INSTITUTO SUPERIOR
UNIVERSITARIO
sucre

GUÍA GENERAL DE ESTUDIO DE INTERNETWORKING

Guía General de Estudio de Internetworking

Carlos Germánico Rivera Liger

Mayra Alejandra Sarzosa Villarroel

Limber Santiago Molina Jaramillo

Andrés Rodrigo Guano Bermeo

Robinson Lema Parco

2026

Esta publicación ha sido sometida a revisión por pares académicos específicos por:

Oscar Omar Gonzales Zurita
Universidad de las Américas

Corrección de estilo:

- Fabricio Manuel Tipantocta Pillajo - Docente - Sucre

Diseño y diagramación:

- Freddy Javier Centeno Martínez - Docente - Sucre

Editorial RIMANA

Primera Edición
Quito – Ecuador

INSTITUTO SUPERIOR UNIVERSITARIO SUCRE

ISBN: 978-9942-590-18-3

MISIÓN

Ser una Institución Superior Universitaria con estándares de calidad académica e innovación, reconocida a nivel nacional con proyección internacional.

VISIÓN

Formamos profesionales competentes con espíritu emprendedor, capaces de contribuir al desarrollo integral del país.

Índice

Presentación de la asignatura

Bienvenidos a la asignatura de Internetworking, eje fundamental de las redes de computadoras. Este curso se dedica a estudiar los principios, protocolos y dispositivos que permiten la interconexión de redes heterogéneas a escala global. Analizaremos en profundidad la arquitectura del modelo TCP/IP y su implementación práctica para la comunicación de datos. Aprenderemos a diseñar, configurar y solucionar problemas en infraestructuras de red mediante el direccionamiento IP, el enrutamiento y la conmutación. La materia combina teoría esencial con laboratorios prácticos, utilizando equipos como routers y switches. Nuestro objetivo es que desarrollen las competencias para construir redes escalables, seguras y eficientes, preparándolos para certificaciones profesionales y desafíos del entorno digital. Comenzaremos desde los fundamentos, avanzando hacia temas complejos como enrutamiento dinámico y servicios de red. Esta asignatura es la piedra angular para cualquier especialista en conectividad y telecomunicaciones.

Resultados del aprendizaje

Describe las características técnicas de los medios inalámbricos y los mecanismos de propagación que se utilizan en exteriores e interiores.

Planifica una red inalámbrica dependiendo del tipo de arquitectura requerida.

Analiza los aspectos fundamentales del diseño de redes de fibra óptica mediante el estudio de sus características y presenta soluciones de conectividad.

UNIDAD 1 FUNDAMENTOS DE INTERNETWORKING

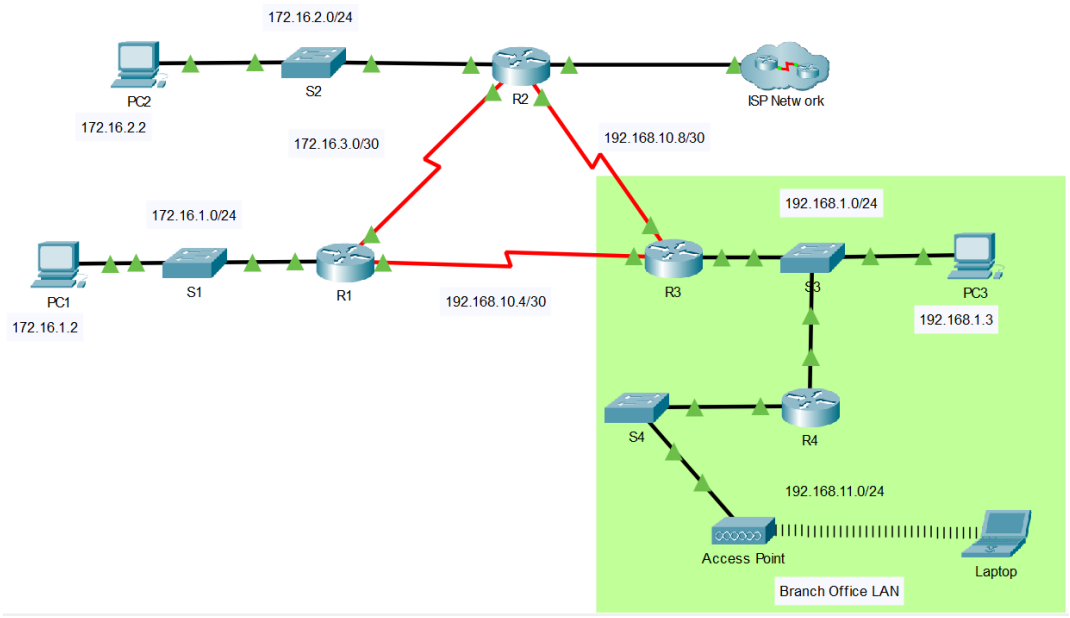
Conceptos y Definiciones Básicas

Internetworking es la disciplina técnica que estudia los principios, protocolos y arquitecturas para la interconexión lógica de múltiples redes de computadoras heterogéneas, formando "una colección de redes interconectadas" que funciona como una sola red de gran escala (Comer, 2018). Su fundamento arquitectónico reside en el modelo de referencia TCP/IP, descrito por (Cerf & Kahn, 1974) como un sistema de conmutación de paquetes basado en datagramas, y en estándares de capa de enlace como IEEE 802.3 (Ethernet). El núcleo operativo incluye el direccionamiento jerárquico IP (Postel, 1981), protocolos de encaminamiento dinámico como OSPF (Moy, 1998) y BGP (Rekhter, Li, & Hares, 2006), y la segmentación de dominios de broadcast mediante switches (Perlman, 1992). La asignatura abarca el diseño de infraestructuras escalables mediante técnicas como VLSM (Fuller & Li, 2006) y VLANs (IEEE 802.1Q-2018), implementando mecanismos de redundancia (IEEE 802.1D), control de congestión (Jacobson, 1988) y calidad de servicio (QoS) para garantizar la entrega confiable de datos a través de sistemas autónomos interconectados.

La Figura 1 muestra esquemáticamente las operaciones fundamentales con arranque de viruta.

FIGURA 1

Elementos básicos de una red de datos



Redes de Comunicación de Datos

Elementos necesarios para crear una red de datos

Conceptos Teóricos:

Una red de datos es un sistema de interconexión de dispositivos que permite el intercambio de información mediante protocolos establecidos. Los elementos fundamentales son:

1. **Dispositivos Finales (End Devices):**
    - Computadoras, servidores, teléfonos IP, cámaras IP
    - Identificados mediante direcciones lógicas (IP) y físicas (MAC)
2. **Dispositivos de Interconexión (Intermediate Devices):**
    - **Switches:** Operan en la capa 2 (Enlace de datos), crean dominios de colisión separados
    - **Routers:** Operan en la capa 3 (Red), interconectan diferentes redes
    - **Hubs:** Dispositivos obsoletos que operan en capa 1, extienden dominios de colisión
    - **Access Points:** Proveen conectividad inalámbrica
3. **Medios de Transmisión:**
    - **Guiados:** Cable UTP (Categorías 5e, 6, 6a), fibra óptica (multimodo/monomodo), coaxial
    - **No guiados:** Ondas de radio (Wi-Fi), infrarrojo, microondas
4. **Protocolos:**
    - Conjunto de reglas que gobiernan la comunicación
    - Ejemplos: TCP/IP, Ethernet, HTTP, FTP, DNS
5. **Software y Servicios:**
    - Sistemas operativos de red
    - Servicios de directorio (Active Directory, LDAP)
    - Servicios de aplicación (web, correo, bases de datos)

Cálculos de Capacidad:

Ancho de banda teórico vs real:

Gigabit Ethernet: 1 Gbps teórico → ~940 Mbps real (debido a overhead)

Cálculo de tiempo de transferencia:

Tiempo = (Tamaño archivo × 8) / Ancho de banda efectivo

Ejemplo: 100 MB archivo en red 100 Mbps:

Tiempo = (100 × 8 × 10^6) / (100 × 10^6) = 8 segundos

FIGURA 2

Ejemplo de una instalación básica de internet

Ventajas de una red de datos

Aplicaciones y Beneficios:

1. **Compartición de Recursos:**
    - Impresoras en red: Ahorro de costos vs impresoras individuales
    - Servidores de archivos: Centralización y backup simplificado
    - Ejemplo: Empresa con 50 empleados comparte 5 impresoras vs 50 individuales
2. **Comunicación Mejorada:**
    - Correo electrónico corporativo
    - Mensajería instantánea (Microsoft Teams, Slack)
    - VoIP: Reducción de costos telefónicos en ~40-60%
3. **Administración Centralizada:**
    - Políticas de seguridad unificadas
    - Actualizaciones de software automatizadas
    - Monitoreo y troubleshooting centralizado
4. **Acceso a Información:**
    - Intranets corporativas
    - Bases de datos compartidas

- Sistemas ERP/CRM

5. **Escalabilidad y Flexibilidad:**
    - Adición modular de dispositivos
    - Cálculo de ROI (Return on Investment):

$$ROI = (Beneficios\ anuales - Costo\ anual) / Costo\ inicial \times 100\%$$

Ejemplo: Red de $50,000 que ahorra $20,000 anuales:

ROI = $20,000 / $50,000 × 100% = 40% anual

Ejemplo Empresarial:

Una PYME que implementa red:

- Antes: 20 PC independientes, backups manuales, comunicación telefónica
- Después: Servidor centralizado, VoIP, backups automatizados
- Ahorro estimado: $15,000 anual en costos operativos

Dominios de Colisión y Broadcast

Dominio de Difusión (Broadcast Domain)

Concepto Teórico

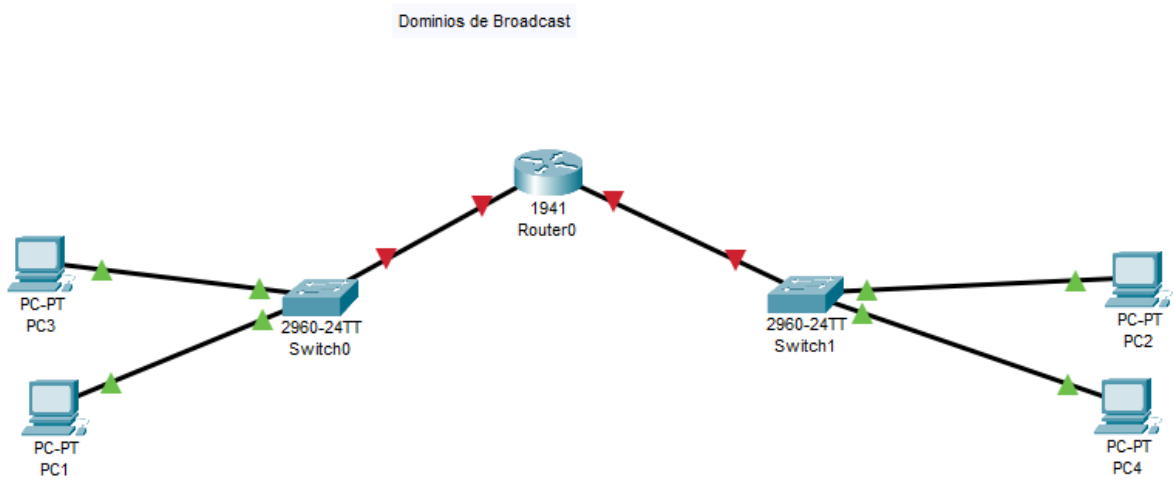
Un dominio de broadcast es el conjunto de dispositivos que reciben una trama de broadcast enviada por cualquier miembro del conjunto. Los routers delimitan dominios de broadcast, ver figura 3.

Características

- Broadcast: Dirección MAC destino es FF:FF:FF:FF:FF:FF
- Protocolos que usan broadcast: ARP, DHCP (inicialmente), NetBIOS
- Cada interfaz de router define un dominio de broadcast separado

FIGURA 3

Topología de un dominio de broadcast



Dominios de Broadcast:

1. PC1, PC3, SW0, interfaz LAN de R0

2. PC2, PC4, SW1, interfaz LAN de R0

Dominio de Colisión (Collision Domain)

Concepto Teórico

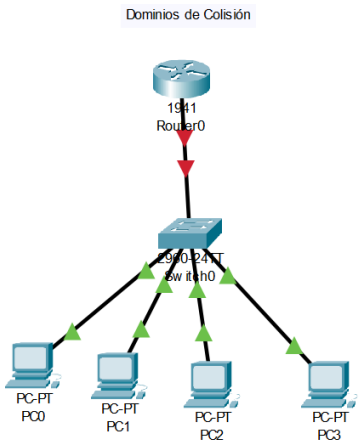
Segmento de red donde las tramas pueden colisionar. Cada puerto de switch define un dominio de colisión separado.

Historia y Evolución:

- Ethernet original (10Base5, 10Base2): Dominio de colisión compartido
- Half-duplex: Posibilidad de colisiones (CSMA/CD)
- Full-duplex (switches modernos): Elimina colisiones

FIGURA 4

Elementos básicos de un dominio de colisión.



Dominios de Colisión:

1. Puerto SW0 a PC1: 1 dominio
2. Puerto SW0 a PC2: 1 dominio
3. Puerto SW0 a PC3: 1 dominio
4. Puerto SW0 a R0: 1 dominio

Total: 4 dominios de colisión

Fórmula general con switches:

Nº Dominios Colisión = Nº Puertos activos de todos los switches + Nº Dispositivos conectados a hubs

Tabla 1

Tabla comparativa entre dominio de colisión y broadcast

Característica	Dominio de Colisión	Dominio de Broadcast
Definición	Segmento donde pueden ocurrir colisiones	Conjunto que recibe tramas broadcast
Delimitado por	Switches (cada puerto)	Routers (cada interfaz)

Característica	Dominio de Colisión	Dominio de Broadcast
Protocolos relacionados	CSMA/CD (obsoleto)	ARP, DHCP, algunos protocolos de routing
Tamaño recomendado	1 dispositivo (con switches)	Máximo ~500 dispositivos (buenas prácticas)
Impacto en rendimiento	Alto (colisiones)	Medio (broadcast storm)
Solución para reducir	Switches	VLANs, routers

Modelo OSI y TCP/IP

Capa de Aplicación

Modelo OSI (Capa 7):

- **Función:** Interfaz entre aplicaciones y servicios de red
- **Protocolos/Estándares:** HTTP, FTP, SMTP, DNS, Telnet
- **Unidad de datos:** APDU (Application Protocol Data Unit)

Modelo TCP/IP (Capa de Aplicación):

- Combina capas 5, 6, 7 del OSI

Ejemplo Detallado - HTTP/HTTPS:

HTTP Request:

GET /index.html HTTP/1.1

Host: www.ejemplo.com

User-Agent: Mozilla/5.0

Accept: text/html

HTTP Response:

HTTP/1.1 200 OK

Content-Type: text/html

Content-Length: 1256

Cálculos de Rendimiento:

- Latencia de aplicación: Tiempo RTT (Round Trip Time) + tiempo procesamiento servidor
- Throughput efectivo: (Tamaño datos útil × 100) / Tamaño total con headers

Flujo, Mensaje (Capas 5 y 6 OSI)

Capa 5 - Sesión:

- **Función:** Establecer, mantener y terminar sesiones entre aplicaciones

Ejemplos:

- ✓ SSL/TLS: Handshake para conexiones seguras
- ✓ NetBIOS: Sesiones en redes Windows
- ✓ RPC: Llamadas a procedimientos remotos

Capa 6 - Presentación:

- **Función:** Traducción, compresión y encriptación de datos

Cálculo de Compresión:

Tasa compresión = (1 - Tamaño comprimido/Tamaño original) × 100%

Ejemplo: Archivo 100KB comprimido a 25KB → 75% compresión

Segmento, Paquete (Capas 4 y 3)

Capa 4 - Transporte (Segmento/Datagrama):

- **TCP (Transmission Control Protocol):**
  - ✓ Orientado a conexión, confiable
  - ✓ Control de flujo (ventana deslizante)
  - ✓ Estructura segmento:

Cabecera TCP (20-60 bytes):

1. Puerto origen/destino (16 bits cada uno)
2. Números de secuencia y acuse (32 bits)
3. Ventana (16 bits), Checksum (16 bits)

4. Flags (SYN, ACK, FIN, etc.)

Cálculo ventana TCP: Ventana = Buffer receptor - Datos no confirmados

- **UDP (User Datagram Protocol):**
    - No orientado a conexión, no confiable
    - Aplicaciones: DNS, VoIP, video streaming
    - Overhead menor: 8 bytes de cabecera

Comparación TCP vs UDP:

Ejemplo: Transferencia archivo 1MB

- TCP: Establece conexión (3-way handshake), envía en segmentos, confirma recepción

- UDP: Envía datagramas sin confirmación (riesgo de pérdida)

Cálculo eficiencia:

Eficiencia TCP = (Datos útiles) / (Datos + Headers + ACKs)

Eficiencia UDP = (Datos útiles) / (Datos + Headers UDP)

Capa 3 - Red (Paquete):

- **IP (Internet Protocol):**
    - Direccionamiento lógico
    - Encaminamiento (routing)
    - Fragmentación/reensamblado
- **Estructura paquete IPv4:**

Cabecera IP (20-60 bytes):

- Versión (4 bits), IHL (4 bits)

- TOS (8 bits), Longitud total (16 bits)

- Identificación, Flags, Offset fragmentación

- TTL (8 bits), Protocolo (8 bits)

- Checksum cabecera (16 bits)

- IP origen/destino (32 bits cada una)

Ejemplo de Encapsulación:

Datos aplicación → Segmento TCP → Paquete IP → Trama Ethernet

[HTTP Data] → [TCP Hdr][Data] → [IP Hdr][TCP][Data] → [Eth Hdr][IP][TCP][Data][Eth Trl]

Capa de Internet (Modelo TCP/IP)

Equivalente a Capa 3 OSI:

- **Protocolos clave:**
- **IP (Internet Protocol):** v4 (32 bits) y v6 (128 bits)
- **ICMP (Internet Control Message Protocol):** Ping, traceroute
- **ARP (Address Resolution Protocol):** IP → MAC
- **Routing Protocols:** OSPF, BGP, EIGRP

Direccionamiento IP - Ejemplo Detallado:

Dirección: 192.168.1.100/24

1. Binario: 11000000.10101000.00000001.01100100
2. Máscara: 255.255.255.0 = /24
3. Red: 192.168.1.0
4. Broadcast: 192.168.1.255
5. Hosts utilizables: 192.168.1.1 - 192.168.1.254

Tabla 2

Comparación entre el modelo OSI y TCP/IP.

Capa OSI	Unidad de Datos	Protocolos	Equivalente TCP/IP
7. Aplicación	APDU	HTTP, FTP, SMTP	Capa Aplicación
6. Presentación	PPDU	SSL, JPEG, MPEG	Capa Aplicación
5. Sesión	SPDU	NetBIOS, RPC	Capa Aplicación
4. Transporte	Segmento	TCP, UDP	Capa Transporte
3. Red	Paquete	IP, ICMP, OSPF	Capa Internet
2. Enlace	Trama	Ethernet, PPP	Capa Acceso Red

Capa OSI	Unidad de Datos	Protocolos	Equivalente TCP/IP
1. Física	Bits	RS-232, 100Base-TX	Capa Acceso Red

Topologías de Red

Topología de Red Física

Definición: Disposición física real de dispositivos y medios.

Tipos y Características:

1. **Topología en Bus:**
    - **Estructura:** Cable principal (backbone) con dispositivos conectados
    - **Ventajas:** Simple, bajo costo inicial
    - **Desventajas:** Single point of failure, difícil troubleshooting
    - **Aplicación histórica:** 10Base2, 10Base5 Ethernet
2. **Topología en Anillo:**
    - **Estructura:** Dispositivos conectados en círculo
    - **Tipos:** Anillo simple, doble anillo (FDDI, Token Ring)
    - **Protocolo:** Token passing
3. **Topología en Estrella:**
    - **Estructura:** Todos dispositivos conectados a concentrador central
    - **Ventajas:** Fácil administración, fallo individual no afecta red completa
    - **Desventajas:** Dependencia del dispositivo central
4. **Topología en Malla:**
    - **Estructura:** Conexiones punto a punto entre todos dispositivos
    - **Tipos:** Malla completa vs parcial
5. **Topología Híbrida:**
    - Combinación de topologías básicas
    - Ejemplo: Estrella extendida (jerárquica)

Topología de Red Lógica

Definición: Camino que siguen las señales a través de la topología física.

Tipos Principales:

1. **Broadcast (Difusión):**
    - Todas estaciones reciben todas las tramas
    - Ejemplo: Ethernet tradicional, Wi-Fi
    - Fórmula probabilidad colisión:
2. **Token Passing (Paso de Testigo):**
    - Estación solo transmite cuando posee el token
    - Ejemplo: Token Ring, FDDI
    - Eficiencia: E = T_transmisión / (T_transmisión + T_token)

Topologías Específicas

Topología de Bus (Detallada):

- **Implementación:** Cable coaxial (10Base2: 185m máximo)
- **Terminadores:** 50 ohmios en extremos
- **Problema:** Reflexiones si conector falla → toda red cae

Cálculo atenuación:

Pérdida (dB) = 10 × log(P_out/P_in); Máximo recomendado: 30 dB pérdida

Topología de Anillo (Detallada):

- **Token Ring IEEE 802.5:** 4/16 Mbps, MAU (Multistation Access Unit)
- **FDDI (Fiber Distributed Data Interface):** 100 Mbps, anillo doble contra fallos
- **Tiempo recuperación fallo:**
    - Token Ring: ~200ms para auto-reconfiguración
    - FDDI: ~50ms para wrap del anillo

Topología de Estrella (Detallada):

- **Evolución:** Hub → Switch
- **Distancia máxima:** 100m UTP (Ethernet)
- **Cálculo ancho de banda compartido:**

Práctica 1: Diseño de Red Básica

Objetivo: Diseñar red para una pequeña empresa

Escenario:

- Empresa: 30 empleados, 2 departamentos (Ventas y Administración)
- Recursos compartidos: 2 impresoras, 1 servidor de archivos

- Conexión a Internet requerida
- Presupuesto: $5,000

Diseño Propuesto:

1. **Topología Física:** Estrella extendida
2. **Dispositivos:**
    - Router multipropósito: 1 unidad ($300)
    - Switch capa 2 48 puertos: 1 unidad ($800)
    - Switch capa 2 24 puertos: 1 unidad ($400)
    - Access Points: 2 unidades ($200 c/u)
    - Servidor: 1 unidad ($2,000)
    - Cableado UTP Cat6: 35 puntos ($1,000)
3. **Esquema de Direccionamiento:**

VLAN 10: Ventas - 192.168.10.0/24

VLAN 20: Administración - 192.168.20.0/24

Servidores: 192.168.100.0/24

4. **Cálculos de Performance:**
    - Throughput requerido: 30 usuarios × 2 Mbps = 60 Mbps
    - Ancho de banda Internet: 100 Mbps dedicado
    - Storage servidor: 30 users × 50GB = 1.5TB + redundancia
5. **Plan de Implementación:**

Semana 1: Cableado estructurado

Semana 2: Instalación equipos activos

Semana 3: Configuración y pruebas

Documentación Por Entregar:

1. Diagrama de topología física
2. Diagrama de topología lógica
3. Esquema de direccionamiento IP
4. Lista de equipos con costos
5. Plan de pruebas de conectividad

UNIDAD 2 DIRECCIONAMIENTO IP

Subnetting, CIDR y VLSM

Mascara de subred de longitud variable

VLSM (Variable Length Subnet Mask) es la técnica más adecuada cuando la red requiere subredes con capacidades diferentes. A diferencia del FLSM, (Fixed Length Subnet Mask), o Máscara de Subred de Longitud Fija, que divide una red IP en subredes del mismo tamaño,

Enrutamiento entre dominios sin clases

El enrutamiento entre dominios sin clases (CIDR) es un método de asignación y enrutamiento de direcciones IP que mejora la eficiencia del uso de direcciones y del enrutamiento de datos en Internet. Cada dispositivo conectado a la red, como máquinas, servidores y equipos de usuario final, posee una dirección IP única, la cual permite su identificación y comunicación con otros dispositivos.

Propósito CIDR y VLSM

Propósito de VLSM: VLSM permite asignar primero los rangos de mayor tamaño y posteriormente ajustar los más pequeños, logrando un uso eficiente de las direcciones IP y un esquema de direccionamiento más organizado.

Propósito CIDR: A diferencia del direccionamiento tradicional basado en clases fijas (A, B y C), CIDR asigna direcciones IP de manera flexible, utilizando un prefijo de red que se ajusta a las necesidades reales de cada organización, optimizando así la gestión de direcciones y el desempeño del enrutamiento en redes modernas.

Utilización CIDR y VLSM

Ejemplo de uso de CIDR

Una empresa mediana requiere diseñar su red interna para conectar aproximadamente 120 dispositivos, entre computadoras, impresoras de red, servidores y equipos de comunicaciones. El objetivo principal es asignar direcciones IP de manera eficiente, evitando el desperdicio de recursos y facilitando el proceso de enrutamiento.

Situación con direccionamiento tradicional por clases

Utilizando el esquema clásico de direccionamiento basado en clases, la empresa debería asignar una red de Clase C, por ejemplo:

Red: 192.168.10.0/24

Máscara de subred: 255.255.255.0

Direcciones totales: 256

Direcciones utilizables para hosts: 254

Aunque solo se requieren 120 direcciones, este esquema obligaría a reservar 254 direcciones, generando un desperdicio considerable de direcciones IP.

Mediante el uso de CIDR, la red puede dimensionarse de acuerdo con las necesidades reales de la organización. Para soportar 120 dispositivos, se asigna el siguiente bloque:

Red: 192.168.10.0/25

Máscara de subred: 255.255.255.128

Direcciones totales: 128

Direcciones utilizables para hosts: 126

Ejemplo de uso de VLSM

Una institución académica dispone del bloque de direcciones privadas **172.16.0.0/24**, el cual ofrece un total de **256 direcciones IP**, de las cuales **254 son utilizables para hosts**. La red debe ser segmentada para cubrir los requerimientos de conectividad de cuatro áreas funcionales, cada una con un número diferente de dispositivos conectados:

Tabla 3

Distribución del número de equipos distribuidos por cada área.

Área / Departamento	Dispositivos requeridos
Centro de Datos	110
Área Administrativa	60
Laboratorio de Redes	30
Enlace punto a punto	2

Dado que los requerimientos de cada segmento son heterogéneos, el uso de una única máscara de subred resultaría ineficiente, provocando desperdicio de direcciones IP.

Metodología de diseño con VLSM

Ordenamiento de las subredes

Como paso inicial, los segmentos de red se ordenan de mayor a menor según el número de hosts requeridos.

1. Centro de Datos (110 hosts)
2. Área Administrativa (60 hosts)
3. Laboratorio de Redes (30 hosts)
4. Enlace punto a punto (2 hosts)

Cálculo de máscaras de subred

Para cada segmento se determina la máscara mínima que permita cubrir el número de hosts requerido, considerando que en IPv4 se reservan dos direcciones por subred (dirección de red y dirección de broadcast).

Asignación detallada de subredes

Subred del Centro de Datos

Hosts requeridos: 110

Potencia de dos inmediata superior: 128 direcciones

Máscara resultante: /25 (255.255.255.128)

Hosts utilizables: 126

Asignación:

Dirección de red: 172.16.0.0/25

Primer host válido: 172.16.0.1

Último host válido: 172.16.0.126

Dirección de broadcast: 172.16.0.127

Esta subred proporciona suficiente capacidad para servidores, dispositivos de almacenamiento, equipos de respaldo y crecimiento moderado futuro.

Subred del Área Administrativa

Hosts requeridos: 60

Potencia de dos inmediata superior: 64 direcciones

Máscara resultante: /26 (255.255.255.192)

Hosts utilizables: 62

Asignación:

Dirección de red: 172.16.0.128/26

Primer host válido: 172.16.0.129

Último host válido: 172.16.0.190

Dirección de broadcast: 172.16.0.191

Esta subred cubre estaciones de trabajo, impresoras de red y dispositivos administrativos, con un margen limitado de expansión.

Subred del Laboratorio de Redes

Hosts requeridos: 30

Potencia de dos inmediata superior: 32 direcciones

Máscara resultante: /27 (255.255.255.224)

Hosts utilizables: 30

Asignación:

Dirección de red: 172.16.0.192/27

Primer host válido: 172.16.0.193

Último host válido: 172.16.0.222

Dirección de broadcast: 172.16.0.223

Esta subred resulta adecuada para equipos de laboratorio, routers de práctica y simuladores de red.

Subred para enlace punto a punto

Hosts requeridos: 2

Potencia de dos inmediata superior: 4 direcciones

Máscara resultante: /30 (255.255.255.252)

Hosts utilizables: 2

Asignación:

Dirección de red: 172.16.0.224/30

Primer host válido: 172.16.0.225

Último host válido: 172.16.0.226

Dirección de broadcast: 172.16.0.227

Este tipo de subred es comúnmente utilizado para enlaces entre routers, ya que minimiza el desperdicio de direcciones IP.

Evaluación del uso del direccionamiento

Gracias a la implementación de VLSM:

Se aprovecha de manera eficiente el bloque 172.16.0.0/24.

Se evita la asignación excesiva de direcciones IP innecesarias.

Se mejora la organización lógica de la red.

Se facilita la futura ampliación del diseño de red.

Flexibilidad CIDR y VLSM

La flexibilidad que ofrecen CIDR (Classless Inter-Domain Routing) y VLSM (Variable Length Subnet Mask) constituye un avance significativo en el diseño y la administración moderna de redes IP, al permitir el uso más eficiente, escalable y adaptable del espacio de direccionamiento.

En primer lugar, CIDR elimina las limitaciones rígidas del direccionamiento basado en clases (A, B y C), posibilitando la asignación de prefijos de longitud variable según las necesidades reales de cada red. Esta característica brinda una elevada flexibilidad en la agregación y desagregación de rutas, lo que reduce significativamente el tamaño de las tablas de enrutamiento y mejora el rendimiento de los routers en redes de gran escala, como Internet.

En contraste, VLSM amplía esta flexibilidad a nivel interno de la red, al permitir que una misma red principal se divida en subredes de diferentes tamaños, cada una con una máscara adaptada a sus requerimientos específicos. De este modo, es posible asignar subredes más grandes a segmentos con alta densidad de dispositivos (por ejemplo, centros de datos o redes de usuarios) y subredes más pequeñas a enlaces punto a punto o redes administrativas, optimizando aún más el uso del espacio de direcciones.

La combinación de CIDR y VLSM ofrece una arquitectura de direccionamiento altamente flexible y eficiente, capaz de adaptarse al crecimiento dinámico de la red y a cambios en la topología sin necesidad de rediseños drásticos. Esta flexibilidad no solo reduce el consumo innecesario de direcciones IP, sino que también simplifica la planificación, mejora la escalabilidad y favorece una gestión más ordenada y sostenible de las infraestructuras de red**.**

Dirección Clases CIDR y VLSM

Un bloque CIDR se define como un rango de direcciones IP que comparten un prefijo de red común y una misma longitud de bits. Los bloques de mayor tamaño contienen una cantidad más amplia de direcciones IP y se caracterizan por un sufijo numérico más reducido.

La Internet Assigned Numbers Authority (IANA) es la entidad responsable de asignar grandes bloques CIDR a los Registros Regionales de Internet (RIR). Posteriormente, estos organismos distribuyen bloques de menor tamaño a los Registros Locales de Internet (LIR), quienes finalmente los asignan a las organizaciones. Por su parte, los usuarios privados obtienen bloques CIDR a través de sus proveedores de servicios de Internet (ISP)

Master CIDR Block 10.10.0.0/16

Tabla 4

Asignación de direcciones IPs para las diferentes subredes.

Subnet 1	10.10.1.0 /24
Subnet 2	10.10.2.0 /24
Subnet 3	10.10.3.0 /24
Subnet 4	10.10.4.0 /24
Subnet 5	10.10.5.0 /24

VLSM (Variable Length Subnet Mask) permite subdividir una red en subredes de distintos tamaños, cada una con una máscara específica según el número de hosts requeridos. A diferencia del modelo tradicional de subredes de tamaño fijo, VLSM optimiza aún más el direccionamiento, ya que evita el

desperdicio de direcciones en segmentos de red pequeños, como enlaces punto a punto, y asigna subredes más grandes solo donde es necesario.

IPV6

Partes de la dirección IPv6

Una dirección IPv6 constituye un identificador numérico de 128 bits, representado mediante notación hexadecimal, cuyo propósito es identificar y localizar de manera unívoca a los dispositivos o nodos que operan dentro de una red basada en la sexta versión del Protocolo de Internet. Este esquema de direccionamiento fue concebido como evolución y reemplazo del IPv4, proporcionando un espacio de direcciones significativamente ampliado, lo que posibilita la interconexión de cantidades masivas de dispositivos y soluciona las limitaciones asociadas al agotamiento de direcciones presentes en el estándar previo

Partes

Estructura: 8 grupos hexadecimales de 16 bits

(ej.2001:0db8:85a3:0000:0000:8a2e:0370:7334).

Prefijo de Red (Network Prefix): Generalmente los primeros 64 bits (o los primeros 4 grupos). Identifica la red específica a la que pertenece el dispositivo.

ID de Interfaz (Interface ID): Los últimos 64 bits (o los últimos 4 grupos). Identifica de forma única el dispositivo o interfaz de red.

Abreviatura de direcciones IPv6

La representación estándar de una dirección IPv6 se expresa como x:x:x:x:x:x:x:x, donde cada segmento (x) corresponde a un valor hexadecimal que representa 16 bits, conformando un total de ocho bloques. Bajo este esquema, el rango de direcciones IPv6 se extiende desde 0000:0000:0000:0000:0000:0000:0000:0000 hasta ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff.

El formato completo, IPv6 admite mecanismos de notación abreviada con el propósito de simplificar la escritura y lectura de las direcciones. El primero consiste en la eliminación de los ceros a la izquierda dentro de cada bloque hexadecimal.

Por ejemplo, la dirección 1050:0000:0000:0000:0005:0600:300c:326b puede representarse como 1050:0:0:0:5:600:300c:326b.

El segundo mecanismo de abreviación permite sustituir una secuencia continua de bloques con valor cero mediante el uso de doble dos puntos (::). Así, la dirección ff06:0:0:0:0:0:0:c3 puede expresarse como ff06::c3. Cabe destacar que esta notación solo puede aplicarse una única vez dentro de una misma dirección IPv6, a fin de evitar ambigüedades en su interpretación.

Prefijos en IPv6

En el protocolo IPv6, los prefijos de dirección cumplen la función de identificar de manera unívoca una red o subred, y se expresan mediante la notación CIDR (Classless Inter-Domain Routing).

Dicha notación se indica con una barra diagonal (/) seguida de un valor decimal comprendido entre 1 y 128, el cual especifica la cantidad de bits destinados a la porción de red dentro de la dirección.

En la práctica, los prefijos /64 se emplean de forma predominante para subredes individuales, mientras que los prefijos /48 suelen asignarse a sitios de clientes, facilitando la creación de múltiples subredes internas.

Desde el punto de vista estructural, el prefijo IPv6 es análogo a la máscara de subred utilizada en IPv4, ya que determina la sección de la dirección que identifica a la red.

Generalmente, esta porción corresponde a los primeros 64 bits de los 128 bits totales que conforman una dirección IPv6. La representación típica de una dirección IPv6 con prefijo adopta la siguiente forma: 2001:db8:abcd:0012::/64.

Existen diversos prefijos comúnmente utilizados en IPv6, cada uno con un propósito específico.

El prefijo /48 se asigna habitualmente a redes de usuarios finales, permitiendo la creación de hasta 2^{16} (65 536) subredes LAN.

El prefijo /64 constituye el estándar para subredes individuales y es un requisito indispensable para el correcto funcionamiento de SLAAC (Stateless Address Autoconfiguration).

El prefijo /128 identifica una única dirección de host.

IPv6 define una serie de prefijos especiales reservados para funciones específicas.

El prefijo::/128 corresponde a la dirección no especificada, mientras que ::1/128 se utiliza como dirección de loopback.

El rango fe80::/10 está destinado a direcciones de enlace local (link-local), ff00::/8 identifica direcciones de multidifusión (multicast), y 2001:db8::/32 se encuentra reservado exclusivamente para documentación y ejemplos.

Los proveedores de servicios de Internet (ISP) suelen recibir prefijos de menor longitud, tales como /32 o /36, los cuales son posteriormente subdivididos para asignar prefijos /48 o /56 a los clientes finales.

Finalmente, cabe señalar que la longitud del prefijo siempre se expresa en formato decimal y se ubica al final de la dirección IPv6.

Direcciones unicast

Las direcciones Unicast IPv6 identifican de forma única una interfaz de red, permitiendo el envío de paquetes desde un origen a un destino específico.

Tienen una longitud de 128 bits, representadas en hexadecimal, y no existen direcciones de difusión (broadcast) en IPv6, usando en su lugar multicast o unicast.

Dirección unicast global

Las direcciones IPv6 de unidifusión global son las direcciones IPv6 de Internet. Este tipo de dirección es similar a las direcciones públicas IPv4 . Son únicas en Internet, al igual que las direcciones públicas IPv4. Son enrutables y accesibles en Internet.

Las direcciones IPv6 de unidifusión global ofrecen una amplia gama que abarca todos los dispositivos IPv6 disponibles en Internet. Esto también es importante en el mundo del Internet de las Cosas (IoT). Estas direcciones IPv6 son asignadas por la IANA, al igual que otras direcciones IP.

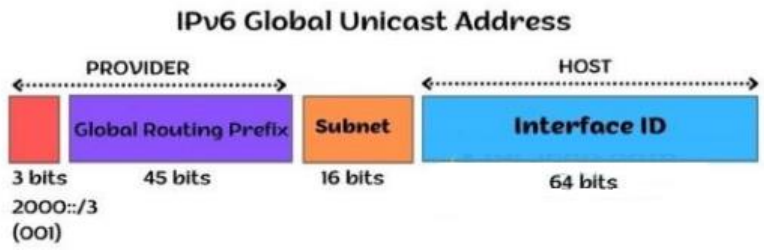
El prefijo de una dirección de unidifusión global IPv6 es 2000::/3 . Sus 3 bits de alto nivel están fijados como 001. Esto significa que una dirección de unidifusión global IPv6 puede comenzar con el dígito hexadecimal 2 o 3, según el valor del cuarto bit.

0010.. (2000::/3)

0011.. (3000::/3)

FIGURA 5

Distribución de los bits en una dirección IPv6 unicast.



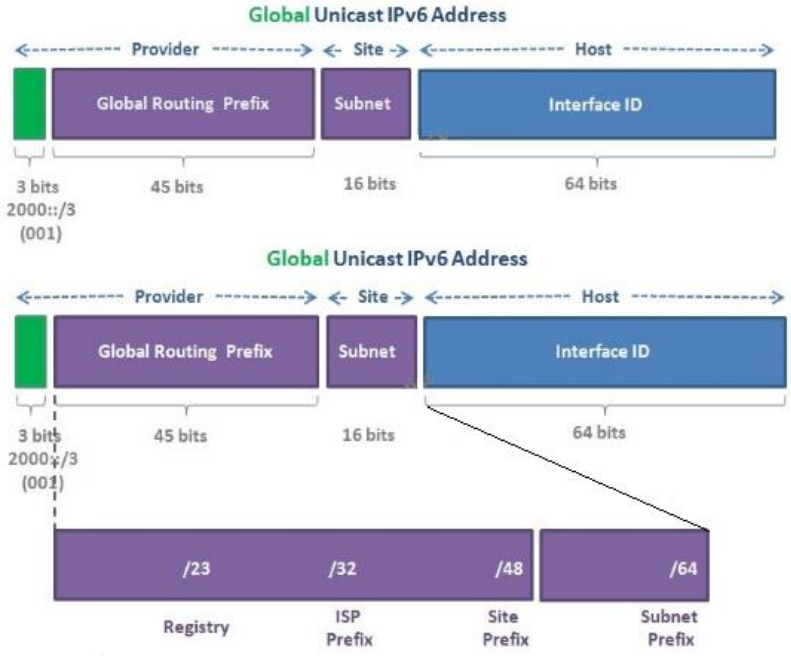
https://ipcisco.com

El, SLA es la parte asignada por su proveedor de servicios. La ID de LAN es la parte que (el cliente) determina para dividir las direcciones en diferentes redes (subredes IPv6).

La parte del host (ID de interfaz) también tiene 64 bits. Generalmente se crea con el formato IPv6 EUI-64.

FIGURA 6

Formato de una IPv6 EUI-64.



https://ipcisco.com

Direcciones de unidifusión global transicionales

La transición del protocolo IPv4 a IPv6 ha requerido el desarrollo de diversos mecanismos técnicos que permitan la coexistencia e interoperabilidad entre ambos protocolos durante un periodo prolongado. Estos mecanismos difieren en su principio de funcionamiento, alcance y nivel de complejidad, y su elección depende de las condiciones técnicas y administrativas de cada red.

Direcciones de unidifusión global de transición (6to4)

El mecanismo 6to4 se basa en el uso de direcciones IPv6 especiales que incorporan una dirección IPv4 pública dentro del prefijo 2002::/16. Este método permite el establecimiento de túneles automáticos, mediante los cuales los paquetes IPv6 son encapsulados dentro de IPv4 para atravesar infraestructuras que aún no soportan IPv6 de forma nativa. Aunque su despliegue inicial es sencillo, presenta limitaciones importantes relacionadas con la confiabilidad, la latencia y la dependencia de direcciones IPv4 públicas, lo que ha reducido su adopción en entornos productivos.

Teredo

Teredo es un mecanismo de transición diseñado para proporcionar conectividad IPv6 a través de dispositivos NAT. Para ello, encapsula paquetes IPv6 dentro de UDP sobre IPv4, permitiendo su transporte en redes donde no es posible utilizar 6to4. En comparación con este último, Teredo ofrece mayor flexibilidad en entornos domésticos o corporativos con NAT, aunque introduce una mayor sobrecarga, complejidad operativa y potenciales riesgos de seguridad. Por estas razones, se considera una solución de último recurso.

ISATAP

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) está orientado principalmente a redes internas y permite el transporte de IPv6 sobre una infraestructura IPv4 dentro de un dominio administrativo controlado. A diferencia de 6to4 y Teredo, ISATAP no está diseñado para conectividad global, sino para facilitar la adopción progresiva de IPv6 en entornos corporativos. Su principal ventaja es el control administrativo, aunque su alcance limitado reduce su utilidad como solución de transición a largo plazo.

Dual Stack

El enfoque de doble pila, o dual stack, consiste en la ejecución simultánea de IPv4 e IPv6 en los dispositivos y redes. Este método permite la comunicación nativa utilizando cualquiera de los dos protocolos, sin necesidad de encapsulación ni traducción. Desde una perspectiva académica, dual stack es considerado el mecanismo de transición más robusto y recomendado, aunque implica un mayor costo operativo y una mayor complejidad en la administración de la red.

Traducción de direcciones (NAT64/DNS64)

Los mecanismos de traducción, como NAT64 y DNS64, permiten la comunicación entre nodos IPv6 e IPv4 mediante la conversión de encabezados de protocolo. Este enfoque resulta especialmente adecuado para redes IPv6-only que requieren acceso a servicios IPv4. Sin embargo, introduce limitaciones relacionadas con la transparencia extremo a extremo y la compatibilidad con ciertas aplicaciones.

Enlace de dirección de unidifusión local

La **dirección de unidifusión local de enlace (Link-Local) en IPv6**, perteneciente al prefijo **FE80::/10**, constituye un elemento necesario en toda interfaz que tenga habilitado el protocolo IPv6. Su función principal es posibilitar la comunicación dentro del ámbito del enlace local, siendo fundamental para procesos como la **detección de vecinos (Neighbor Discovery Protocol, NDP)**, el **enrutamiento básico** y el soporte de **DHCPv6**. Estas direcciones no son enrutables más allá del segmento local, no requieren un servidor DHCP para su configuración y se emplean como **dirección del gateway predeterminado** en entornos IPv6.

Técnicamente, las direcciones Link-Local presentan las siguientes características esenciales:

Alcance: Su validez se restringe estrictamente al enlace local, entendido como un segmento físico de red o una VLAN, por lo que no pueden ser reenviadas por routers.

Prefijo: Se identifican por el prefijo **FE80::/10**, comúnmente representado en la práctica como **FE80::/64**.

Asignación: Se generan de manera automática al activar IPv6 en una interfaz de red, de forma análoga a las direcciones APIPA (169.254.0.0/16) en IPv4.

Formato: Están compuestas por el prefijo FE80:: seguido de un **identificador de interfaz de 64 bits**, el cual puede derivarse del método **EUI-64** o ser generado de manera aleatoria para mejorar la privacidad.

Uso: Resultan indispensables para la comunicación entre dispositivos conectados al mismo switch, la interacción con el router local y el funcionamiento de los mecanismos de descubrimiento y resolución de vecinos.

En contraste con las **direcciones de unidifusión global**, las direcciones Link-Local poseen un carácter estrictamente local y temporal en relación con el enlace, por lo que no pueden emplearse para la comunicación directa con hosts ubicados fuera de la subred local. Su importancia radica en servir como base operativa para el correcto funcionamiento de IPv6, incluso en ausencia de conectividad global.

UNIDAD 3: ENRUTAMIENTO ESTÁTICO Y DINÁMICO

El enrutamiento constituye uno de los procesos fundamentales en el funcionamiento de las redes de computadoras, ya que permite determinar el camino más adecuado para que los paquetes de datos viajen desde un origen hasta un destino a través de múltiples dispositivos interconectados. A medida que las redes han evolucionado en complejidad y tamaño, los mecanismos de enrutamiento han debido adaptarse para garantizar eficiencia, confiabilidad y escalabilidad (Kurose & Ross, 2021).

Configuración y direccionamiento de CLI

La interfaz de línea de comandos, conocida como CLI (Command Line Interface), constituye el principal medio de interacción entre el administrador y los dispositivos de red, tales como routers y switches. A través de esta interfaz es posible acceder al sistema operativo del dispositivo y ejecutar instrucciones precisas para configurar parámetros críticos, incluyendo el direccionamiento IP, la habilitación de interfaces y la definición de políticas de enrutamiento (Cisco Networking Academy, 2023).

El uso de la CLI ofrece un control detallado sobre el comportamiento del dispositivo, permitiendo realizar configuraciones avanzadas que no siempre están disponibles mediante interfaces gráficas. De la misma forma, la CLI facilita la automatización de tareas, el diagnóstico de fallos y la supervisión del estado de la red, lo que la convierte en una herramienta indispensable para los profesionales del área de redes y telecomunicaciones.

Comandos del modo Configuración

Los dispositivos de red emplean una estructura jerárquica de modos de operación que regula el alcance de los comandos disponibles para el usuario. Entre los principales modos se encuentran el modo usuario, el modo privilegiado, el modo de configuración global y los modos de configuración específicos, como el de interfaz o el de protocolo de enrutamiento (Forouzan, 2017).

Esta organización jerárquica cumple una función esencial en la seguridad y estabilidad del sistema, ya que restringe el acceso a comandos críticos únicamente a usuarios autorizados. Además, facilita la administración ordenada de la configuración, reduciendo la probabilidad de errores operativos que puedan afectar la conectividad o el rendimiento de la red.

Tabla 5

Comandos a usar acorde al Modo de Configuración

Modo	Comando	Descripción	Ejemplo
Usuario EXEC (>)	enable	Permite acceder al modo privilegiado EXEC	Router> enable
	exit	Cierra la sesión del dispositivo	Router> exit
	ping	Verifica conectividad con otro dispositivo	Router> ping 192.168.1.1
Privilegiado EXEC (#)	disable	Regresa del modo privilegiado al modo usuario	Router# disable
	show running-config	Muestra la configuración actual del equipo	Router# show running-config
	show ip interface brief	Muestra un resumen de interfaces y direcciones IP	Router# show ip interface brief
	configure terminal	Accede al modo de configuración global	Router# configure terminal
	copy running-config startup-config	Guarda la configuración en memoria	Router# copy run start
Configuración Global (config)	hostname	Cambia el nombre del dispositivo	Router(config)# hostname R1
	enable password	Configura una contraseña sin cifrado	R1(config)# enable password cisco
	enable secret	Configura una contraseña cifrada	R1(config)# enable secret cisco123
	no ip domain-lookup	Desactiva la resolución de nombres DNS	R1(config)# no ip domain-lookup
	service password-encryption	Cifra las contraseñas en texto plano	R1(config)# service password-encryption
	banner motd	Configura un mensaje de advertencia	R1(config)# banner motd #Acceso restringido#
	interface g0/0	Accede al modo configuración de interfaz	R1(config)# interface g0/0
	line console 0	Accede a la configuración de la consola	R1(config)# line console 0
	line vty 0 4	Accede a la configuración de líneas remotas	R1(config)# line vty 0 4
	ip route	Configura una ruta estática	R1(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.254
	router rip	Habilita el protocolo RIP	R1(config)# router rip

Configuración de Interfaz (config-if)	ip address	Asigna dirección IP y máscara a la interfaz	R1(config-if)# ip address 192.168.1.1 255.255.255.0
	no shutdown	Activa la interfaz	R1(config-if)# no shutdown
	shutdown	Desactiva la interfaz	R1(config-if)# shutdown
	description	Agrega una descripción a la interfaz	R1(config-if)# description RED_LAN
Configuración de Línea (config-line)	password	Configura contraseña de acceso	R1(config-line)# password cisco
	login	Habilita la solicitud de contraseña	R1(config-line)# login
	transport input telnet ssh	Define protocolos de acceso remoto	R1(config-line)# transport input telnet ssh
Configuración de Router (config-router)	network	Define redes para enrutamiento dinámico	R1(config-router)# network 192.168.1.0
Cualquier modo	exit	Sale del modo actual	R1(config-if)# exit
	end	Regresa al modo privilegiado	R1(config)# end

Rutas estáticas con dirección del "siguiente salto"

Otra modalidad de configuración de rutas estáticas consiste en especificar la dirección IP del siguiente router en el camino hacia la red de destino. En este caso, el dispositivo utiliza dicha dirección como referencia para reenviar los paquetes, lo que proporciona mayor flexibilidad en redes con múltiples saltos.

Este enfoque es ampliamente utilizado en redes empresariales, ya que facilita la comprensión lógica del recorrido del tráfico y permite una gestión más clara de las rutas configuradas. No obstante, al igual que otras formas de enrutamiento estático, requiere intervención manual ante cualquier cambio topológico.

Rutas estáticas con interfaz de salida

Una ruta estática puede configurarse indicando directamente la interfaz de salida por la cual deben reenviarse los paquetes destinados a una red específica. Este método es comúnmente utilizado en enlaces punto a punto, donde existe una única ruta posible hacia el destino.

La principal ventaja de este tipo de configuración radica en su simplicidad y claridad, ya que el router no necesita realizar procesos adicionales de resolución de direcciones para determinar el siguiente salto.

Sin embargo, su uso requiere un conocimiento preciso de la topología de la red, ya que una configuración incorrecta puede provocar problemas de encaminamiento o pérdida de conectividad.

Configuración de rutas estáticas con interfaz de salida

Desde el punto de vista operativo, cuando un router recibe un paquete cuya dirección de destino coincide con una ruta estática configurada por interfaz de salida, el dispositivo reenvía dicho paquete directamente por la interfaz indicada. Este proceso elimina la necesidad de realizar una búsqueda adicional para resolver la dirección del siguiente salto, lo que puede contribuir a una mayor eficiencia en el encaminamiento, especialmente en enlaces punto a punto donde existe un único camino posible hacia la red remota (Forouzan, 2017).

La sintaxis utilizada para configurar una ruta estática con interfaz de salida en routers Cisco se basa en la definición de la red de destino, su máscara de subred y la interfaz correspondiente. Conceptualmente, esta configuración puede representarse de la siguiente forma:

Red de destino + máscara de red → interfaz de salida

Cuando usar rutas estáticas

El uso de rutas estáticas en una red de computadoras responde a criterios técnicos, administrativos y operativos que deben ser evaluados cuidadosamente durante el diseño de la infraestructura. A diferencia del enrutamiento dinámico, las rutas estáticas no se actualizan de manera automática, sino que son definidas manualmente por el administrador de la red. Esta característica, lejos de ser una desventaja en todos los escenarios, convierte a las rutas estáticas en una solución eficiente y confiable en contextos específicos (Kurose & Ross, 2021).

Uno de los escenarios más apropiados para el uso de rutas estáticas es aquel en el que la red presenta un tamaño reducido y una topología sencilla. En redes con pocos routers y enlaces bien definidos, la administración manual de las rutas resulta viable y permite un control total sobre el flujo del tráfico. En estos casos, la complejidad asociada a la implementación de protocolos de enrutamiento dinámico puede resultar innecesaria y contraproducente (Forouzan, 2017).

Además, en entornos con topologías estables, donde los cambios son poco frecuentes, las rutas estáticas ofrecen un comportamiento predecible y fácil de documentar, lo que simplifica las tareas de mantenimiento y diagnóstico.

Enrutamiento dinámico por vector distancia

El enrutamiento dinámico por vector distancia constituye uno de los enfoques clásicos para el intercambio automático de información de enrutamiento entre routers dentro de una red. Este método se basa en la idea de que cada router mantiene una tabla de enrutamiento que contiene la distancia hacia las redes conocidas y la dirección del siguiente salto correspondiente. Periódicamente, los routers comparten esta información con sus vecinos directos, permitiendo que la red construya de manera progresiva una visión distribuida de la topología (Kurose & Ross, 2021).

A diferencia de otros enfoques de enrutamiento dinámico, el vector distancia no requiere que cada router posea un conocimiento completo de la topología de la red. En su lugar, cada dispositivo confía en la información recibida de sus vecinos, lo que simplifica la implementación del protocolo, pero introduce desafíos en términos de convergencia y estabilidad.

El funcionamiento del enrutamiento por vector distancia se fundamenta en el intercambio periódico de mensajes de actualización entre routers adyacentes. Cada mensaje contiene un vector de distancias que indica el costo estimado para alcanzar cada red de destino conocida por el emisor. Al recibir esta información, el router receptor evalúa si la nueva ruta ofrece un costo menor que el actualmente registrado en su tabla de enrutamiento y, de ser así, actualiza su información (Forouzan, 2017).

Este proceso se basa en algoritmos matemáticos como el algoritmo de Bellman-Ford, el cual permite calcular el camino más corto hacia un destino mediante la comparación iterativa de costos. La simplicidad del algoritmo ha contribuido a su amplia adopción en los primeros protocolos de enrutamiento dinámico.

Las aplicaciones del enrutamiento dinámico abarcan una amplia variedad de contextos, desde redes empresariales hasta infraestructuras de Internet a gran escala, consolidándose como un componente esencial de las arquitecturas de comunicación contemporáneas.

Enrutamiento dinámico por estado de enlace

El enrutamiento por estado de enlace se fundamenta en la construcción de una visión completa de la topología de la red por parte de cada router. Para ello, los dispositivos generan anuncios de estado de enlace que describen sus conexiones y los costos asociados, los cuales son difundidos a todos los nodos de la red.

Con esta información, cada router ejecuta algoritmos matemáticos, como el algoritmo de Dijkstra, para calcular las rutas más cortas hacia cada destino. Este enfoque ofrece una convergencia rápida y una mayor eficiencia en redes complejas, aunque implica un mayor consumo de recursos computacionales.

Aprendizaje de red

El aprendizaje de la red mediante el estado de enlace no depende de la información parcial proporcionada por routers vecinos, sino de la difusión sistemática de datos topológicos que describen la conectividad y el costo de los enlaces. Gracias a este enfoque, los routers pueden calcular rutas óptimas de manera autónoma y consistente, lo que se traduce en una mayor estabilidad y eficiencia del enrutamiento.

El aprendizaje de la red se materializa a través de la construcción de una base de datos de estado de enlace (Cisco Networking Academy, 2023), que almacena una copia sincronizada de todos los LSAs recibidos. Cada router mantiene su propia LSDB, la cual representa un mapa lógico completo de la topología de la red (Forouzan, 2017).

Este mapa topológico permite a los routers conocer no solo las rutas hacia los destinos, sino también la estructura global de la red, lo que facilita la toma de decisiones informadas en el proceso de encaminamiento. La sincronización de la LSDB entre todos los routers del dominio garantiza coherencia y evita inconsistencias en la selección de rutas.

Reducción del ancho de banda de información routing por los protocolos de estado de enlace

Uno de los principales desafíos en el diseño de protocolos de enrutamiento dinámico es minimizar el consumo de ancho de banda generado por el intercambio de información de control. Los protocolos de enrutamiento por estado de enlace, como OSPF, han sido diseñados con mecanismos específicos que permiten reducir de manera significativa la cantidad de tráfico de routing necesario para mantener

actualizada la información topológica de la red, sin comprometer la precisión ni la velocidad de convergencia (Kurose & Ross, 2021).

A diferencia de los protocolos basados en vector distancia, que intercambian periódicamente tablas completas de enrutamiento, los protocolos de estado de enlace emplean un enfoque más eficiente basado en la difusión selectiva de información relevante. Este diseño contribuye a un uso más racional del ancho de banda, especialmente en redes de gran tamaño y alta complejidad.

Enrutamiento dinámico externo

Protocolo RIP

RIP (Routing Information Protocol) es un protocolo de enrutamiento basado en el algoritmo de vector distancia. Utiliza el número de saltos como métrica principal para la selección de rutas, estableciendo un límite máximo que restringe el tamaño de la red.

La simplicidad de RIP facilita su comprensión e implementación, lo que lo convierte en una herramienta útil en entornos educativos. Sin embargo, sus limitaciones en términos de escalabilidad y convergencia reducen su aplicabilidad en redes de gran tamaño.

Protocolo OSPF

OSPF (Open Shortest Path First) es un protocolo de enrutamiento dinámico basado en el algoritmo de estado de enlace. Se caracteriza por su rápida convergencia, soporte para jerarquización mediante áreas y capacidad para manejar redes de gran escala.

Estas características han convertido a OSPF en uno de los protocolos más utilizados en redes empresariales modernas, donde la eficiencia y la confiabilidad son factores críticos.

Protocolo en la familia IGP

Los protocolos de enrutamiento dinámico constituyen la implementación práctica de los algoritmos de vector distancia y estado de enlace. Estos protocolos se clasifican, de manera general, en protocolos de gateway interior (IGP), utilizados dentro de un sistema autónomo, y protocolos de gateway exterior (EGP), empleados para el intercambio de información entre sistemas autónomos.

Virtualización de equipos de red

La virtualización de equipos de red consiste en la creación de instancias virtuales que replican el comportamiento de dispositivos físicos mediante software especializado. Esta tecnología ha adquirido gran relevancia en los ámbitos educativo, investigativo y profesional, al permitir la simulación de topologías complejas sin incurrir en elevados costos de infraestructura.

El uso de entornos virtualizados facilita la experimentación segura, la validación de diseños de red y el aprendizaje práctico del enrutamiento, consolidándose como una herramienta clave en la formación contemporánea en redes de computadoras (Cisco Networking Academy, 2023).

Comparación entre la virtualización externa e interna de la red

La virtualización interna de la red se refiere a la creación de múltiples redes lógicas dentro de una misma infraestructura física, sin que estas sean visibles o accesibles desde dominios externos. Este enfoque se utiliza comúnmente en redes locales y centros de datos, donde tecnologías como VLAN, redes virtuales privadas internas y conmutación virtual permiten segmentar el tráfico y aislar distintos servicios o departamentos dentro de una organización (Forouzan, 2017).

Por otro lado, la virtualización externa de la red implica la abstracción de recursos de red que se extienden más allá de un único dominio administrativo, permitiendo la interconexión de redes virtuales a través de infraestructuras compartidas, como Internet o redes de proveedores de servicios. Tecnologías como VPN, MPLS y redes definidas por software (SDN) facilitan este tipo de virtualización, proporcionando conectividad segura y flexible entre ubicaciones geográficamente dispersas (Cisco Networking Academy, 2023).

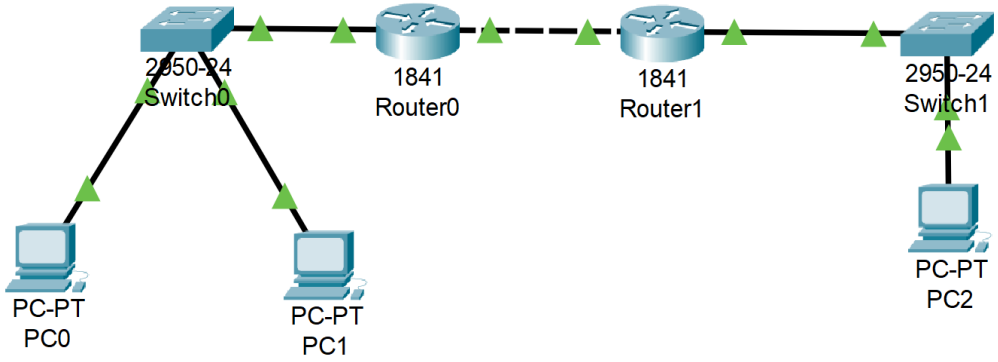
Desde una perspectiva funcional, la virtualización interna se centra principalmente en la eficiencia y el aislamiento dentro de la red local, mientras que la virtualización externa prioriza la conectividad, la seguridad y la escalabilidad en entornos distribuidos (Tanenbaum & Wetherall, 2021). Ambas modalidades comparten el objetivo de optimizar el uso de la infraestructura física, pero difieren en su alcance, complejidad y requisitos de gestión.

Ejercicios

Configurar y verificar la conectividad entre dos redes LAN diferentes interconectadas mediante dos routers, utilizando rutas estáticas con dirección IP de siguiente salto, empleando Cisco Packet Tracer.

Figura 7

Topología planteada en el ejercicio1



Configuraciones de las Computadoras:

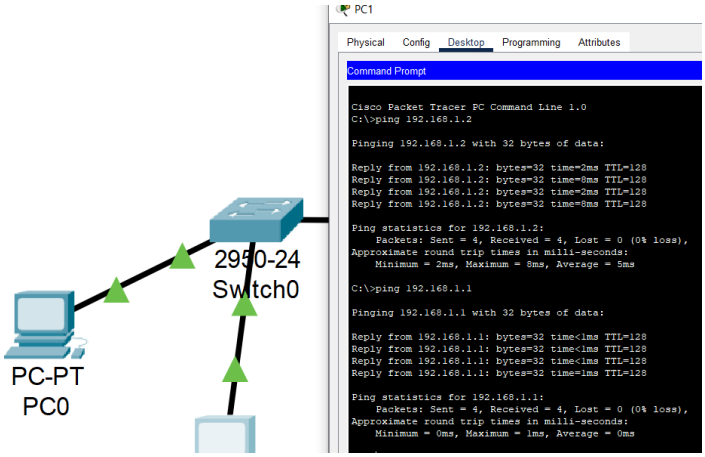
IP PC 1: 192.168.1.1 255.255.255.0 192.168.1.254

IP PC 2: 192.168.1.2 255.255.255.0 192.168.1.254

IP PC 3: 172.16.0.1 255.255.0.0 172.16.1.254

Figura 8

Verificación de conectividad atreves del comando ping IP



Configuración Router:

Router 1:

Fast Ethernet 0/0 192.168.1.254 255.255.255.0

Fast Ethernet 1/0 10.0.0.1 255.0.0.0

Router 2:

Fast Ethernet 0/0 172.16.1.254 255.255.0.0

Fast Ethernet 1/0 10.0.0.2 255.0.0.0

Configurar el Router 1

Router>enable

Router#configure

Configuring from terminal, memory, or network [terminal]?

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#interface fastEthernet 0/0

Router(config-if)#no shutdown

Router(config-if)#

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Router(config-if)#ip address 192.168.1.254 255.255.255.0

Router(config-if)#exit

Router(config)#exit

Configurar Router 2

Router>enable

Router#configure

Configuring from terminal, memory, or network [terminal]?

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#interface fastEthernet 0/0

Router(config-if)#no shutdown

Router(config-if)#

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Router(config-if)#ip address 172.16.1.254 255.255.0.0

Router(config-if)#exit

Router(config)#exit

Configurar los dos router a la dirección 10.0.0.0

Configurar el Router 1

Router#configure

Configuring from terminal, memory, or network [terminal]?

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#interface fastEthernet 0/1

Router(config-if)#no shutdown

Router(config-if)#

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

Router(config-if)#ip address 10.0.0.1 255.0.0.0

Router(config-if)#exit

Router(config)#exit

Configurar el Router 2

Router#Configure

Configuring from terminal, memory, or network [terminal]?

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#interface fastEthernet 0/1

Router(config-if)#no shutdown

Router(config-if)#

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Router(config-if)#ip ad

Router(config-if)#ip address 10.0.0.2 255.0.0.0

Router(config-if)#exit

Router(config-if)#exit

Router(config)#exit

Realizar de las tablas de ruteo para los equipos

Router 1

Router#configure

Configuring from terminal, memory, or network [terminal]?

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#ip route 172.16.0.0 255.255.0.0 10.0.0.2

Router(config)#exit

Router#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

Router#

Router 2

Router#configure

Configuring from terminal, memory, or network [terminal]?

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#ip route 192.168.1.0 255.255.255.0 10.0.0.1

Router(config)#exit

Router#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

Router#

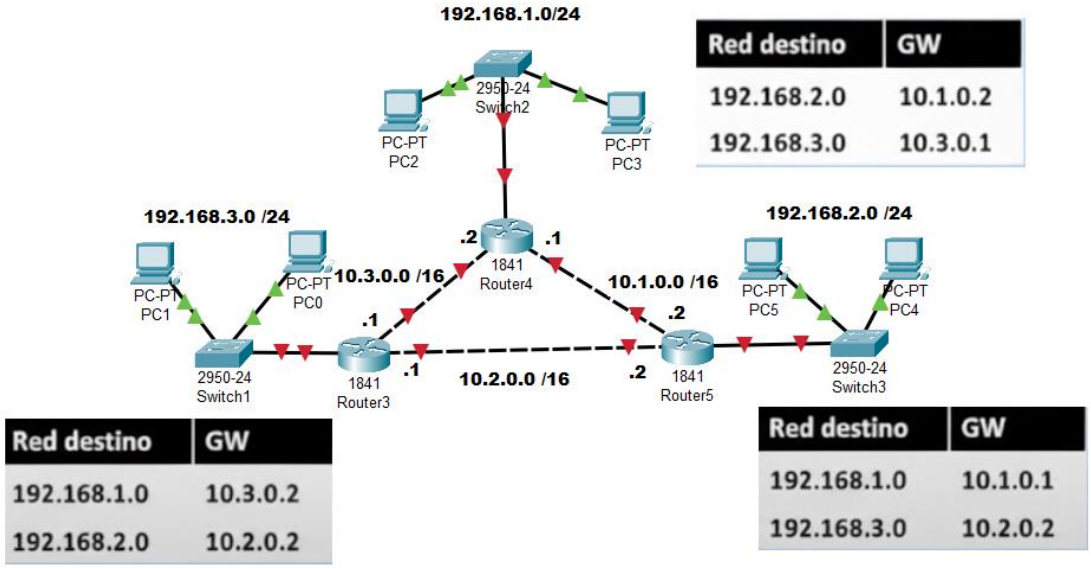
Ejercicios Planteados

a) Realizar el ejercicio anterior mediante RIP

b) Configurar y verificar la conectividad entre dos redes LAN diferentes interconectadas mediante dos routers, utilizando rutas estáticas con dirección IP de siguiente salto, empleando Cisco.

Figura 9

Topología planteada en el ejercicio



Red destino	GW
192.168.2.0	10.1.0.2
192.168.3.0	10.3.0.1

Red destino	GW
192.168.1.0	10.3.0.2
192.168.2.0	10.2.0.2

Red destino	GW
192.168.1.0	10.1.0.1
192.168.3.0	10.2.0.2

UNIDAD 4: SERVIDORES

Introducción general de la unidad

La presente unidad aborda el concepto de servidores como componentes fundamentales dentro de las redes de datos modernas. Un servidor es un dispositivo, físico o virtual, diseñado para ofrecer servicios, recursos o información a otros dispositivos denominados clientes, a través de una red local o de Internet. En el contexto del Internetworking, los servidores permiten la operación de servicios críticos como la resolución de nombres, la asignación automática de direcciones IP, el alojamiento de sitios web, el intercambio de archivos y la comunicación electrónica (Kurose & Ross, 2021; Stallings, 2019).

El estudio de esta unidad proporciona al estudiante los fundamentos teóricos y prácticos necesarios para comprender cómo se implementan y administran los servicios de red más comunes. Asimismo, se presentan ejercicios de ejemplo que permiten relacionar la teoría con escenarios reales de configuración y uso.

Introducción a servidores y requerimientos mínimos para la instalación de un sistema operativo

Un servidor se define como un sistema computacional diseñado para ofrecer servicios a múltiples clientes de manera simultánea, con altos niveles de disponibilidad y confiabilidad. A diferencia de los equipos de uso personal, los servidores están optimizados para operar de forma continua y gestionar cargas de trabajo de red (Forouzan, 2017).

Un servidor se caracteriza por su capacidad de operar de forma continua, atender múltiples solicitudes simultáneas y mantener altos niveles de disponibilidad y seguridad. A diferencia de un equipo de uso personal, el servidor está optimizado para el procesamiento de servicios de red.

Requerimientos mínimos de hardware: Para la instalación de un sistema operativo de servidor se deben considerar, como mínimo, los siguientes recursos:

Procesador (CPU): Arquitectura de 64 bits, preferiblemente multinúcleo.

Memoria RAM: Mínimo 4 GB, aunque se recomienda 8 GB o más según los servicios a implementar.

Almacenamiento: Discos duros o unidades SSD con suficiente capacidad y, de ser posible, configuraciones RAID.

Interfaz de red: Tarjeta de red Ethernet de al menos 1 Gbps.

Fuente de energía confiable: Uso de sistemas de alimentación ininterrumpida (UPS).

Desde el punto de vista del software, el sistema operativo debe ser estable, seguro y compatible con los servicios que se desean ofrecer.

Ejemplo resuelto: Selección de servidor para un instituto educativo

Contexto del caso: Un instituto educativo de nivel tecnológico cuenta con aproximadamente 250 estudiantes y 40 docentes. La institución requiere implementar un servidor interno que permita alojar su sitio web institucional (informativo) y brindar un servicio DNS para la resolución de nombres dentro de la red local. El servidor operará únicamente dentro del campus y no manejará bases de datos de gran tamaño ni aplicaciones críticas.

Análisis de requerimientos: Para cumplir con las necesidades planteadas, se identifican los siguientes requerimientos mínimos:

Procesador: CPU de 64 bits con al menos 2 núcleos, suficiente para atender solicitudes HTTP y consultas DNS simultáneas.

Memoria RAM: 8 GB, lo que garantiza estabilidad del sistema operativo y correcto funcionamiento de los servicios DNS y Web.

Almacenamiento: 500 GB en disco duro o SSD, considerando el sistema operativo, archivos del sitio web y posibles respaldos.

Interfaz de red: Tarjeta de red Ethernet de 1 Gbps para garantizar una adecuada velocidad de acceso.

Sistema de energía: Uso recomendado de una UPS para evitar interrupciones del servicio.

Elección del sistema operativo: Se selecciona Ubuntu Server LTS como sistema operativo de servidor debido a las siguientes razones:

Es un sistema operativo estable y ampliamente utilizado en entornos educativos y empresariales.

Ofrece soporte a largo plazo (LTS), lo que reduce la necesidad de actualizaciones frecuentes.

Incluye soporte nativo para servicios DNS (BIND) y servidores Web (Apache o Nginx).

No requiere licencias comerciales, lo que disminuye los costos de implementación.

Conclusión: La combinación de un servidor con recursos de hardware moderados y un sistema operativo Linux de servidor permite cubrir de forma eficiente las necesidades del instituto educativo, garantizando disponibilidad, seguridad y escalabilidad básica.

Estructuras de servidor y ejemplos de sistemas operativos de servidor

Los servidores pueden organizarse bajo distintas estructuras, dependiendo de su función y arquitectura:

Servidor dedicado: Dispositivo exclusivo para uno o varios servicios específicos.

Servidor virtualizado: Uso de máquinas virtuales sobre un mismo hardware físico.

Servidor en la nube: Infraestructura ofrecida por proveedores externos a través de Internet.

Sistemas operativos de servidor: Entre los sistemas operativos de servidor más utilizados se encuentran:

Windows Server: Entorno gráfico, integración con Active Directory y servicios empresariales.

Linux Server (Ubuntu Server, CentOS, Debian): Alta estabilidad, seguridad y uso extendido en servicios web y de red.

UNIX/BSD: Uso especializado en entornos de alto rendimiento.

Implementación de servicios de DNS, correo y Web

Los servicios de red permiten la comunicación eficiente entre dispositivos dentro de una infraestructura de internetworking. Entre los más relevantes se encuentran el servicio DNS, que traduce nombres de dominio en direcciones IP, y el servicio Web, que posibilita la distribución de información mediante el protocolo HTTP/HTTPS (Kurose & Ross, 2021; W3C, 2022).

Los servicios de red permiten que los dispositivos se comuniquen de manera eficiente. Entre los más importantes se encuentran el DNS, el correo electrónico y el servicio web.

DNS (Domain Name System): Traduce nombres de dominio en direcciones IP.

Correo electrónico: Permite el intercambio de mensajes entre usuarios.

Web: Facilita el acceso a información mediante navegadores.

Configurar el dispositivo como servidor DNS

Un servidor DNS almacena registros que asocian nombres de dominio con direcciones IP. Su correcta configuración es esencial para el funcionamiento de otros servicios.

Configurar el dispositivo como cliente DNS

El cliente DNS es cualquier equipo que consulta al servidor DNS para resolver nombres de dominio. La configuración consiste en asignar la dirección IP del servidor DNS.

Ejercicio resuelto: Configurar un servidor DNS

La actividad está diseñada para ser desarrollada en Cisco Packet Tracer, permitiendo al estudiante simular entornos reales de red, configurar servidores y clientes, y verificar el correcto funcionamiento de los servicios.

Objetivo: Configurar un servidor DNS y comprobar la resolución de nombres desde equipos clientes.

Topología utilizada: - 1 Servidor - 1 Switch - 2 PCs cliente

Configuración del servidor: - Dirección IP: 192.168.10.10 - Máscara: 255.255.255.0 - Puerta de enlace: 192.168.10.1

En Packet Tracer, se accede al servidor, pestaña Config → DNS y se activa el servicio DNS. Se crean los siguientes registros tipo A: - www.instituto.local → 192.168.10.10 - servidor.instituto.local → 192.168.10.10

Configuración de los clientes: Cada PC se configura con una dirección IP dentro del rango 192.168.10.0/24 y se asigna como servidor DNS la dirección 192.168.10.10.

Verificación: Desde la consola del cliente se comprueba la resolución del nombre de dominio configurado.

Resultado obtenido: Los clientes resuelven correctamente los nombres configurados en el servidor DNS.

Configurar el dispositivo como servidor Web

Un servidor web aloja páginas y aplicaciones accesibles mediante el protocolo HTTP o HTTPS. Ejemplos de software de servidor web son Apache, Nginx e IIS.

Configurar el dispositivo como cliente Web

El cliente web utiliza un navegador para acceder a los recursos publicados por un servidor web.

Ejercicio resuelto: Implementación de un servidor Web

La actividad está diseñada para ser desarrollada en Cisco Packet Tracer, permitiendo al estudiante simular entornos reales de red, configurar servidores y clientes, y verificar el correcto funcionamiento de los servicios.

Objetivo: Configurar un servidor Web y comprobar el acceso desde un navegador cliente.

Topología utilizada: - 1 Servidor - 1 Switch - 1 PC cliente

Configuración del servidor: - Dirección IP: 192.168.20.10 - Servicio HTTP: Activado

En Packet Tracer, se accede al servidor, pestaña Services → HTTP y se habilita el servicio. Se edita la página index.html con un mensaje institucional de bienvenida.

Configuración del cliente: El PC cliente se configura con una dirección IP válida dentro de la misma red.

Verificación: Desde el navegador web del cliente se ingresa la dirección http://192.168.20.10.

Resultado obtenido: El cliente visualiza correctamente la página alojada en el servidor.

Servicios DHCP y FTP

El servicio DHCP permite la asignación automática de direcciones IP, mientras que el servicio FTP facilita la transferencia de archivos entre clientes y servidores.

Configurar el dispositivo como servidor FTP

Un servidor FTP centraliza el almacenamiento y distribución de archivos.

Ejercicio resuelto: Configuración de servidor FTP

La actividad está diseñada para ser desarrollada en Cisco Packet Tracer, permitiendo al estudiante simular entornos reales de red, configurar servidores y clientes, y verificar el correcto funcionamiento de los servicios.

Objetivo: Permitir la transferencia de archivos entre un cliente y un servidor FTP.

Topología utilizada: - 1 Servidor - 1 Switch - 1 PC cliente

Configuración del servidor: - Dirección IP: 192.168.40.10 - Servicio FTP activado - Usuario creado: - Usuario: estudiante - Contraseña: redes123 - Permisos: lectura y escritura

Configuración del cliente: El cliente se configura con una dirección IP válida y accede al servidor mediante el símbolo del sistema utilizando comandos FTP.

Verificación: Se establece conexión, se autentica el usuario y se realiza la transferencia de un archivo de prueba.

Resultado obtenido: El cliente puede transferir archivos correctamente con autenticación válida.

Configurar el dispositivo como cliente FTP

El cliente FTP se conecta al servidor para subir o descargar archivos.

Configurar el dispositivo como servidor DHCP

El servidor DHCP administra un rango de direcciones IP y otros parámetros de red.

Ejercicio resuelto: Configuración de servidor DHCP

La actividad está diseñada para ser desarrollada en Cisco Packet Tracer, permitiendo al estudiante simular entornos reales de red, configurar servidores y clientes, y verificar el correcto funcionamiento de los servicios.

Objetivo: Implementar un servidor DHCP que asigne direcciones IP dinámicas.

Topología utilizada: - 1 Servidor - 1 Switch - 2 PCs cliente

Configuración del servidor: - IP del servidor: 192.168.30.10 - Servicio DHCP activado - Pool de direcciones configurado: - Red: 192.168.30.0 - Máscara: 255.255.255.0 - Gateway: 192.168.30.1 - DNS: 192.168.30.10 - Rango: 192.168.30.100 – 192.168.30.150

Configuración de los clientes: Los equipos cliente se configuran en modo DHCP.

Verificación: Al obtener automáticamente la configuración de red, los clientes reciben direcciones IP válidas.

Resultado obtenido: El servidor DHCP asigna correctamente los parámetros de red a los clientes.

Configurar el dispositivo como cliente DHCP

El cliente DHCP obtiene su configuración de red de manera automática.

Servidor de archivos

Un servidor de archivos es un sistema que centraliza el almacenamiento de información digital y permite que múltiples usuarios accedan a ella de manera controlada. Su propósito es garantizar la disponibilidad de documentos, la seguridad de los datos y la eficiencia en la colaboración. En entornos empresariales

y educativos, el servidor de archivos constituye un recurso esencial para la gestión de proyectos, la administración documental y la protección de la información institucional.

Cómo funciona un file server

El funcionamiento de un servidor de archivos se basa en tres componentes fundamentales:

Gestión de usuarios y permisos: El administrador define qué usuarios pueden acceder, modificar o eliminar archivos. Esto se realiza mediante políticas de seguridad y autenticación.

Ejemplo: un estudiante puede tener permisos de lectura sobre un repositorio académico, mientras que el docente posee permisos de escritura y edición.

Protocolos de acceso: Los protocolos más utilizados son:

- SMB (Server Message Block): empleado principalmente en sistemas Windows, permite compartir archivos e impresoras en una red local.

- NFS (Network File System): utilizado en sistemas Unix/Linux, facilita el acceso remoto a archivos como si fueran locales.

- Disponibilidad y redundancia: Los servidores de archivos suelen implementar sistemas de respaldo y redundancia (RAID, copias de seguridad automáticas) para garantizar la continuidad del servicio y evitar pérdida de información.

Ejercicio práctico: Configurar un servidor de archivos en Linux utilizando NFS, creando una carpeta compartida y asignando permisos diferenciados para dos usuarios

Dropbox

Dropbox es un servicio de almacenamiento en la nube que permite sincronizar archivos entre múltiples dispositivos. Sus principales características son:

Sincronización automática: cualquier archivo guardado en la carpeta de Dropbox se actualiza en todos los dispositivos vinculados.

Acceso multiplataforma: disponible en Windows, macOS, Linux, Android e iOS.

Colaboración: permite compartir carpetas y documentos con otros usuarios, asignando permisos de lectura o edición.

Versionado de archivos: conserva versiones anteriores de los documentos, lo que facilita la recuperación en caso de errores.

Ejercicio práctico: El estudiante debe instalar Dropbox en su computadora y dispositivo móvil, crear una carpeta compartida y verificar la sincronización automática de un archivo de texto.

OneDrive

OneDrive es el servicio de almacenamiento en la nube de Microsoft, integrado de manera nativa en sistemas Windows y en la suite de productividad Microsoft 365.

Integración con Windows: OneDrive aparece como una carpeta dentro del explorador de archivos, lo que facilita su uso.

Colaboración en tiempo real: permite la edición simultánea de documentos en Word, Excel y PowerPoint.

Seguridad avanzada: incluye cifrado de datos y autenticación multifactor.

Acceso empresarial: OneDrive for Business ofrece almacenamiento ampliado y administración centralizada para organizaciones.

Ejercicio práctico: El estudiante debe crear un documento en Word almacenado en OneDrive y compartirlo con un compañero, verificando la edición simultánea en tiempo real.

Box

Box es una plataforma de almacenamiento y colaboración orientada a entornos empresariales.

Gestión avanzada de usuarios: permite definir roles y permisos detallados para equipos de trabajo.

Integración con aplicaciones empresariales: se conecta con Salesforce, Google Workspace y Microsoft 365.

Seguridad corporativa: ofrece auditorías, cifrado y cumplimiento de normativas internacionales (ISO, GDPR).

Colaboración externa: facilita compartir archivos con clientes y proveedores de manera segura.

Ejercicio práctico: El estudiante debe crear una cuenta en Box, subir un archivo y compartirlo con un enlace protegido por contraseña, verificando el acceso controlado.

Referencias Bibliográficas

Cerf, V. G., & Kahn, R. E. (1974). A Protocol for Packet Network Intercommunication. *IEEE Transactions on Communications, 22*(5), 637-648.

Cisco Networking Academy. (2023). *Routing and Switching Essentials.* Cisco Systems.

Comer, D. E. (2018). *Internetworking with TCP/IP: Principles, Protocols, and Architecture* (6th ed.). Boston: Pearson.

Forouzan, B. (2017). *Data Communications and Networking* (5 ed.). McGraw-Hill Education.

Fuller, V., & Li, T. (2006). *Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan.* IETF. Obtenido de https://tools.ietf.org/html/rfc4632

IEEE. (2004). *IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges.* IEEE.

IEEE. (2018). *IEEE Standard for Local and Metropolitan Area Networks—Bridges and Bridged Networks.* IEEE.

Jacobson, V. (1988). Congestion Avoidance and Control. *ACM SIGCOMM Computer Communication Review, 18*(4), 314-329.

Kurose, J., & Ross, K. (2021). *Computer networking: A top-down approach* (8th ed ed.). Pearson.

Moy, J. (1998). *OSPF Version 2.* IETF. Obtenido de https://tools.ietf.org/html/rfc2328

Perlman, R. (1992). *Interconnections: Bridges, Routers, Switches, and Internetworking Protocols.* Addison-Wesley.

Postel, J. (1981). *Internet Protocol.* IETF. Obtenido de https://tools.ietf.org/html/rfc791

Rekhter, Y., Li, T., & Hares, S. (2006). *A Border Gateway Protocol 4 (BGP-4).* IETF. Obtenido de https://tools.ietf.org/html/rfc4271

Tanenbaum, A., & Wetherall, D. (2021). *Computer networks* (6 ed.). Pearson.

INSTITUTO SUPERIOR UNIVERSITARIO sucre

ISBN: 978-9942-590-18-3

SUCREInstitutooficial @SUCREInstituto @SUCREInstituto