoque que permite a los ISP proporcionar conectividad IPv4 a sus suscriptores IPv6 mediante túneles.

Traducción (*Translation*):

Descripción: Convierte directamente paquetes IPv6 a IPv4 y viceversa, permitiendo que *hosts* que solo soportan un protocolo se comuniquen con *hosts* que solo soportan el otro. Es una solución de último recurso debido a sus limitaciones.

Funcionamiento: Un dispositivo intermedio (como un *router* o un *proxy*) realiza la reescritura del encabezado del paquete de un formato a otro, incluyendo la traducción de direcciones.

Ventaja: Permite una comunicación limitada entre islas de IPv4 e IPv6 sin necesidad de doble pila o túneles en los *hosts* finales.

Desventaja: Es la técnica más compleja de implementar y mantener. Rompe el principio de comunicación "extremo a extremo" de IP, lo que puede causar problemas con algunas aplicaciones que esperan una conectividad directa. No todas las aplicaciones son compatibles, y la latencia puede aumentar.

- **Ejemplos comunes:**
- **NAT64:** Permite que *hosts* IPv6 inicien comunicación con *hosts* IPv4. Un servidor DNS64 traduce los nombres de dominio de *hosts* IPv4 a direcciones IPv6 sintéticas, y el *router* NAT64 realiza la traducción del encabezado del paquete.
- **DNS64:** Un servidor DNS que, cuando un cliente IPv6 solicita un registro AAAA (IPv6) y solo existe un registro A (IPv4), sintetiza una dirección IPv6 que apunta a un *router* NAT64.

Tabla 13. Comparación de los mecanismos de transición a IPv6

Técnica	Ventaja	Desventaja
Dual Stack	Operación nativa y paralela	Requiere doble configuración
Túneles	No modifica infraestructura IPv4	Añade latencia
Traducción	Permite acceso entre protocolos	Compleja, rompe extremo a extremo

Fuente: Elaboración propia basada en Hagen (2006) y RFC 4213 (2005).

Estas estrategias son implementadas según el contexto técnico, los recursos disponibles y la estrategia económica de la organización, buscando minimizar interrupciones del servicio y facilitar una migración ordenada y progresiva hacia un entorno completamente IPv6 (RFC 4213, 2005).

4.10. Práctica Guiada: Configuración de Enrutamiento IPv6 en Cisco Packet Tracer

Objetivo: Configurar una red que utilice direccionamiento IPv6 con enrutamiento dinámico RIPng, verificando conectividad y tablas de enrutamiento en un entorno simulado de Cisco Packet Tracer.

Escenario:

Se dispone de tres *routers* (R1, R2, R3) interconectados en cadena. Cada *router* conecta a una red LAN con dirección IPv6 única para *hosts* finales.

Topología:

- R1 ↔ R2 ↔ R3
- LAN1: 2001:db8:1::/64
- LAN2: 2001:db8:2::/64
- LAN3: 2001:db8:3::/64

Materiales requeridos:

- Cisco Packet Tracer (v8.2 o superior)
- Dispositivos: 3 *routers* (Cisco 2901), 3 *switches*, 3 PCs (una por LAN)

Pasos de Configuración:

1. **Activar el enrutamiento unicast en todos los routers:**

Router(config)# ipv6 unicast-routing

2. **Asignar direcciones IPv6 a interfaces:**

- **En R1:**

Router(config)# interface g0/0

Router(config-if)# ipv6 address 2001:db8:1::1/64

Router(config-if)# ipv6 rip RED enable

Router(config-if)# no shutdown

Router(config-if)# exit

Router(config)# interface g0/1

Router(config-if)# ipv6 address 2001:db8:2::1/64

Router(config-if)# ipv6 rip RED enable

Router(config-if)# no shutdown

Router(config-if)# exit

- **En R2:**

Router(config)# interface g0/0 (Conexión a R1)

Router(config-if)# ipv6 address 2001:db8:2::2/64

Router(config-if)# ipv6 rip RED enable

Router(config-if)# no shutdown

Router(config-if)# exit

Router(config)# interface g0/1 (Conexión a R3)

Router(config-if)# ipv6 address 2001:db8:4::1/64

Router(config-if)# ipv6 rip RED enable

Router(config-if)# no shutdown

Router(config-if)# exit

- **En R3**

Router(config)# interface g0/0 (Conexión a R2)

Router(config-if)# ipv6 address 2001:db8:4::2/64

Router(config-if)# ipv6 rip RED enable

Router(config-if)# no shutdown

Router(config-if)# exit

Router(config)# interface g0/1 (Conexión a LAN3)

Router(config-if)# ipv6 address 2001:db8:3::1/64

Router(config-if)# ipv6 rip RED enable

Router(config-if)# no shutdown

Router(config-if)# exit

3. **Crear la instancia de proceso RIPng en todos los *routers*:**

Router(config)# ipv6 router rip RED

(El nombre "RED" es arbitrario, pero debe ser el mismo en todas las interfaces donde se habilita RIPng).

4. **Configurar direcciones IPv6 en las PCs finales:**

Asignar direcciones IPv6 estáticas a las PCs, con la máscara /64 y el *gateway* predeterminado apuntando a la dirección IPv6 de la interfaz del

router local (ej., para PC1 en LAN1, IP: 2001:db8:1::10/64, Gateway: 2001:db8:1::1).

5. **Verificar conectividad y enrutamiento:**

   Router# show ipv6 route

   Router# show ipv6 protocols

   Router# ping 2001:db8:3::10 (desde PC1 hacia PC3)

   Router# debug ipv6 rip (con precaución)

Resultados esperados:

- Cada *router* debe aprender dinámicamente las redes vecinas (LANs y enlaces entre *routers*) a través de RIPng.
- Las rutas aprendidas por RIPng deben aparecer en la tabla de enrutamiento IPv6 de cada *router* con el código R.
- La conectividad debe confirmarse con *ping* exitoso entre *hosts* de diferentes redes LAN.

Preguntas de reflexión:

1. **¿Por qué es necesario habilitar RIPng en cada interfaz y no de forma global como en IPv4?**

Porque RIPng opera a nivel de interfaz, debido a que IPv6 ya no utiliza el concepto de red de clase ni declaración de redes globales, lo que obliga a especificar manualmente en qué interfaces opera el protocolo (Cisco Networking Academy, 2024).

2. **¿Qué función cumple la dirección link-local durante la propagación de rutas?**

Es utilizada como origen de los mensajes RIPng. Cada router se comunica con sus vecinos utilizando direcciones link-local ya que estas son únicas en el enlace y no requieren configuración manual (Hagen, 2006).

3. **¿Qué indicaría que no hay conectividad entre dos redes IPv6 después de aplicar RIPng?**

Podría indicar errores en la activación del protocolo, omisión en la habilitación por interfaz, direcciones mal configuradas, o simplemente la falta de habilitación del comando ipv6 unicast-routing (Forouzan, 2012).

4. **¿Qué ventaja ofrece esta práctica frente a la configuración estática de rutas?**

Reduce errores manuales, facilita la escalabilidad de la red y permite mayor flexibilidad al adaptarse dinámicamente a cambios topológicos sin intervención del administrador.

4.11. Evaluación del Capítulo

1. **¿Cuál es la longitud de una dirección IPv6?**

a) 64 bits

b) 32 bits

c) 128 bits ✅

d) 256 bits

2. ¿Qué tipo de dirección se utiliza para la comunicación dentro del mismo enlace?

a) Global Unicast

b) Multicast

c) Anycast

d) Link-local ✅

3. ¿Qué comando permite habilitar el enrutamiento IPv6 en un router Cisco?

a) ip routing

b) ipv6 enable

c) ipv6 unicast-routing ✅

d) enable ipv6

4. ¿Qué protocolo se utiliza para enrutamiento dinámico en IPv6?

a) RIP v2

b) EIGRP clásico

c) RIPng ✅

d) BGPv4

5. ¿Qué dirección representa la dirección loopback en IPv6?

a) 127.0.0.1

b) fe80::1

c) ::1 ✅

d) ff02::1

6. ¿Qué comando permite verificar las rutas aprendidas a través de RIPng en IPv6?

a) show ip route

b) show ipv6 route ✅

c) debug rip

d) show ipv6 ospf

7. ¿Cuál es el prefijo que indica direcciones link-local en IPv6?

a) 2001::/16

b) ff00::/8

c) fe80::/10 ✅

d) fc00::/7

8. ¿Cuál de las siguientes técnicas permite operar IPv4 e IPv6 de forma paralela?

a) NAT64

b) Túneles

c) Traducción

d) Dual Stack ✅

Referencias Bibliográficas

Cisco Networking Academy. (2024). Enterprise Networking, Security, and Automation Companion Guide (CCNA v7). Cisco Press. ISBN: 9781587134869

Doyle, J., & Carroll, J. (2005). *Routing TCP/IP, Volume I* (2nd ed.). Cisco Press. ISBN: 9781587052026

Forouzan, B. A. (2012). Data Communications and Networking (5th ed.). McGraw-Hill Education. ISBN: 9780073376226

Hagen, S. (2006). IPv6 Essentials (2nd ed.). O'Reilly Media. ISBN: 9780596100582

IETF. (2006). RFC 4291: IP Version 6 Addressing Architecture. https://www.rfc-editor.org/info/rfc4291

IETF. (2005). RFC 4213: Basic Transition Mechanisms for IPv6 Hosts and Routers. https://www.rfc-editor.org/info/rfc4213

IETF. (2010). RFC 5952: A Recommendation for IPv6 Address Text Representation. https://www.rfc-editor.org/info/rfc5952

Kurose, J. F., & Ross, K. W. (2021). Computer Networking: A Top-Down Approach (8th ed.). Pearson. ISBN: 9780136681557

Glosario de Términos

ACL

Lista de Control de Acceso. Conjunto de reglas que controlan el tráfico que puede ingresar o salir de una interfaz en un router o switch.

Algoritmo de Enrutamiento.

Un conjunto de reglas y procedimientos que un router utiliza para determinar la mejor ruta para reenviar un paquete de datos a través de una red. Los dos tipos principales son el de vector de distancia y el de estado de enlace.

CLI

Interfaz de Línea de Comandos. Medio textual para interactuar con el sistema operativo de red mediante instrucciones escritas.

Configuración estática

Asignación manual de direcciones IP y parámetros de red sin el uso de protocolos dinámicos.

Convergencia

El proceso mediante el cual todos los routers en una red logran un estado consistente y actualizado en sus tablas de enrutamiento después de un cambio en la topología. Un tiempo de convergencia más corto es deseable, ya que minimiza el tiempo de inactividad de la red.

DHCP

Protocolo de Configuración Dinámica de Host. Asigna automáticamente direcciones IP a los dispositivos de una red.

Distancia Administrativa (AD)

Un valor que indica la confiabilidad de la fuente de información de enrutamiento de una ruta. Cuando un router tiene múltiples rutas hacia un mismo destino, selecciona la que tiene el valor de AD más bajo, ya que se considera la más fiable.

DNS

Sistema de Nombres de Dominio. Traduce nombres de dominio legibles para humanos (como google.com) en direcciones IP.

Dirección IP

Identificador único para cada dispositivo en una red basada en el protocolo IP.

EIGRP

Protocolo de enrutamiento dinámico propietario de Cisco que combina características de protocolos de vector de distancia y estado de enlace.

Enrutamiento

Proceso de determinar la ruta óptima para enviar paquetes de datos entre redes.

Estado de enlace

Algoritmo de enrutamiento basado en el conocimiento completo de la topología de la red.

Flash

Memoria no volátil donde se almacena el sistema operativo IOS en los routers Cisco.

Gateway

Dispositivo que sirve como punto de acceso o salida hacia otra red, generalmente un router.

IOS

Sistema Operativo Internetwork de Cisco utilizado para gestionar y configurar dispositivos de red.

IPv4

Versión 4 del protocolo IP. Utiliza direcciones de 32 bits representadas en formato decimal.

IPv6

Versión 6 del protocolo IP. Utiliza direcciones de 128 bits para superar las limitaciones de IPv4.

Interfaz

Conexión física o lógica de un dispositivo de red con otros dispositivos o redes.

LAN

Local Area Network/Red de Área Local. Red que interconecta dispositivos dentro de un área geográfica limitada como una oficina.

Loopback

Interfaz virtual utilizada para pruebas y administración del dispositivo.

Máscara de subred

Número que define qué parte de una dirección IP pertenece a la red y cuál al host.

Métrica de Enrutamiento

Un valor numérico utilizado por los protocolos de enrutamiento para determinar la "mejor" ruta hacia un destino, basándose en criterios como el conteo de saltos, el ancho de banda, el retardo o la carga de la red.

NAT

Traducción de Direcciones de Red. Técnica para modificar direcciones IP en tránsito entre redes.

NVRAM

Memoria no volátil donde se almacena la configuración de inicio del router.

OSPF

Protocolo de enrutamiento de estado de enlace que utiliza el algoritmo Dijkstra para determinar la mejor ruta.

Packet Tracer

Simulador de redes desarrollado por Cisco que permite diseñar, configurar y probar redes sin hardware físico.

RAM

Memoria volátil donde se carga la configuración activa y las tablas de enrutamiento mientras el dispositivo está encendido.

Resumen de rutas

Técnica que agrupa varias rutas IP en una sola entrada para optimizar las tablas de enrutamiento.

RIP

Protocolo de enrutamiento basado en vector de distancia que utiliza el conteo de saltos como métrica.

RIPng

Versión de RIP para redes IPv6.

ROM

Memoria de solo lectura que contiene instrucciones básicas de arranque y diagnóstico.

Router

Dispositivo de red que determina la mejor ruta para enviar datos entre redes distintas.

Ruta Estática

Una ruta configurada manualmente por un administrador de red. Se utiliza en redes pequeñas o cuando se requiere un control estricto sobre el flujo de tráfico. Su desventaja principal es que requiere mantenimiento manual ante cambios en la topología de la red.

Ruta Predeterminada

Una ruta especial, también conocida como "ruta por defecto", que dirige el tráfico hacia un destino cuando no existe una ruta específica en la tabla de enrutamiento.

Sistema Autónomo (AS)

Una colección de redes IP bajo una única administración. El enrutamiento dentro de un AS se gestiona con protocolos IGP, mientras que la

comunicación entre diferentes AS se maneja con protocolos EGP.

SSH

Protocolo seguro para acceder remotamente a dispositivos de red mediante CLI.

Subnetting

División lógica de una red en subredes más pequeñas.

Subredes Solapadas

Un error en el diseño de direccionamiento IP donde los rangos de direcciones de dos o más subredes se superponen, creando conflictos de enrutamiento y pérdida de conectividad.

TFTP

Protocolo de Transferencia de Archivos Trivial. Usado para transferir archivos como imágenes de IOS o configuraciones.

Tabla de enrutamiento

Base de datos que mantiene información sobre rutas conocidas y cómo alcanzarlas.

Telnet

Protocolo de red usado para acceso remoto no cifrado a través de CLI.

Topología

Forma en que los dispositivos de red están organizados y conectados entre sí.

VLSM

Máscara de Subred de Longitud Variable. Permite subredes de distintos tamaños dentro de una misma red.

Vector de distancia

Algoritmo de enrutamiento basado en la distancia (saltos) hacia la red de destino.

Rodrigo Fernando Morocho Román es Magíster en Seguridad Informática Aplicada por la Escuela Superior Politécnica del Litoral (ESPOL) y Magíster en Docencia y Gerencia en Educación Superior por la Universidad de Guayaquil. Posee un Diplomado Superior en Auditoría Informática, también otorgado por ESPOL, y obtuvo el título de Ingeniero de Sistemas en la Universidad Católica de Cuenca. Actualmente cursa una Especialización en Internet de las Cosas (IoT) en la Universidad de Buenos Aires, consolidando así una trayectoria académica y profesional profundamente vinculada con la innovación tecnológica y la educación superior.

Es profesional certificado por Cisco Systems, con credenciales en CCNA, CCNA Security y CCNA CyberOps, y ha sido acreditado como Cisco Certified Academy Instructor (CCAI) por Cisco Networking Academy. Entre 2015 y 2018 se desempeñó como Legal Main Contact de la academia Cisco-UTMACH, reforzando su compromiso con el desarrollo de talento local en tecnologías de redes.

Desde el año 2004, ejerce como docente en la Facultad de Ingeniería Civil de la Universidad Técnica de Machala, donde imparte cátedras relacionadas con Redes de Computadoras, Seguridad y Auditoría Informática. Su experiencia docente se complementa con la dirección de trabajos de titulación y tesis de maestría e ingeniería en áreas como redes, ciberseguridad y gobierno de tecnologías de la información.

Comprometido con la formación de profesionales altamente capacitados en Tecnologías de la Información, el autor combina su sólida formación académica con una profunda vocación pedagógica, aportando a la comunidad académica herramientas actualizadas y prácticas fundamentadas en estándares internacionales y experiencias de campo.

ISBN: 978-9942-53-058-5

9 789942 530585

Compás
capacitación e investigación