Guía Académica
Fundamentos de Redes de Datos

Elaborado por:

Santiago Aguilar Cárdenas

Facultad de Ingeniería Electrónica

Universidad Santo Tomás

Seccional Tunja

Información Académica

Guía Académica

Fundamentos de Redes de Datos

Elaborado por:

Santiago Aguilar Cárdenas

Director del Trabajo de Grado:
Ph.D. William Fabián Chaparro Becerra

Codirectores del Trabajo de Grado:
M.Sc. Angélica María Salazar Madrigal
M.Sc. Cristian David Parra Camacho

Facultad de Ingeniería Electrónica
Universidad Santo Tomás
Seccional Tunja

Información del Documento

Asignatura:	Transmisión de Datos
Nivel:	Pregrado – Ingeniería Electrónica
Duración estimada:	Estudio autónomo
Modalidad:	Estudio teórico previo a prácticas de laboratorio

PREÁMBULO

Resumen

Esta guía académica reúne los fundamentos esenciales de redes de datos que el estudiante requiere para abordar con criterio técnico las prácticas posteriores (simulación, configuración y validación) en entornos Cisco. Se desarrollan conceptos de arquitectura de redes, Ethernet, sistemas de numeración, direccionamiento IP, subnetting/VLSM y enrutamiento, articulándolos con el diseño de topologías y la toma de decisiones de configuración.

Presentación

El presente documento ha sido diseñado para proporcionar los fundamentos teóricos de redes de datos necesarios para comprender e implementar configuraciones en dispositivos Cisco y, posteriormente, aplicar controles de ciberseguridad en escenarios reales y simulados.

De acuerdo con el **Syllabus del espacio académico Transmisión de Datos**, el curso se desarrolla por **unidades temáticas** que integran: fundamentos de redes y modelos de referencia (OSI/TCP), direccionamiento y subdivisión de redes (CIDR/VLSM), principios de enrutamiento y principios de conmutación.

Con el fin de favorecer una progresión **de lo conceptual a lo aplicado**, esta guía académica desagrega el Syllabus en **seis unidades** más específicas: se separa Ethernet de los modelos de referencia, se incluye una unidad de fundamentos matemáticos (sistemas de numeración) y se divide el bloque de direccionamiento en dos (IP y Subnetting/VLSM). Esta decisión facilita que cada tema se construya sobre el anterior y que el estudiante cuente con prerrequisitos claros para las prácticas de laboratorio y ejercicios evaluativos.

Estructura de la Guía (alineación con el Syllabus)

El **Syllabus del espacio académico Transmisión de Datos** organiza el curso en unidades temáticas amplias. Para facilitar el estudio autónomo, esta guía académica desarrolla esos mismos contenidos en **seis unidades** más específicas, manteniendo la secuencia y los prerrequisitos definidos en el Syllabus.

Unidad en la guía	Unidad del Syllabus	Justificación
Unidad 1	Unidad Temática 1	Establece el marco conceptual (tipos de red, topologías y modelos OSI/TCP) para interpretar cualquier tecnología posterior.
Unidad 2	Unidad Temática 1	Profundiza en la capa de enlace (Ethernet, MAC, conmutación básica y segmentación).
Unidad 3	Soporte a Unidad Temática 2	Incluye los fundamentos matemáticos requeridos para direccionamiento: binario/hexadecimal y operaciones lógicas usadas en máscaras y prefijos.
Unidad 4	Unidad Temática 2	Aborda direccionamiento IPv4/IPv6, CIDR y direcciones especiales: prerrequisito directo de subnetting y configuración básica.
Unidad 5	Unidad Temática 2	Desarrolla, de forma aplicada, los métodos de subdivisión de redes (Subnetting y VLSM) para diseños coherentes y eficientes.
Unidad 6	Unidad Temática 3	Integra enrutamiento (lectura de tablas, rutas estáticas) y diseño de topologías, conectando la teoría con el trabajo en simuladores/laboratorio.

Unidades de la guía:

Unidad 1: **Clasificación y Arquitectura de Redes** – Tipos de redes, topologías, modelos OSI/TCP/IP y protocolos base (corresponde al bloque conceptual del Syllabus).

Unidad 2: **Protocolo Ethernet y Capa de Enlace** – Tramas, direcciones MAC, conmutación básica y segmentación (introducción a conmutación/VLAN, articulada con seguridad).

Unidad 3: **Sistemas de Numeración** – Binario/hexadecimal y operación lógica AND, indispensables para comprender prefijos, máscaras y tablas de direccionamiento.

Unidad 4: **Direccionamiento IP** – IPv4/IPv6, CIDR, direcciones especiales y lectura de notación de red.

Unidad 5: **Subnetting y VLSM** – Diseño de subredes, cálculo de rangos y optimización del direccionamiento para escenarios con diferentes requerimientos.

Unidad 6: **Enrutamiento IP** – Tablas de enrutamiento y rutas estáticas.

Competencias

Competencias:

- Reconocer la historia, evolución, estándares y elementos característicos de una red de datos, tanto cableada como inalámbrica.
- Reconocer las características y principios de los riesgos y amenazas cibernéticas, así como las estrategias de protección dentro de sistemas de información y redes de comunicaciones
- Comprender y aplicar los principios de protección y control de accesos, incluyendo autenticación, autorización, cifrado y segmentación de información en sistemas y redes.

Objetivos

Objetivos de aprendizaje de la guía:

1. **Comprender** los fundamentos de redes (topologías, modelos OSI/TCP y protocolos) como base para el análisis técnico.
2. **Aplicar** direccionamiento IP (IPv4/IPv6), CIDR y VLSM para proponer esquemas de red coherentes.
3. **Interpretar** el funcionamiento de Ethernet y la conmutación básica (MAC, dominios, segmentación) como fundamento de LAN seguras.
4. **Analizar** principios de enrutamiento y diseñar topologías simples que puedan configurarse y verificarse en laboratorio/simulador.

Resultados de Aprendizaje

Resultados de aprendizaje esperados (alineados al Syllabus):

- Conoce la historia, evolución, estándares y elementos característicos de una red de datos y los relaciona con el modelo OSI/TCP.
- Diseña soluciones de interworking a pequeña/mediana escala: propone direccionamiento, CIDR/VLSM y justifica decisiones de diseño.
- Identifica las características y principios de enrutamiento: interpreta tablas y selecciona rutas (con énfasis en rutas estáticas como base).
- Identifica las características y principios de conmutación: explica aprendizaje MAC, reenvío y segmentación lógica (VLAN) y su relación con seguridad.

Índice

1 Clasificación y Arquitectura de Redes

Competencias

- Explicar topologías de red y su relación con disponibilidad, escalabilidad y seguridad.
- Explicar modelos OSI y TCP/IP, y mapear capas, funciones y protocolos comunes.
- Relacionar la arquitectura de red con requerimientos de ciberseguridad (segmentación, control de acceso y protección del perímetro).

Objetivos

- Describir hitos básicos de la evolución de las redes de datos y el rol de estándares (p. ej., IEEE 802).
- Identificar topologías de red (estrella, malla, anillo, híbridas) y justificar su uso según el contexto.
- Identificar y describir los tipos de redes según su alcance geográfico (PAN, LAN, MAN, WAN).
- Explicar la función de cada capa en los modelos OSI y TCP/IP y su equivalencia.
- Identificar protocolos específicos en cada capa del modelo TCP/IP y relacionarlos con escenarios de uso.

Resultados de Aprendizaje

- Explica, con ejemplos, la función de cada capa OSI/TCP/IP y la relación con protocolos comunes.
- Reconoce topologías de red y selecciona la más adecuada para un escenario, justificando criterios técnicos.
- Clasifica un escenario de red por alcance (PAN/LAN/MAN/WAN) y argumenta implicaciones de seguridad.

1.1 Historia y evolución de las redes de datos

La transmisión de datos ha evolucionado desde enlaces dedicados y redes aisladas hacia infraestructuras interoperables basadas en estándares. Hitos como ARPANET, la estandarización de Ethernet y la adopción de TCP/IP como suite dominante permitieron la expansión de Internet y la integración de servicios en redes empresariales (Tanenbaum y Wetherall, 2011; Comer, 2018). En la práctica, la estandarización (por ejemplo, la familia IEEE 802 para redes LAN/MAN) facilita que equipos de distintos fabricantes puedan comunicarse bajo reglas comunes.

Hitos (visión general)

- **1970s:** consolidación de redes de paquetes y aparición de Ethernet como tecnología LAN.
- **1980s:** adopción de **TCP/IP** y crecimiento de interconexión entre redes.
- **1990s–hoy:** masificación de Internet, estandarización y aumento de velocidades (Fast/Gigabit/10G/40G/100G).

1.2 Topologías de Red

Una **topología** describe cómo se interconectan los nodos y enlaces (físicamente o de forma lógica). La elección de topología impacta disponibilidad, costo, facilidad de mantenimiento y superficie de ataque.

Topología	Descripción	Notas (diseño/seguridad)
Estrella	Nodos conectados a un dispositivo central (switch/AP).	Facilita gestión y segmentación; el nodo central es crítico (punto único si no hay redundancia).
Malla	Múltiples enlaces entre nodos. Puede ser parcial o completa.	Alta tolerancia a fallas; mayor costo. Reduce impacto de caída de enlaces.
Anillo	Nodos conectados en forma circular.	Requiere mecanismos para evitar interrupciones; hoy es menos común en LAN modernas.
Bus	Todos comparten un mismo medio.	Poco escalable; mayor exposición a colisiones/interferencias (referencia histórica).
Híbrida	Combinación de topologías.	La más común en redes reales: mezcla de estrella/malla jerárquica.

Cuadro 1: Topologías básicas y consideraciones

1.3 Arquitectura de la Red

La arquitectura de red se refiere al conjunto de tecnologías, estándares, reglas y protocolos que soportan la infraestructura, los servicios y las aplicaciones que trasladan datos a través de la red (Tanenbaum y Wetherall, 2011). Una red bien diseñada debe cumplir con cuatro características fundamentales:

Características Básicas de una Red Confiable

Tolerancia a fallas:

Capacidad de la red para continuar operando sin interrupción cuando uno o más de sus componentes fallan. Se implementa mediante redundancia: múltiples enlaces y rutas alternativas para llegar a cada destino, de modo que, si una ruta falla, el tráfico se redirige automáticamente por otra (Comer, 2018).

Escalabilidad:

Permite expandir la red para admitir nuevos usuarios, dispositivos y aplicaciones sin degradar el rendimiento de los servicios existentes (Tanenbaum y Wetherall, 2011).

Calidad de Servicio (QoS):

Mecanismo principal para administrar congestión y garantizar el envío confiable de datos. El enfoque QoS consiste en priorizar el tráfico urgente o sensible a la latencia (como voz y video) sobre el tráfico menos crítico (Cisco Systems, 2020b).

Seguridad:

Protección tanto de la infraestructura física de la red como de la información que circula por ella. Los tres objetivos principales de la seguridad son: confidencialidad, integridad y disponibilidad, definidos por estándares internacionales de seguridad de la información (*ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems* 2013).

1.4 Clasificación de Redes por Alcance Geográfico

Las redes se clasifican según la extensión geográfica que cubren. Esta clasificación es fundamental para diseñar políticas de seguridad apropiadas, ya que cada tipo de red presenta diferentes niveles de confianza y requiere medidas de protección específicas (Tanenbaum y Wetherall, 2011).

Tipo	Alcance	Descripción	Tecnologías
PAN	$<$ 10 metros	Red de área personal. Interconecta dispositivos personales en un radio muy pequeño. Ejemplo: smartphone con auriculares inalámbricos.	Bluetooth, USB, NFC
LAN	Edificio / campus	Red de área local. Interconecta dispositivos en espacios geográficos limitados como oficinas, edificios o campus universitarios. Es la red más común en entornos empresariales y educativos.	Ethernet, Wi-Fi 802.11
MAN	Ciudad / región	Red de área metropolitana. Interconecta múltiples redes LAN dentro de una ciudad o región. Ejemplo: sucursales bancarias distribuidas en una ciudad.	Fibra óptica, WiMAX
WAN	País / continente	Red de área amplia. Permite la comunicación entre ubicaciones geográficamente distantes mediante enlaces de telecomunicaciones. Internet es la WAN más grande del mundo.	MPLS, Frame Relay, Internet

Cuadro 2: Clasificación de redes por alcance geográfico

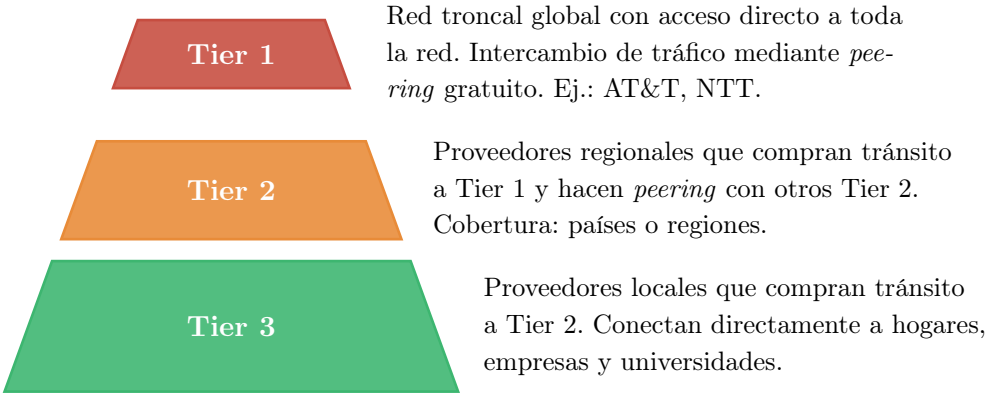
Relevancia para Ciberseguridad

La distinción entre tipos de red es crítica para la ciberseguridad:

- **Redes LAN** se consideran "confiables"; sin embargo, requieren seguridad interna mediante VLANs, control de acceso físico y segmentación.
- **Redes WAN** se consideran "no confiables"; requieren cifrado de datos mediante VPNs e IPsec.
- El **perímetro** (punto de intersección LAN–WAN) es la zona crítica donde se implementan firewalls, sistemas IDS/IPS y control de acceso perimetral.

1.5 Jerarquía de Proveedores de Internet (ISP Tiers)

Los proveedores de servicios de Internet se organizan jerárquicamente en tres niveles o *tiers*, según su alcance y cobertura:



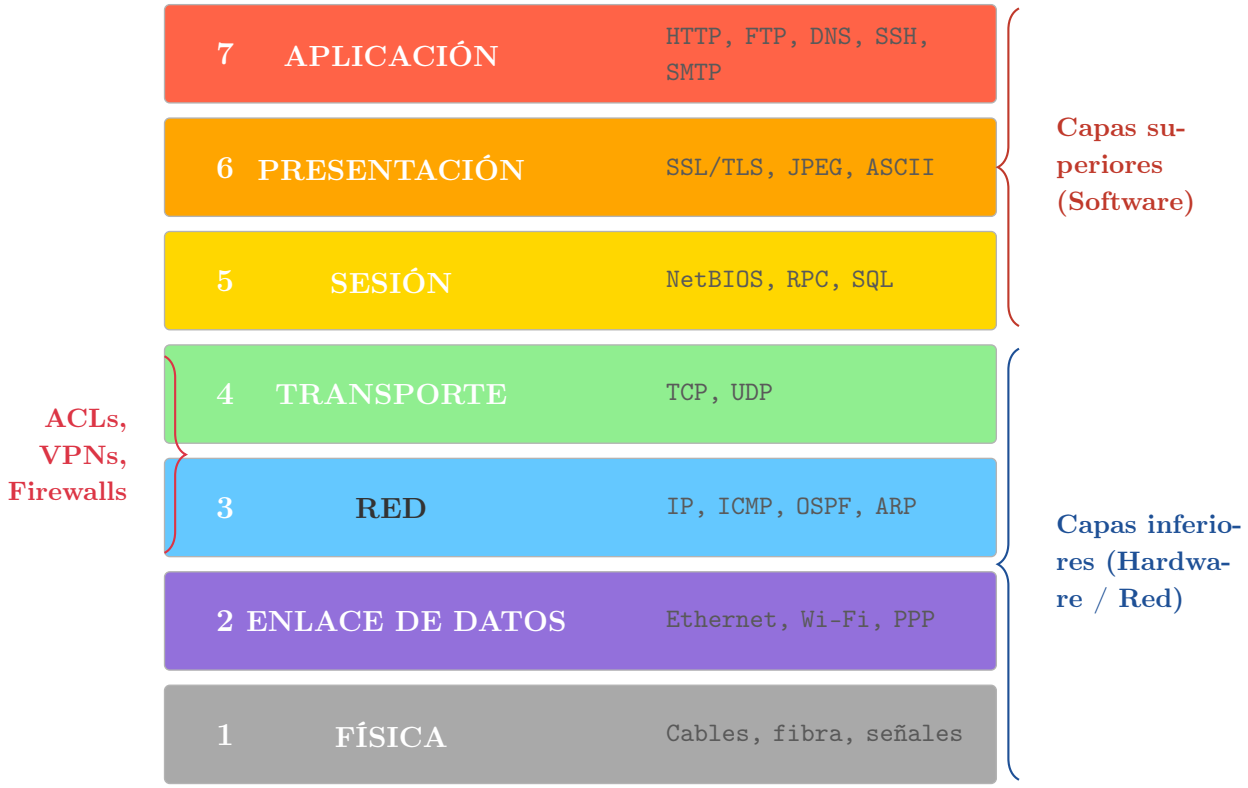
1.6 Modelos de Referencia

Los modelos de referencia organizan la comunicación en capas jerárquicas. Cada capa proporciona servicios a la capa superior y utiliza los de la capa inferior. Los dos modelos fundamentales son:

- **OSI (Open Systems Interconnection):** Modelo conceptual de 7 capas, útil para entender cómo interactúan protocolos y tecnologías.
- **TCP/IP:** Modelo práctico implementado en Internet y redes reales, con 4 capas.

1.6.1 Modelo OSI – Open Systems Interconnection

El modelo OSI divide las funciones de red en **7 capas**, cada una con responsabilidades, protocolos y PDU específicos:



Descripción resumida de cada capa:

Capa 7 – Aplicación:
Proporciona servicios directamente a las aplicaciones: navegación web (HTTP/HTTPS), transferencia de archivos (FTP), correo electrónico (SMTP), resolución de nombres (DNS) y acceso remoto (SSH, Telnet).

Capa 6 – Presentación:
Se encarga de traducir, cifrar y comprimir datos. Protocolos: SSL/TLS; formatos de datos: JPEG, GIF, ASCII.

Capa 5 – Sesión:
Administra sesiones entre aplicaciones, controlando diálogos y puntos de verificación para recuperación ante fallos.

Capa 4 – Transporte:
Comunicación de extremo a extremo. Protocolos principales: **TCP** (fiable, orientado a conexión) y **UDP** (rápido, no fiable). PDU: *segmento*.

Capa 3 – Red:
Maneja direccionamiento lógico (IP) y enrutamiento de paquetes entre redes. Protocolos: IP, ICMP, ARP, OSPF, EIGRP, BGP. Aquí operan las ACLs.

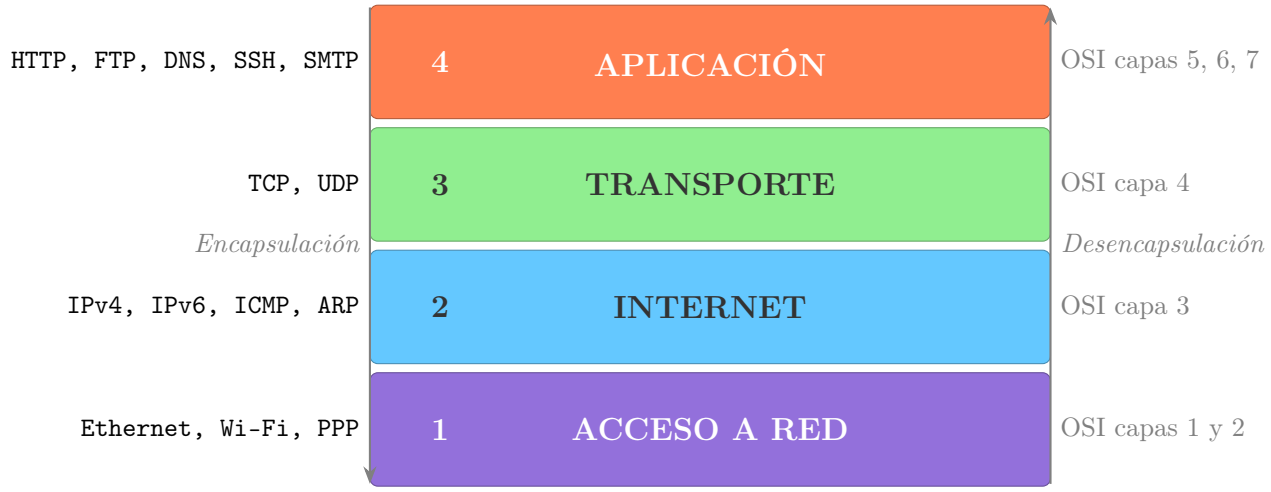
Capa 2 – Enlace de Datos:
Acceso al medio físico y direccionamiento MAC. Subcapas: LLC (IEEE 802.2), MAC (IEEE 802.3/802.11). Dispositivos: switches.

Capa 1 – Física:

Transmisión de bits a través del medio físico. Define cables, conectores y señales. PDU: *bits*.

1.6.2 Modelo TCP/IP – Modelo Práctico de Internet

El modelo TCP/IP es el modelo utilizado en la implementación real de Internet y redes empresariales. Condensa las funciones del modelo OSI en **4 capas**:



Resumen de capas y equivalencias con OSI:

Comparación OSI vs TCP/IP

Modelo OSI	Modelo TCP/IP	Protocolos principales
Capas 5–7	Aplicación	HTTP, HTTPS, FTP, SMTP, DNS, SSH, Telnet, DHCP
Capa 4	Transporte	TCP (fiable, orientado a conexión), UDP (rápido, no fiable)
Capa 3	Internet	IPv4, IPv6, ICMP, ARP, OSPF, EIGRP, BGP
Capas 1–2	Acceso a Red	Ethernet (802.3), Wi-Fi (802.11), PPP, HDLC

Preguntas de repaso

1. **Explique con sus propias palabras la función de cada una de las cuatro características básicas de una red confiable** (Tolerancia a fallos, Escalabilidad, Calidad de Servicio y Seguridad).
2. **¿Por qué es importante para un ingeniero en seguridad conocer la diferencia entre una red LAN y una WAN?** Mencione dos implicaciones de seguridad para cada tipo de red.
3. **¿Qué significa que un ISP sea Tier 1?** ¿Cómo se diferencia de un ISP Tier 2 en términos

de conectividad y acuerdos de *peering*?

Caso de Estudio: Diseñando la Red de una Pequeña Empresa

Una pequeña empresa de diseño gráfico, **Creativos S.A.**, está mudándose a una nueva oficina. Necesitan una red para 15 empleados que sea confiable, segura y que permita el acceso a Internet. La oficina tiene una sala de servidores pequeña y un punto de reunión con proyectores que se conectan por cable.

Preguntas:

1. **Topología:** ¿Qué topología de red (estrella, malla, bus) recomendarías para la oficina de Creativos S.A.? Justifica tu respuesta basándote en la facilidad de gestión, la tolerancia a fallos y el costo.

2. **Modelo OSI:** Un empleado envía un archivo a imprimir en una impresora de red. Explica brevemente el viaje de esos datos a través de las capas del modelo OSI, desde la capa de Aplicación hasta la capa Física (y viceversa en la impresora).

3. **Alcance y Seguridad:** ¿Cómo clasificarías la red de la oficina (PAN, LAN, MAN, WAN)? Si necesitan conectar esta oficina con una nueva sucursal en otra ciudad, ¿qué tipo de red (WAN, LAN, MAN) se requeriría y qué consideraciones de seguridad (cifrado, VPN) serían prioritarias?

Referencias de la unidad

Cisco Systems (2020a). *Introduction to Networking Technologies*. Inf. téc. Cisco Systems. URL: https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-networking.html.

— (2020b). *Quality of Service Solutions Overview*. Inf. téc. Cisco Systems. URL: https://www.cisco.com/c/en/us/products/quality-of-service-qos/index.html.

Comer, Douglas E. (2018). *Internetworking with TCP/IP Volume 1: Principles, Protocols, and Architecture*. 6th. Boston, MA, USA: Pearson.

ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems (2013). ISO/IEC.

Leinwand, Allan y Bruce Pinsky (2001). *Configuración de Routers Cisco*. Madrid: Cisco Press.

Odom, Wendell (2012). *CISCO CCENT/CCNA ICND1, ICND2 Official Cert Guide, Book 2*. Indianapolis: Cisco Press.

Olifer, Natalia y Víctor Olifer (2009). *Redes de Computadoras: Principios, tecnología y protocolos para el diseño de redes*. McGraw-Hill/Interamericana.

Stallings, William (2000). *Comunicaciones y Redes de Computadores*. Pearson Educación.

Tanenbaum, Andrew S. y David J. Wetherall (2011). *Computer Networks*. 5th. Upper Saddle River, NJ, USA: Prentice Hall.

Vacca, John R., ed. (2013). *Network and System Security*. Waltham, MA: Elsevier.

2 Protocolo Ethernet y Capa de Enlace

Competencias

- **Comprender:** Interpretar tramas Ethernet y sus campos principales.
- **Comprender / Hacer:** Explicar el direccionamiento MAC y la operación básica de switches (aprendizaje y reenvío).
- **Hacer:** Analizar dominios de colisión/broadcast y su impacto en segmentación (VLAN) y seguridad.

Objetivos

- Explicar la estructura de la trama Ethernet y la función de sus campos.
- Comprender el direccionamiento MAC y el proceso de conmutación en switches.
- Diferenciar dominios de colisión y broadcast, y su relación con VLANs.

Resultados de Aprendizaje

- **Comprender:** Reconoce campos de una trama Ethernet (MAC origen/destino, tipo/longitud, FCS).
- **Comprender:** Explica cómo un switch aprende direcciones MAC y reenvía tramas.
- **Hacer:** Argumenta por qué la segmentación (VLAN) reduce broadcast y apoya controles de seguridad.

2.1 Fundamentos de Ethernet

Ethernet es la tecnología más utilizada en la capa de enlace de datos para redes LAN. Definida por los estándares **IEEE 802.2** (subcapa LLC) y **IEEE 802.3** (subcapa MAC y capa física), Ethernet facilita el diseño de dispositivos, promueve la interoperabilidad y fomenta la competencia entre fabricantes.

Evolución de Ethernet

Desde su creación en **1973**, Ethernet ha experimentado un desarrollo constante. Cada versión tiene un estándar y una nomenclatura específica. Por ejemplo, `100Base-T` indica:

- **100**: Velocidad en Mbps
- **Base**: Transmisión en banda base (*baseband*)
- **T**: Tipo de cable (T = par trenzado, F = fibra óptica)

Estándar	Velocidad	Medio	Distancia máx.
IEEE 802.3u (Fast Ethernet)	100 Mbps	Cobre / Fibra	100 m (cobre)
IEEE 802.3z (Gigabit Ethernet)	1 Gbps	Fibra óptica	550 m (multimodo)
IEEE 802.3ab (Gigabit Ethernet)	1 Gbps	Cobre (Cat 5e/6)	100 m
IEEE 802.3an (10G Ethernet)	10 Gbps	Cobre (Cat 6a/7)	100 m
IEEE 802.3ba	40/100 Gbps	Fibra óptica	Variable

2.2 Subcapas de Enlace de Datos

Los protocolos IEEE 802 (LAN/MAN) utilizan dos subcapas independientes:

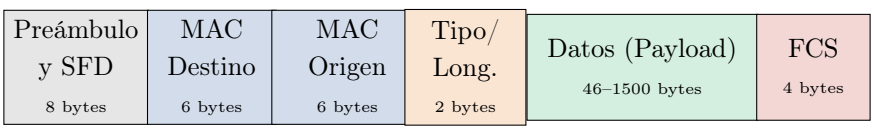
- **Subcapa LLC** (IEEE 802.2): Conecta el software de red de las capas superiores con el hardware de las capas inferiores. Permite que múltiples protocolos de capa 3, como IPv4 e IPv6, compartan la misma red y medios físicos.
- **Subcapa MAC** (IEEE 802.3, 802.11, 802.15): Implementada en hardware, se encarga de encapsular datos en tramas, gestionar el direccionamiento físico mediante direcciones MAC y controlar el acceso al medio.

2.3 Dirección MAC (Media Access Control)

La dirección MAC es un identificador único de **48 bits** (6 bytes) asignado a cada interfaz de red. Se representa en **notación hexadecimal**, normalmente en el formato `XX:XX:XX:XX:XX:XX`, donde cada par de dígitos corresponde a un byte.

2.4 Campos de la Trama Ethernet

El tamaño mínimo de una trama Ethernet es de **64 bytes** y el máximo esperado es de **1518 bytes** (puede ser mayor con etiquetado VLAN: 1522 bytes).



Preámbulo y SFD:
Sincronizan los dispositivos emisores y receptores. Estos primeros bytes indican al receptor que se prepare para recibir una nueva trama.

MAC Destino:
Se compara con la dirección MAC del dispositivo receptor; si coinciden, la trama es aceptada.

MAC Origen:
Identifica la interfaz o tarjeta de red (NIC) de origen de la trama.

Tipo/Longitud:
Indica el protocolo de capa superior encapsulado. Valores comunes: `0x0800` para IPv4, `0x86DD` para IPv6, `0x0806` para ARP.

Datos (Payload):
Contiene los datos encapsulados de la capa superior, generalmente un paquete IP.

FCS:
Secuencia de Verificación de Trama. Se utiliza para detectar errores de transmisión mediante un cálculo CRC.

Preguntas de repaso

1. **¿Qué significan los números y letras en el estándar 1000Base-T?** Desglose cada parte.
2. **¿Cuál es la diferencia entre las subcapas LLC y MAC de la capa de enlace de datos?**
3. **Una dirección MAC es A4:B1:C2:34:56:78. ¿Cuál es el OUI (Identificador Único del Organismo) en esta dirección?**
4. **Enumere los campos principales de una trama Ethernet y explique brevemente la función de cada uno.**

Referencias de la unidad

Referencias de la unidad

Cisco Systems (2020). *Ethernet Frame and Switching Concepts*. Documentación / material de referencia Cisco.

IEEE (2022). *IEEE 802.3 Ethernet*. Estándar IEEE 802.3.

Kurose, James F. y Keith W. Ross (2017). *Computer Networking: A Top-Down Approach*. 7th. Pearson.

3 Sistemas de Numeración

Competencias

- Convertir números entre decimal, binario y hexadecimal.
- Interpretar notación de direcciones (hex para MAC, binario para máscaras) y aplicar operación AND.

Objetivos

- Realizar conversiones entre sistemas decimal, binario y hexadecimal.
- Relacionar los sistemas de numeración con direcciones IP y MAC.

Resultados de Aprendizaje

- Convierte valores y prefijos (CIDR) a binario y viceversa.
- Interpreta direcciones MAC en formato hexadecimal y su representación binaria.

3.1 Sistema Binario (Base 2)

Los dispositivos de red operan internamente en binario. Cada posición en un número binario de 8 bits (un **octeto**) representa una potencia de 2:

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	**64**	**32**	**16**	**8**	**4**	**2**	**1**

Ejemplo : Conversión Decimal → Binario

Ejemplo 1: Convertir 192 **a binario**

1. Identificar las potencias de 2 menores o iguales a 192: $128, 64, 32, 16, 8, 4, 2, 1$.
2. Comparar y restar paso a paso:

- $192 \geq 128$? Sí → bit = **1**, resta $192 - 128 = 64$
- $64 \geq 64$? Sí → bit = **1**, resta $64 - 64 = 0$
- $0 \geq 32$? No → bit = **0**
- $0 \geq 16$? No → bit = **0**
- $0 \geq 8$? No → bit = **0**
- $0 \geq 4$? No → bit = **0**
- $0 \geq 2$? No → bit = **0**
- $0 \geq 1$? No → bit = **0**

$$192_{10} = \mathbf{11000000}_2$$

Ejemplo 2: Convertir 170 **a binario**
1. Potencias de 2: $128, 64, 32, 16, 8, 4, 2, 1$.
2. Comparar y restar:

- $170 \geq 128$? Sí $\rightarrow$ bit $=$ **1**, resta $170 - 128 = 42$
- $42 \geq 64$? No $\rightarrow$ bit $=$ **0**
- $42 \geq 32$? Sí $\rightarrow$ bit $=$ **1**, resta $42 - 32 = 10$
- $10 \geq 16$? No $\rightarrow$ bit $=$ **0**
- $10 \geq 8$? Sí $\rightarrow$ bit $=$ **1**, resta $10 - 8 = 2$
- $2 \geq 4$? No $\rightarrow$ bit $=$ **0**
- $2 \geq 2$? Sí $\rightarrow$ bit $=$ **1**, resta $2 - 2 = 0$
- $0 \geq 1$? No $\rightarrow$ bit $=$ **0**

$$170_{10} = \mathbf{10101010}_2$$

Ejemplo : Conversión Binario → Decimal

Ejemplo 1: Convertir 10101000_2 a decimal paso a paso:

- Escribimos cada bit con su valor posicional (potencia de 2):

$$10101000_2 = 1 \cdot 128 + 0 \cdot 64 + 1 \cdot 32 + 0 \cdot 16 + 1 \cdot 8 + 0 \cdot 4 + 0 \cdot 2 + 0 \cdot 1$$

- Multiplicamos cada bit por su valor:

$$= 128 + 0 + 32 + 0 + 8 + 0 + 0 + 0$$

- Sumamos los resultados:

$$128 + 32 + 8 = 168$$

Por lo tanto:

$$10101000_2 = \mathbf{168}_{10}$$

Ejemplo 2: Convertir 11001101_2 a decimal paso a paso:

- Valor posicional de cada bit:

$$11001101_2 = 1 \cdot 128 + 1 \cdot 64 + 0 \cdot 32 + 0 \cdot 16 + 1 \cdot 8 + 1 \cdot 4 + 0 \cdot 2 + 1 \cdot 1$$

- Multiplicamos cada bit por su valor:

$$= 128 + 64 + 0 + 0 + 8 + 4 + 0 + 1$$

- Sumamos los resultados:

$$128 + 64 + 8 + 4 + 1 = 205$$

Por lo tanto:

$$11001101_2 = \mathbf{205}_{10}$$

3.2 Sistema Hexadecimal (Base 16)

Cada dígito hexadecimal representa exactamente 4 bits (1 nibble). Dos dígitos hexadecimales = 1 byte.

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

Ejemplo : Binario → Hexadecimal

Ejemplo 1: Convertir 11000000_2 a hexadecimal:

- Se divide el número binario en *nibbles* de 4 bits, de izquierda a derecha:

$$11000000_2 = \underbrace{1100}_{C}\ \underbrace{0000}_{0}$$

- Cada nibble se convierte a su valor hexadecimal correspondiente:

$$1100_2 = C_{16}, \quad 0000_2 = 0_{16}$$

Resultado:

$$11000000_2 = \mathbf{C0}_{16} \quad \text{(equivalente a 192 en decimal)}$$

Ejemplo 2: Convertir 10101010_2 a hexadecimal:

- Dividimos en nibbles:

$$10101010_2 = \underbrace{1010}_{A}\ \underbrace{1010}_{A}$$

- Convertimos cada nibble a hexadecimal:

$$1010_2 = A_{16}, \quad 1010_2 = A_{16}$$

Resultado:

$$10101010_2 = \mathbf{AA}_{16} \quad \text{(equivalente a 170 en decimal)}$$

Preguntas de repaso y ejercicios

1. Convierta el número decimal 209 a binario de 8 bits. Muestre el proceso paso a paso.
2. Convierta el número binario 11010110 a decimal. Muestre el proceso paso a paso.
3. ¿Cuántos bits hay en 4 dígitos hexadecimales? ¿Y en una dirección MAC completa?
4. Convierta el número binario 11011010 11110000 (16 bits) a notación hexadecimal. Muestre el proceso dividiéndolo en nibbles.
5. Dado el número hexadecimal 3F8A, conviértalo primero a binario y luego a decimal.

Referencias de la unidad

Referencias de la unidad

Cisco Networking Academy (2020). *Binary, Decimal and Hexadecimal Conversions*. Material de apoyo NetAcad.

Postel, J. (1981). *Internet Protocol (IPv4)*. https://www.rfc-editor.org/rfc/rfc791.txt.

Stallings, William (2013). *Data and Computer Communications*. Pearson.

4 Direccionamiento IP

Competencias

- **Comprender:** Explicar componentes de una dirección IP (red/host) y el uso de prefijos CIDR.
- **Hacer:** Identificar tipos de direcciones (públicas/privadas, especiales) y proponer asignaciones coherentes.

Objetivos

- Explicar las características básicas de IPv4 e IPv6.
- Identificar tipos de direcciones (pública/privada) y rangos especiales.
- Comprender CIDR y la notación de prefijos para el diseño de redes.

Resultados de Aprendizaje

- **Comprender:** Diferencia IPv4 e IPv6 y explica el propósito de cada una.
- **Hacer:** Reconoce direcciones especiales (loopback, link-local, privadas) y justifica su uso.
- **Hacer:** Interpreta y escribe direcciones en notación CIDR de forma correcta.

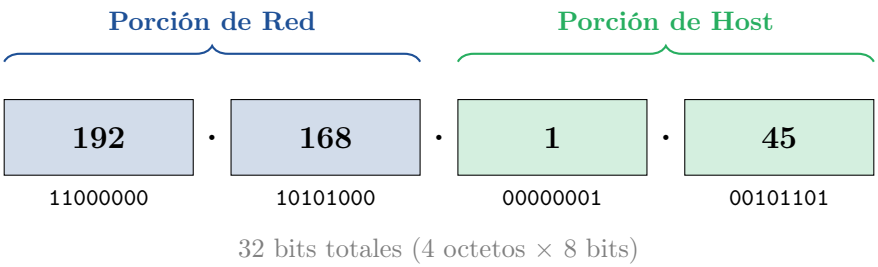
4.1 IPv4 – Estructura

IPv4 utiliza direcciones de **32 bits**, representadas en **notación decimal punteada** mediante cuatro octetos separados por puntos. Cada octeto está compuesto por 8 bits y puede tomar valores desde 0 hasta 255.

Una dirección IPv4 se divide en dos partes:

- **Porción de red:** Identifica la red a la que pertenece el dispositivo.
- **Porción de host:** Identifica específicamente al dispositivo dentro de esa red.

La división entre red y host depende de la máscara de subred utilizada.



32 bits totales (4 octetos × 8 bits)

4.2 Clasificación por Clases (Histórica)

En los primeros años de Internet, las direcciones IPv4 se organizaron en **clases**. Este esquema se creó para facilitar la asignación de direcciones según el tamaño de las organizaciones.

La idea era simple:

- Organizaciones muy grandes necesitaban millones de direcciones.
- Organizaciones medianas necesitaban miles.
- Organizaciones pequeñas necesitaban cientos.

Por ello, se dividió el espacio de direcciones en clases predefinidas (A, B y C), cada una con una máscara fija. Sin embargo, este sistema resultó poco eficiente, ya que desperdiciaba muchas direcciones. Posteriormente fue reemplazado por el direccionamiento sin clases (CIDR), que permite una asignación más flexible.

Clase	Rango	Máscara	Hosts por Red
A	1.0.0.0 – 126.255.255.255	/8	16,777,214
B	128.0.0.0 – 191.255.255.255	/16	65,534
C	192.0.0.0 – 223.255.255.255	/24	254
D	224.0.0.0 – 239.255.255.255	Multicast	
E	240.0.0.0 – 255.255.255.255	Experimental / Reservado	

Identificación por primer octeto La clase de una dirección podía identificarse observando los primeros bits del primer octeto:

- Clase A: comienza con bit 0
- Clase B: comienza con bits 10
- Clase C: comienza con bits 110
- Clase D: comienza con bits 1110
- Clase E: comienza con bits 1111

Actualmente, la clasificación por clases tiene valor principalmente histórico y académico, ya que en redes modernas se utiliza CIDR para una asignación más eficiente de direcciones.

4.3 Direcciones Privadas (RFC 1918)

Las direcciones privadas fueron definidas en el RFC 1918 para permitir la creación de redes internas sin consumir direcciones públicas de Internet.

No son enrutables en Internet, es decir, los routers de Internet descartan estos rangos. Se utilizan dentro de redes locales (LAN) como hogares, escuelas y empresas.

Para que estos dispositivos puedan acceder a Internet, se emplea **NAT** (Network Address Translation), un mecanismo que traduce direcciones privadas internas en una dirección pública antes de salir a Internet.

¿Por qué se crearon? Con el crecimiento acelerado de Internet, comenzó a agotarse el espacio de direcciones IPv4. Las direcciones privadas permitieron:

- Reutilizar los mismos rangos en múltiples redes internas.
- Reducir el consumo de direcciones públicas.
- Mejorar la seguridad al no exponer directamente las direcciones internas.

Clase	Rango Privado	CIDR	Total Direcciones
A	10.0.0.0 – 10.255.255.255	10.0.0.0/8	16,777,216
B	172.16.0.0 – 172.31.255.255	172.16.0.0/12	1,048,576
C	192.168.0.0 – 192.168.255.255	192.168.0.0/16	65,536

Ejemplo práctico: Un router doméstico suele asignar direcciones como 192.168.1.10 a los dispositivos internos. Luego, mediante NAT, todas esas direcciones salen a Internet utilizando una única dirección pública.

4.4 Direcciones Especiales

Existen direcciones IPv4 que cumplen funciones específicas dentro de una red. No se asignan a dispositivos de manera normal, sino que tienen propósitos técnicos definidos.

Dirección	Propósito
`0.0.0.0`	Representa "esta red" o dirección no especificada. Se usa como ruta por defecto.
`127.0.0.0/8`	Loopback (localhost). Permite que un equipo se comunique consigo mismo para pruebas.
`169.254.0.0/16`	APIPA. Se asigna automáticamente cuando falla el servidor DHCP.
`255.255.255.255`	Broadcast limitado. Envía un mensaje a todos los hosts de la red local.
`x.x.x.0` (según máscara)	Dirección de red. Identifica la red; los bits de host están en 0.
`x.x.x.255` (según máscara)	Broadcast de subred. Identifica a todos los dispositivos de la subred; los bits de host están en 1.

Notas importantes

- La dirección de red no puede asignarse a un host.
- La dirección de broadcast tampoco puede asignarse a un host.
- Loopback (127.0.0.1) se usa comúnmente para verificar que el protocolo TCP/IP está funcionando correctamente en el equipo.
- APIPA aparece cuando un dispositivo no logra obtener configuración automática desde DHCP.

4.5 Notación CIDR

CIDR (*Classless Inter-Domain Routing*) es un método moderno de direccionamiento que reemplazó el antiguo sistema por clases.

Permite dividir redes de forma flexible, asignando únicamente la cantidad de direcciones necesarias y evitando el desperdicio de direcciones IPv4.

Se representa mediante la notación:

`dirección/prefijo`

El **prefijo** indica cuántos bits pertenecen a la porción de red dentro de los 32 bits totales de IPv4.

¿Qué significa el prefijo? Por ejemplo:

- `192.168.1.0/24` → los primeros 24 bits son de red.
- Los 8 bits restantes (32 - 24) son para hosts.

Nota Importante

Fórmula de hosts utilizables:

$$\text{Hosts} = 2^{(32-\text{prefijo})} - 2$$

Se restan 2 direcciones porque:

- Una corresponde a la **dirección de red** (bits de host en 0).
- Una corresponde al **broadcast** (bits de host en 1).

Ejemplo práctico Si tenemos la red `/26`:

- Bits de host = 32 - 26 = 6
- Total de direcciones = $2^6 = 64$

- Hosts utilizables $= 64 - 2 = 62$

Esto significa que una subred /26 permite asignar hasta 62 IPs.

CIDR	Máscara Decimal	Hosts Utilizables
/24	255.255.255.0	254
/25	255.255.255.128	126
/26	255.255.255.192	62
/27	255.255.255.224	30
/28	255.255.255.240	14
/29	255.255.255.248	6
/30	255.255.255.252	2

Ventajas de CIDR

- Permite un uso más eficiente del espacio de direcciones.
- Elimina las limitaciones rígidas de las clases A, B y C.
- Facilita la agregación de rutas (resumen de rutas), reduciendo el tamaño de las tablas de enrutamiento.

4.6 Direccionamiento IPv6

IPv6 utiliza direcciones de **128 bits**, lo que permite un espacio de direcciones extremadamente amplio (2^{128} direcciones posibles).

Se representan en **notación hexadecimal**, divididas en 8 grupos de 16 bits (4 dígitos hexadecimales cada uno), separados por dos puntos:

```
2001:0db8:85a3:0000:0000:8a2e:0370:7334
```

IPv6 fue desarrollado principalmente para solucionar el agotamiento de direcciones IPv4 y mejorar aspectos como la agregación de rutas, la seguridad y la eficiencia del enrutamiento.

Características importantes

- No utiliza notación decimal punteada.
- No requiere NAT para conectividad global.
- Incorpora soporte nativo para autoconfiguración.

Reglas de compresión

Las direcciones IPv6 pueden abreviarse aplicando las siguientes reglas:

1. **Eliminar ceros iniciales** dentro de cada grupo hexadecimal.

   Ejemplo:

   $$\texttt{0db8} \rightarrow \texttt{db8}$$

2. **Reemplazar un único grupo consecutivo de secciones formadas solo por ceros** con `::`. Esta sustitución solo puede utilizarse **una vez** en la dirección.

   Ejemplo:

   $$\texttt{2001:db8:85a3:0000:0000:8a2e:0370:7334}$$

   se comprime como:

   $$\texttt{2001:db8:85a3::8a2e:370:7334}$$

Prefijo en IPv6 Al igual que en IPv4 con CIDR, IPv6 utiliza la notación:

$$\texttt{dirección/prefijo}$$

Ejemplo:

$$\texttt{2001:db8::/64}$$

El `/64` indica que los primeros 64 bits corresponden a la porción de red y los restantes 64 bits identifican la interfaz (host).

En redes IPv6 modernas, el prefijo /64 es el más común para redes locales.

Tipos principales de direcciones IPv6

Tipo	Prefijo	Uso
Unicast Global	`2000::/3`	Dirección pública enrutable en Internet
Unique Local	`fc00::/7`	Similar a direcciones privadas IPv4
Link-Local	`fe80::/10`	Comunicación dentro del mismo enlace físico
Loopback	`::1/128`	Equivalente a 127.0.0.1 en IPv4
Multicast	`ff00::/8`	Entrega de paquetes a múltiples destinos

Notas importantes

- IPv6 no utiliza broadcast; en su lugar emplea multicast.

- Toda interfaz IPv6 posee automáticamente una dirección Link-Local.
- Las direcciones Global Unicast son equivalentes a las direcciones públicas en IPv4.

Preguntas de repaso

1. ¿Cuál es la principal diferencia entre una dirección IPv4 y una IPv6 en términos de longitud de bits y capacidad de direcciones?
2. ¿Por qué se crearon las direcciones privadas (RFC 1918)? Mencione los tres rangos principales y para qué tipo de organizaciones se usaría típicamente la clase C.
3. ¿Qué significa la notación CIDR `192.168.20.0/26`? ¿Cuántas direcciones de host utilizables tiene esta red? (Aplique la fórmula).
4. Explique para qué sirve la dirección `127.0.0.1`. ¿Qué comando usaría en su computador para probar que la pila TCP/IP está funcionando correctamente?

Referencias de la unidad

Referencias de la unidad

Cisco Systems (2020). *IP Addressing and Subnetting for New Users*. Documento de referencia Cisco.

Deering, S. and Hinden, R. (1998). *Internet Protocol, Version 6 (IPv6)*. https://www.rfc-editor.org/rfc/rfc2460.txt.

Fuller, V. and Li, T. (2006). *Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan*. https://www.rfc-editor.org/rfc/rfc4632.

Postel, J. (1981). *Internet Protocol (IPv4)*. https://www.rfc-editor.org/rfc/rfc791.txt.

Rekhter, Y. and Moskowitz, R. and Karrenberg, D. and de Groot, G. J. and Lear, E. (1996). *Address Allocation for Private Internets*. https://www.rfc-editor.org/rfc/rfc1918.

5 Subnetting y VLSM

Competencias

- Explicar el propósito del subnetting y las máscaras de subred.
- Aplicar VLSM para diseñar esquemas de direccionamiento eficientes según requerimientos de hosts/enlaces.

Objetivos

- Explicar el proceso de subnetting y su utilidad en redes.
- Aplicar VLSM para asignar subredes de diferentes tamaños.
- Resolver ejercicios de división de redes y asignación de direcciones.

Resultados de Aprendizaje

- Calcula subredes y rangos de hosts a partir de un prefijo dado.
- Diseña un esquema con VLSM para diferentes segmentos y lo documenta de forma ordenada.
- Justifica por qué VLSM optimiza el direccionamiento y reduce desperdicio.

5.1 Concepto de Subnetting

El **subnetting** (división en subredes) es una técnica que permite segmentar una red grande en subredes más pequeñas mediante la modificación de la máscara de subred. Esto se logra "prestando" bits de la porción de host para crear la porción de subred.

Ventajas del Subnetting

Seguridad: Aísla segmentos de red, permitiendo aplicar políticas de seguridad específicas por subred.

Rendimiento: Reduce los dominios de broadcast, disminuyendo el tráfico innecesario.

Administración: Facilita la gestión por función, departamento o ubicación física.

Eficiencia: Optimiza el uso del espacio de direcciones IP disponible.

5.2 Proceso de Subnetting Paso a Paso

Paso 1: **Determinar** cuántas subredes o cuántos hosts se necesitan.

Paso 2: **Calcular bits prestados:** $2^n \geq$ número de subredes necesarias.

Paso 3: **Nueva máscara** = máscara original + n bits prestados.

Paso 4: Calcular incremento $= 2^{\text{bits de host restantes}}$.

Paso 5: Calcular rangos: dirección de red, primera IP utilizable, última IP utilizable, broadcast.

Ejemplo : Subnetting Básico

Escenario: Red `192.168.1.0/24` – Se necesitan **4 subredes**.
Paso 1: $2^2 = 4$ subredes $\Rightarrow$ 2 bits prestados.
Paso 2: Nueva máscara:

$$/24 + 2 = /26$$

Máscara decimal: 255.255.255.192
Paso 3: Bits de host restantes:

$$8 - 2 = 6 \text{ bits}$$

Paso 4: Incremento:

$$2^6 = 64$$

Hosts por subred:

$$2^6 - 2 = 62$$

Subred	Dir. de Red	Primera IP	Última IP	Broadcast
1	192.168.1.0	192.168.1.1	192.168.1.62	192.168.1.63
2	192.168.1.64	192.168.1.65	192.168.1.126	192.168.1.127
3	192.168.1.128	192.168.1.129	192.168.1.190	192.168.1.191
4	192.168.1.192	192.168.1.193	192.168.1.254	192.168.1.255

Ejemplo : Subnetting por Número de Hosts

Escenario: Red `10.0.0.0/24` – Se necesitan al menos **30 hosts por subred**.
Paso 1: Buscamos una potencia de 2 que cubra al menos 30 hosts:

$$2^5 = 32$$

Se restan 2 direcciones:

$$32 - 2 = 30 \text{ hosts}$$

Se necesitan 5 bits para hosts.
Paso 2: Bits totales del último octeto = 8
Bits prestados:

$$8 - 5 = 3$$

Paso 3: Nueva máscara:

$$/24 + 3 = /27$$

Máscara decimal: 255.255.255.224
Paso 4: Incremento:

$$2^5 = 32$$

Subred	Dir. de Red	Primera IP	Última IP	Broadcast
1	10.0.0.0	10.0.0.1	10.0.0.30	10.0.0.31
2	10.0.0.32	10.0.0.33	10.0.0.62	10.0.0.63
3	10.0.0.64	10.0.0.65	10.0.0.94	10.0.0.95
4	10.0.0.96	10.0.0.97	10.0.0.126	10.0.0.127

Resultado: Cada subred /27 permite 30 hosts utilizables.

5.3 Tabla de Referencia Rápida de Subnetting

CIDR	Máscara	Incremento	Hosts/Subred
/24	255.255.255.0	256	254
/25	255.255.255.128	128	126
/26	255.255.255.192	64	62
/27	255.255.255.224	32	30
/28	255.255.255.240	16	14
/29	255.255.255.248	8	6
/30	255.255.255.252	4	2

5.4 VLSM (Variable Length Subnet Mask)

VLSM (Máscara de Subred de Longitud Variable) permite utilizar máscaras de diferente longitud dentro de la misma red principal.

A diferencia del subnetting tradicional (donde todas las subredes tienen el mismo tamaño), VLSM optimiza el uso de direcciones asignando a cada segmento únicamente la cantidad de direcciones que realmente necesita.

Regla fundamental Siempre se debe asignar **de mayor a menor**:

1. Ordenar los segmentos según la cantidad de hosts requeridos.
2. Asignar primero la subred más grande.
3. Continuar con las redes más pequeñas utilizando el espacio restante.

Ejemplo : Diseño VLSM Completo

Red base: `192.168.10.0/24`
Requerimientos:

- Segmento A: 100 hosts
- Segmento B: 50 hosts
- Segmento C: 25 hosts
- 3 enlaces punto a punto (2 hosts cada uno)

Paso 1: Determinar prefijos necesarios

- 100 hosts $\rightarrow 2^7 = 128$ direcciones $\rightarrow$ /25 (126 hosts útiles)
- 50 hosts $\rightarrow 2^6 = 64$ direcciones $\rightarrow$ /26 (62 hosts útiles)
- 25 hosts $\rightarrow 2^5 = 32$ direcciones $\rightarrow$ /27 (30 hosts útiles)
- Enlaces p2p (2 hosts) $\rightarrow 2^2 = 4$ direcciones $\rightarrow$ /30 (2 hosts útiles)

Asignación de mayor a menor:

Segmento	Hosts Req.	Prefijo	Red Asignada	Rango Utilizable
A	100	/25	192.168.10.0	192.168.10.1 – 192.168.10.126
B	50	/26	192.168.10.128	192.168.10.129 – 192.168.10.190
C	25	/27	192.168.10.192	192.168.10.193 – 192.168.10.222
Enlace 1	2	/30	192.168.10.224	192.168.10.225 – 192.168.10.226
Enlace 2	2	/30	192.168.10.228	192.168.10.229 – 192.168.10.230
Enlace 3	2	/30	192.168.10.232	192.168.10.233 – 192.168.10.234

Espacio restante disponible:
192.168.10.236 – 192.168.10.255

Relevancia para Ciberseguridad

- VLSM permite crear subredes específicas para **zonas de seguridad** (DMZ, gestión, usuarios).
- Los enlaces `/30` son ideales para conexiones **punto a punto** entre routers (solo 2 hosts utilizables).
- La segmentación facilita la implementación de **ACLs**: una ACL puede permitir o denegar tráfico de una subred específica.
- Siempre se debe reservar espacio para **crecimiento futuro**.

Preguntas de repaso

1. ¿Cuál es la principal ventaja de usar VLSM (Máscara de Subred de Longitud Variable) sobre el subnetting tradicional con máscara fija (FLSM)?

2. ¿Cuál es la regla fundamental o el orden correcto que se debe seguir al asignar host en un diseño VLSM?

Referencias de la unidad

Referencias de la unidad

Cisco Networking Academy (2020). *Subnetting Practice*. Guías y ejercicios NetAcad.

Cisco Systems (2020). *Subnetting and VLSM Concepts*. Documento de referencia Cisco.

Fuller, V. and Li, T. (2006). *Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan*. https://www.rfc-editor.org/rfc/rfc4632.

6 Enrutamiento IP

Competencias

- Explicar el rol del enrutamiento y la estructura básica de una tabla de enrutamiento.
- Proponer rutas estáticas y justificar decisiones en una topología pequeña.
- Relacionar diseño jerárquico de red con disponibilidad y controles de seguridad.

Objetivos

- Explicar el funcionamiento de las tablas de enrutamiento IP.
- Comprender rutas estáticas y su uso en redes pequeñas.
- Analizar el diseño jerárquico de topologías y su relación con seguridad.

Resultados de Aprendizaje

- Lee una tabla de enrutamiento y determina el siguiente salto para un destino.
- Propone rutas estáticas mínimas para alcanzar redes remotas en una topología dada.

6.1 Conceptos Fundamentales de Enrutamiento

El **enrutamiento** es el proceso mediante el cual los routers determinan la mejor ruta para reenviar paquetes entre redes diferentes. La **tabla de enrutamiento** almacena la información sobre las redes conocidas por el router: prefijo de red, máscara, interfaz de salida, dirección del siguiente salto (*next hop*) y métricas asociadas.

Ejemplo: Tabla de enrutamiento (show ip route)

```
Router# show ip route
C    192.168.1.0/24 is directly connected, GigabitEthernet0/0
S    192.168.2.0/24 [1/0] via 10.0.0.2
S    192.168.3.0/24 [1/0] via 10.0.0.3
S*   0.0.0.0/0 [1/0] via 10.0.0.1
```

C = Conectada directamente **S** = Ruta estática **S*** = Ruta por defecto
[1/0] = [Distancia Administrativa / Métrica]

6.2 Rutas Estáticas

Las rutas estáticas son configuradas manualmente por el administrador de red. No cambian dinámicamente ante cambios en la topología.

Sintaxis de rutas estáticas en Cisco IOS

```
! Ruta hacia una red remota via next-hop
Router(config)# ip route 192.168.2.0 255.255.255.0 10.0.0.2

! Ruta por defecto (default route)
Router(config)# ip route 0.0.0.0 0.0.0.0 10.0.0.1

! Ruta hacia interfaz de salida
Router(config)# ip route 192.168.3.0 255.255.255.0 Serial0/0/0
```

Preguntas de repaso

1. ¿Cuál es la función principal de un router y en qué capa del modelo OSI opera?

2. ¿Qué información clave se puede encontrar en una tabla de enrutamiento?

Referencias de la unidad

Baker, F. (1995). *Requirements for IP Version 4 Routers*. https://www.rfc-editor.org/rfc/rfc1812.

Cisco Systems (2020a). *Configuring Static Routes*. Guía de configuración Cisco IOS.

— (2020b). *Hierarchical Network Design*. Buenas prácticas de diseño de redes (Cisco).

Postel, J. (1981). *Internet Protocol (IPv4)*. https://www.rfc-editor.org/rfc/rfc791.txt.

Glosario de Términos

Glosario

Término	Definición
ACL	Access Control List. Lista de reglas para controlar acceso a recursos de red.
ARP	Address Resolution Protocol. Mapea direcciones IP a direcciones MAC.
Broadcast	Transmisión enviada a todos los dispositivos del segmento de red.
CIDR	Classless Inter-Domain Routing. Notación dirección/prefijo para representar redes.
DMZ	Demilitarized Zone. Zona semi-protegida para servidores públicos.
FCS	Frame Check Sequence. Campo de detección de errores en tramas Ethernet.
Firewall	Dispositivo que controla el tráfico entre redes según políticas de seguridad.
IPsec	Internet Protocol Security. Suite de protocolos para comunicaciones seguras.
LAN	Local Area Network. Red de área local.
LLC	Logical Link Control. Subcapa de enlace de datos (IEEE 802.2).
MAC	Media Access Control. Dirección física de 48 bits / Subcapa de enlace de datos.
Máscara	Valor de 32 bits que define la porción de red y host en una dirección IPv4.
NAT	Network Address Translation. Traducción de direcciones IP públicas/privadas.
Next Hop	Siguiente salto: dirección IP del próximo router en la ruta al destino.
OSPF	Open Shortest Path First. Protocolo de enrutamiento de estado de enlace.
PDU	Protocol Data Unit. Forma que toma un bloque de datos en cada capa del modelo.
QoS	Quality of Service. Calidad de servicio para administrar congestión en la red.
Subred	División lógica de una red IP más grande.
VLAN	Virtual LAN. Segmentación lógica de redes en un switch.
VLSM	Variable Length Subnet Mask. Máscaras de subred de longitud variable.
VPN	Virtual Private Network. Red privada virtual sobre infraestructura pública.
WAN	Wide Area Network. Red de área amplia.