Capa de Red

Juegos en Red - Grado en Desarrollo de Videojuegos

Ruben Rodríguez
ruben.rodriguez@urjc.es
URJC

Natalia Madrueño
natalia.madrueno@urjc.es
URJC

2025-09-09

Universidad Rey Juan Carlos

DSLAB
DATA SCIENCE LABORATORY

Tabla de contenidos

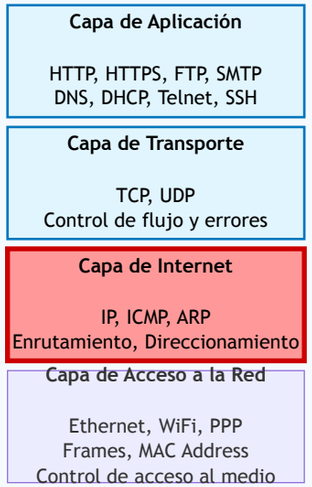
Introducción

¿Qué es la Capa de Red?

> La Capa de Red es el **tercer nivel del modelo TCP/IP** y forma el núcleo del sistema de comunicaciones de Internet

Función principal:

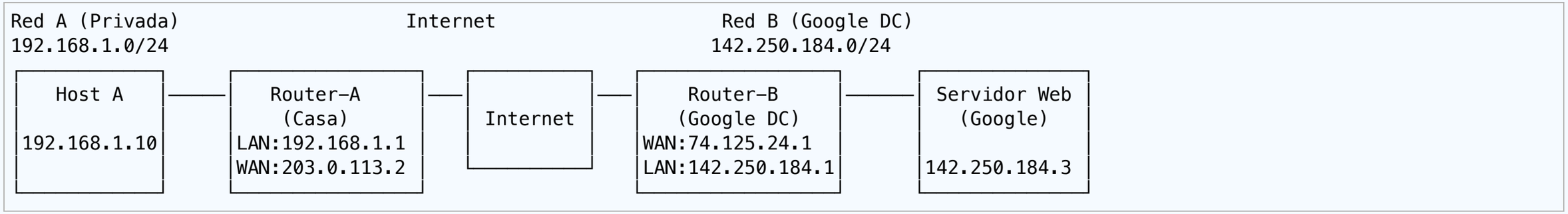
- Proporcionar comunicación end-to-end entre dispositivos
- Potencialmente separados por múltiples redes intermedias
- Independiente de la tecnología subyacente

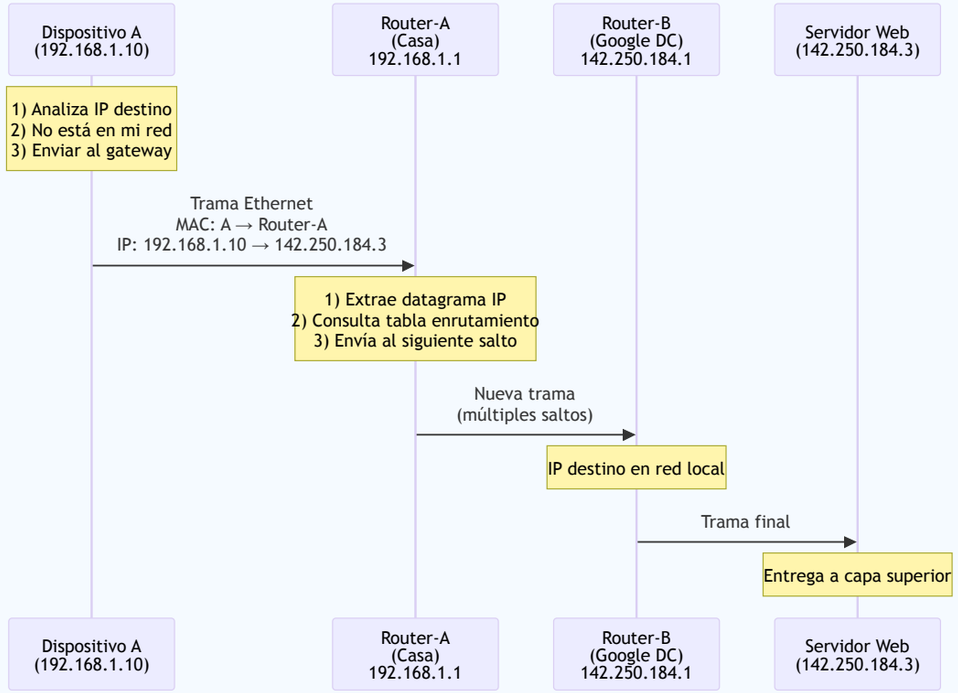


Importante

La comunicación funciona de igual forma independientemente del medio físico utilizado

Ejemplo Simplificado: Host A → Servidor Google





Funciones Fundamentales

Enrutamiento vs Reenvío

Enrutamiento

Proceso global que determina rutas óptimas

- Considera toda la topología de red
- Tiempo: segundos a minutos
- Algoritmos: RIP, OSPF, BGP
- Genera tabla de enrutamiento completa

Reenvío

Proceso local de mover paquetes

- Puerto entrada → puerto salida
- Tiempo: microsegundos
- Implementado en hardware
- Usa tabla de reenvío optimizada

> **Tip**
>
> Los algoritmos de enrutamiento generan la tabla de enrutamiento → se traduce en tabla de reenvío con next-hop

Responsabilidades por Dispositivo

Host Emisor

- Recibe segmentos de TCP/UDP
- Encapsula en datagramas IP
- Fragmenta si excede MTU
- Determina si destino es local o remoto

Routers Intermedios

- Examinan cabecera IP (dirección destino)
- Consultan tabla de enrutamiento
- Determinan siguiente salto
- Reenvían por interfaz correspondiente

Host Receptor

- Reensambla fragmentos
- Verifica integridad (checksum)
- Extrae segmentos
- Entrega a capa de transporte

Modelos de Servicio

Redes de Circuitos Virtuales

Funcionamiento en 3 fases:

1. **Establecimiento:** SETUP, reserva recursos
2. **Transferencia:** Usa VC ID, ruta fija
3. **Terminación:** TEARDOWN, libera recursos

Ventajas:

- QoS predecible
- Overhead reducido (solo VC ID)
- Orden garantizado

Desventajas:

- Complejidad alta
- Mantiene estado por conexión
- Rigidez ante cambios

Tecnologías: ATM, Frame Relay, X.25, MPLS

Redes de Datagramas

Características:

- Cada paquete tratado independientemente
- Sin estado de conexión en routers
- Dirección destino completa en cada paquete
- Diferentes rutas posibles por paquete

Ventajas:

- Simplicidad de diseño
- Robustez ante fallos
- Flexibilidad y balanceo de carga
- Escalabilidad superior

Limitaciones:

- Sin garantías QoS
- Posible desorden de paquetes
- Servicio best-effort

Importante

Fundamento de Internet por su adaptabilidad a condiciones cambiantes

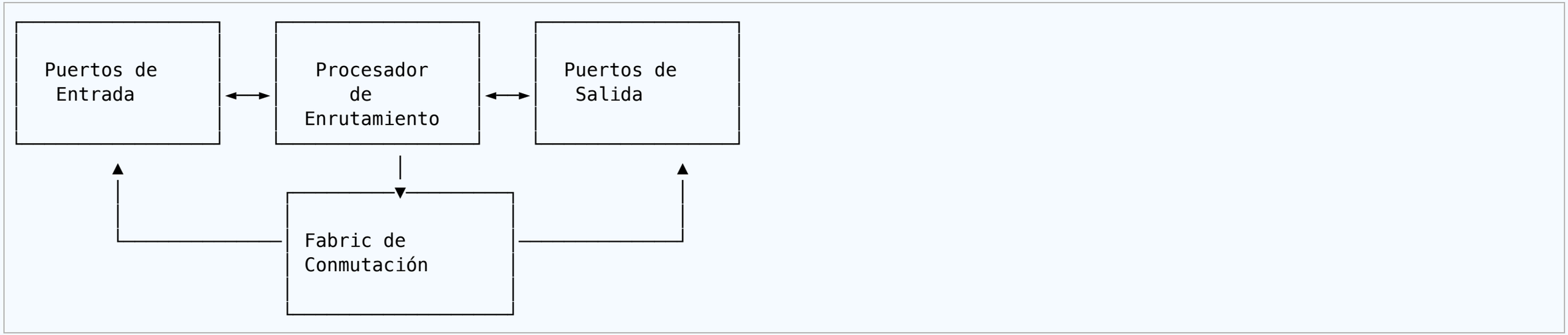
Circuitos Virtuales vs Datagramas

Aspecto	Circuitos Virtuales	Datagramas
Establecimiento	Requerido	No requerido
Estado en routers	Sí, por conexión	No
Direccionamiento	VC ID	IP completa
Enrutamiento	Ruta fija	Por paquete
QoS	Garantías posibles	Best effort
Recuperación fallos	Difícil	Automática
Escalabilidad	Limitada	Alta

Internet usa el modelo de **datagramas** por su simplicidad, robustez y escalabilidad

Dispositivos de Capa de Red

Arquitectura del Router



Plano de Control:

- Ejecuta enrutamiento (software)
- Genera tablas de enrutamiento

Plano de Datos:

- Ejecuta reenvío (hardware)
- Puertos entrada/salida + fabric

Proceso de Reenvío de Paquetes

1. **Recepción:** Llega paquete, se procesa capa enlace, se extrae datagrama IP
2. **Verificación:** Checksum de cabecera, TTL > 0
3. **Decisión:** Extrae IP destino, aplica longest prefix matching
4. **Modificación:** Decrementa TTL, recalcula checksum
5. **Resolución:** ARP si necesario para MAC siguiente salto
6. **Encapsulación:** Nueva trama según protocolo salida
7. **Transmisión:** Envío por interfaz física

> ⚠ **Advertencia**
>
> Si TTL llega a 0 → descarta paquete y envía ICMP “Time Exceeded”

Switches Layer 3

Un switch Ethernet (L3) que combina switching de alta velocidad por hardware (ASICs) con capacidades básicas de enrutamiento IP para redes LAN.

Aspecto	Router Tradicional	Switch L3
Reenvío	Software/ASIC	Hardware puro
Latencia	Microsegundos	Nanosegundos
Throughput	Limitado por CPU	Wire-speed
Flexibilidad	Alta	Limitada

Los switches L3 combinan la velocidad del switching con las capacidades del routing. Útiles en redes locales.

Protocolo

Protocolo IP

Características fundamentales:

- **Sin conexión:** No requiere establecimiento previo
- **No confiable:** No garantiza entrega, orden, o integridad
- **Best effort:** Hace el “mejor esfuerzo” por entregar paquetes
- **Independiente del medio:** Funciona sobre cualquier tecnología de enlace

Responsabilidades principales:

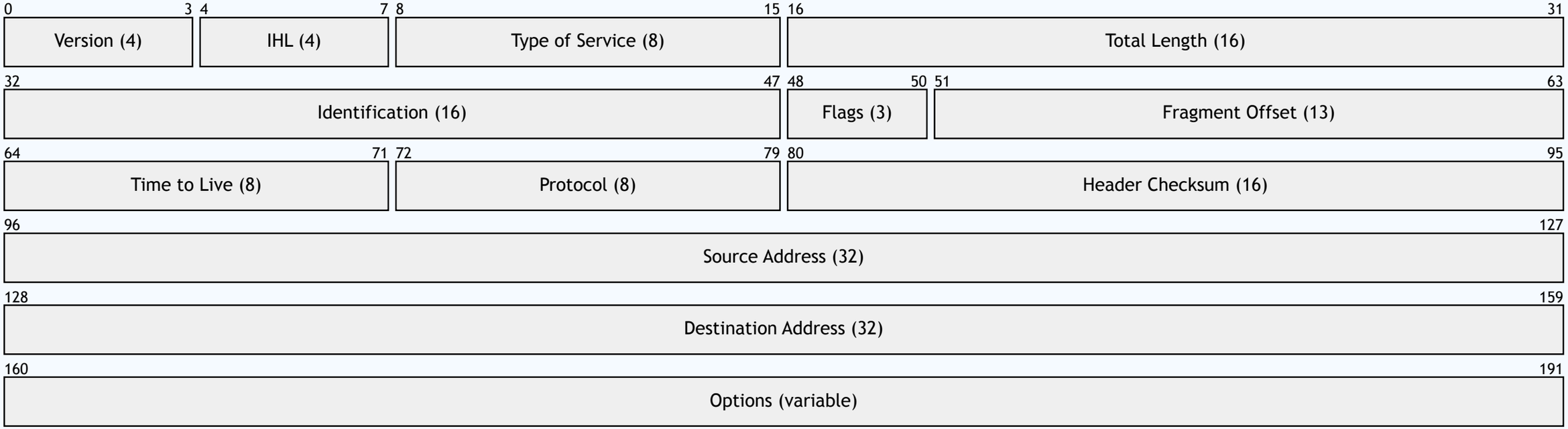
- Define estructura de datagramas
- Establece sistema de direccionamiento
- Mecanismos básicos de entrega
- Fragmentación y reensamblado
- Control de vida del paquete (TTL)

Importante

IP NO garantiza: Entrega, orden entre datagramas diferentes, ni detección de duplicados. Estas funciones se delegan a capas superiores (TCP).

Versiones: IPv4 (32 bits, diseñado años 70) e IPv6 (128 bits, soluciona limitaciones IPv4)

IPv4: Estructura Básica



IPv4 Header Format

- Source address y Destination address para identificación de hosts
- Protocol para identificar el protocolo de la capa superior
- Checksum para integridad de datos.

IPv4: Direccionamiento

Formato: 32 bits (4 octetos)

Ejemplo: 192.168.1.1 con máscara 255.255.255.0 (/24)

- Parte azul: **Red**
- Parte roja: **Host**
- Total direcciones: $2^{32} \approx 4.3$ mil millones

Obtención dirección de red:

```
192.168.1.1 AND 255.255.255.0 = 192.168.1.0
```

> **Tip**
>
> La división red/host permite enrutamiento jerárquico eficiente

Sistema de Clases (Histórico)

Clase	Rango	Bits Red	Bits Host	Redes	Hosts/Red	Uso
A	0.0.0.0 - 127.255.255.255	7	24	126	16,777,214	ISPs, gobiernos
B	128.0.0.0 - 191.255.255.255	14	16	16,384	65,534	Universidades
C	192.0.0.0 - 223.255.255.255	21	8	2,097,152	254	Empresas pequeñas

⚠ **Advertencia**

Problema: Organización con 1,000 hosts

- Clase B: desperdicia 64,534 direcciones (98.5%)
- Clase C: insuficiente

CIDR: Solución Moderna

Classless Inter-Domain Routing

Notación: 192.168.1.0/**24** → 24 bits para red

Ventajas:

- Asignación flexible (cualquier potencia de 2)
- Utilización: 20-30% → 95-98%
- Agregación de rutas eficiente

Longest Prefix Matching

Seleccionamos en nuestra tabla de rutas aquella con la coincidencia **mas grande**.

Tabla con rutas:

- 192.168.0.0/16
- 192.168.1.0/24 ← **Seleccionada**
- 192.168.1.128/25

Direcciones Especiales

Direcciones Reservadas

Dirección	Propósito	Descripción
0.0.0.0/32	Este host	Sin IP configurada (DHCP)
127.0.0.0/8	Loopback	Pruebas locales (127.0.0.1)
255.255.255.255/32	Limited broadcast	Solo red local
x.x.x.0	Dirección de red	Identifica la red
x.x.x.255	Directed broadcast	Broadcast a red específica

Rangos Privados (RFC 1918)

- **10.0.0.0/8** → 16.7 millones hosts (grandes organizaciones)
- **172.16.0.0/12** → 1 millón hosts (empresas medianas)
- **192.168.0.0/16** → 65,000 hosts (hogares/oficinas)

No enrutables en Internet público → Requieren NAT

Direcciones Especiales (Práctica)

- Broadcast: Cuando queremos enviar un paquete a todos los dispositivos de la red local. Ejemplo: 192.168.1.255 (para red 192.168.1.0/24)

```
ifconfig
ipconfig /all en windows
```

- Gateway: Dirección del router que conecta nuestra red local con otras redes/Internet. Ejemplo: 192.168.1.1 (típicamente la primera IP utilizable de la red)

```
route -n get default (macOS/Linux)
ip route show default (Linux)
ipconfig /all (Windows)
```

Fragmentación

MTU (Maximum Transmission Unit)

Tecnología	MTU (bytes)
Ethernet	1500
Token Ring	4464
FDDI	4352
PPP	Variable (~1500)

Proceso:

1. Si datagrama > MTU → fragmentar
2. Enviar fragmentos por separado
3. Reensamblar en destino
4. IP preserva integridad del datagrama original

Importante

IP garantiza orden dentro del datagrama, NO entre datagramas diferentes

IPv6: La Evolución

Motivación

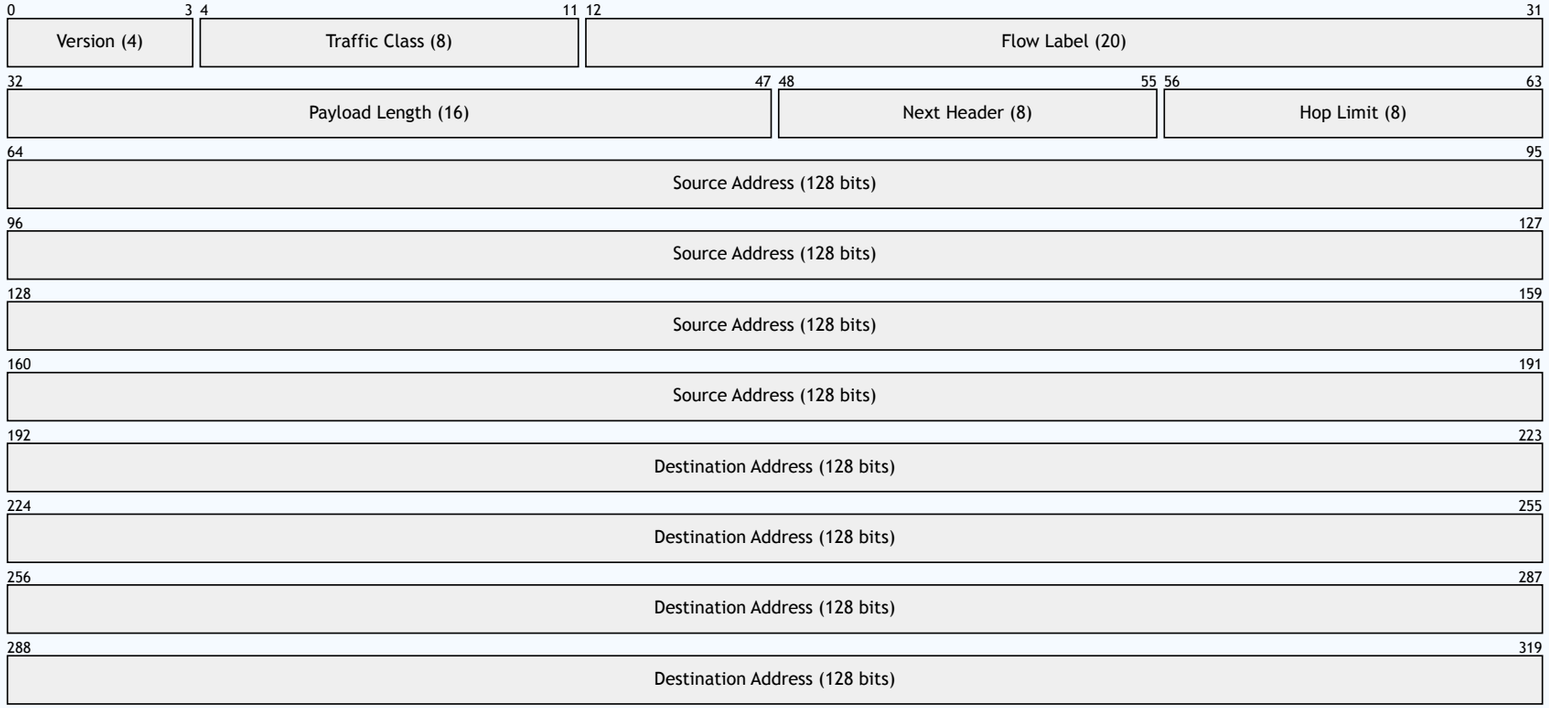
Limitaciones IPv4:

- Agotamiento de direcciones (4.3×10^9)
- Fragmentación ineficiente en routers
- Sin autoconfiguración
- Seguridad opcional (IPSec)
- QoS limitado

Características IPv6

- **Direcciones:** 128 bits (3.4×10^{38} direcciones)
- **Cabecera:** Fija 40 bytes
- **Sin checksum** en cabecera
- **IPSec obligatorio**
- **Autoconfiguración SLAAC**
- **Mejor QoS** (Traffic Class, Flow Label)

Cabecera IPv6



- Migración gradual IPv4 → IPv6 mediante mecanismos de interoperabilidad
- Las direcciones IP ahora ocupan el doble de tamaño
- Se elimina el checksum
- El siguiente protocolo es ahora “Next Header”

Protocolos Complementarios

ICMP: Control y Diagnóstico

Internet Control Message Protocol

Características:

- Complementario a IP
- Usa IP para transporte
- No orientado a conexión
- Implementación obligatoria (en IPv6)

Tipos de Mensajes

Mensajes de Error:

Mensajes de Consulta:

- Echo Request/Reply (Type 8/0)
- Timestamp Request/Reply (Type 13/14)

ICMP: Herramientas de Diagnóstico

Ping - Verificación de Conectividad

```
$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=55 time=15.1 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=55 time=14.9 ms
```

Echo Request (Type 8) → Echo Reply (Type 0)

Traceroute - Descubrimiento de Ruta

```
$ traceroute google.com
 1  192.168.1.1 (192.168.1.1)  3.414 ms
 2  100.70.0.1 (100.70.0.1)  5.245 ms
 3  10.14.0.53 (10.14.0.53)  7.091 ms
 4  * * *
 5  72.14.195.182 (72.14.195.182)  4.665 ms
```

Incrementa TTL progresivamente → Time Exceeded (Type 11)

NAT: Network Address Translation

Problema y Solución

Problema:

- Agotamiento direcciones IPv4
- Múltiples dispositivos, una IP pública

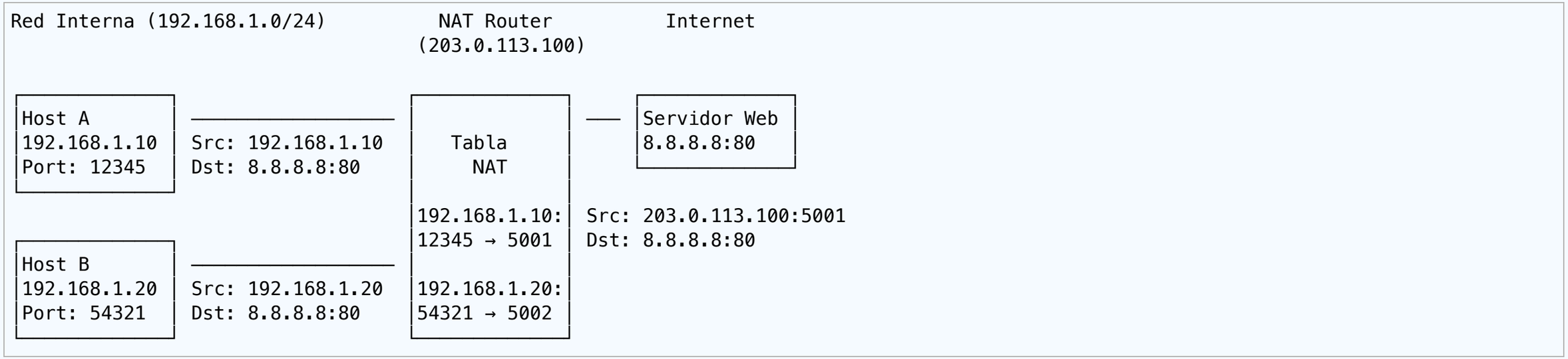
Solución NAT:

- Usa direcciones privadas internamente
- Traduce a IP pública en router
- Mantiene tabla de traducción

Funcionamiento:

1. Host interno inicia conexión
2. Router reemplaza IP:puerto origen
3. Registra en tabla NAT
4. Respuesta llega a router
5. Consulta tabla y reenvía internamente

NAT: Ejemplo Práctico



- Traducción de direcciones: El router NAT convierte las IP privadas a su IP pública
- Mapeo de puertos: Asigna puertos únicos externos (5001, 5002) a cada host interno para distinguir las conexiones simultáneas en la tabla NAT
- Enmascaramiento de red interna: Permite que múltiples dispositivos privados compartan una sola IP pública

NAT: Limitaciones y Soluciones

Limitaciones

- No permite conexiones entrantes directas
- Complicaciones con protocolos que embeben IPs
- Pérdida del principio end-to-end

Técnicas para Atravesar NAT

Hole Punching:

- Ambos conectan simultáneamente
- Crea “agujeros” temporales

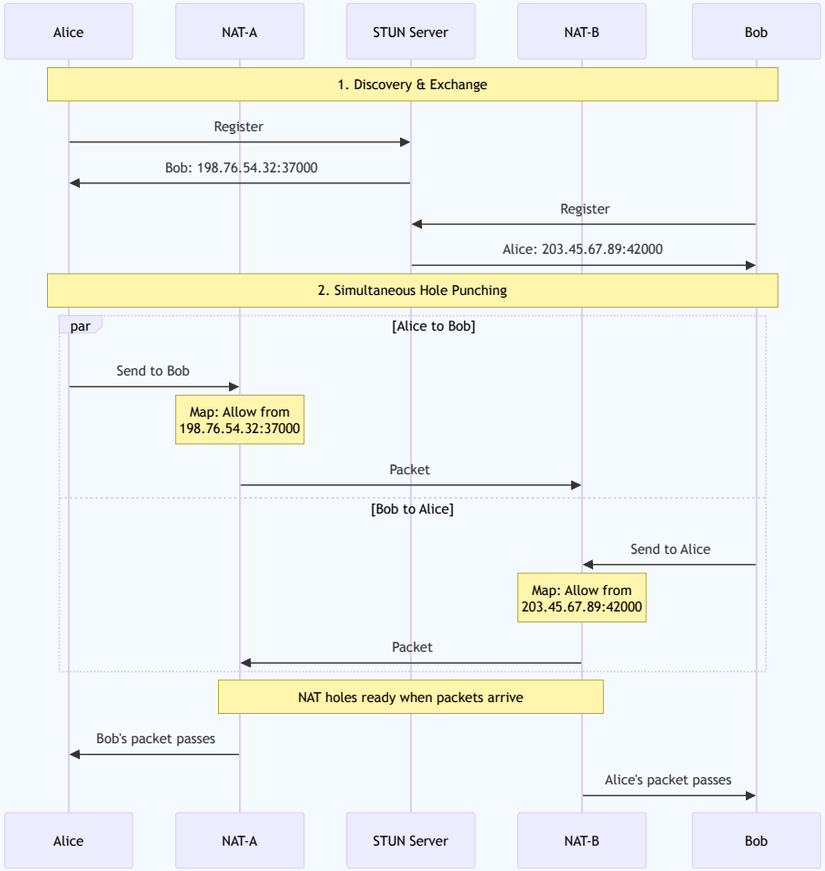
STUN:

TURN:

- Servidor relay intermedio
- Más confiable pero más recursos

UPnP:

Hole punching



- Descubrimiento: servidor STUN para obtener sus IPs/puertos
- Envío simultáneo: Envían paquetes UDP al **mismo tiemp** -> mappings en sus NATs
- Agujeros listos: Los mappings NAT se crean **ANTES** de recibir

Resumen

Puntos Clave

- La **Capa de Red** proporciona comunicación end-to-end entre dispositivos en diferentes redes
- **Dos funciones principales:** Enrutamiento (global) y Reenvío (local)
- **Modelos de servicio:** Circuitos Virtuales vs Datagramas (Internet usa datagramas)
- **IPv4:** 32 bits, sistema de clases → CIDR para eficiencia
- **IPv6:** 128 bits, soluciona limitaciones de IPv4
- **ICMP:** Herramientas de diagnóstico (ping, traceroute)
- **NAT:** Permite compartir IP pública, pero limita conectividad directa
- **MTU:** Define tamaño máximo, fragmentación si se excede
- Los **routers** operan con plano de control (enrutamiento) y plano de datos (reenvío)