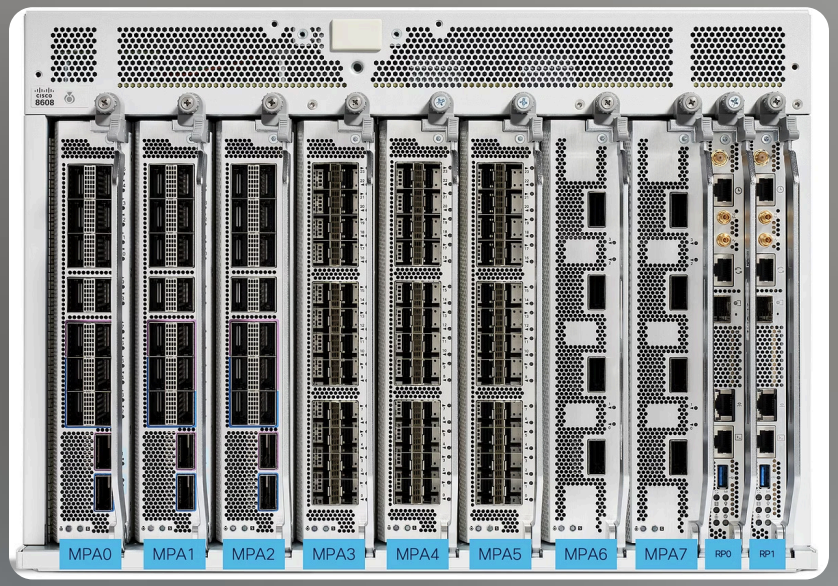


Fundamentos de Routing y Herramientas de Diagnóstico

Emanuel Rodriguez

Slides: 27 | Enfoque: Fundamentos técnicos + herramientas CLI

¿Qué es un Router?

Un router es un dispositivo de red de **Capa 3 (Red)** del modelo OSI que toma decisiones de reenvío de paquetes basadas en direcciones IP. Su función principal es determinar la mejor ruta para que los datos lleguen desde el origen hasta el destino a través de múltiples redes interconectadas.

Funciones Fundamentales

- **Routing**: Determinación de la mejor ruta usando tablas de enrutamiento
- **Forwarding**: Reenvío físico de paquetes hacia el siguiente salto
- **Filtrado**: Control de acceso mediante ACLs
- **NAT/PAT**: Traducción de direcciones de red
- **QoS**: Calidad de servicio y priorización de tráfico
- **Seguridad**: Firewall, VPN, autenticación

1.1 Historia de los Routers

El concepto de enrutamiento de paquetes nace en los años 1960 con el proyecto ARPANET, la precursora de Internet. Los primeros "routers" eran computadoras especializadas llamadas **Interface Message Processors (IMPs)**.

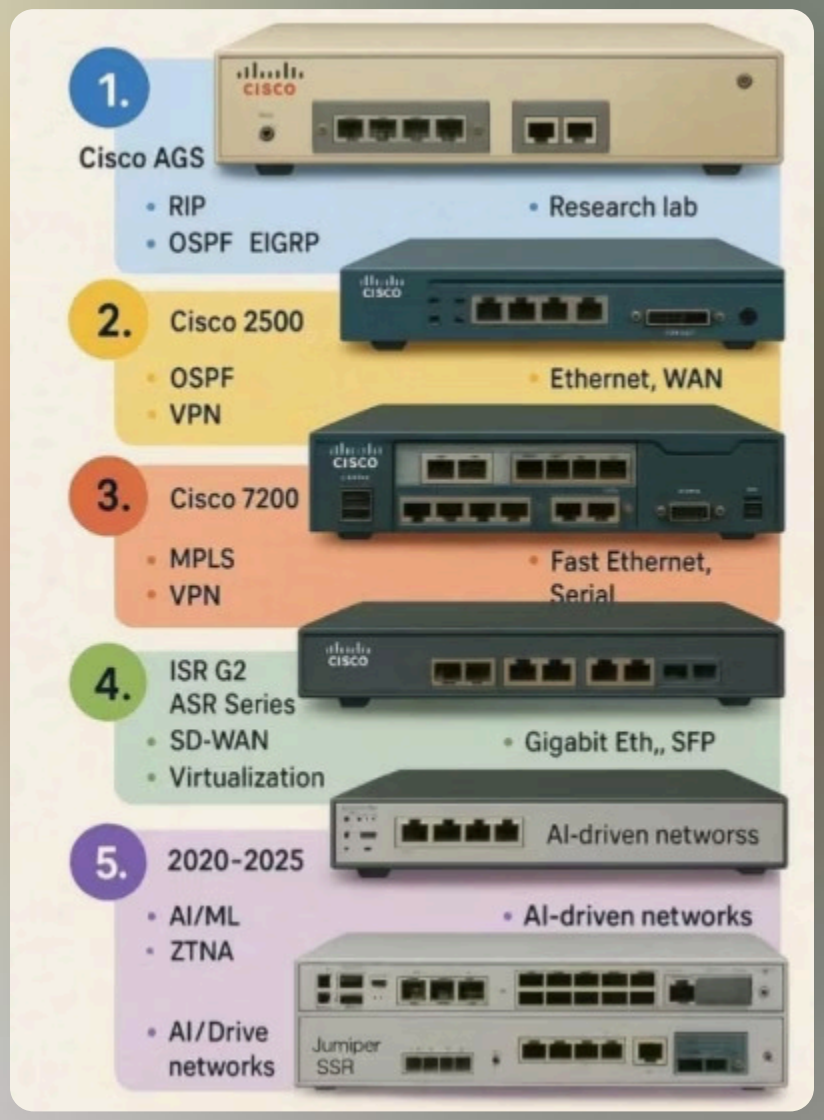
Timeline Histórico:

- **1969:** Primer IMP instalado en UCLA
- **1974:** Vint Cerf y Bob Kahn desarrollan TCP/IP
- **1981:** Cisco Systems funda por Leonard Bosack y Sandy Lerner
- **1984:** Primer router comercial Cisco (AGS)
- **1995:** Aparecen routers para el mercado masivo
- **2000s:** Routers inalámbricos y multi-servicio
- **2010s:** Software Defined Networking (SDN)
- **2020s:** Cloud-native routing y 5G integration

1.2 Evolución de RouterOS (MikroTik)

MikroTik fue fundada en 1996 en Letonia por John Tully y Arnis Riekstins. Su historia:

- **1997:** Primera versión de RouterOS
- **2002:** Introducción de RouterBOARD hardware
- **2005:** Expansión global y certificaciones
- **2010:** Integración de tecnologías inalámbricas avanzadas
- **2015:** Container y virtualization support
- **2020:** Cloud integration y API REST



Evolución Histórica

1. Primera Generación - Cisco AGS (1990s) Características:

Protocolos: RIP, OSPF, EIGRP Contexto: Laboratorios de investigación Velocidades: Interfaces seriales T1/E1 Memoria: Limitada, procesamiento básico

Impacto: Estableció los fundamentos del routing moderno con protocolos de estado de enlace.

2. Segunda Generación - Cisco 2500 (Late 1990s-2000s) Evolución:

Nuevas capacidades: OSPF mejorado, VPN básicas Conectividad: Ethernet 10 Mbps, interfaces WAN Mercado objetivo: Oficinas pequeñas y medianas

Innovación: Introdujo conceptos de VPN y routing más sofisticado.

3. Tercera Generación - Cisco 7200 (2000s-2010s) Revolución tecnológica:

MPLS: Multiprotocol Label Switching VPN avanzadas: IPSec, DMVPN Fast Ethernet: 100 Mbps Interfaces seriales: Alta densidad

Importancia: Era del MPLS y redes de proveedores de servicios.

4. Cuarta Generación - ISR G2/ASR Series (2010-2020) Transformación digital:

SD-WAN: Software-Defined Wide Area Networks Virtualización: Servicios en contenedores Gigabit Ethernet: 1 Gbps estándar SFP: Interfaces modulares de fibra

Paradigma: Transición hacia redes definidas por software.

5. Quinta Generación - AI-Driven Networks (2020-2025) Era actual:

AI/ML: Inteligencia artificial y machine learning ZTNA: Zero Trust Network Access Automatización: Self-healing networks Edge computing: Procesamiento distribuido

Análisis Tecnológico por Generaciones

Protocolos de Routing

Evolución cronológica:
RIP (1980s) → OSPF (1990s) → EIGRP (1990s) → BGP/MPLS (2000s) → SD-WAN (2010s) → Intent-Based (2020s)

Velocidades de Interface

Timeline de conectividad:
56K/T1 (1990s) → Ethernet 10M (2000s) → Fast Ethernet 100M (2005s) → Gigabit 1G (2010s) → 10G/100G (2020s)

Arquitecturas

1. **Monolítica**: Hardware dedicado, un propósito
2. **Modular**: Interfaces intercambiables
3. **Virtualizada**: NFV, contenedores
4. **Cloud-native**: Microservicios, API-first
5. **AI-driven**: Automatización, self-healing

Cisco vs Otras Marcas Líderes

MikroTik

Fortalezas:

- **RouterOS**: Sistema operativo extremadamente flexible
- **Precio-rendimiento**: Excelente relación calidad-precio
- **Modelos destacados**:
  - **CCR2004**: 16 núcleos ARM64, hasta 100 Gbps
  - **RB5009**: Wi-Fi 6, routing avanzado
- **Mercado**: WISP, pequeñas empresas, educación

Debilidades: Soporte empresarial limitado, curva de aprendizaje empinada.

Juniper Networks

Especialización:

- **Junos OS**: Sistema operativo unificado
- **MPLS/BGP**: Líderes en routing de proveedores
- **Modelos emblemáticos**:
  - **MX Series**: Core routing hasta 80 Tbps
  - **SRX Series**: Security + routing integrado
- **Segmentación**: Carriers, grandes empresas

Ventaja competitiva: Arquitectura modular y escalabilidad masiva.

Fortinet

Enfoque integrado:

- **FortiOS**: Security + networking unificado
- **SD-WAN nativo**: Integración security-first
- **Modelos principales**:
  - **FortiGate 4400F**: 1.8 Tbps throughput
  - **FortiGate 60F**: Branch offices
- **Diferenciador**: Security Fabric ecosystem

Recomendaciones por Escenario

Pequeñas Empresas

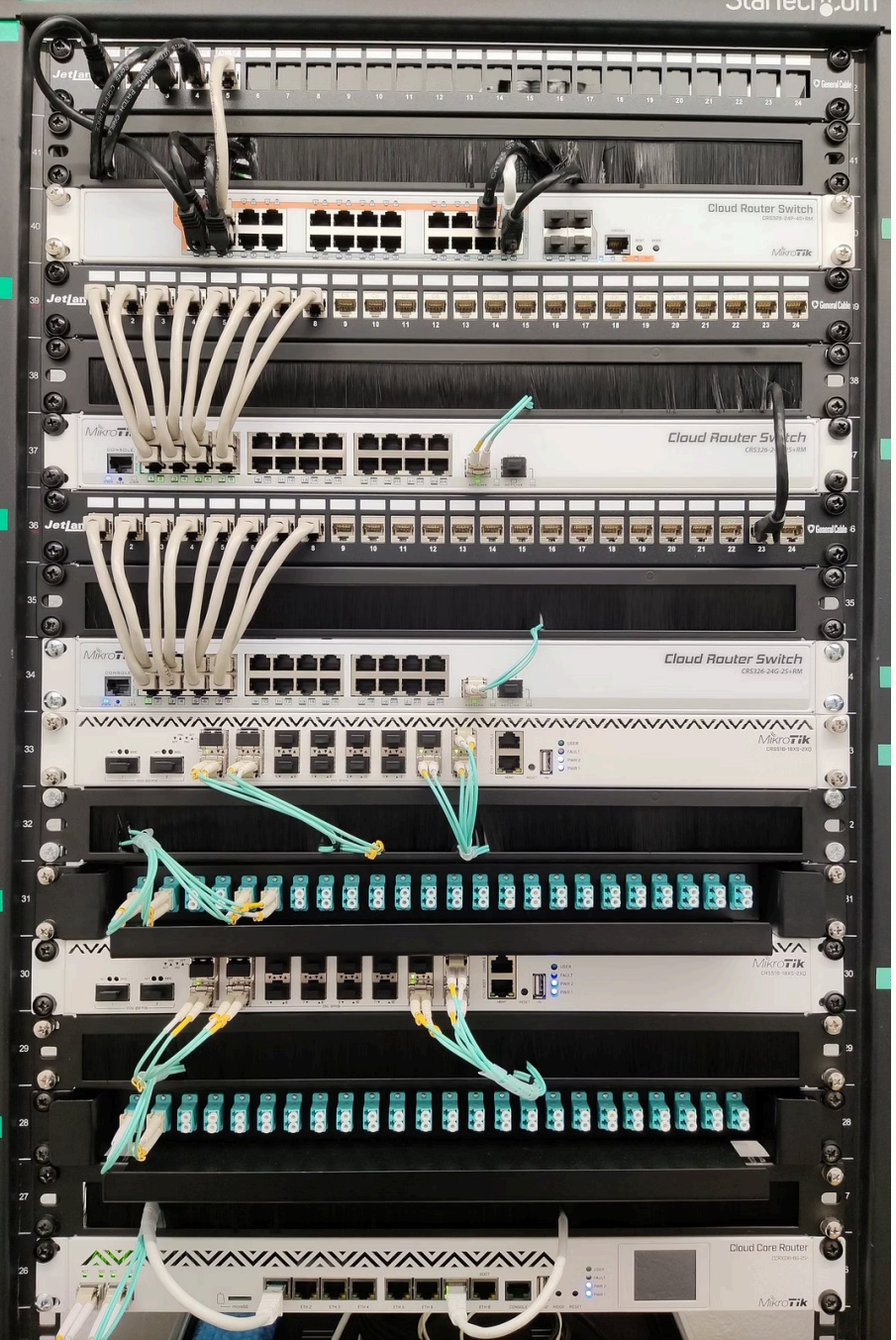
- **MikroTik:** Flexibilidad y precio
- **Cisco ISR:** Soporte empresarial
- **Fortinet:** Security integrada

Medianas Empresas

- **Cisco Catalyst:** SD-WAN + seguridad
- **Fortinet FortiGate:** SASE completo
- **Juniper SRX:** Performance superior

Grandes Empresas/Carriers

- **Cisco ASR/NCS:** Escalabilidad masiva
- **Juniper MX:** Core routing
- **Fortinet chassis:** Security + performance



Tendencias Futuras (2025+)

Tecnologías Emergentes

- **400G/800G interfaces**: Ultra-alta velocidad
- **Quantum-safe encryption**: Seguridad post-cuántica
- **5G integration**: Edge computing masivo
- **Digital twins**: Simulación de redes
- **Autonomous networks**: Auto-configuración y optimización

Desafíos Actuales

1. **Latencia ultra-baja**: Aplicaciones críticas
2. **Sostenibilidad**: Green networking
3. **Seguridad**: Zero-trust architecture
4. **Complejidad**: Simplificación operacional
5. **Costos**: TCO optimization

Elementos funcionales en Routing

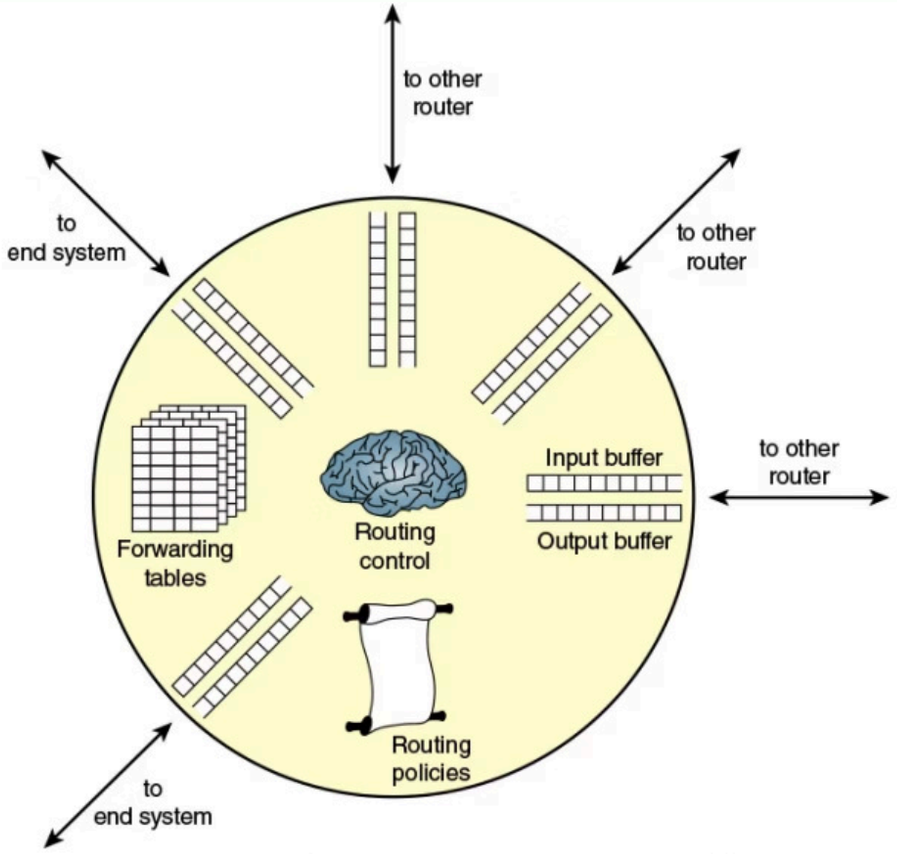


FIGURE 2.10 Elements of a Router

Neighbors managing queues

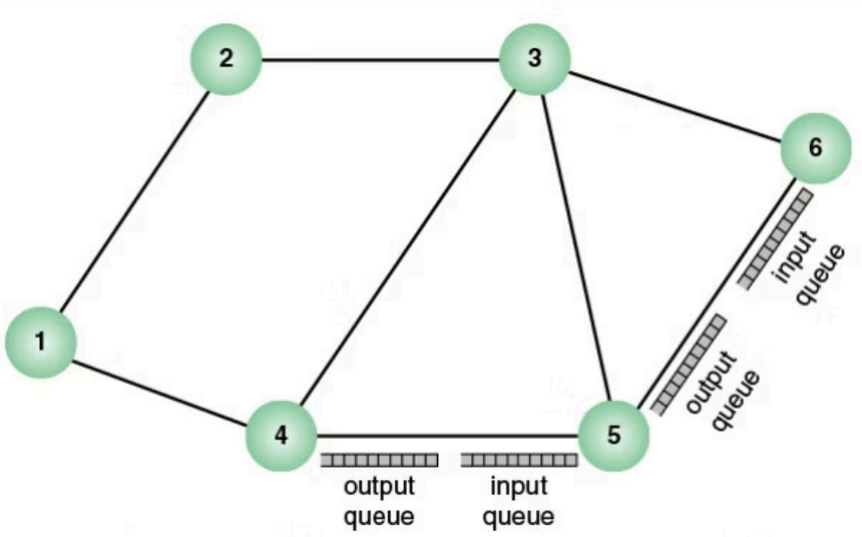
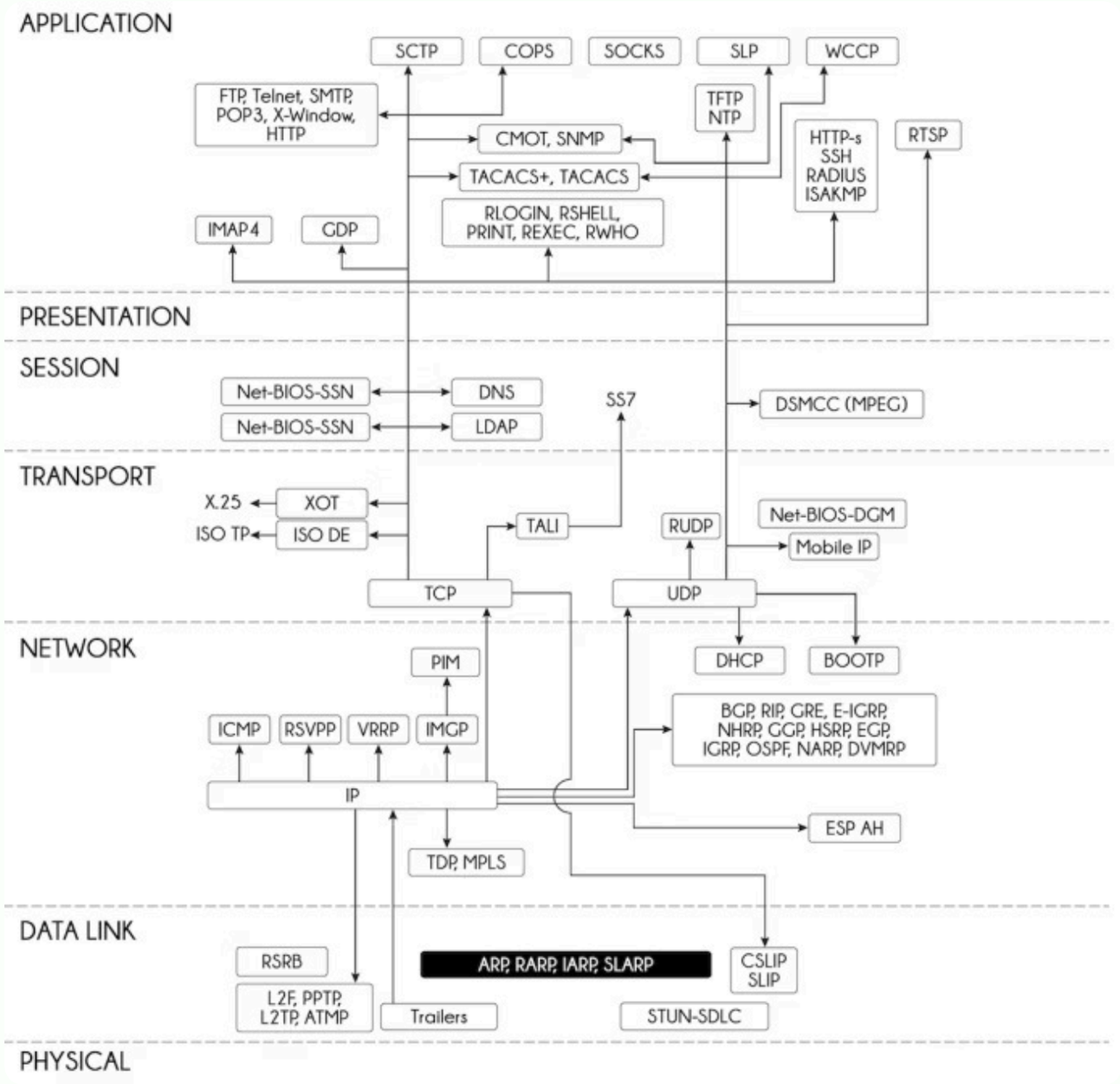


FIGURE 2.11 Interaction of Queues in a Data Network

Foundations of Modern Networking SDN, NFV, QoE, IoT, and Cloud

William Stallings



Mapa de Protocolos en modelo OCI|TCP/IP

Análisis de Protocolos L2/L3

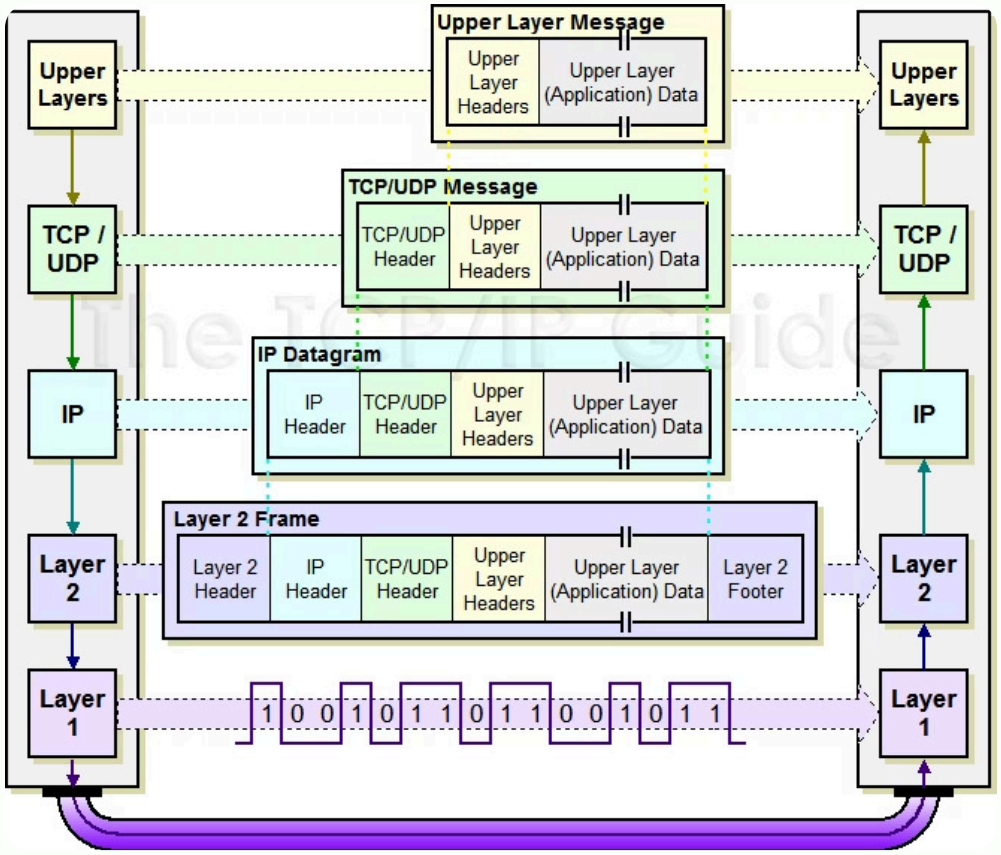
Estructura de Frame Ethernet (L2)

Preamble	DA	SA	Type/Len	Payload	FCS
8 bytes	6 bytes	6 bytes	2 bytes	46-1500 bytes	4 bytes

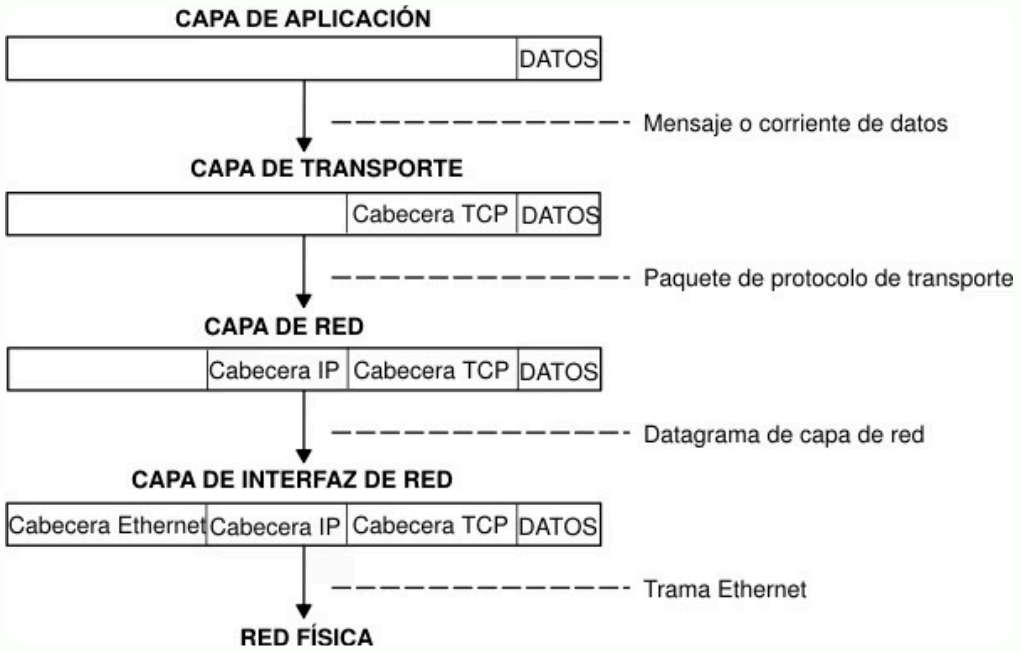
Campos críticos para routing

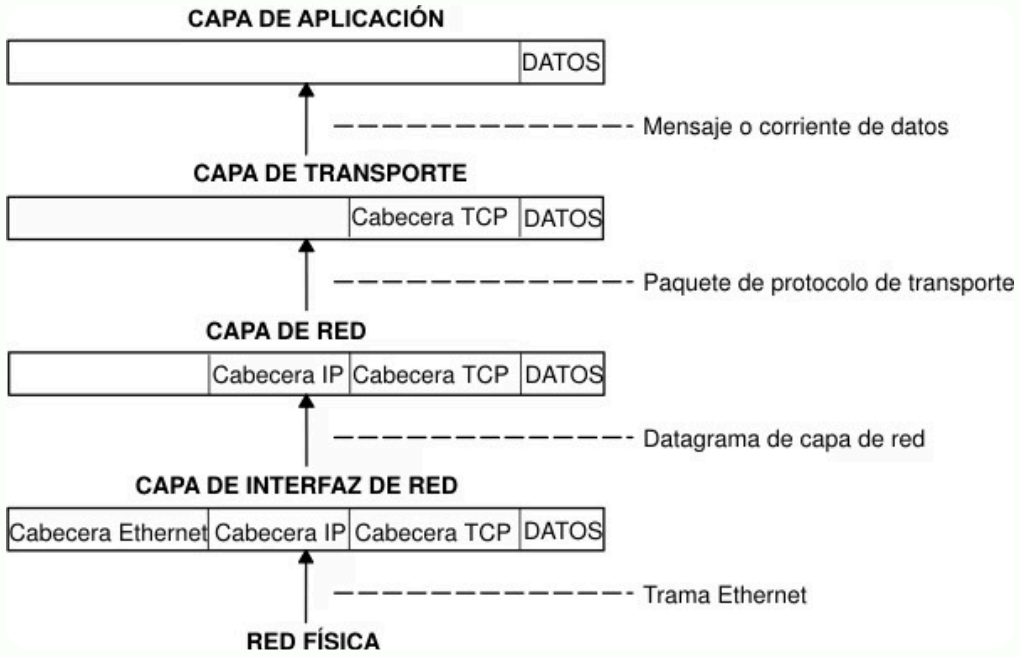
- TTL: Decrementado en cada hop, packet dropped si TTL=0
- Protocol: TCP=6, UDP=17, ICMP=1, OSPF=89
- Flags: DF=Don't Fragment (importante para PMTU)

Cabecera IPv4 (L3)



Fuente de la imagen: http://www.tcpipguide.com/free/diagrams/ipencap.png





Fuente»https://www.goconqr.com/p/14997235-puertos-l-gicos-y-protocolo-tcp-ip-notes/note_page/757035-protocolo-tcp-ip-2-2

Switching vs Routing - Comparación Técnica

Aspecto	Switch (L2)	Router (L3)
Base de decisión	Tabla de direcciones MAC	Tabla de routing
Alcance	Dominio de broadcast	Red/Subred
Procesamiento	Hardware (ASIC)	Híbrido (CPU+ASIC)
Latencia	2-5 µs	10-100 µs
Modificación de paquetes	No modifica	Decremento de TTL, recálculo de checksum
Dominio de colisión	Por puerto	N/A
Manejo de broadcast	Inunda desconocidos	Enruta/descarta según tabla

Frame vs Packet processing

L2: Examina solo DA/SA MAC, decisión de switching

L3: Examina cabecera IP completa, decisión de routing + reescritura L2

Proceso de Forwarding Detallado

Recepción y validación

Frame recibido → Verificación FCS (Frame Check Sequence)

Longest Prefix Match

Búsqueda en FIB por coincidencia más específica (LPM):

- 192.168.1.5/32 (host específico)
- 192.168.1.0/24 (subnet)
- 192.168.0.0/16 (supernet)
- 0.0.0.0/0 (ruta por defecto)

Procesamiento L3

Extracción de cabecera L3 → Decremento de TTL

Reescritura y envío

Resolución ARP si next-hop L2 desconocido → Reescritura cabecera L2 → Forward

Métricas de rendimiento críticas: Latencia típica <50 µs | Jitter <10 µs | Throughput a velocidad de línea (wire speed)

Tabla de Routing - Análisis Detallado

Estructura de RIB (Routing Information Base)

Prefix	Máscara	Next-Hop	Interfaz	Protocolo	Métrica	AD
192.168.1.0	/24	Connected	Gio/1	C	0	0
10.0.0.0	/8	192.168.1.1	Gio/1	S	1	1
172.16.0.0	/16	10.0.1.2	Gio/0	OSPF	65	110
0.0.0.0	/0	203.0.113.1	Gio/2	OSPF	1	110

Administrative Distance (AD) - Cisco

Connected: 0 | Static: 1 | EIGRP: 90 | OSPF: 110 | RIP: 120 | eBGP: 20 | iBGP: 200

Algoritmo de selección

1. Longest prefix match (más específico gana)
2. Administrative Distance (menor AD gana)
3. Metric (menor métrica gana del mismo protocolo)
4. Load balancing si hay rutas de igual coste

Herramientas CLI Avanzadas - Windows PowerShell

Comandos esenciales para análisis de red

```
# Análisis detallado de interfaces
Get-NetAdapter | Select Name,LinkSpeed,OperationalStatus,DriverVersion

# Routing table con métricas
Get-NetRoute | Format-Table DestinationPrefix,NextHop,RouteMetric,Protocol

# Conexiones TCP/UDP con procesos
Get-NetTCPConnection | Where-Object State -eq Established |
  Select LocalAddress,LocalPort,RemoteAddress,RemotePort,OwningProcess

# Monitoreo de ancho de banda
Get-Counter "\\Network Interface(*)\\Bytes Total/sec" -SampleInterval 1 -
MaxSamples 10
```

Test-NetConnection avanzado

```
# Análisis detallado de conectividad
Test-NetConnection google.com -Port 443 -
InformationLevel Detailed

# Retorna información detallada:
# - PingSucceeded
# - NameResolutionResults
# - MatchingIPsecRules
# - NetworkIsolationContext
# - TcpTestSucceeded
```

Herramientas CLI Avanzadas - Linux

iproute2 (reemplazo de net-tools)

```
# Estadísticas detalladas de interfaz
ip -s -s link show eth0
# Muestra RX/TX bytes, packets,
errors, dropped, overruns

# Routing con métricas y protocolos
ip route show table all
# Tablas: kernel, main, local, default

# Tabla de vecinos (ARP) con estados
ip neigh show
# Estados: REACHABLE, STALE, DELAY,
PROBE, FAILED, NOARP, PERMANENT
```

Traffic control (QoS)

```
# Mostrar disciplinas de cola
tc qdisc show dev eth0

# Mostrar clases de tráfico
tc class show dev eth0
```

Monitoreo avanzado

```
# Ancho de banda por proceso
iftop -P -i eth0

# Desglose por puerto
nethogs eth0

# Seguimiento de conexiones
ss -tuln --processes --extended
# Muestra: timer info, socket memory,
congestion algorithm
```

VLSM y Subnetting Avanzado

Variable Length Subnet Mask - Caso práctico

Escenario: Red 192.168.1.0/24, requisitos:

1

Sales: 50 hosts

/26 (62 hosts disponibles)

192.168.1.0/26 (.1-.62)

2

Engineering: 25 hosts

/27 (30 hosts disponibles)

192.168.1.64/27 (.65-.94)

3

Management: 10 hosts

/28 (14 hosts disponibles)

192.168.1.96/28 (.97-.110)

4

P2P links: 2 hosts cada uno

/30 (2 hosts disponibles)

P2P-1: 192.168.1.112/30 (.113-.114)

P2P-2: 192.168.1.116/30 (.117-.118)

Agregación de rutas (Route Summarization)

192.168.1.0/26 + 192.168.1.64/27 = 192.168.1.0/25

192.168.1.96/28 + 192.168.1.112/28 = 192.168.1.96/27

Configuración Avanzada de VLANs

Creación de VLAN con configuración extendida

```
vlan 10
 name USERS
 state active
 mtu 1500
```

Configuración de interfaz con seguridad

```
interface FastEthernet0/1
 switchport mode access
 switchport access vlan 10
 switchport port-security
 switchport port-security maximum 2
 switchport port-security violation restrict
 switchport port-security mac-address sticky
```

Configuración de trunk con DTP deshabilitado

```
interface FastEthernet0/24
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10,20,30
 switchport nonegotiate  # Disable DTP
```

Configuración STP para convergencia rápida

```
spanning-tree mode rapid-pvst
spanning-tree portfast default
spanning-tree extend system-id
```

Inter-VLAN Routing - Configuración Detallada

Router-on-a-stick (Legacy)

```
interface GigabitEthernet0/0
 no shutdown

interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 192.168.10.1 255.255.254.0
 ip helper-address 192.168.20.100  # DHCP relay

interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.0
```

Limitaciones: Cuello de botella en enlace troncal

Layer 3 Switch (Preferido)

```
ip routing
vlan 10
vlan 20

interface vlan 10
 ip address 192.168.10.1 255.255.254.0
 no shutdown

interface vlan 20
 ip address 192.168.20.1 255.255.255.0
 no shutdown
```

Ventajas: Conmutación por hardware, rendimiento a velocidad de línea

Troubleshooting Sistemático L2/L3

Physical (L1)

- Continuidad de cable (prueba TDR)
- Estado de LED de enlace
- Estadísticas de puerto (errores CRC, colisiones)

Data Link (L2)

- Tabla de direcciones MAC: `show mac address-table`
- Pertenencia a VLAN: `show vlan brief`
- Estado de trunk: `show interfaces trunk`
- Estado STP: `show spanning-tree`

Network (L3)

- Configuración IP: `show ip interface brief`
- Tabla de routing: `show ip route`
- Tabla ARP: `show arp`
- Protocolos de routing: `show ip protocols`

Problemas comunes en L2

VLAN mismatch

Trunk no transporta las VLANs requeridas

STP blocking

Puerto en estado de bloqueo debido a prevención de bucles

Duplex mismatch

Fallo en negociación half/full duplex

Herramientas de Monitoreo y Análisis

SNMP monitoring - OIDs esenciales

Estadísticas de interfaz

- 1.3.6.1.2.1.2.2.1.10.X # ifInOctets
- 1.3.6.1.2.1.2.2.1.16.X # ifOutOctets
- 1.3.6.1.2.1.2.2.1.14.X # ifInErrors
- 1.3.6.1.2.1.2.2.1.20.X # ifOutErrors

Información del sistema

- 1.3.6.1.2.1.1.1.0 # sysDescr
- 1.3.6.1.2.1.1.3.0 # sysUpTime
- 1.3.6.1.2.1.1.5.0 # sysName

Filtros Wireshark para networking

```
# Tramas con etiqueta VLAN
vlan

# Spanning Tree Protocol
stp

# Tráfico DHCP
bootp

# Peticiones/respuestas ARP
arp

# Mensajes ICMP
icmp.type == 8 || icmp.type == 0  # ping
icmp.type == 3  # destination unreachable
```

Topología VLAN Empresarial

Diseño jerárquico de 3 capas

Core Switch

Backbone de alta velocidad

Distribution Switches

Distribution SW1 y SW2

Enrutamiento entre VLANs

Access Switches

Access SW1, SW2, SW3, SW4

Conexión directa a dispositivos finales

Diseño VLAN empresarial

VLAN 10: Users (/23) - 192.168.10.0/23

VLAN 20: Servers (/24) - 192.168.20.0/24

VLAN 30: Management (/26) - 192.168.30.0/26

VLAN 40: Guest (/24) - 192.168.40.0/24

VLAN 99: Native (unused) - 192.168.99.0/24

Protocolos de Descubrimiento

CDP (Cisco Discovery Protocol)

```
# Habilitar CDP globalmente
cdp run

# Habilitar por interfaz
interface gigabitethernet 0/1
 cdp enable

# Verificación
show cdp neighbors detail

# Muestra: Device ID, Platform,
# Interface, IP, Version
```

LLDP (Link Layer Discovery Protocol)

```
lldp run
interface range gi0/1-24
 lldp transmit
 lldp receive

show lldp neighbors detail

# Información: System name, description,
# capabilities, management address
```

Consideraciones de seguridad

CDP/LLDP pueden revelar información sensible sobre la red y los dispositivos

Mejores prácticas:

- Deshabilitar en interfaces hacia internet/usuarios
- Usar solo en enlaces entre dispositivos de red

Fundamentos de Quality of Service (QoS)

Clasificación de tráfico

Crítico para el negocio:

- Voz (RTP): <150ms latencia, <30ms jitter
- Video: <400ms latencia, <50ms jitter
- Señalización (SIP/H.323): <150ms latencia

Aplicaciones estándar:

- Navegación web: <4s carga de página
- Email: <10s entrega
- Transferencia de archivos: Best effort

Background:

- Tráfico de backup: Clase scavenger
- Aplicaciones P2P: Prioridad más baja
- Actualizaciones de software: Preferiblemente en horario no laboral

Mecanismos QoS

01

Clasificación

Marcado DSCP (AF41, EF, CS7)

02

Policing

Limitación de tasa (CIR, PIR, burst)

03

Shaping

Suavizado de tráfico

04

Queuing

FIFO, WFQ, CBWFQ, LLQ

Fundamentos de Seguridad en Switching

Port Security

```
interface FastEthernet0/1
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security aging time 60
 switchport port-security violation {protect|restrict|shutdown}
```

DHCP Snooping

```
ip dhcp snooping
ip dhcp snooping vlan 10,20,30

interface FastEthernet0/1
 ip dhcp snooping trust  # Uplink to DHCP server

interface range FastEthernet0/2-24
 ip dhcp snooping limit rate 10  # Max 10 DHCP
                                 # requests/sec
```

Dynamic ARP Inspection

```
ip arp inspection vlan 10,20,30

interface FastEthernet0/1
 ip arp inspection trust  # Trusted interface
```

Beneficios de seguridad en capa 2

Estas técnicas proporcionan una defensa completa contra los ataques más comunes en la capa de acceso, como la suplantación de identidad, el envenenamiento ARP y la interceptación DHCP.

Certificaciones Profesionales - Roadmap Técnico

01

Entry Level

CompTIA Network+ (N10-008):

- Comprensión profunda del modelo OSI
- Fundamentos TCP/IP
- Conceptos básicos de routing/switching
- Fundamentos de seguridad de red
- Metodología de troubleshooting

MikroTik MTCNA:

- Dominio de RouterOS CLI
- Routing/switching básico
- Configuración de firewall
- Conceptos básicos de wireless

02

Professional Level

Cisco CCNA (200-301):

- Fundamentos de redes
- Acceso a red (VLANs, STP)
- Conectividad IP (routing)
- Servicios IP (DHCP, NAT, ACL)
- Fundamentos de seguridad
- Automatización y programabilidad

MikroTik MTCRE:

- Routing avanzado (OSPF, BGP)
- Implementación MPLS
- Firewall avanzado

Demanda del mercado (Argentina 2024)

CCNA: $80K-120K ARS/mes | MTCNA+MTCRE: $70K-100K ARS/mes | CompTIA Network+: $60K-80K ARS/mes