Redes Tema 4. Capa de red

Martín González Dios

8 de noviembre de 2024

1. Introducción

Lleva los **paquetes** del **host origen** (acepta un paquete de la capa de transporte, lo encapsula en un datagrama y lo entrega a la capa de enlace) al **host destino** (desencapsula el datagrama y entrega el segmento a la capa de transporte). Está **implementada en sistemas finales y routers** (tienen capas de transporte y aplicación para control).

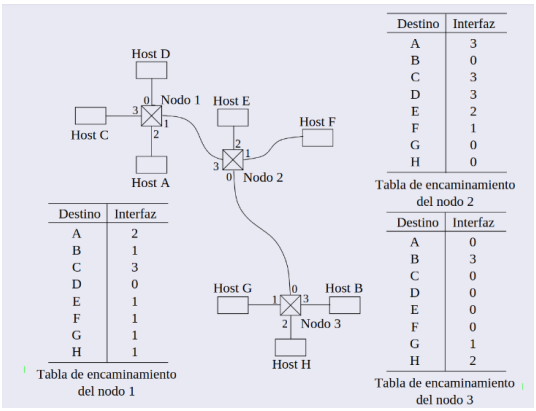
- **Reenvío(forwarding)**: al llegar un paquete al router, lo hace pasar a la interfaz de salida apropiada según la tabla de reenvío y la información en la cabecera del paquete (dirección destino y etiqueta).
- **Encaminamiento/Rutado (routing)**: determina la ruta que debe seguir un paquete mediante algoritmos de encaminamiento (intentan obtener la mejor ruta y determinar valores de las tablas).
- **Tablas de envío**: almacenan la información necesaria para el reenvío de paquetes. Asigna el valor del campo de la cabecera a la interfaz de salida apropiada.

La capa de red busca **encaminar los paquetes, realizar los reenvíos, controlar errores** (suma de comprobación de la cabecera, protocolo ICMP), **controlar el flujo, controlar la congestión, controlar la calidad de servicio (QoS) y controlar la seguridad**.

2. Redes de conmutación de paquetes

- **Redes de datagramas**: cada paquete incluye en la cabecera la IP destino. En el reenvío el router examina la cabecera y lo coloca en la salida más apropiada según la tabla de reenvío. **No mantiene información de estado**, cada paquete se encamina de forma independiente.
  La capa de red en internet **es de datagrama no fiable** (servicio de mejor esfuerzo). Permite interred (tecnologías distintas).

- **Redes de circuitos virtuales**: se establece la **conexión planificando la ruta** (circuito virtual, CV) **al destino**. A cada paquete se le escribe el identificador de CV que usan los routers para el reenvío. **Estos routers sí que mantienen información de estado** (tabla de circuitos virtuales).
  En una tabla de circuitos virtuales cada nodo tiene una tabla de encaminamiento con interfaz de entrada del CV, VCI (identificador del circuito virtual) e interfaz de salida por la que los paquetes de ese circuito dejan el nodo e identificador de salida del CV. Un paquete que llega por una interfaz con un VCI se coloca en la interfaz indicada en la tabla con el nuevo VCI.



Destino	Interfaz
A	2
B	1
C	3
D	0
E	1
F	1
G	1
H	1

Tabla de encaminamiento del nodo 1

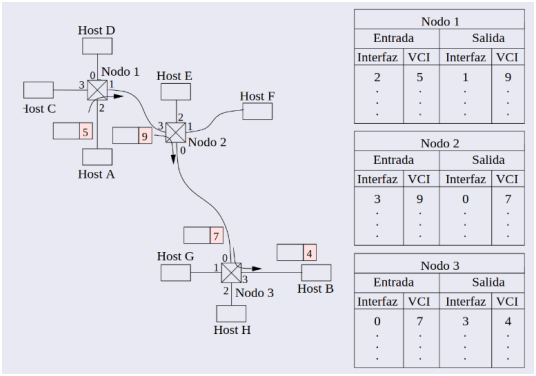
Destino	Interfaz
A	3
B	0
C	3
D	3
E	2
F	1
G	0
H	0

Tabla de encaminamiento del nodo 2

Destino	Interfaz
A	0
B	3
C	0
D	0
E	0
F	0
G	1
H	2

Tabla de encaminamiento del nodo 3

Figura 1: Red de datagramas



Nodo 1			
Entrada		Salida	
Interfaz	VCI	Interfaz	VCI
2	5	1	9

Nodo 2			
Entrada		Salida	
Interfaz	VCI	Interfaz	VCI
3	9	0	7

Nodo 3			
Entrada		Salida	
Interfaz	VCI	Interfaz	VCI
0	7	3	4

Figura 2: Redes de circuitos virtuales

3. Algoritmos de encaminamiento

Son los encargados de encontrar el **camino mínimo entre origen y destino**. Cada host está conectado a un router (router por defecto) y el problema se limita a encontrar el **camino mínimo entre routers teniendo en cuenta el coste** (equivalente grafos).

Los algoritmos pueden ser **globales**, **de estado de los enlaces** (cada nodo tiene la información de todos los nodos y el coste de los enlaces con lo que puede calcular su tabla de encaminamiento) o pueden ser **descentralizados**, **de vector de distancias** (el cálculo de los caminos mínimos se hace entre todos los nodos, intercambiando información con los vecinos, solo conocen la distancia a los demás nodos y por dónde empezar).

Por otro lado los algoritmos también **pueden ser estáticos** (solo cambian al cambiar la topología de red o se modifican parámetros) o **dinámicos** (se ejecutan periódicamente) y **sensibles** (el coste de los enlaces varía dinámicamente, por lo que pueden quedar mensajes atrapados en ciclos) o **insensibles a la carga**.
*En Internet son dinámicos e insensibles a la carga.

- **Algoritmo de Dijkastra** (estado de los enlaces): busca el **camino más corto entre 2 vértices de un grafo pesado**. Es una variante del algoritmo forward search. Es cuadrático, con estabilización rápida, respuesta rápida a cambios de topología o fallos de nodos, pero tiene problemas de escalabilidad.
  El **nodo N quiere calcular su tabla de routing a partir de los LSP** (link state packet) que ha recibido. Cada **nodo tiene 2 listas**: **Confirmado y Provisional**, los elementos de estas indican el coste para alcanzar un nodo y el siguiente salto: **(M, 5, L) → N alcanza M a coste 5 a través de L**.
  Se inicializa la tabla Confirmado con una entrada para N a coste 0 (N, 0, -) y **se repite** lo siguiente:

  1. Para el último nodo añadido a Confirmado (nodo S) se examina su LSP
  2. Para cada vecino (V) de S, se calcula el coste (Coste) para alcanzar V como la suma del coste de N a S y de S a V.
     - Si V no está en ninguna lista, se añade a la lista Provisional de la forma (V, Cost, SigSalto)
     - Si V está en Provisional, y Coste es menor que el indicado, se reemplaza por (V, Cost, SigSalto)
  3. Si Provisional está vacía, acaba; si no pasa la entrada de Provisional con menor coste a Confirmado
  4. Volver al paso 1

- **Encaminamiento de vector de distancia**: es un algoritmo descentralizado donde **todos los nodos colaboran**. Inicialmente los nodos solo conocen el coste a sus vecinos, pero **iterativamente comunican la información que tienen hasta que las actualizaciones convergen**. El intercambio de actualizaciones puede hacerse periódicamente o al cambiar la tabla de un nodo o el coste de un enlace (si disminuye se actualiza rápido, si aumenta surgen problemas).
  Este algoritmo **puede necesitar muchas iteraciones**, más que uno de estado de los enlaces, y es **menos robusto**, ya que si un nodo calcula mal sus distancias se lo pasará a todos los nodos.

- **Sistemas autónomos** (SA): son regiones en que se dividen las redes grandes como Internet. Las operan empresas u organismos.
  Los routers pasarela de frontera centralizan el tráfico de salida del SA, dentro del mismo los routers solo conocen el encaminamiento dentro de su región. Este **encaminamiento** puede ser **intradominio** (cada SA elige su algoritmo) o **interdominio** (algoritmo común para todos los SA).

4. Encaminamiento en Internet

En Internet se usan protocolos de encaminamiento como **RIP y OSPF (intradominio) o BGP (interdominio)**.

Categoría	Protocolo	Tipo	Protocolos transporte/red
intra-autónomo	RIP	VD	UDP/IP (puerto 520)
	OSPF	EE	propio/IP (puerto 89)
inter-autónomo	BGP	VD	TCP/IP (puerto 179)

Figura 3: Protocolos de capa aplicación para mandar mensaje entre routers

- **RIP (Routing Information Protocol)**: protocolo intradominio de VD(Vector de Distancias) que manda a los nodos vecinos mensajes RIP de petición (solicitan información) y respuesta (lista de hasta 25 redes internas al SA). Se **actualizan cada 30s** y si en 180s un router no actualiza se considera caído.
  Utiliza el conteo de saltos para determinar la distancia de la red. El coste de los enlaces (salto a otro router) es 1, y la distancia máxima es 15 (si no se considera inalcanzable).

- **OSPF (Open Shortest Path First)**: protocolo abierto (algoritmo libre) intradominio de EE (Estado de los Enlaces) más avanzado que RIP. **Los mensajes OSPF se mandan a todos los nodos al producirse cambios y cada 30 mins**, teniendo todos los routers información completa del SA. Manda mensajes HELLO a cada vecino para comprobar el enlace y puede interrogar a un vecino para obtener toda la información. El coste de los mensajes los pone el administrador.
  Es seguro, ya que **implementa un protocolo de transporte propio** con todos los mensajes autentificados y considerando solo los routers autentificados. Guarda caminos de mismo coste para repartir el tráfico y permite subdividir los SA en áreas (**soporte de jerarquía**). Cada área ejecuta OSPF sobre los routers de ese área y entre áreas se comunican mediante routers de frontera de área (igual que SA) que se interconectan en un área troncal.

- **BGP (Border Gateway Protocol)**: **protocolo interdominio similar a VD** (intercambia rutas completas) que comunica routers pasarela de frontera y permite que cada SA use el protocolo intradominio que desee. La **comunicación** puede ser **entre routers BGP vecinos** (pares BGP, E-BGP) **o entre routers del mismo SA** (vecinos lógicos, I-BGP). Cada SA tiene un identificador único y los administradores pueden decidir las políticas de encaminamiento.

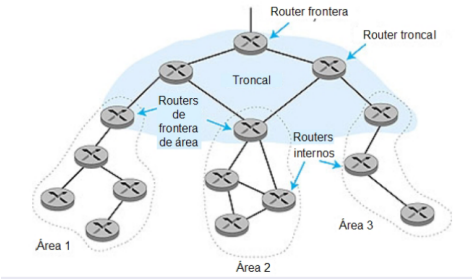


Figura 4: OSPF jerárquico

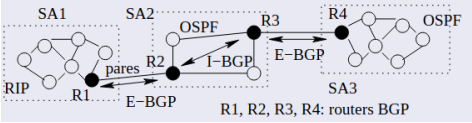


Figura 5: BGP (Protocolo de pasarela de frontera)

5. Protocolo de Internet (IP)

Protocolo **basado en datagramas (sin conexión)** cuya fiabilidad recae en capas superiores (TCP).
Está diseñado para interconectar redes diferentes.
Los componentes de la capa de red en Internet son el **protocolo de red IP** (define el formato de las direcciones, de los datagramas y las acciones de los routers según los campos de los datagramas), el **protocolo de encaminamiento** y el **protocolo de mensajes de control de Internet** (ICMP).
Los nodos en una red tienen una dirección IP por interfaz (unión de un host o router con un enlace).
En IPv4 cada IP se codifica con 4 bytes escritos generalmente en decimal y se dividen en clases.
*Un campo de red o de host no puede estar todo a 0 o 1.

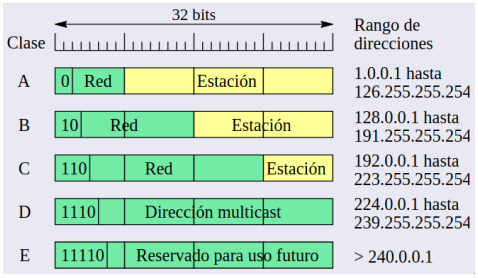


Figura 6: BGP (Direccionamiento IPv4)

Hay **direcciones reservadas**:

- Número de red y resto a 0 → Identificador de red
- Número de red y resto a 1 → Dirección de broadcast
- 0.0.0.0 → Esta red. Para arrancar sistemas sin disco. (protocolo DHCP y encaminamiento por defecto).
- 127.0.0.0 – 127.255.255.255 → Dir. propia, loopback.
- 240.0.0.0 – 255.255.255.254 → Uso futuro.
- 255.255.255.255 → Difusión para toda la red (DHCP).

El número de estaciones en una red puede ser muy grande para administrar, por lo que **se divide en subredes** que se gestionan de independientes pero que actúan como 1 para el exterior.
Usamos **parte del campo estación para indicar la subred y máscaras** (máscara de n bits: 32 bits de los que los n más significativos están a 1 y el resto a 0) para delimitarla.

193.168.17.133/27 (C) → 11000001.10101000.00010001.10000101
24 bits red, 3 bits subred (subred 3), 5 bits estación (estación 5).

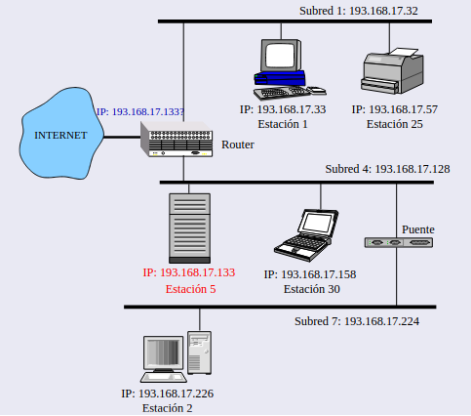


Figura 7: Esquema de red con subredes

En 1993 se suprimen las clases y **se adopta CIDR** (Classless Inter-Domain Routing) en el cual se añade a la IP un sufijo /s donde s bits indican la red y 32-s bits la estación.
193.168.64.0/18 → 11000001.10101000.10101101.11111101 → Estación 11773 Red 193.168.128.0
Dentro de una red se pueden establecer subredes. (Las rutas similares pueden agruparse para simplificar la tabla de enrutamiento)

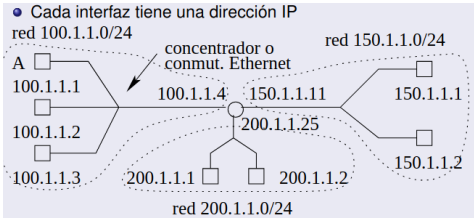


Figura 8: Redes conectadas a un router

Cada interfaz tiene una dirección IP

Tabla de rutas del host A			
destino	interfaz	gateway	métrica
100.1.1.0/24	eth0 (=100.1.1.1)	*	0
150.1.1.0/24	eth0 (=100.1.1.1)	100.1.1.4	1
200.1.1.0/24	eth0 (=100.1.1.1)	100.1.1.4	1

Tabla de rutas del router			
destino	interfaz	gateway	métrica
100.1.1.0/24	eth0 (=100.1.1.4)	*	0
150.1.1.0/24	eth1 (=150.1.1.11)	*	0
200.1.1.0/24	eth2 (=200.1.1.25)	*	0

Figura 9: Redes conectadas a un router

El router elige la entrada con el prefijo con más bits en común con la dirección del paquete.
Las redes pueden especificar un tamaño máximo de datagrama IP que puede enviarse en una trama **(MTU, maximun transmission unit)**, cuando un datagrama lo supera debe fragmentarse.
Hay 2 niveles de numeración: no de datagrama y desplazamiento dentro del mismo (bytes enviados/8).

- Bit MF: a 1 indica que hay más fragmentos detrás.
- Bit NF: indica que el datagrama no debe fragmentarse.

El reensamblado se realiza en el sistema destino.

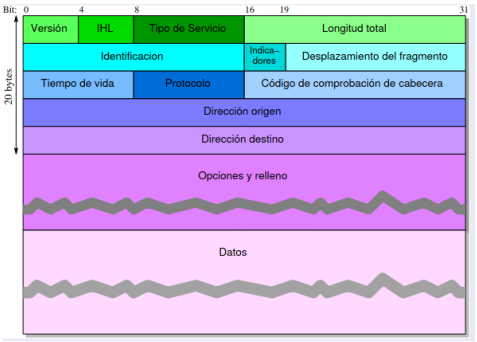


Figura 10: Formato del datagrama IP

En IPv4 hay varios problemas de seguridad:

- **Rastreo de paquetes (packet sniffing)**: ataque pasivo en el que se recolectan paquetes de una red, se evitan cifrando.
- **Spoofing**: suplantación de identidad (IP falsa). Se evita con mecanismos de autenticación del origen.
- **Modificación de paquetes**: se soluciona usando mecanismos de integridad de datos.

Para solucionarlo existe **IPSec**, que se usa con IP y crea un servicio orientado a conexión entre 2 entidades proporcionando una definición de algoritmos y claves, cifrado de paquetes, integridad de los datos y autenticación del origen.

La capacidad de direccionamiento de IPv4 tiene un límite, su seguridad debía mejorarse y se necesitaba simplificar el protocolo para que los encaminadores fueran más eficientes. Por todo esto apareció **IPv6**, con **direcciones de 128 bits, sin clases, envío multicast, servicios en tiempo real y servicios de autenticación y seguridad**.

Se representa con 8 campos de 16 bits que se pueden compactar si hay cadenas de 0s.
47CD:0000:0000:0000:0000:0000:A456:0124 ↔ 47CD::A456:0124
Al igual que IPv4 tiene máscaras para dividir red y host y direcciones unicast, multicast y anycast.

La cabecera IPv6 son **40 bytes en 8 campos**. Elimina la longitud de cabecera, las opciones (indicadas en cabeceras adicionales), la fragmentación (si un datagrama es muy grande devuelve un mensaje ICMP), la numeración de paquetes y la suma de comprobación (queda en la capa de transporte y enlace).

Añade la clase de tráfico (8 bits) y la etiqueta de flujo (20 bits) relacionados con la QoS.
La transición IPv4 a IPv6 debe ser gradual, **coexistiendo ambas con túneles** (tunneling: encapsular cuando los paquetes deban pasar por routers que no soporten IPv6, añadiendo cabeceras IPv4 y eliminándolas cuando no sean necesarias).

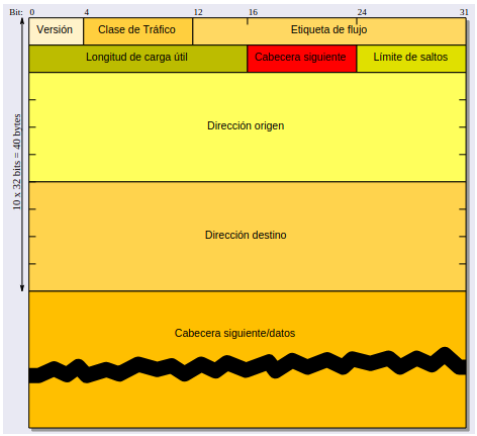


Figura 11: Formato del datagrama IPv6

Cabe mencionar la existencia de las **VPN (redes privadas virtuales)**, que son redes de una organización que usan la red pública para comunicarse de forma segura. Emplean sistemas de encriptación y autenticación. (IPSec o túneles IP)

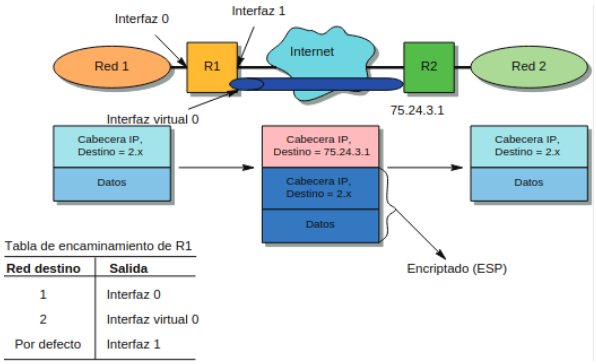


Figura 12: Túneles IP

6. ICMP (Internet Control Messages Protocol)

Protocolo para que **hosts y routers puedan informarse sobre el estado de la red o errores**. Funciona sobre IP pero no garantiza su entrega. Se encapsula en un datagrama IP.

Los mensajes ICMP **especifican el tipo y código (motivo) del mensaje**.

Los **mensajes de error** informan al origen de errores durante el procesamiento. En el campo datos se incluye la cabecera del datagrama original y los 8 primeros bytes de datos de ese datagrama. Los errores pueden ser destino inalcanzable (tipo 3, códigos 0-15), silenciar origen (tipo 4), redirección (tipo 5), tiempo excedido (tipo 11) o problema de parámetros (tipo 12).

Los **mensajes de consulta** sondean la actividad de routers y hosts, obtiene el RTT entre dispositivos, averigua si los relojes están sincronizados, envía pares de mensajes petición respuesta de eco (tipos 8 y 0) y de marca de tiempo (tipos 13 y 14) y mensajes declarados obsoletos por el IETF.

7. DHCP (Dynamic Host Configuration Protocol)

Asigna direcciones IP a los hosts estáticamente (por el administrador) **o dinámicamente** (con DHCP, solicita una IP temporal cada vez que se inicia). Además permite obtener información para un host como su IP, el gateway por defecto o los servidores DNS disponibles.
Al descubrir un servidor DHCP se manda un mensaje DHCPDISCOVER con la IP destino (broadcast) y origen. El DHCP ofrece su servicio (respuesta con una IP, máscara de red, ...) y el tiempo de concesión. El cliente solicita un servicio con la petición DHCP y el servidor la confirma con el ACK DHCP.

8. NAT (Network Adress Translation)

Traduce direcciones de red permitiendo usar la misma IP en varios ordenadores. Las direcciones sin conexión a Internet son especiales para uso en redes privadas y los routers de Internet ignoran los paquetes con estas IPs.
Un servidor NAT **necesita 2 interfaces y 2 IPs**, una IP válida para conectar al exterior y otra para conectar a la red interna. Los ordenadores de la red privada tendrán como gateway la IP privada del servidor NAT y este cambia la IP privada y puerto origen de los paquetes internos por la IP del NAT y un puerto libre.
En una **tabla almacena IP origen, puerto origen y puerto usado** (por el que sabe a qué máquina enviar la respuesta). (Todo esto puede combinarse fácilmente con filtrado de paquetes)

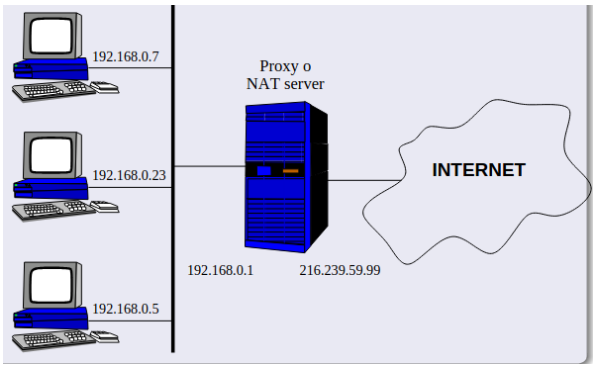


Figura 13: Traducción de direcciones de red