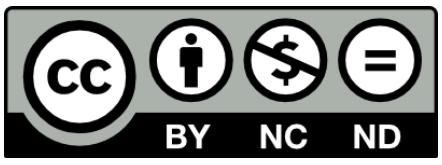
Fundamentos de Redes

Los Del DGIIM, losdeldgiim.github.io

Doble Grado en Ingeniería Informática y Matemáticas
Universidad de Granada



Fundamentos de Redes

Los Del DGIIM, losdeldgiim.github.io

Irina Kuzyshyn Basarab
José Juan Urrutia Milán
Arturo Olivares Martos

Granada, 2023-2024

Índice general

Siglas **5**

1. Introducción a los fundamentos de redes **9**
1.1. Sistemas de comunicación y redes 9
1.1.1. Motivación para usar redes 10
1.1.2. Topologías de redes 11
1.1.3. Clasificación de redes 12
1.1.4. Nomenclatura típica en figuras (Iconos) 12
1.2. Diseño y estandarización de redes 13
1.2.1. Modelo OSI vs TCP/IP 14
1.3. Terminología, conceptos y servicios 15
1.3.1. Retardos en la comunicación 17
1.3.2. Tipos de servicios 18
1.4. Internet: topología y direccionamiento 18
1.4.1. Organización topológica 19
1.4.2. Red Iris 19
1.4.3. Direccionamiento por capas 19

2. Capa de red **21**
2.1. Funcionalidades 21
2.2. Conmutación 22
2.2.1. Conmutación de circuitos 22
2.2.2. Conmutación de paquetes 23
2.2.3. Conmutación con circuitos virtuales 23
2.3. El protocolo IP 24
2.3.1. Direccionamiento 25
2.3.2. Network Address Translation (NAT) 28
2.3.3. Encaminamiento 32
2.3.4. Protocolos de intercambio de información de encaminamiento 35
2.3.5. Cabecera IP 37
2.3.6. Fragmentación 39
2.4. Asociación con la capa de enlace: Address Resolution Protocol (ARP) 42
2.4.1. Cabecera ARP 43
2.5. El protocolo ICMP 44
2.5.1. Paquete ICMP 44
2.6. Autoconfiguración de la capa de red (DHCP) 45

3. Capa de transporte **47**
3.1. Introducción . . . 47
3.2. Protocolo de datagrama de usuario (UDP) . . . 48
3.2.1. Cabeceras UDP . . . 48
3.2.2. Multiplexación/demultiplexación . . . 49
3.3. Protocolo de control de transmisión (TCP) . . . 49
3.3.1. Cabecera TCP . . . 50
3.3.2. Multiplexación/demultiplexación . . . 51
3.3.3. Control de conexión . . . 51
3.3.4. Control de errores . . . 54
3.3.5. Control de flujo . . . 56
3.3.6. Control de congestión . . . 56
3.4. Extensiones TCP . . . 58

4. Seguridad en redes **59**
4.1. Introducción . . . 59
4.2. Cifrado . . . 61
4.2.1. Cifrado simétrico . . . 61
4.2.2. Cifrado asimétrico . . . 62
4.3. Autenticación . . . 64
4.3.1. Reto-respuesta . . . 64
4.3.2. Intercambio de Diffie-Hellman . . . 65
4.4. Funciones Hash . . . 66
4.4.1. Ataque por Extensión . . . 67
4.5. Firma digital y certificados digitales . . . 68
4.5.1. Firma digital con clave secreta. *Big Brother*. . . . 68
4.5.2. Firma digital con clave asimétrica. Doble cifrado . . . 69
4.6. Protocolos seguros . . . 70
4.6.1. Seguridad en la Capa de Aplicación. PGP. . . . 71
4.6.2. Seguridad en la Capa de Sesión. SSL y TLS. . . . 72
4.6.3. Seguridad en la Capa de Red. IPSec. . . . 74

5. Relaciones de Problemas **75**
5.1. Introducción . . . 75
5.2. Capa de red . . . 82

Siglas

ACK Acknowledgment. 81,

APDU Application Paquet Data Unit.

ARP Address Resolution Protocol. 3, 21, 42, 43,

ARQ Automatic Repeat Request.

AS Autonomous System. 35, 36,

ATM Asyncronous Transfer Mode. 21, 24,

BGP Border Gateway Protocol. 36,

BOOTP Bootstrap Protocol. 43,

CDN Content Delivery Network.

CSMA/CA Carrier Sense Multiple Access / Collision Avoidance. 12,

CSMA/CD Carrier Sense Multiple Access / Collision Detection. 11,

DDoS Distributed Denial of Service. 60,

DES Data Encryption Standard. 62,

DF Don't Fragment. 38,

DHCP Dynamic Host Configuration Protocol. 3, 43, 45, 46,

DNAT Destination NAT. 29, 31, 32,

DNS Domain Name System. 19, 45,

EGP Exterior Gateway Protocol. 36,

FNMT Fábrica Nacional de Moneda y Timbre. 70,

FTTH Fiber to the home.

HMAC Hash-based MAC. 66, 68,

HTTP Hypertext Transfer Protocol. 30–32,

HTTPS HTTP Secure. 72,

IANA Internet Assigned Numbers Authority. 28,

ICANN Internet Corporation for Assigned Names and Numbers. 28,

ICMP Internet Control Message Protocol. 3, 21, 34, 44, 45, 77,

IDEA International Data Encryption Algorithm. 62, 71,

IDS Intrusion Detection System. 70,

IETF Internet Engineering Task Force. 15,

IGMP Internet Group Management Protocol. 26,

IGP Interior Gateway Protocol. 35,

IMAP Internet Message Access Protocol.

IMAPS IMAP Secure. 72,

IP Internet Protocol. 3, 19, 21, 23–25, 37, 39, 43–45, 74,

IPSec IP Security. 4, 59, 71, 74,

IPv4 IP versión 4. 24, 27, 28, 37, 43,

IPv6 IP versión 6. 24, 28, 37,

IRS Intrusion Response System. 70,

ISN Initial Sequence Number. 52,

ISO International Organization for Standardization. 15,

ISP Internet Service Provider. 19, 77,

LAN Local Area Network. 12, 13,

LLC Logical Link Control. 14, 75,

MAC Media Access Control. 14, 19, 42, 43,

MAC Message Authentication Code. 66, 75,

MAN Metropolitan Area Network. 12,

MD5 Message Digest Algorithm 5. 66, 67, 71,

MF More Fragments. 38,

MSL Maximum Segment Lifetime.

MTU Maximum Transfer Unit. 24, 39, 40,

NAT Network Address Translation. 3, 13, 28, 29, 78,

NOS Network Operating System. 9, 21,

OSI Open System Interconnection. 9, 14, 15, 21, 71, 75,

OSPF Open Shortest Path First. 34, 35, 37,

PAN Personal Area Network. 12,

PAP Password Authentication Protocol. 64,

PDU Protocol Data Unit. 15, 16, 28, 47, 76,

PGP Pretty Good Privacy. 4, 71,

POP Post Office Protocol. 72,

PPP Point to Point Protocol.

QoS Quality of Service.

RARP Reverse ARP. 43,

RFC Request for Comments. 18,

RIP Routing Information Protocol. 34–37,

RSA Rivest, Shamir y Adleman. 63,

RTT Round Trip Time. 55, 57, 58,

SAP Service Access Point. 16, 39,

SDU Service Data Unit. 15, 16, 23, 42, 44, 47, 76,

SHA-1 Secure Hash Algorithm 1. 67,

SNAPT Source Network Address and Port Translation.

SNAT Source NAT. 29, 30, 32,

SNOC Service No Oriented to Connection. 18,

SOC Service Oriented to Connection. 18,

SSH Secure Shell. 71,

SSL Secure Sockets Layer. 4, 71–73,

STP Spanning Tree Protocol. 11,

TCP Transmission Control Protocol. 16, 18, 47, 73,

TFTP Trivial File Transport Protocol.

TLS Transport Layer Security. 4, 59, 71–73,

TPDU Transmission Paquet Data Unit. 48,

TS/TOS Tipe of Service.

TTL Time To Live. 38, 39, 44, 45, 77,

UDP User Datagram Protocol. 16, 18, 36, 45, 47,

VLAN Virtual LAN. 13,

VPN Virtual Private Network. 72,

WAN Wide Area Network. 12,

WLAN Wireless LAN. 79,

1. Introducción a los fundamentos de redes

Objetivos

- Conocer y comprender los principios básicos de las comunicaciones.
- Entender el diseño funiconal en capas de las redes y los conceptos y terminología fundamentales involucrados.
- Comprender desde un punto de vista teórico-conceptual el modelo de referencia OSI y su correspondencia con el modelo de capas usado en Internet.

Introducción

La arquitectura lógica de Internet está diseñada por capas. Veremos el modelo TCP/IP (aunque mencionaremos el modelo OSI):

Aplicación que hace uso de la red
Transporte **(TCP/UDP)**
Red **(IP)**
Enlace
Física

Tabla 1.1: Modelo de capas del protocolo TCP/IP.

Las dos últimas capas están implementadas en Hardware y las tres primeras en Software, también llamado Network Operating System (NOS). En la asignatura veremos las capas altas, las implementadas en software.

1.1. Sistemas de comunicación y redes

Definición 1.1 (Sistema de comunicación)**.** Es una infraestructura (hw + sw) que permite el intercambio de información. Un sistema típico es el siguiente:

- Tenemos una fuente y un transmisor en un mismo equipo (que es el que va a mandar la información). La fuente genera la información y el transmisor adapta la información al medio.
- Después tenemos el canal de comunicación, el cual produce errores: ruidos, interferencias, diafonías (cuando hay muchos cables en paralelo juntos, puede suceder que la información de un cable se meta en otro)...

- Al final tenemos un receptor y el destino (en un mismo equipo). El receptor adapta la información para el destino y éste espera los datos a recibir.

1.1.1. Motivación para usar redes

Para entender su uso hablaremos de la primera red de comunicaciones, que era una red de telefonía móvil. Cada usuario contaba con su línea de teléfono, que conectaba con una central de conmutación local, luego regional y luego nacional, la cual debía conectarse con la central local del destino. Se usaba conmutación de circuitos.

- Inicialmente se creaba un camino físico juntando cables, llamado circuito.
- Era ineficiente porque no se está hablando todo el tiempo, y los tiempos de silencio el circuito se desaprovecha.
- Era un problema de seguridad el mal funcionamiento de una central, pues dejaba a miles de teléfonos sin servicio.

Si ahora pensamos en ordenadores (o equipos más generales, móviles, PCs, portátiles, móviles...) en vez de móviles, y cambiamos las centrales de conmutación por routers, contamos con muchísimos caminos para conectar dos ordenadores, haciendo más segura la red.

En la actualidad ya no tenemos un camino físico, sino que son los routers quienes deciden por dónde enviar los paquetes y en qué momento. Estos tienen colas, lo que supone algo de retardo, pero tienen la ventaja de que se usa mucho mejor el canal y hay más seguridad, pues hay más de un camino.

Definición 1.2 (Red)**.** Sistema de comunicación con sistemas finales o terminales autónomos (con capacidad para procesar información) que facilita el intercambio eficaz y transparente de información. Concretamente tenemos:

- **Hosts:** sistemas finales o terminales autónomos. Son los que transmiten y reciben datos.
- **Subred:** infraestructura para el transporte de información, formada por líneas de transmisión y nodos o elementos de conmutación: routers y switches.

De una red esperamos:

- Autonomía.
- Interconexión.
- Intercambio de información con eficacia y transparencia.

En cuanto a medios de transmisión, originalmente se usaban cables de pares (pensados para transmitir 4 kHz, la media de la voz humana), luego cables coaxiales, que mejoraron mucho; y fibra óptica que puede transmitir sin interferencias, por lo que es el mejor medio guiado existente. Los cables trenzados son para distancias más cortas, Ethernet por ejemplo.

1.1.2. Topologías de redes

Dada una subred, su topología es el patrón de interconexión entre sus nodos. Las más relevantes las veremos a continuación.

En bus: Todos los nodos tienen acceso a un mismo medio, conocido como bus. Es la más sencilla, pero como el medio es común, todos intentan acceder y se producen colisiones.

En anillo: un círculo en el que tenemos los distintos nodos. Es similar al bus pues el medio es compartido. Una versión habitual es **token ring**, testigo de anillo, en el que se usa un testigo que se van pasando, de forma que así se evitan colisiones.

En estrella: todos están conectados a un centro principal, típicamente un switch.

A diferencia del bus, en este caso cada cable es independiente del resto. Si un PC pone algo en una toma el resto no lo escuchan. Cada línea tienen una cola para guardar a dónde enviar los paquetes y el switch tiene un procesador que coge los paquetes de dichas colas y los envían a las salidas. Es una topología mucho más segura por el hecho de no compartir el medio.

En árbol: típica en redes empresariales. Se suele estructurar en tres niveles:

- Primer nivel: red troncal.
- Segundo nivel: red de división.
- Tercer nivel: red de acceso.

Los equipos de primer y segundo nivel suelen ser switches.

Como potencial riesgo, pueden aparecer ciclos en el árbol. Ethernet no tiene ningún mecanismo para evitar que un paquete se mueva en círculo, lo que echaría la red abajo. El protocolo Spanning Tree Protocol (STP) elimina en cualquier topología los enlaces redundantes que formen bucles.

Mallada: todos los nodos están conectados entre sí por medios independientes.

Es muy fiable, ya que si se cae un enlace tienes más caminos para llegar a tu destino. No obstante, no es escalable, ya que si metemos un $n-$ésimo nodo hay que meter $n-1$ enlaces. Para redes pequeñas es de gran utilidad.

Dentro de una empresa, la red troncal puede seguir esta topología para evitar caídas importantes.

Híbrida: se usa una mezcla de todas. Es la más utilizada.

En cuanto a las topologías que comparten el medio, para evitar el ya mencionado problema de las colisiones, se usan los dos protocolos que veremos a continuación.

Definición 1.3 (CSMA/CD)**.** El protocolo Carrier Sense Multiple Access / Collision Detection (CSMA/CD) se encarga de detectar colisiones en topologías que comparten el medio, y dar error en caso de que se produzcan. Estas se detectan comprobando si lo que hay en el bus es lo que se acaba de poner.

Es el protocolo que usa Ethernet.

Definición 1.4 (CSMA/CA)**.** El protocolo Carrier Sense Multiple Access / Collision Avoidance (CSMA/CA) se encarga de evitar colisiones en topologías que comparten el medio. Para ello, primero escucha el medio y, si no hay ningún mensaje, envía el mensaje. Si no recibe confirmación, hay colisión.

Es el protocolo que usa Wi-Fi.

1.1.3. Clasificación de redes

Según tamaño y extensión:

- Personal Area Network (PAN): Red de área personal. Incluye todo lo que puede tener una persona: relojes, portátiles, cascos...
- Local Area Network (LAN): Red de área local. Abarca unas decenas de metros,suele ser un mismo edificio.
- Metropolitan Area Network (MAN): Red de área metropolitana. Se usa para conectar un campus o una ciudad.
- Wide Area Network (WAN).: Red de área extensa. Son redes desponibles en todo el país, como las redes telefónicas.

Según tecnología de transmisión:

- Difusión: lo que pone un nodo en el medio le llega a todos. Ejemplo de esto es un HUB.
- Punto a punto: Cada nodo solo está unido a otro. Ejemplo de esto es un switch.

Según el tipo de tranferencia de datos:

- Simple: solo transmite o recibe. Por ejemplo los TDT (para que una televisión analógica reciba señal digital).
- Half-duplex: transmite y recibe, pero no simultáneamente. Por ejemplo el Wi-Fi, aunque como cambia muy rápido no nos damos cuenta.
- Full-duplex: transmite y recibe simultáneamente. Por ejemplo, Ethernet.

1.1.4. Nomenclatura típica en figuras (Iconos)

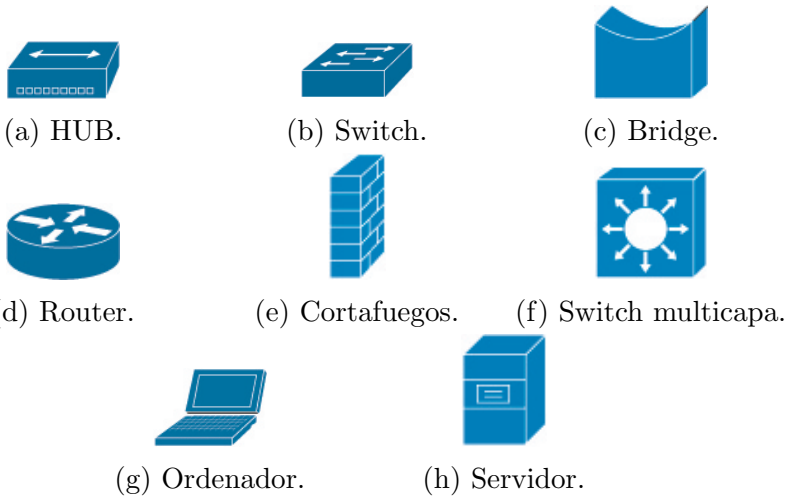
HUB: es un concentrador: permite centralizar los nodos de una red de computadoras. Se implementa mediante un bus.

Switch: tiene muchas bocas y conecta dispositivos dentro de la misma red LAN. Funciona en el nivel de enlace (nivel 2).

Bridge: funciona como un switch, pero uniendo tecnologías distintas. También funciona en el nivel de enlace.

Router: tiene pocas bocas, y se usa para conectar distintas redes.

Cortafuegos: bloquea el acceso no autorizado a una red, permitiendo tan solo el autorizado.



(a) HUB. (b) Switch. (c) Bridge.

(d) Router. (e) Cortafuegos. (f) Switch multicapa.

(g) Ordenador. (h) Servidor.

Figura 1.1: Iconos de los distintos elementos de una red.

NAT: dispotivo en el que se ejecuta el protocolo Network Address Translation (NAT), que permite que una red privada pueda acceder a Internet. Se explicará más adelante.

Switch multicapa: todas las bocas de un switch pertenecen a la misma LAN, pero esto a veces no nos interesa. Podemos hacer distintas redes virtuales (VLAN) dividiendo un mismo switch en varias redes, permitiéndonos esto conectar dos switches distintos dentro de la misma VLAN. Esto no nos permite movernos por distintas redes en el mismo switch, ya habría que pasar por un router al necesitar movernos a nivel de red para cambiar de red[1].

Esta es la funcionalidad que sí se puede hacer con un switch multicapa, no necesitar pasar por un router para cambiar de red.

Todos estos elementos los veremos representados en distintos esquemas para mostrarnos las topologías de las redes. Estos vendrán identificados por los símbolos de la Figura 1.1.

1.2. Diseño y estandarización de redes

La idea principal que se sigue al diseñar redes es solucionar los problemas en capas. Se estandarizan Modelos de Referencia (no son implementaciones, solo una referencia), en los que se definen las distintas capas y las funcionalidades de cada una. Los principios que se siguen son que las funcionalidades distintas tienen que estar en distintas capas y minimizar el flujo de información entre las capas.

A continuación detallamos las capas de los modelos de referencia más importantes, junto a las funcionalidades de cada una y los problemas que han de solventar.

Capa física: se encarga de transmitir los datos. Hay distintos tipos de codificaciones para enviar bits de información.

[1]No se verá en la asignatura.

Capa de enlace: se encarga de los mecanismos de acceso al medio. Si hay un medio común, antes de transmitir datos tiene que asegurarse de que ningún equipo está transmitiendo. Suele seguir dos protocolos:

- Media Access Control (MAC), control de acceso al medio.
- Logical Link Control (LLC), control de acceso lógico para las primeras retransmisiones. Si algún paquete llega mal, retransmite varias veces.

Capa de red: una vez llegado a este punto, se asume que no han habido colisiones en la comunicación. Esta capa se encarga principalmente de:

- El direccionamiento: saber dar una dirección y tener un identificador dentro de la red.
- El encaminamiento: saber cómo llegar al destino.

Capa de transporte: se encarga de recuperar los paquetes que en la capa de enlace no se ha podido. Es la capa encargada de la fiabilidad.

- Corrige errores.
- Gestiona la congestión de la red.
- Control de flujos: si hay un receptor más lento que el emisor, debe decirle al emisor que disminuya la velocidad de emisión, para adecuarse a la del receptor.

Además se encarga de la multiplexación de datos: mediante puertos (los veremos más adelante) le indica al SO a qué aplicación corresponde cada paquete.

Capa de aplicación: los clientes y los servidores deben buscar alguna forma de comunicarse.

Los dos modelos de referencia más importantes son el OSI y el TCP/IP, que describiremos a continuación.

1.2.1. Modelo OSI vs TCP/IP

Aplicación
Presentación
Sesión
Transporte
Red
Enlace
Física

Tabla 1.2: Modelo OSI.

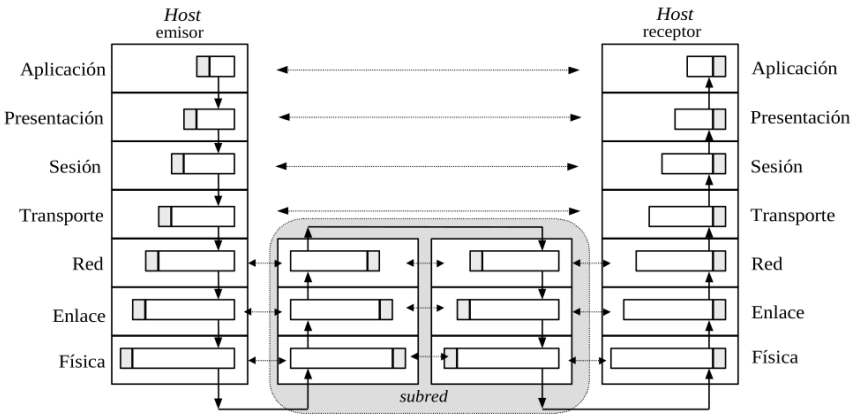


Figura 1.2: Comunicación real frente a comunicación virtual.

Aplicación
Transporte
Red
Red subyacente

Tabla 1.3: Modelo TCP/IP.

El modelo Open System Interconnection (OSI) fue propuesto por la ISO y el TCP/IP por el IETF. Las tres primeras capas del modelo OSI se corresponden con la capa de aplicación, y las dos última con la red subyacente, que es la parte física. Esta última en el modelo TCP/IP depende un poco de la tecnología está implementada de una forma u otra, pero la comunicación con la capa de red no puede variar, pues la capa de red si está estandarizada.

- Las capas físicas solo se encargan de hacer la primera conexión.
- La capa de red, salto a salto se encarga de llegar al destino, usando routers y sus tablas de encaminamiento.
- Una vez hecho el encaminamiento, las capas superiores son solo de los extremos, son los computadores de los extremos los que se comunican.
- Por tanto, los computadores tienen las 5 capas (en el caso de TCP/IP) y los routers solo las 3 más bajas.

1.3. Terminología, conceptos y servicios

En la Figura 1.2 vemos el camino que siguen los datos que le manda un emisor a un receptor. A la hora de emitir, cada capa recibe los datos de la capa superior, conocidos como Unidad de Datos de Servicio (Service Data Unit (SDU)), y le añade una cabecera, formando la Unidad de Datos de Paquete (Protocol Data Unit (PDU)). Decimos que los datos de la capa superior se han *encapsulado* en la capa inferior. Por tanto, cada capa envía el PDU a la capa inferior convirtiéndose en el SDU de la

capa inferior. La capa física, al no tener capa inferior, manda señales eléctricas en vez de bits.

Por otra parte, en la recepción, cada capa recibe de la inferior el PDU, al cual le quita la cabecera quedándose con el SDU. En función de la cabecera, se estudia qué ha de hacerse en cada capa y, posteriormente, se envía el SDU a la capa superior.

En función de la capa en la que nos encontremos, el SDU recibe un nombre distinto:

- Capa de enlace: trama.
- Capa de red: datagrama.
- Capa de transporte: depende del protocolo:
  - TCP: segmento.
  - UDP: datagrama.
- Capa de aplicación: mensaje.

La información que se envía desde un host a otro ha de pasar por todas las capas para llegar al destino, lo que se conoce como *comunicación real* o vertical, y viene representada en la Figura 1.2 por las flechas continuas. No obstante, y tan solo en sentido abstracto, decimos que nos capas del mismo tipo en distintos equipos hablan entre sí, lo que se conoce como *comunicación virtual* u horizontal, y viene representada en la Figura 1.2 por las flechas discontinuas. Esta comunicación virtual, como ya hemos mencionado, no es directa, sino que se realiza a través de recursos que nos proporcionan otras capas adyacentes.

Además de las definiciones que acabamos de dar, otros términos relevantes son los siguientes:

Entidad de nivel n: entidad que se encuentra en la capa $n-$ésima.

Entidades pares: entidades de la misma capa, que se comunican horizontalmente entre sí.

Protocolo: reglas que describen cómo han de comunicarse las entidades pares. En ellos, se especifican los paquetes que se mandan, etc.

Interfaz: a diferencia del protocolo, que se refiere a cómo se comunican las entidades pares, la interfaz se refiere a cómo se comunican las entidades de capas adyacentes.

Service Access Point (SAP): punto de acceso al servicio. Es un punto específico en la interfaz entre dos capas donde se proporciona un servicio.

Servicio: conjunto de funciones que una capa proporciona a la capa superior.

Capa proveedora/usuaria del servicio: en la comunicación vertical, la capa que proporciona el servicio es la proveedora, y la que lo usa es la usuaria.

Pila de protocolos: conjunto de protocolos que se usan en cada capa.

Arquitectura de red: modelo de referencia, junto a la pila de protocolos.

Otro concepto importante es el de *retardo*, que describireos a continuación.

1.3.1. Retardos en la comunicación

Supongamos que queremos transmitir un paquete entre dos equipos (terminales), por medio de otro, un router. Veamos los retardos que tenemos en la comunicación.

1. En primer lugar, hemos de considerar el **tiempo de transmisión**, que es el tiempo que se tarda en poner el paquete en el medio.

   Si el tamaño del paquete es de L Bytes y la velocidad de transmisión es de v_t bps, el tiempo de transmisión t_t es de:

   $$t_t = \frac{L \cdot 8}{v_t} \text{ s}$$

   La velocidad de transmisión depende exclusivamente de la tarjeta de red.

2. En segundo lugar, tenemos el **tiempo de propagación**, que es el tiempo desde que se escribe el último bit en el medio hasta que llega este último bit al siguiente equipo.

   Este tiempo depende de la distancia entre los equipos y de la velocidad de transmisión, que depende del medio. En el caso de una transmisión inalámbrica, la velocidad de transmisión es la velocidad de la luz, mientras que en una transmisión por cable suele ser de $^2/_3$ de la velocidad de la luz.

   Si la distancia entre los equipos es de d m y la velocidad de transmisión es de v_p $^{\text{m}}/_{\text{s}}$, el tiempo de propagación t_p es de:

   $$t_p = \frac{d}{v_p} \text{ s}$$

3. En tercer lugar, tenemos el tiempo que se encuentra en el equipo intermedio, en nuestro caso el router. Cuando el paquete llega al equipo intermedio, éste lo mete en una cola hasta que pueda procesarlo. El tiempo que el paquete está en la cola se conoce como **tiempo de cola**, y depende de la situación del equipo. Además, el equipo ha de procesar el paquete, lo que le lleva un tiempo conocido como **tiempo de procesamiento**, que suele ser del orden de milisegundos. Por último, y para poder continuar con la comunicación, el equipo ha de obtener acceso al medio, lo que le lleva un tiempo conocido como **tiempo de acceso al medio**.

   Por tanto, el tiempo que el paquete está en el equipo intermedio es la suma de estos tres tiempos.

4. Por último, la comunicación deberá continuar, por lo que se obtienen nuevos retardos de transmisión, propagación, etc. No obstante, en estos casos, estos no serán los mismos, pues la distancia entre equipos, tarjetas de red, etc., serán distintos.

1.3.2. Tipos de servicios

Relacionado con el nivel de transporte, hay dos clasificaciones importantes:

Según la conexión: En función de si, antes de enviar un paquete, se comprueba que el otro equipo esté encendido o no, tenemos dos tipos de servicios:

- Service Oriented to Connection (SOC): sí se comprueba.
- Service No Oriented to Connection (SNOC): no se comprueba.

Según la fiabilidad: En función de si se asegura que todo funcione bien o no, (por ejemplo, que todos los bits de un archivo estén bien), tenemos dos tipos de servicios:

- Fiable: se asegura de que todo funcione bien. Si algo falla, la conexión se termina.
- No fiable: no comprueba que todo funcione bien. La finalidad de estos protocolos es ser rápidos.

Para tener un protocolo fiable, contamos con los siguientes mecanismos:

- Control de conexión. Ser fiable implica ser orientado a conexión.
- Control de errores.
- Control de congestión. Hablamos de congestión cuando las colas de los routers se llenan y empiezan a descartar paquetes.
- Control de flujo.
- Entrega ordenada. Si se envían muchos paquetes, estos deben llegar en orden.

Algunos protocolos que estudiaremos más adelante:

- TCP es un servicio fiable, y por tanto orientado a conexión.
- UDP es un servicio no orientado a conexión, y por tanto no fiable.

1.4. Internet: topología y direccionamiento

Internet tiene dos aspectos importantes:

- Los protocolos de comunicación.
- Cómo se organiza Internet, el direccionamiento.

Todo esto se describe en las conocidas Request for Comments (RFC).

1.4.1. Organización topológica

Los operadores se establecen según la siguiente jerarquía:

- **Tier 3**: son los más cercanos a los usuarios. Ofrecen servicios de conectividad a empresas y particulares, y se conocen como Internet Service Provider (ISP). Algunos conocidos en España son Movistar, Vodafone, Orange...
- **Tier 2**: son de ámbito más regional. Necesitan pasar por una Tier 1 para llegar a toda Internet y ofrecen servicios de conectividad a operadores de Tier 3.
- **Tier 1**: son los que componen la estructura troncal de Internet. Están todos comunicados entre sí y están como mínimo en dos continentes.

Hay dos tipos de relaciones entre operadores:

- **Tránsito:** conexiones entre distintos tier. Por ejemplo un tier 3 paga a un tier superior para enviar datos.
- **Peering:** conexiones entre el mismo tier.

Antiguamente, para que un ISP de un país hablase con otro del mismo país había que ir hasta EEUU por falta de recursos. Más tarde se pusieron puntos neutros en cada país para comunicar operadores dentro de un mismo país.

1.4.2. Red Iris

La Red Iris la red española para investigación. Todas las universidades públicas y centros de investigación están conectados a ella.

La red se divide según autonomía (en Andalucía, se denomina Red RICA) y por otro lado tiene conexiones externas con la red científica europea.

1.4.3. Direccionamiento por capas

Según la capa en la que nos encontremos, hemos de realizar el direccionamiento de una forma u otra.

- Capa de Enlace: La dirección depende de la tarjeta de red. Las direcciones MAC son de la forma AA:BB:CC:DD:EE:FF, y son teóricamente únicas en todo el mundo. No obstante, en la realidad se ponen aleatorias para evitar seguimientos (puesto que si sabemos la dirección MAC de una tarjeta podemos hacer seguimiento de paquetes).
- Red: Se usan direcciones IP de la forma A.B.C.D. Las públicas son únicas en todo el mundo, las privadas no.
- Transporte: Direccionamiento a través de puertos, que identifican a qué proceso va un determinado paquete.
- Aplicación: Nombres de dominio mediante DNS.

2. Capa de red

En el presente tema, estudiaremos a fondo la capa de red. Recordemos que seguimos el Modelo TCP/IP descrito en la Tabla 1.1. Esta capa es la capa de más bajo nivel que pertenece al NOS, y será la primera estudiada en la asignatura.

Objetivos

- Comprender las funcionalidades y servicios de la capa de red.
  - Concepto de conmutación de paquetes y datagramas.
  - Direccionamiento en Internet.
  - Encaminamiento salto a salto.
  - Asociación con la capa de enlace a través del protocolo ARP.
  - Señalización de errores mediante el protocolo ICMP.

2.1. Funcionalidades

Funcionalidades y servicios TCP/IP:

- **Direccionamiento:** identificación de equipos dentro de la red.
- **Encaminamiento:** llegar salto a salto desde el origen al destino. Especifica el camino que deben seguir los paquetes.
- **Fragmentación:** las tarjetas suelen tener un tamaño máximo de paquete, y si queremos enviar un paquete más grande tenemos que fragmentarlo y, en el destino, ensamblarlo.
- **Conmutación.**
- **Interconexión de redes.**
- En OSI: **control de gestión.**

El protocolo que desarrollaremos en este tema es IP por ser el que en la actualidad se ha impuesto, aunque existen otros como ATM, x25...

2.2. Conmutación

Definición 2.1 (Conmutación)**.** Acción de establecer o determinar caminos de extremo a extremo que permitan transmitir información.

Uno de los primeros ejemplos claros de conmutación que se vio en la tecnología de las comunicaciones fue la conmutación de circuitos para la telefonía, que desarrollamos a continuación.

2.2.1. Conmutación de circuitos

Antiguamente existía una conmutación física de circuitos, muy usada en telefonía. De esta forma, hay muchos cables entre los usuarios y las centrales (uno por cada usuario), y menos cables entre cada par de centrales, ya que no todos los usuarios hablan al mismo tiempo.

La comunicación por conmutación de circuitos implica tres fases:

1. El establecimiento del circuito. Cada central une los cables que correspondan y se genera el camino.

2. La trasferencia de datos a través del circuito dedicado.

3. La desconexión del circuito, se libera el circuito para su reutilización.

Beneficios

- Recursos dedicados (tenemos un cable solo para nosotros), lo que facilita las comunicaciones a tiempo real y sin retardos.

- El recurso se mantiene dedicado toda la sesión.

- No hay competición por conseguir el medio.

- El circuito es fijo, no hay decisiones de encaminamiento una vez establecido.

- Simplicidad en la gestión de los nodos intermedios.

Desventajas

- Cuando un usuario no usa su cable no lo usa nadie más. Uso ineficiente de recursos.

- Hay establecimiento de llamada (para que todos los cables se toquen).

- Es poco tolerable a fallos, si algo no funciona, todo deja de funcionar.

2.2.2. Conmutación de paquetes

En la actualidad, no se envía una señal analógica; sino que, como sabemos, se envía el SDU junto con la cabecera. En la capa de red, vimos que el SDU se denomina *datagrama*, y veremos que este se ha de fragmentar en distontos bloques, a los que denominaremos *paquetes*. Por tanto, los paquetes son cada uno de los bloques de un datagrama, y es lo que se envía como tal por la red.

Observación. En general, cuando se quiera hacer referencia a un conjunto de datos que se envía por la red, sin especificar en qué capa nos encontramos, o sin ser más precisos, también usaremos el término de *paquete*.

A la hora de realizar la conmutación, hay dos formas de hacerlo, la conmutación mediante datagramas y la conmutación mediante circuitos virtuales.

Conmutación de datagramas

Las características de la conmutación de datagramas son:

- No hay establecimiento de conexión: enviamos un paquete y no sabemos si el otro extremo está encendido.
- El envío de los distintos paquetes se hace independientemente. El encaminamiento se hace paquete a paquete, por lo que se pueden seguir caminos distintos. Por este motivo, los paquetes pueden llegar desordenados, algo que controlarán otras capas.

  Además, si se produce fragmentación, no se ensamblarán los paquetes hasta que lleguen al destino, ya que distintos paquetes de un mismo datagrama pueden seguir distintos caminos.
- En cada nodo intermedio los paquetes que llegan se almacenan en una cola, y cuando sea posible se envían al próximo nodo.
- Como el encaminamiento se hace salto a salto, todos los paquetes han de tener la dirección de origen (para las respuestas o encaminamientos específicos, aunque esto no lo veremos en la asignatura) y de destino. A veces, para hacer difusiones de datos, nos puede interesar taner varias direcciones de destino.

Como el medio es común, los nodo de interconexión necesitan colas para poder gestionar los paquetes que le llegan. A la hora de esta conmutación, se hace el mejor esfuerzo, pero si algo falla la capa de red no se encarga de gestionar el fallo.

Un protocolo que lleve a cabo esta conmutación es IP, que desarrollaremos más adelante. Este es el tipo de conmutación que se usa mayoritariamente en la actualidad, y es en el que nos centraremos en la asignatura.

2.2.3. Conmutación con circuitos virtuales

En este caso, la conmutación difiere ligeramente de la conmutación por datagramas vista, siendo una mezcla entre la conmutación de circuitos y la de paquetes.

En este caso, para enviar un paquete de un origen a un destino, aunque haya distintos caminos posibles, se establece el camino desde el principio denominado

circuito (siguiendo la idea de la conmutación de circuitos). Este circuito no obstante es virtual, ya que los recursos no son dedicados completamente, sino que se reservan temporalmente pero se pueden reutilizar.

Cada router decide el camino que seguirá cada paquete, y los paquetes del mismo datagrama seguirán el mismo camino. Por tanto, el primer paquete en llegar al router reservará los recursos para los próximos paquetes.

- Hay que establecer conexión para averiguar la ruta a seguir.
- Si un router se cae, se cambia el camino.

Un protocolo que lleva a cabo esta conmutación es Asyncronous Transfer Mode (ATM), que estaba presente en el inicio de la telefonía digital.

2.3. El protocolo IP

El Internet Protocol (IP) es un protocolo para la interconexión de redes. Existen dos versiones:

- IPv4: Es la que se diseñó inicialmente, aunque tiene una limitación en la cantidad de direcciones.
- IPv6: Pasó de 32 a 128 bits, lo que supone una cantidad en la práctica ilimitada de direcciones.

En la actualidad la limitación de direcciones se empieza a notar, por lo que hay una transición gradual hacia IPv6, aunque sigue predominando IPv4. Desorrallaremos IPv4 en este tema, aunque mencionaremos algunas diferencias con IPv6.

Características de IPv4

- Resuelve el direccionamiento en Internet en la capa de red, ya que cada tarjeta de red tiene una dirección IP.
- Realiza el encaminamiento (o retransmisión) salto a salto entre equipos y routers.
- Ofrece un servicio no orientado a conexión y no fiable, ya que:
  - No hay establecimiento de conexión lógica entre las entidades.
  - No hay control de errores ni de flujos. Los errores que se produzcan tienen que arreglarlos una capa superior si se precisa.
- Gestiona la fragmentación para adaptarse al MTU de cada tarjeta de red, como veremos. A la unidad de datos completa se le llama datagrama y a los fragmentos paquetes.
- Es un protocolo de máximo esfuerzo, los datagramas se pueden perder, duplicar, retrasar, llegar desordenados...

2.3.1. Direccionamiento

Para identificar cada equipo en la red, se usan direcciones IP. El lector posiblemente esté más familiarizado con las direcciones red, como `www.google.com`, pero estas en realidad son nombres de dominio que se traducen a direcciones IP, como veremos en el Capítulo dedicado a la capa de aplicación. Mientras tanto, hemos de saber que todo equipo en la red tiene una dirección IP asociada. Además, esta (a priori) es única y no se puede repetir, lo que supone una limitación. Como más adelante veremos, para solventar este problema se usan también direcciones privadas, algo que no contemplaremos por el momento.

Una dirección IP consta de 32 bits y la nomenclatura usada es: `A.B.C.D` donde cada letra es un número decimal en el rango `0-255` (ya que codificará 8 bits). El rango por tanto que tenemos es `0.0.0.0-255.255.255.255.` Una dirección tiene dos partes bien diferenciadas, la que identifica la red y la que identifica el equipo en cuestión (en realidad, identifica la tarjeta de red).

Para saber qué parte de la dirección IP identifica el equipo y cuál la red, se emplea la máscara de red.

Definición 2.2 (Máscara de red)**.** Es un conjunto de 32 bits (al igual que una dirección IP) que se usa para identificar qué parte de la dirección IP identifica la red y cuál el equipo.Contiene los primeros n bits consecutivos a 1, y el resto a 0.

¿Cómo se usa la máscara?
Para saber cuál es la dirección de la red, se hace un `AND` lógico entre la dirección IP y la máscara (por lo que nos quedaremos con los primeros n bits de la dirección IP). El resto de bits identificará al equipo dentro de dicha red.

Notemos por tanto que, dentro de las posibles direcciones IP de una misma red, la dirección con todos los bits de equipo a 0 está *reservada* para la dirección de la red, y no podrá asignarse a ningún equipo.

Notación. Es común querer dar una dirección IP junto a su máscara de red. Para esto, se podrá usar la notación `A.B.C.D/n`, donde `A.B.C.D` es la dirección IP en sí y `n` es el número de bits a 1 de la máscara de red. Como ya hemos mencionado que estos bits han de estar al inicio y consecutivos, sabiendo el valor de `n` sabremos cuál es la máscara de red.

Ejemplo. Supongamos que tenemos una dirección IP `192.168.1.27/24`, y queremos saber cuál es la dirección de la red. Pasando a binario y haciendo un `AND`, tenemos:

	1100 0000 . 1010 1000 . 0000 0001 . 0001 1011	(dirección IP)
AND	1111 1111 . 1111 1111 . 1111 1111 . 0000 0000	(máscara de red)
	1100 0000 . 1010 1000 . 0000 0001 . 0000 0000	(dirección de la red)

Por tanto, pasando de nuevo a decimal, la dirección de la red es `192.168.1.0`.

Direccionamiento jerárquico

Internet usa direccionamiento jerárquico basado en clases. Cada clase contiene las direcciones IP de un rango determinado:

- Clase A → `0xx...x/8` ⟹ `0.0.0.0 - 127.255.255.255`. Tenemos $2^7 = 128$ redes con $2^{24} \approx 16 \cdot 10^6$ equipos en cada una.
- Clase B → `10xx...x/16` ⟹ `128.0.0.0 - 191.255.255.255`. Tenemos $2^{14} = 16384$ redes con $2^{16} = 65536$ equipos en cada una.
- Clase C → `110xx...x/24` ⟹ `192.0.0.0 - 223.255.255.255`. Tenemos $2^{21} \approx 2 \cdot 10^6$ de redes con $2^8 = 256$ equipos en cada una.
- Clase D → `1110xx...x` ⟹ `224.0.0.0 - 239.255.255.255`. No se usa para identificar equipos ni redes sino para multidifusión (*multicast*). Cada dirección identifica a todo un grupo de equipos. Para gestionar esto existe el protocolo IGMP para suscribirse a grupos.
- Clase E → `1111xx...x` ⟹ `240.0.0.0 - 255.255.255.255`. Es el rango experimental; es decir, las direcciones que se dejan para hacer pruebas.

Direcciones reservadas

Además de las restricciones de cada clase, hay determinadas direcciones que están reservadas y no se pueden asignar a ningún equipo. Algunas de estas direcciones son:

- Dirección de red: Cualquier dirección IP con todos los bits de equipo a 0. Está dedicada para identificar la red en sí.
- Dirección de difusión (*broadcast*): Cualquier dirección IP con todos los bits de equipo a 1. Se usa para enviar un paquete a todos los equipos de la red.

  Cuando se tiene que encontrar un equipo y no se sabe cuál, se manda por la dirección de difusión y lo escuchará quien tenga que escucharlo.
- `127.a.b.c`: Denominada dirección de *loopback*, *localhost* o *localloop*. Se usa para hacer pruebas, y es una conexión que hacemos a nuestra propia máquina. Originalmente (y la más común) era `127.0.0.1`, pero en la actualidad se ha aumentado el rango. Estas redes no requieren de una tarjeta de red específica, y su interfaz de red se denomina `lo`.

Llegados a este punto, podemos dar una definición más correcta de router, que ya habíamos mencionado anteriormente.

Definición 2.3 (Router)**.** Es un dispositivo de la capa de red cuya funcionalidad principal es conectar distintas redes y encaminar los paquetes a través de ellas.

Cuenta con varias tarjetas de red (también llamadas interfaces), una por cada red a la que se conecta, y cada una cuenta con una dirección IP asociada en cada red.

Como curiosidad, es posible crear routers en un ordenador con varias tarjetas de red con `Linux`. Con el comando `sysctl -a` podemos consultar el valor de la variable `net.ipv4.ip_forward`, que nos informa sobre si redirigimos paquetes o no. Si está con el valor 1, dicho equipo es un router.

Observación. Como un switch funciona a nivel de enlace, todo lo conectado a dicho switch está en la misma red. Por tanto, tampoco tiene dirección IP asignada.

Direccionamiento sin clases

Si usamos solo el direccionamiento con clases estaríamos desperdiciando muchísimas direcciones IP. Por ejemplo, si tenemos 1000 equipos ($2^8 < 1000 < 2^{16}$) tendríamos que usar una red de clase B, con la que desperdiciaríamos más de 60.000 direcciones. La solución a este problema es usar el direccionamiento sin clase, que nos permite usar la máscara de red deseada.

- **Subredes**

  Si, por ejemplo, queremos una red de menos de 256 equipos, podemos aumentar el número de bits de la máscara a 1, para conseguier más bits dedicados a identificar la red y menos para identicar equipos. Cada vez que añadimos un bit a la máscara, estamos dividiendo una red en dos mitades.

  Ejemplo. Supongamos que queremos identificar 100 equipos dentro de una misma red. Contando además con la dirección de red y la de difusión, necesitamos 102 direcciones. Como $2^6 < 102 < 2^7$, necesitamos 7 bits para identificar a los equipos. Por tanto, la máscara a usar será `/25`.

- **Superredes**

  Si hacemos el procedimiento inverso, quitarle un bit a la máscara, duplicamos la cantidad de equipos que podemos direccionar. Por ejemplo, en `/23` estamos juntando dos redes de clase C.

  Ejemplo. Supongamos que queremos una red de 1000 equipos. Contando con la dirección de red y la de difusión, necesitamos 1002 direcciones. Como $2^9 < 1002 < 2^{10}$, necesitamos 10 bits para identificar a los equipos. Por tanto, la máscara a usar será `/22`.

Como vemos el funcionamiento es igual que en el direccionamiento con clase, pero reduce significativamente (aunque no elimina) el desperdicio de direcciones. A nivel práctico red, subred y superred no se diferencian, y nos referimos a todas ellas como redes.

Direcciones privadas

Como hemos venido mencionando en distintas ocasiones, la escasez de direcciones es un gran problema presente en IPv4, ya que tan solo hay 2^{32} direcciones posibles, las cuales ya se agotaron en Noviembre de 2019. Aunque se vayan recopilando direcciones de sitios obsoletos, empresas desaparecidas, etc. el problema sigue existiendo.

Hay varias soluciones posibles para solventarlo.

- Direccionamiento sin clase: es una solucion que reduce el desperdicio de direcciones, peero aun así tiene la limitación de 2^{32} direcciones.

- IPv6, el cual usa 128 bits para las direcciones. La notación utilizada es

  `FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF`, en el que cada dígito es un número hexadecimal.

  En total hay 2^{128} direcciones posibles (más de 10^{37}), lo que en la práctica las hace ilimitadas. Aunque sea compatible con IPv4, la transición está siendo lenta.

- Direcciones privadas: esta es la principal solución que se usa en la actualidad, ya que hace el número de direcciones prácticamente ilimitado. Desarrollaremos este concepto a continuación.

Direcciones públicas: Cada dirección se asigna a un único dispositivo en todo Internet. Se asignan centralizadamente[1], y como son limitadas, hay que pagar por cada una.

Direcciones privadas: Solo se pueden usar en redes privadas o *intranets*, sin acceso directo al resto de Internet. Por tanto, al no ser accesibles desde fuera, se pueden repetir en distintas redes privadas, lo que aumenta el número de direcciones disponibles.

Para poder comunicarse con el resto de Internet (ya que si no tendrían poca utilidad), será necesario una dirección pública por la cual se haga la comunicación. Para esto se usa el NAT, que veremos más adelante.

Respecto al direccionamiento jerárquico con clases, dentro de cada clase se definen algunos rangos de direcciones a usar como IP privadas. Estos rangos son:

- Clase A → `10.x.y.z/8`
- Clase B → `172.16-32.y.z/16`
- Clase C → `192.168.y.z/24`

2.3.2. Network Address Translation (NAT)

Como hemos mencionado anteriormente, para que una red privada pueda comunicarse con el resto de Internet, es necesario que haya una dirección pública que haga de intermediario. Para esto se usa la técnica de NAT, que posibilita la traducción de direcciones. Al encontramos en la capa de red, el PDU contiene la cabecera IP[2] que contiene, entre otros datos:

- Dirección IP origen (IPsrc) junto con el puerto origen (sport).
- Dirección IP destino (IPdest) junto con el puerto destino (dport).

[1] Inicialmente por IANA, actualmente por ICANN.

[2] En realidad, los puertos se encuentran en la cabecera de la capa de transporte; pero tras encapsularlo se puede acceder desde la capa de red.

El concepto de puerto lo veremos más adelante y desarrollaremos a fondo en la Capa de Transporte. Por el momento, tan solo es necesario saber que es un número que se asigna a cada proceso que se comunica en la red, y que se usa para saber a qué proceso enviar la respuesta.

Para posibilitar la traducción, se usa una tabla de direcciones a modo de "diccionario", tal y como introducimos a continuación.

Definición 2.4 (Tabla de traducciones)**.** La Tabla de Traducciones es una tabla que se guarda en la memoria de todo router que haga NAT. Por cada traducción que deba hacerse, se guarda una entrada en la tabla que relaciona la dirección IP y puerto originales con la dirección IP y puerto traducidos.

La tabla se va actualizando con cada nueva traducción, y cuenta con un temporizador (normalmente de 5 minutos) que borra las entradas que lleven un tiempo sin usarse. De esta forma, se evita que la tabla se sature y se libera memoria.

En el caso de que llegue una petición que ya esté en la tabla, se reutiliza la información de la tabla, sin crearse una nueva entrada.

Definición 2.5 (*Masquerading*)**.** Proceso de enmascaramiento que hace el router al traducir la dirección privada del equipo en su dirección pública.

Se "enmascara" la dirección privada, de forma que el servidor no sabe a qué equipo de la red privada está respondiendo.

Observación. El uso de NAT plantea un problema de seguridad. Un atacante, conociendo la IP pública del router, puede hacer un barrido de puertos y puede conseguir que algún paquete entre. En tal caso, el router le responderá, y el atacante sabrá que hay un equipo detrás de esa IP pública y puerto, por lo que podrá intentar atacar a ese equipo.

Para evitar esto, para cada traducción puede guardarse tanto las IP y puerto de origen y destino sin traducir, como las traducidas. De esta forma, si llega una petición que coincide con la IP y puerto origen, pero no con la IP y puerto destino, se descarta directamente. Esta técnica se denomina *NAT estricto*.

Hay dos tipos de NAT, en función de dónde y cuándo se haga la traducción.

Source NAT (SNAT): el origen de los datos está en una red privada. Por tanto, al enviarse se cambia la dirección IP de origen, y la traducción a la correcta (en la respuesta) se hará tras el encaminamiento (*postrouting*).

Destination NAT (DNAT): el origen de los datos está en la red pública. Por tanto, al recibir los datos se cambia la dirección IP de destino, y la traducción a la correcta (en la respuesta) se hará antes del encaminamiento (*prerouting*).

En este caso la tabla de traducciones del router que realiza DNAT ha de ser estática (la inserción debe ser a mano), ya que en otro caso el router no sabrá a donde redirigir las peticiones entrantes. Este proceso se denomina *port forwarding*.

Planteemos un primer ejemplo de SNAT, que nos ayudará a comprender cómo funciona esta técnica.

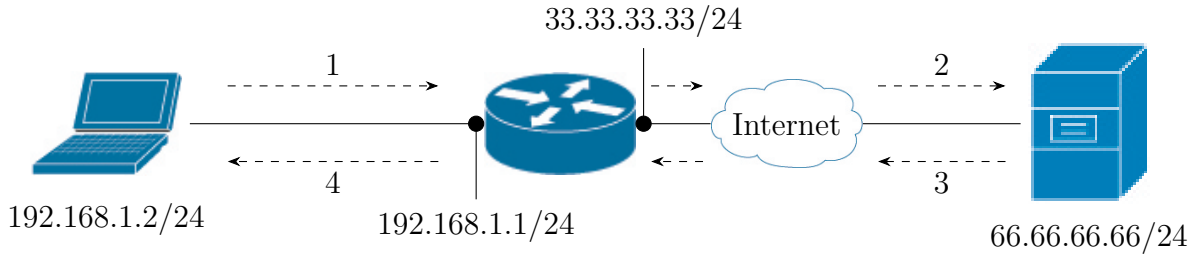


Figura 2.1: Ejemplo de red con SNAT.

Ejemplo. Supongamos la situación de la Figura 2.1, en la que un portátil dentro de una red privada quiere acceder a un servidor HTTP en Internet.

El equipo envía una petición al router (1), que este reenvía al servidor (2). El servidor responde al router (3), que a su vez reenvía la respuesta al equipo (4). Se trata de SNAT, ya que la petición parte de una red privada. Veamos qué ocurre en cada uno de los pasos:

(1) El ordenador envía una petición HTTP al router.

El puerto de origen, el cual asignará alteatoriamente el SO (ya se verá), pongamos que es el 1075. El puerto de destino, en el caso de HTTP, es el 80. Por tanto, la cabecera IP del paquete que envía el portátil al router contendrá:

- IPsrc:sport: `192.168.1.2:1075`.
- IPdest:dport: `66.66.66.66:80`.

(2) El router ha de realizar la traducción de direcciones, ya que la IP del portátil es privada y no puede ser usada en Internet. Para esto, modifica la cabecera IP poniendo como IP origen su propia IP pública, y como puerto origen un puerto que aún no haya sido usado (por ejemplo, 12345). La cabecera IP así:

- IPsrc:sport: `33.33.33.33:12345`.
- IPdest:dport: `66.66.66.66:80`.

La tabla de traducciones del router quedaria (donde notamos con "′" la traducida):

IPsrc	sport	IPsrc′	sport′
`192.168.1.2`	`1075`	`33.33.33.33`	`12345`

Tabla 2.1: Tabla de traducciones del router con SNAT.

Tras esta traducción, el router envía el paquete al servidor.

(3) Tras el procesamiento del paquete en el servidor, este envía la respuesta al router. La cabecera IP del paquete de respuesta contendrá:

- IPsrc:sport: `66.66.66.66:80`.
- IPdest:dport: `33.33.33.33:12345`.

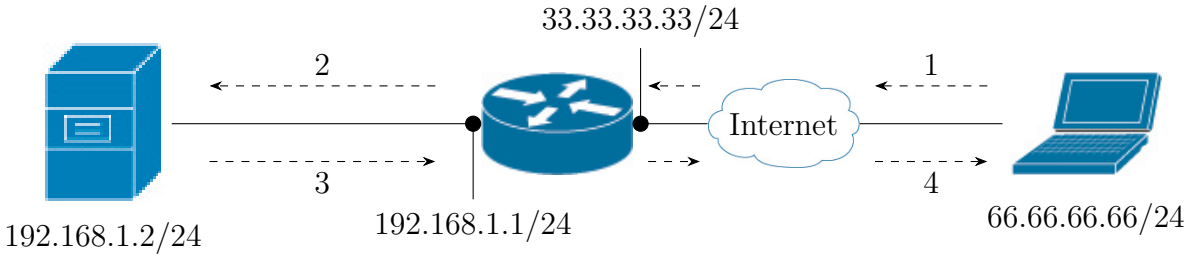


Figura 2.2: Ejemplo de red con DNAT.

(4) El paquete llega sin problema al router, ya que la IP de destino es pública. El router debe realizar de nuevo la traducción para saber a qué equipo de la red privada debe enviar la respuesta. Para ello, consulta la tabla de traducciones (Tabla 2.1) y, tras modificar de nuevo la cabecera IP (*postrouting*), esta queda:

- IPsrc:sport: `66.66.66.66:80`.
- IPdest:dport: `192.168.1.2:1075`.

Planteamos ahora el siguiente ejemplo de DNAT, que nos ayudará ahora a comprender cómo funciona esta técnica.

Ejemplo. Supongamos la situación de la Figura 2.2, en la que un portátil dentro de una red privada quiere acceder a un servidor HTTP en Internet.

El equipo envía una petición al router (1), que este reenvía al servidor (2). El servidor responde al router (3), que a su vez reenvía la respuesta al equipo (4). Se trata de DNAT, ya que la petición parte de la red pública. Veamos qué ocurre en cada uno de los pasos:

(1) El ordenador envía una petición HTTP al router.

El puerto de origen pongamos que es el 1050. El puerto de destino, tras la traducción efectivamente ha de ser el 80 (ya que es un servidor HTTP). No obstante, antes de la traducción este puerto ha de ser el correspondiente al puerto que hayamos asignado al servidor HTTP al que queremos acceder. Por ejemplo, sea la tabla de traducciones del router la de la Tabla 2.2 (que hemos de haber configurado previamente en el *port forwarding*).

IPdest	dport	IPdest′	dport′
`33.33.33.33`	23456	`192.168.1.2`	80

Tabla 2.2: Tabla de traducciones del router con DNAT.

En tal caso, el puerto de destino será el 23456. Por tanto, la cabecera IP del paquete que envía el portátil al router contendrá:

- IPsrc:sport: `66.66.66.66:1050`.
- IPdest:dport: `33.33.33.33:23456`.

Notemos que la IP de destino no es el servidor como tal, sino el router (ya que es es al que tiene acceso el portátil), y el puerto de destino es el que hemos asignado en la tabla de traducciones para el servidor HTTP al que queremos acceder.

(2) Tras llegar al router, este ha de realizar la traducción de direcciones (*prerouting*), ya que la IP de destino era el router mismo. Consultando la tabla de traducciones (Tabla 2.2), la cabecera IP del paquete que envía el router al servidor quedará:

- IPsrc:sport: `66.66.66.66:1050`.
- IPdest:dport: `192.168.1.2:80`.

Tras esta traducción, el router envía el paquete al servidor (ya en la red privada).

(3) Tras el procesamiento del paquete en el servidor, este envía la respuesta al router. La cabecera IP del paquete de respuesta contendrá:

- IPsrc:sport: `192.168.1.2:80`.
- IPdest:dport: `66.66.66.66:1050`.

(4) El paquete llega sin problema al router, ya que la IP de destino es pública. El router debe realizar de nuevo la traducción para saber ahora de qué equipo de la red privada proviene la petición. Para ello, consulta de nuevo la tabla de traducciones (Tabla 2.1) y, tras modificar de nuevo la cabecera IP, esta queda:

- IPdest:dport: `33.33.33.33:23456`.
- IPdest:dport: `66.66.66.66:1050`.

Notemos que, en el SNAT, la tabla de traducciones se va actualizando con cada nueva traducción, mientras que en el DNAT la tabla de traducciones ha de ser estática, ya que en otro caso el router no sabrá a donde redirigir las peticiones entrantes.

2.3.3. Encaminamiento

Se dice del proceso de encontrar el mejor camino para llevar la información (paquetes) de un origen a un destino dado. Como se vió en la Sección 2.2.2, este se realiza salto a salto y paquete a paquete en función de la dirección IP destino del paquete y de las tablas de encaminamiento que hay en cada uno de los routers.

Tablas de encaminamiento

Las tablas de encaminamiento son tablas que se guardan en la memoria de todo equipo conectado a la red (tanto hosts como routers), que informan sobre las redes a las que se puede llegar y la mejor forma de llegar a ellas.

Veamos los campos que tienen estas tablas, donde notaremos entre paréntesis aquellos que tienen menor relevancia y que incluso no son siempre necesarios.

- Red destino: Red a la que pertenecerá la dirección IP de destino, y a la cual queremos llegar.
- Máscara de red: Máscara de red correspondiente a dicha red de destino.
- Siguiente salto: Nodo al que debemos reenviar el paquete para que llegue a la red de destino.
- (Interfaz de salida del equipo), dato que puede ser redundante.
- (Protocolo).
- (Flags).
- (Coste): Coste esperado para llegar a dicha dirección IP de destino. Este se puede medir, por ejemplo, mediante el número de saltos que se han de realizar.

Hay distntos tipos de rutas que se pueden almacenar en una tabla de encaminamiento:

Rutas directas: (marcadas con $*$ en el campo de "Siguiente salto"). Estas son las redes a las que tenemos conexión directa, sin realizar ningún salto. Podemos enviar directamente el paquete al destinatario sin necesidad de pasar por nodos intermedios.

Un router tiene acceso directo a las redes que interconecta (por lo que tendrá una entrada de este tipo por cada red), mientras que un host suele estar en una única red (por lo que tan solo tendrá una entrada de este tipo).

En la mayoría de los casos, cuando se asigna una dirección IP a determinada tarjeta de red de un equipo, se almacena la entrada de esta ruta directa de forma automática.

Rutas indirectas: Estas son las redes a las que no tenemos conexión directa, pero sí a través de un intermediario. Por tanto, es necesario dar mínimo un salto para llegar al destino.

Entrada por defecto: (notado por `0.0.0.0` o `default` en red destino y `/0` en máscara). Hace referencia a cualquier red que no haya sido aceptada por el resto de entradas. El equipo que se encuentra en el campo de "Siguiente salto" será el que nos conexta con el exterior, y lo denominaremos *pasarela* o *gateway*.

Esta entrada no siempre es necesaria, aunque permite que no se produzcan errores (puesto que siempre habrá, al menos, una entrada válida para cada dirección IP, como más adelante veremos).

Entrada de `localhost`: En el caso de que queramos usar esta técnica, también debe haber una entrada en la tabla de encaminamiento con este fin. Su red de destino será `localhost`, y su interfaz, como mencionamos anteriormente, será `lo`.

Tenemos dos tipos de encaminamientos:

Estático: La tabla de encaminamiento se rellena a mano.

Red de Destino	Máscara	Siguiente Salto	Interfaz
192.168.0.0	/27	*	-
192.168.0.0	/24	*	-
192.168.0.0	/16	*	-
`default`	/0	`IP_Exterior`	-

Tabla 2.3: Tabla de encaminamiento de R6 para la Figura 2.3.

Dinámico: La tabla de encaminamiento se rellena de forma automática, ya que hay un protocolo (RIP, OSPF...) que se encarga de actualizarla. Tiene como ventaja que es dinámica (puede cambiar), ya que si se cae cierto router se puede buscar otro camino para llegar al destino.

Observación. En casos muy específicos (menos del 0,1 %), se puede encaminar en función de la dirección IP origen, pero este caso no se desarrollará en la asignatura.

Observación. Como curiosidad, para consultar la tabla de encaminamiento de un equipo con `Linux` se puede emplear el comando `route -n`.

Uso de la tabla de encaminamiento

En esta sección entenderemos cómo funcionan estas tablas. Dada una dirección IP de destino, buscamos saber cuál es la dirección IP del nodo al que debemos enviarle el paquete para que este, finalmente, llegue al destino.

Para esto, buscamos las redes de destino de la tabla de encaminamiento que admitan a la dirección IP de destino. Para ello, se hace la operación lógica `AND` entre la dirección IP de destino y la máscara de cada entrada, y si el resultado coincide con la red de destino entonces dicha entrada es válida para dicha IP.

- Si no hay ninguna entrada válida, se envía un mensaje de error ICMP, pero no se intenta solventar dicho error.
- Si hay más de una entrada válida, se escogerá aquella con la máscara de red más restrictiva, ya que la red de destino será más pequeña, teniendo así (a priori) una conexión más directa. Esto lo veremos en detalle en el próximo ejemplo.

Por tanto, una vez que tenemos la entrada asignada a la dirección IP de destino, se envía el paquete a la dirección IP del siguiente salto, continuando así el encaminamiento hasta llegar al destino.

Ejemplo. Veamos un ejemplo de encaminamiento. Supongamos que estamos en la situación de la Figura 2.3, y que la tabla de encaminamiento de R6 es la que se muestra en la Tabla 2.3 (donde hemos notado por `IP_Exterior` a la IP del siguiente router que nos conecta con Internet).

Supongamos que a R6 le llega un paquete con destino L1 (dirección IP de destino `192.168.0.1`). Tras hacer el `AND` con cada una de las máscaras, vemos que las 4 entradas son válidas para dicha dirección IP. No obstante, la máscara más restrictiva es `/27`, por lo que se elegirá dicha entrada y, por tanto, reenviará el paquete por

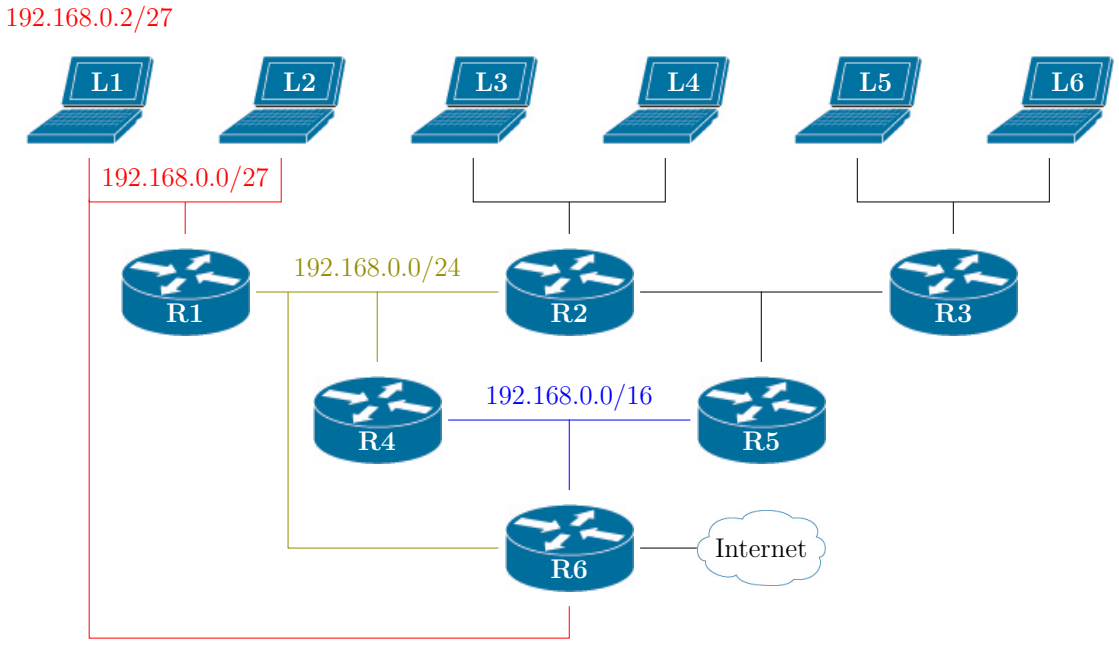


Figura 2.3: Situación para el ejemplo de la página 34.

la interfaz de red de R6 que pertenece a dicha red de destino. Esto permite que el camino se haga directo, con menos saltos.

En la mayoría de los casos, se buscará minimizar las tablas de encaminamiento agrupando las redes con las que se trabaja, permitiendo así que el encaminamiento sea más eficiente. Lo ideal es tener una entrada por cada interfaz del dispositivo, ya que así por cada dirección IP de destino sabremos qué interfaz usar. Además, a menudo tenemos que compartir las tablas de encaminamiento (como veremos en algunos de los siguientes protocolos), y para ello lo mejor es que sean lo más compactas posible.

2.3.4. Protocolos de intercambio de información de encaminamiento

Para facilitar la administración y aumentar la escalabilidad, Internet se jerarquiza en Autonomous System (AS), que son redes muy grandes (en la mayoría de los casos, abarcan todo un país) gestionadas por una única autoridad.

Observación. Cada AS tiene un número único de 32 bits que lo identifica. Por ejemplo, La red Iris tiene el número `AS766`.

De esta forma, cada AS informará al resto de los demás AS sobre las redes que tienen, de forma que compartirán su información de encaminamiento. Hay dos niveles de intercambio de tablas de encaminamiento:

- Algoritmos Interior Gateway Protocol (IGP): protocolos de intercambio de información de encaminamiento dentro de un mismo AS. Cada autoridad tiene libertad de elección, y los más comunes son RIP, OSPF....

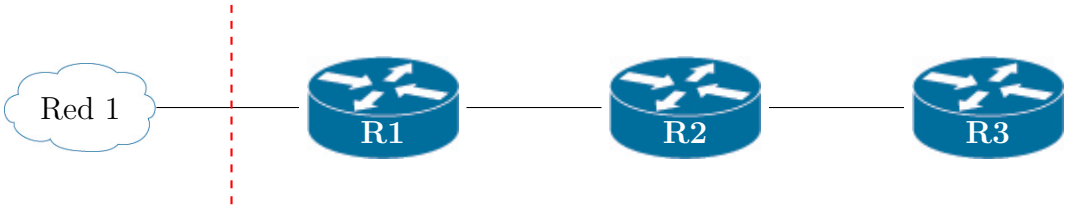


Figura 2.4: Problema de la cuenta al infinito en RIP.

- Algoritmos Exterior Gateway Protocol (EGP): protocolo de intercambio de información de encaminamiento entre distintos AS. Al ser estos distintas, se usa un único protocolo, BGP.

Routing Information Protocol (RIP)

Aunque es una funcionalidad de la capa de red, se implementa sobre la capa de aplicación (opera sobre UDP en el puerto 520), ya que la funcionalidad y la implementación son independientes.

Es un protocolo que adopta un algoritmo vector-distancia; es decir, se basa exclusivamente en el número de saltos, ignorando la velocidad de cada una de las conexiones. Una vez que un router aprende un camino para llegar a cierta red, no aprende otro a no ser que el número de saltos sea menor.

Cuando un router RIP se enciende y es configurado, envía cada cierto tiempo (por defecto 30 s) a todos los routers de sus respectivas redes un mensaje en el que informa de las redes a las que sabe llegar, junto con el coste que le supone para cada una de ellas. Además, recibirá de forma periódica la información correspondiente de los demás routers. Cuando un router recibe información de un vecino, si encuentra una ruta que no conocía, la añade a su tabla de encaminamiento, con el coste que le ha anunciado dicho vecino más 1 (el salto al correspondiente vecino). En el resto de casos, tan solo si el coste es menor que el que ya tenía, se actualiza la entrada.

Toda esta información se comparte por la dirección multicast `224.0.0.9`, en la que escuchan todos los routers que soportan RIP.

Problema de la cuenta al infinito

Un problema que puede surgir al emplear RIP es la convergencia lenta, ya que las malas noticias tardan en propagarse. Puede ocurrir que algún camino se rompa y, dada la naturaleza del protocolo, esta información tarda en notificarse.

Este se maximiza en el conocido "problema de la cuenta al infinito", que se muestra en la Figura 2.4. En dicha figura, podemos ver que, inicialmente, R1 tenía acceso a la red 1, aunque posteriormente dicho camino se rompe y R1 es notificado de que ha perdido acceso a dicha red. No obstante, R2, que aún no ha sido notificado de que ya no puede llegar a dicha red, al comparte a R1 su tabla de encaminamiento le informa de que él si sabe llegar a la red 1, por lo que R1 lo aprende (aumentando en una unidad el coste), y así sucesivamente. Cuando R2 reciba la información del corte, aprenderá el camino por R1, y así sucesivamente. Esto podría llegar a repetirse

indefinidamente (de ahí del nombre) hasta 16 (ya que ese es el límite para RIP en el que se asume que no se sabe llegar a dicha red), sin que ninguno en realidad supiese llegar a dicha red. Veamos algunas posibles soluciones:

Split horizon: Se basa en que a un router se le prohíbe compartir una ruta por la misma interfaz por la que la aprendió en primer lugar.

De esta forma, R2 no podría enseñarle a R1 cómo llegar a la red 1, por lo que el problema no empieza a sucederse.

Hold down: Retrasa los mensajes que nos llegan de una dirección que ya conocemos 180 segundos, esperando a que nos respondan los anteriores, si siguen activos.

Poison reverse: Si no sabemos llegar a un destino, informamos de que nuestro coste es infinito (coste 16).

Open Shortest Path First (OSPF)

A diferencia de RIP (que siempre consideraba el coste como el número de saltos), OSPF es un protocolo que permite al administrador definir el coste en función de distintos aspectos (velocidad, latencia, etc.). Como criterio por defecto, el coste de un enlace es el inverso del ancho de banda (la velocidad) de dicho enlace. Este protocolo busca el camino global que minimiza la suma de todos los costes, usando para ello el algoritmo de Dijkstra[3].

Permite definir áreas, de forma que la difusión se hace en unas áreas concretas. Esto hace que sea mucho más escalable, al contrario que RIP.

Los mensajes que se envían entre los routers que usan OSPF son:

- `Hello`: mensaje empleado para establecer la conexión, en el que se avisa a los routers que se van a comunicar.
- `Database description`: mensaje empleado para informar sobre la topología de las redes que conocemos.
- `Link status request/update/ack`: mensajes enviados para consultar, actualizar, o confirmar cambios.

2.3.5. Cabecera IP

En la presente sección profundizaremos en la cabecera IP, junto con sus campos. Esta se puede ver en la Tabla 2.4. Como vemos, está organizada en palabras de 32 bits (4 Bytes), y como mínimo ocupa 20 Bytes (ya que el campo *opciones* es opcional, y el de *relleno* se emplea para que sean múltiplos de 32 bits).

Veamos los campos, en orden, que la componen:

Versión: (4 bits) Indica la versión de IP que se está utilizando. Contiene `0100` si es IPv4 y `0110` si es IPv6.

[3]Trata en la asignatura de Algorítmica

0-3	4-7	8-15	16-18	19-31
V	LC	TS	Longitud Total	
Identificador			I	Desplazamiento
TTL		Protocolo	Checksum	
Dirección IP de Origen				
Dirección IP de Destino				
Opciones				Relleno

Tabla 2.4: Cabecera IP.

Tamaño de cabecera: (4 bits) Indica el tamaño de la cabecera en palabras de 32 bits. Su valor mínimo es de 5 palabras (20 Bytes) y su máximo de 15 palabras (60 Bytes).

Tipo de Servicio: (8 bits) Indica la calidad de servicio deseada durante el tránsito del paquete por una red. Algunas redes ofrecen prioridades de servicios, considerando determinados tipos de paquetes más prioritarios que otros (especialmente cuando la carga de la red es alta).

Longitud total: (16 bits) Indica el tamaño total, en bytes (también llamados octetos), del datagrama, incluyendo el tamaño de la cabecera y el de los datos.

Identificador: (16 bits) Identificador único del datagrama. Se utiliza en caso de que el datagrama deba ser fragmentado, para poder distinguir los fragmentos de un datagrama de los de otro. Resaltamos por tanto que todos los fragmentos de un mismo datagrama tienen el mismo identificador.

Indicadores: (3 bits) En la actualidad se utiliza para especificar valores relativos a la fragmentación. Los tres bits (por orden de mayor a menor peso) son:

0	DF	MF

donde:

- Bit 0: Reservado, debe ser 0.
- Bit 1 (Don't Fragment (DF)): indica si el datagrama puede ser fragmentado (0) o no (1). Si un paquete necesita ser fragmentado para enviarse y este bit es 1, se descartará.
- Bit 2 (More Fragments (MF)): indica si el fragmento es el último (0) o si le siguen más fragmentos (1).

Desplazamiento: (13 bits) En paquetes fragmentados, indica la posición, en unidades de $64\,\text{b} = 8\,\text{B}$, que ocupa dentro del datagrama original.

Time To Live (TTL): (8 bits) Indica el número de saltos máximo de un paquete en una red para evitar que los paquetes naveguen en la red indefinidamente. En cada salto, el campo se reduce en una unidad; y si este campo llega a 0, el paquete se descarta.

Protocolo: (8 bits) Valor numérico que indica el protocolo de las capas superiores al que debe entregarse el paquete[4].

Checksum: (16 bits) Es una comprobación de la corrección del datagrama. Se recalcula cada vez que algún nodo cambia alguno de sus campos (como el TTL).

El método de cálculo consiste en sumar en complemento a 1 cada palabra de 16 bits de la cabecera (considerando como 0 el campo del *checksum*) y hacer el complemento a 1 del valor resultante. Así, cuando llega al destino, se hace esta misma operación y se comprueba si es correcta la cabecera.

Dirección IP de origen: (32 bits) Dirección IP del emisor del paquete.

Dirección IP de destino: (32 bits) Dirección IP del destino del paquete.

Opciones: (opcional) Campo que puede contener información adicional, como la ruta que ha seguido el paquete.

Relleno: Este campo tiene tantos bits como sean necesarios para que la cabecera tenga un tamaño múltiplo de $32\,\mathrm{b} = 4\,\mathrm{B}$.

2.3.6. Fragmentación

Como hemos visto en el aprtado anterior, el tamaño máximo de un paquete que se envíe usando el protocolo IP es de $2^{16} - 1$ Bytes, aunque este es un valor teórico que ninguna red suele aceptar. Dentro de una red, cada tarjeta de red tiene un Maximum Transfer Unit (MTU), un valor numérico que indica el tamaño máximo de un paquete que se pasar a la capa de enlace para ser enviado por la red.

Como hemos mencionado, el MTU depende del estándar de cada tarjeta de red. Algunos ejemplos son:

- Ethernet: 1500 Bytes.
- Wifi: Aunque el valor es mayor, normalmente el SAP lo restringe a 1500 Bytes.

Notemos que, en la cabecera IP vista en la sección anterior, los campos de *identificación*, *desplazamiento* e *Indicadores* son los que se usan para controlar la fragmentación.

Algunas observaciones importantes son:

- Si hay algún error y no llegan todos los fragmentos de un datagrama se descarta todo y debe ser una capa superior la que se encargue de arreglar el problema.
- Un datagrama solo se fragmentará cuando vaya a pasar por una tarjeta de red con un MTU menor que el del paquete. Esta fragmentación se hará cuando sea necesaria, y puede ser en cualquier nodo del encaminamiento.

[4]Estos valores se pueden consultar aquí.

Figura 2.5: Red para el ejemplo de la Página 40.

- Los datagramas tan solo se podrán ensamblar en el destino, ya que distintos fragmentos podrán seguir caminos distintos, dependiendo del encaminamiento.

Observación. Es común hablar del MTU de una red. Esto se dirá cuando las tarjetas de red de dicha red tengan el mismo valor MTU.

Ejemplo. Supongamos que queremos enviar un datagrama con 4180 B de datos desde la red A a la red B, según el diagrama de la Figura 2.5. Supongamos que su identificador es X. Veamos si se produce fragmentación, y en qué paquetes se fragmenta.

Como la cabecera ocupa 20 Bytes, el tamaño a enviar es de 4200 B. Este no se podrá enviar por la red que une R1 y R2, pues su MTU es de 1500 B. Por tanto, se fragmentará en R1. Veamos cada uno de los paquetes, teniendo en cuenta que de los 1500 B de límite, 20 han de ser para la cabecera:

1. Paquete 1. Faltan por enviar 4180 B de datos, por lo que se envían:

20	1480

   La cabecera IP de este paquete tendrá los campos:

   $$\text{Identificador} = X, \qquad \text{MF} = 1, \qquad \text{Desplazamiento} = 0$$

2. Paquete 2. Faltan por enviar 4180 B − 1480 B = 2700 B de datos, por lo que se envían:

20	1480

   La cabecera IP de este paquete tendrá los campos:

   $$\text{Identificador} = X, \qquad \text{MF} = 1, \qquad \text{Desplazamiento} = 1480$$

3. Paquete 3. Faltan por enviar 2700 B − 1480 B = 1220 B de datos, por lo que se envían:

20	1220

   La cabecera IP de este paquete tendrá los campos:

   $$\text{Identificador} = X, \qquad \text{MF} = 0, \qquad \text{Desplazamiento} = 2960$$

Cuando cada uno de estos paquetes llegue a R2, como el MTU de la red que lo conecta con R3 es de 1000 B y todos los paquetes tienen un tamaño mayor, se fragmentarán en R2. Veamos cada uno de los paquetes, teniendo en cuenta que de los 1000 B de límite, 20 han de ser para la cabecera:

1. Paquete 1.1. Faltan por enviar 1480 B de datos, por lo que se envían:

20	980

   La cabecera IP de este paquete tendrá los campos:

$$\text{Identificador} = X, \qquad \text{MF} = 1, \qquad \text{Desplazamiento} = 0$$

2. Paquete 1.2. Faltan por enviar 1480 B − 980 B = 500 B de datos, por lo que se envían:

20	500

   La cabecera IP de este paquete tendrá los campos:

$$\text{Identificador} = X, \qquad \text{MF} = 1, \qquad \text{Desplazamiento} = 980$$

3. Paquete 2.1. Faltan por enviar 1480 B de datos, por lo que se envían:

20	980

   La cabecera IP de este paquete tendrá los campos:

$$\text{Identificador} = X, \qquad \text{MF} = 1, \qquad \text{Desplazamiento} = 1480$$

4. Paquete 2.2. Faltan por enviar 1480 B − 980 B = 500 B de datos, por lo que se envían:

20	500

   La cabecera IP de este paquete tendrá los campos:

$$\text{Identificador} = X, \qquad \text{MF} = 1, \qquad \text{Desplazamiento} = 2460$$

5. Paquete 3.1. Faltan por enviar 1220 B de datos, por lo que se envían:

20	980

   La cabecera IP de este paquete tendrá los campos:

$$\text{Identificador} = X, \qquad \text{MF} = 1, \qquad \text{Desplazamiento} = 2960$$

6. Paquete 3.2. Faltan por enviar 1220 B − 980 B = 240 B de datos, por lo que se envían:

20	240

   La cabecera IP de este paquete tendrá los campos:

$$\text{Identificador} = X, \qquad \text{MF} = 0, \qquad \text{Desplazamiento} = 3940$$

Cuando cada uno de estos paquetes llegue a R3, este los reenviará a la IP de destino, dentro de la red B. Allí, se ensamblarán de vuelta los paquetes, obteniendo así el datagrama original.

Figura 2.6: Red para el funcionamiento de ARP.

2.4. Asociación con la capa de enlace: Address Resolution Protocol (ARP)

Cuando queremos enviar un datagrama desde un origen a un destino, usando la tabla de encaminamiento del nodo en cuestión podemos saber la dirección IP del siguiente salto. No obstante, al bajar a la capa de enlace, ya no contemplamos direcciones IP, ya que el direccionamiento en esta capa se hace mediante direcciones MAC. Además, debido a que el encaminamiento en la capa de enlace se hace punto a punto, las direcciones MAC de origen y de destino cambian en cada salto.

Como hemos visto, sabemos las dirección IP de origen y la del siguiente salto, pero no la dirección MAC del siguiente salto. Esto nos lo proporcionará el protocolo ARP, que es un protocolo de la capa de enlace que se encarga de resolver direcciones MAC a partir de direcciones IP.

Funcionamiento

Supongamos la situación de la Figura 2.6, en la que PC1 quiere mandar un datagrama a PC2 (notemos que no consideramos intermedirarios, puesto que en el nivel de enlace el encaminamiento se hace punto a punto). El nodo PC1 conoce de sí mismo tanto su dirección IP como su dirección MAC, mientras que del siguiente salto (PC2) tan solo conoce la dirección IP tras haber consultado la tabla de encaminamiento. Para poder enviarle la trama[5] a PC2, necesita saber la dirección MAC de PC2. Esto nos lo proporciona el protocolo ARP, que funciona de la siguiente forma:

- PC1 manda una petición `ARP Request` a nivel de enlace por la dirección `FF:FF:FF:FF:FF:FF` (la dirección de difusión a nivel de enlace), preguntando por la dirección MAC de la dirección IP de PC2.

- PC2, que habrá recibido dicha petición, identifica que la dirección IP de la petición es la suya, por lo que contesta con un mensaje `ARP Reply` con su dirección MAC en unicast a PC1 (cuya dirección MAC ya conoce).

Este proceso no se hace (pues introduciría mucho tráfico) cada vez que se quiera mandar una trama, sino que las direcciones MAC que recibimos se van guardando en una caché y, tras cierto tiempo, expiran.

Observación. Como curiosidad, para consultar dicha caché en un equipo con `Linux` se puede emplear el comando `arp -a`.

[5]El datagrama ya se ha encapsulado en una trama, ya que en el nivel de enlace el SDU se denomina trama.

0-7	8-15	16-23	24-31
Htipo		Ptipo	
Hlen	Plen	Operacion	
Hemisor (Bytes 0-3)			
Hemisor (Bytes 4-5)		Pemisor (Bytes 0-1)	
Pemisor (Bytes 2-3)		Hsol (Bytes 0-1)	
Hsol (Bytes 2-5)			
Psol (Bytes 0-3)			

Tabla 2.5: Cabecera ARP.

2.4.1. Cabecera ARP

La cabecera de una trama ARP se muestra en la Tabla 2.5, donde notemos que "H" indica "Hardware" (capa de enlace) y "P" indica "Protocol" (capa de red). Los campos de dicha cabecera son:

Htipo: (2 Bytes) Número que indica el protocolo que se usa en el nivel de enlace (por ejemplo, Ethernet es `1`).

Ptipo: (2 Bytes) Número que indica el protocolo que se usa en el nivel de red (por ejemplo, IP es `0x0800`).

Hlen: (1 Byte) Número que indica la longitud de la dirección hardware (en Bytes). Para direcciones MAC es 6.

Plen: (1 Byte) Número que indica la longitud de la dirección del protocolo de red (en Bytes). Para direcciones IPv4 es 4.

Operación: (2 Bytes) Número que indica si es una petición o una respuesta. El valor `1` indica `Request` y el valor `2` indica `Reply`.

Hemisor: (6 Bytes) Dirección hardware (normalmente MAC) del emisor.

Pemisor: (4 Bytes) Dirección de red (normalmente IP) del emisor.

Hsol: (6 Bytes) Dirección hardware (normalmente MAC) del receptor.

Psol: (4 Bytes) Dirección de red (normalmente IP) del receptor.

Notemos que, en una petición, el campo de Hsol no será válido, puesto que es el valor que se está pidiendo.

Por último, destacar que el protocolo ARP tiene su homólogo Reverse ARP (RARP) que hace lo contrario, es decir, dado una dirección MAC nos devuelve su dirección IP. Cuando Internet comenzó, había equipos sencilos con pocas características, incluso sin disco duro. Al no tener disco duro, estos no podían almacenar su dirección IP, aunque las tarjetas de red si guardaban su dirección MAC. Era por tanto necesario un protocolo que nos diera la dirección IP a partir de la dirección MAC, y así nació el protocolo RARP. En la actualidad se encuentra en desuso, pero fue el precursor de BOOTP, el cual más tarde fue sustituido por DHCP.

0-7	8-15	16-31
Tipo	Código	Comprobación

Tabla 2.6: Cabecera ICMP.

Tipo	Descripción
8/0	Solicitud/Respuesta "echo" (`ping`)
3	Destino inalcanzable
4	Ralentización del origen
5	Redireccionamiento
11	TTL excedido
12	Problema de parámetros
13/14	Solicitud/Respuesta de sello de tiempo
17/18	Solicitud/Respuesta de máscara de red

Tabla 2.7: Tipos de mensajes ICMP.

2.5. El protocolo ICMP

El Internet Control Message Protocol (ICMP) es un protocolo que, aunque no es imprescindible, es de gran ayuda. En general, sirve para informar al origen de que ha habido un error. Este protocolo es útil pues, aunque IP no arregla ningún tipo de problema, este protocolo informa para que las capas superiores decidan qué hacer. Este es un protocolo de nivel de red que se encapsula también en el nivel de red, en un datagrama IP.

2.5.1. Paquete ICMP

La cabecera, que se muestra en la Tabla 2.6, se compone de 32 bits. Veamos cada uno de los campos que la componen:

Tipo: (1 Byte) Indica el tipo de mensaje que se está enviando. Los tipos más comunes se muestran en la Tabla 2.7.

Código: (1 Byte) Para cada tipo de mensaje, indica el subtipo que se está enviando, para detallarlo aún más.

Comprobación: (2 Bytes) Es un campo de checksum de la cabecera.

Respecto a la parte de datos, este paquete contiene los primeros 64 bytes del paquete que provocó el error. Es decir (suponiendo que la cabecera IP no tiene campo de "Opciones"), contiene los 20 Bytes de la cabecera IP y los 44 Bytes de datos del paquete IP que provocó el error. De esta forma, cuando el origen reciba este paquete podrá encontrar información sobre el paquete que provocó el error.

No debemos olvidar que ICMP se encapsula sobre el protocolo IP. Por tanto, el datagrama que se envía por la red (que es correcto) contiene una cabecera IP y en el SDU contiene el paquete ICMP, que contiene su respectiva cabecera y, en la parte

de datos, la cabecera IP y los primeros 44 Bytes de datos del paquete que provocó el error. Por tanto, en el mismo datagrama se enviará tanto la cabecera del paquete IP que provocó el error como la cabecera IP que se envía encapsulando el mensaje ICMP que informa del error.

Como aspectos relevantes, además de informar de errores nos permite conocer la situación de la red usando el comando `ping`, que envía un paquete ICMP de tipo "echo" (tipo 8) y espera una respuesta de tipo "echo" (tipo 0). Además, nos permite conocer la ruta que sigue un paquete usando el comando `traceroute`, que envía paquetes ICMP de tipo "echo" (tipo 8) con un TTL creciente (1,2,...). De esta forma, en cada salto, un paquete excederá su TTL, por lo que se enviará un mensaje ICMP de tipo "TTL excedido" (tipo 11) que informará de que el paquete no ha podido llegar a su destino. Esto nos permitirá saber todos los nodos que se encuentran en la ruta que sigue el paquete.

2.6. Autoconfiguración de la capa de red (DHCP)

El Dynamic Host Configuration Protocol (DHCP) es un protocolo para configurar de forma automática la capa de red. Este protocolo se encarga de asignar direcciones IP, máscaras, pasarelas por defecto e IP del servidor DNS. Su funcionalidad es a nivel de red, aunque se implementa en capa de aplicación y se encapsula en UDP.

Contamos con un cliente, que inicialmente no tiene dirección IP asignada (emplearemos la `0.0.0.0`), y un servidor DHCP, el cual se encargará de asignársela. Se trata de un protocolo de *leasing* (alquiler), ya que la dirección IP que se asigna al cliente es válida durante un tiempo.

Para conseguir una dirección IP, se intercambian los siguientes mensajes entre el cliente y el servidor DHCP (donde cada par pregunta-respuesta se etiqueta con un identificador de transacción para que el cliente sepa que el mensaje va para él):

- `DHCP Discover`: El cliente envía un mensaje para que saber si hay algún servidor DHCP en la red. Lo envía por tanto a la dirección de difusión.

$$\begin{aligned} \text{Dirección IP origen} &= \texttt{0.0.0.0} \\ \text{Dirección IP destino} &= \texttt{255.255.255.255} \\ \text{ID transacción} &= X \end{aligned}$$

- `DHCP Offer`: El servidor responde identificándose y proponiéndole una dirección IP al cliente, que será válida durante cierto tiempo (*lease time*), el cual se configura en el servidor DHCP. Notemos que esto es solo una oferta, no una imperativa.

  Como el cliente aún no tiene dirección IP asignada, se envía de nuevo a la

dirección de difusión.

$$\begin{aligned}\text{Dirección IP origen} &= \text{Dirección IP del servidor}\\ \text{Dirección IP destino} &= \texttt{255.255.255.255}\\ \text{ID transacción} &= X\\ \text{Dirección IP ofrecida} &= Y\\ \text{Lease time} &= Z\,\text{s}\end{aligned}$$

- `DHCP Request`: El cliente le solicita al servidor la dirección IP que le ha ofrecido el servidor (o la misma que ya estaba usando, en el caso de que se trate de una renovación).

  Aunque ya no es necesario que se envíe a la dirección de difusión (ya que el cliente conoce la dirección IP del servidor DHCP que le ha hecho la oferta), el estándar establece que se envíe aun así a la dirección de difusión (aunque permite ambas formas).

$$\begin{aligned}\text{Dirección IP origen} &= \texttt{0.0.0.0}\\ \text{Dirección IP destino} &= \texttt{255.255.255.255}\\ \text{ID transacción} &= X'\\ \text{Dirección IP solicitada} &= Y\\ \text{Lease time} &= Z\,\text{s}\end{aligned}$$

- `DHCP ACK`: El servidor responde con la dirección IP del cliente definitiva, y esta sí es imperativa.

  De nuevo, en este caso el servidor se ve obligado a enviar a la dirección de difusión.

$$\begin{aligned}\text{Dirección IP origen} &= \text{Dirección IP del servidor}\\ \text{Dirección IP destino} &= \texttt{255.255.255.255}\\ \text{ID transacción} &= X'\\ \text{Dirección IP asignada} &= Y\\ \text{Lease time} &= Z\,\text{s}\end{aligned}$$

Como hemos mencionado, la IP de destino en toda la transacción es la de difusión, y la de origen es la `0.0.0.0` en caso de ser el cliente el origen, o la del servidor DHCP en caso de ser él el origen.

Por último, para liberar la direcciín IP de forma correcta (sin que surja ningún error), el cliente debe enviar el mensaje `DHCP Release` al servidor DHCP antes de que termine el tiempo de alquiler. En caso contrario, el servidor liberará la IP igualmente, ya que es posible que el cliente ya no la esté usando y sea necesario liberarla para no quedarnos sin direcciones IPs disponibles. En el caso de que el cliente busque renovar su alquiler, volverá a enviará un mensaje `DHCP Request` al servidor DHCP.

Observación. Es posible configurar un servidor para que algunas IPs fijas se asignen a ciertos dispositivos.

3. Capa de transporte

En el presente tema, estudiaremos a fondo la capa de transporte. Recordemos que seguimos el Modelo TCP/IP descrito en la Tabla 1.1.

Objetivos

- Comprender las funiconalidades y servicios de la capa de transporte.
  - Servicio de **multiplexación/demultiplexación**.
  - Servicio **orientado a conexión** frente a **no orientado a conexión**.
  - Cómo conseguir una transferencia de datos **fiable**.
  - Cómo proporcionar **control de flujo**.
  - Cómo proporcionar **control de congestión**.
  - Cómo se han implementado estas funcionalidades en Internet.

3.1. Introducción

Tanto la capa de red como la de enlace realizan encaminamiento punto a punto, pero la capa de transporte en cambio se encarga de la comunicación extremo a extremo. Por tant,o solo los dispositivos extremos (normalmente los hosts) cuentan con la capacidad de procesamiento a nivel de transporte.

Como vimos en el primer tema, el PDU de la capa de transporte se denomina "datagrama" si se usa el protocolo UDP y "segmento" si se trata de TCP. El SDU de esta capa, como es lógico pensar, es el PDU de la capa de aplicación.

Funciones y servicios

- Comunicación extremo a extremo.
- Multiplexación y demultiplexación de aplicaciones por puertos (cualquier protocolo de transporte debe implementar esta funcionalidad): esto es que en el origen puede entrar en la red información de muchos procesos distintos (multiplexación) y al llegar al destino se distribuye la información entre los procesos necesarios (demultiplexación). Esto se hace a través de puertos.

Definición 3.1 (Puertos)**.** Es un número que le dice al SO "Cuando llegue un paquete por este puerto, está asociado a cierto proceso". Los puertos que están por

debajo de 1024 el SO los ofrece a los usuarios root y los que están por encima están a disposición del desarrollador y no se necesitan permisos de root para utilizarlos. Los puertos de TCP y UDP (que veremos más adelante) son independientes.

UDP
: Es un servicio no orientado a conexión, no fiable. Su intención no es ser iable, sino ir rápido.

TCP
: Es un servicio orientado a conexión, fiable. Hace control de errores, de flujo, de conexión y de congestión. En redes cableadas TCP siempre asume que los errores son por congestión (ya que la tasa de fallo es de 1 entre 1 millón). Sin embargo, en redes inalámbricas sí hay que asumir que puede ser por otras razones (la tasa de fallo es del 10 %).

La velocidad en UDP depende de la aplicación, va sobre una media. En TCP va a la máxima velocidad que puede pero controlando que no haya errores ni pérdidas.

3.2. Protocolo de datagrama de usuario (UDP)

Es un protocolo "best effort" (intenta hacerlo lo mejor posible, pero si hay algún error no intenta solucionarlo). No es orientado a conexión: no hay *hand-shaking*, no hay retardos de establecimiento. Cada paquete es totalmente independiente. Cada Transmission Paquet Data Unit es independiente. Cada paquete UDP se encapsula en un datagrama IP.

Ofrece un servicio no fiable, puede haber pérdidas. Sin embargo esto no significa que no puedan haber aplicaciones fiables sobre UDP, pero quien tiene que encargarse de arreglar los posibles errores es la capa de aplicación.

Los datos pueden llegar desordenados (por haber tomado distintos caminos en el encaminamiento, o por distintas prioridades) pero UDP no hace nada para arreglarlo.

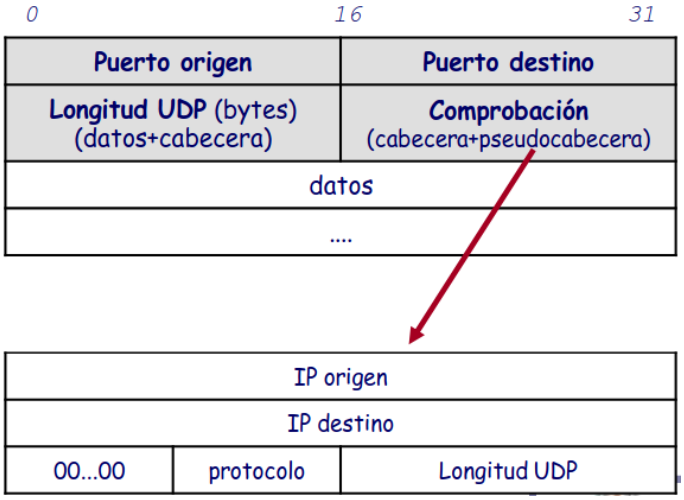
No hay control de congestión, los datos se **intentan** entregar lo más rápido posible.

Lo único que hace UDP (al igual que cualquier protocolo de transporte) es multiplexar y demultiplexar.

UDP se usa frecuentemente para aplicaciones multimedia que son tolerantes a fallos y sensibles a retardos.

3.2.1. Cabeceras UDP

Son 8 Bytes de cabecera.



- Puerto origen (16 bits): donde escucha el emisor.
- Puerto destino (16 bits): donde escucha el receptor.
- Longitud UDP (16 bits): en bytes, datos + cabecera.
- Comprobación, checksum (16 bits): no comprueba los datos, sino la cabecera y pseudocabecera, que es una parte de la cabecera IP con datos relevantes para UDP.
  - IP origen.
  - IP destino.
  - Protocolo.
  - Longitud UDP.

3.2.2. Multiplexación/demultiplexación

Existen puertos preasignados con servicios normalizados:

Puerto	Aplicación/Servicio	Descripción
7	echo	Eco
13	daytime	Fecha
37	time	Hora
42	nameserver	Servicio de nombres
53	**domain**	Servicio de nombres de domino
69	**tftp**	Transferencia simple de ficheros
123	**ntp**	Protocolo de tiempo de red

3.3. Protocolo de control de transmisión (TCP)

- Es un protocolo punto a punto (UDP no), ya que va desde un origen hasta un destino concreto. Cuando se manda un paquete multicast necesariamente tiene que ser en UDP, puesto que TCP es punto a punto, no puede hablar con muchos.

- Es un servicio orientado a conexión, utiliza un protocolo (hand-shaking, aunque se traduce como protocolo es más bien un intercambio muy específico de mensajes). Exige un estado común entre el emisor y el receptor.
- Los datos deben entregarse ordenados (esto no significa que necesariamente lleguen ordenados, pero esto se gestiona de tal forma que parezca que sí para la aplicación que usa los datos).
- Es transmisión full-duplex.
- Tiene un mecanismo de detección y recuperación de errores, retransmitiendo si es necesario (ARQ). Lo consigue usando confiramaciones, que son positivas (solo confirma lo que ha llegado bien, no se dice nada de lo que ha llegado mal o no ha llegado) y acumulativas (si se ha confirmado hasta cierto byte, entonces todo lo anterior ha llegado bien).
- Es un servicio fiable: control de flujo y de congestión.
- Usa piggybacking: al mandar una confirmación (ACK) se puede aprovechar y mandar datos a la vez.

3.3.1. Cabecera TCP

- Puerto origen (16 bits): identifica el puerto del emisor.
- Puerto destino (16 bits): identifica el puerto del receptor.
- Número de secuencia (32 bits): identifica el byte del flujo de datos enviados por el emisor al receptor que representa el offset del segmento.
- Número de acuse de recibo (32 bits): el valor del siguiente número de secuencia que el receptor del segmento espera recibir. De esta forma se confirma todo lo anterior también.
- Longitud de cabecera (4 bits): indica el tamaño de la cabecera en palabras de 32 bits. De normal el tamaño es de **20 bytes**.
- Reservado: por si dentro de unos años hacen falta más bits.
- Flags:

  U: Urgente. De normal los datos se van introduciendo en el buffer del receptor por la derecha y sacando por la izquierda, buffer circular con ventana deslizante. Pero hay datos urgentes que precisan que este orden no se siga.

  A: ACK es una confirmación. Si vale 0 el campo de acuse no es de utilidad.

  P: Push. En TCP el paquete no se manda a la aplicación hasta que no se llene cierto tamaño. Es más eficiente de esta forma, pero a veces necesitamos que los datos se envíen en un momento preciso y para ello sirve este flag, para decir que se manden los datos.

R: Reset. Se resetea la conexión.

S: Sincronismo. Esta a 1 en el momento del establecimiento de conexión.

F: Fin. Cuando está a 1 es porque quiero terminar la conexión.

- Ventana ofertada para el control de flujo (16 bits): nos indica cuanto espacio libre le queda al buffer del receptor.
- Comprobación (16 bits): incluye cabecera y datos.
- Puntero de datos urgentes (16 bits): si el flag **P** está activo, este campo nos indica donde empiezan los datos urgentes, puesto que puede que no todo el segmento sea urgente.
- Opciones: son opcionales (por ejemplo las características de las extensiones de TCP).

3.3.2. Multiplexación/demultiplexación

Existen puertos preasignados con servicios normalizados:

Puerto	Aplicación/Servicio	Descripción
20	FTP-DATA	Transferencia de ficheros: datos
21	FTP	Transferencia de ficheros: control
22	SSH	Terminal seguro
23	TELNET	Acceso remoto
25	SMTP	Correo electrónico
53	DNS	Servicio de nombres de domino
80	HTTP	Acceso hipertexto (web)
110	POP3	Descarga de correo

La conexión TCP se identifica por: puerto e IP origen y puerto e IP destino.

3.3.3. Control de conexión

Como ya hemos comentado, TCP ofrece un servicio orientado a conexión. El intercambio de mensajes tiene tres fases:

- Establecimiento de conexión (sincroniza el número de secuencia y se reservan recursos).
- Intercambio de datos, full-duplex.
- Cierre de conexión, libera recursos.

Establecimiento de conexión

Se le conoce como "three-way handshake". Supongamos que A se quiere comunicar con B.

1. A manda una solicitud a B para activar una conexión, activando para ello el flag de sincronismo y en el campo de secuencia se pone un byte aleatorio X.

2. Cuando B lo recibe, activa el flag de A (para confirmar el sincronismo) y en el campo de acuse pone X+1 (esto es por convenio). Además, por piggybacking, enviamos el sincronismo en el sentido contrario, activando el bit S y poniendo en el campo de secuencia otro número aleatorio Y.

3. A recibe esto último y confirma poniendo el flag A a 1 y poniendo en el campo de acuse Y+1. En este mensaje se pueden mandar datos (piggybacking). (Aunque por simplicidad en los ejercicios no lo haremos).

Entonces tenemos que A realiza una **apertura activa**, siendo el cliente; y B realiza una **apertura pasiva** siendo el servidor. Los campos que tenemos involucrados son: el bit de sincronismo S, el número de secuencia, el número de acuse, y el bit de ACK A.

La conexión es iniciada siempre por el cliente. Esto se denomina **apertura activa**. El servidor por su lado siempre está escuchando y cuando le llega una petición hace una **apertura pasiva**.

Observación. No es posible garantizar un establecimiento de conexión fiable teniendo en cuenta que los mensajes van sobre IP (que no es fiable). Para garantizarlo hay temporizadores y si expiran se reenvían paquetes.

Número de secuencia

- Es un campo para indicar el orden de los paquetes. Tiene 32 bits. Cuando el número de secuencia llega al máximo (2^{32}) se reinicia.

- El número de secuencia no empieza normalmente en 0, sino en un valor denominado Initial Sequence Number (ISN), teóricamente aleatorio.

- Realmente el ISN es elegido por el SO normalmente. Lo que hace es tener un contador que se va incrementando cada $4\,\mu s$. Por lo que tarda en repetirse un ISN casi 5 horas.

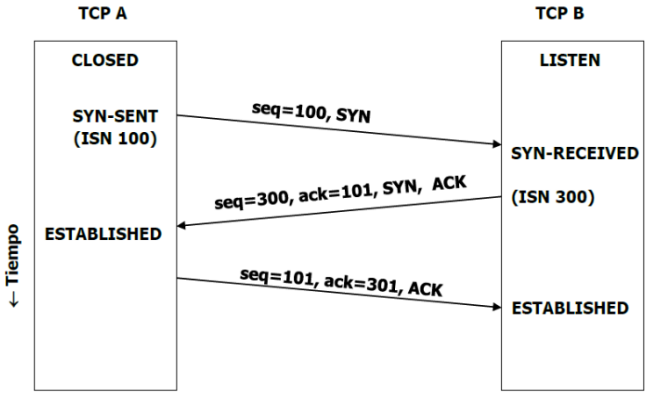
- Este mecanismo de selección de ISN es suficiente para proteger evitar coincidencias, pero no es un mecanismo de protección frente a sabotajes. Es muy fácil averiguar el ISN de una conexión y suplantar a alguno de los participantes.

- Se incrementa el número de secuencia de cada segmento según los bytes del segmento anterior.

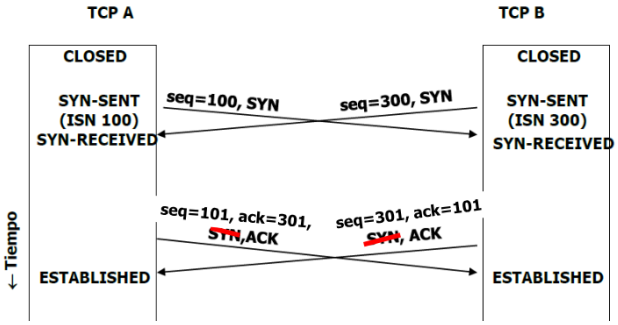
- Cuando los flags S y F están activados se incrementa en 1 el número de secuencia.

Veamos algunos ejemplos de establecimientos de conexión particulares:

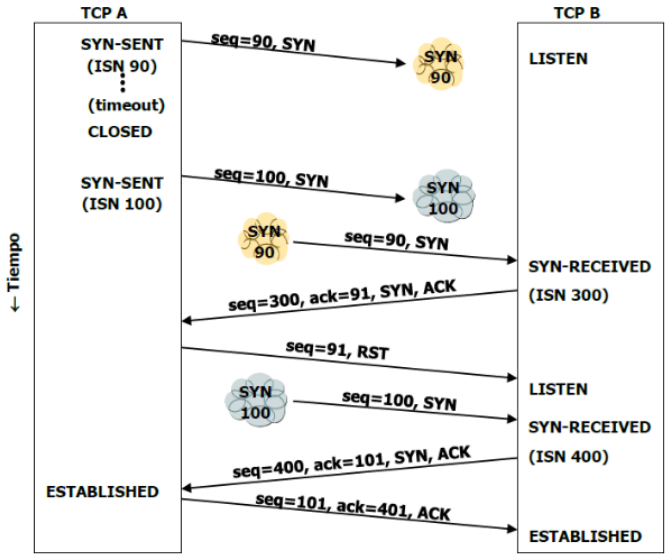
Establecimiento sin incidencias:



Caso de conexión simultánea: En este caso simplemente en el segundo mensaje no es necesario el SYN (pues ya se ha mandado antes).



Caso con SYN retrasados y duplicados: En este caso cuando el emisor recibe el ACK de la petición que ya ha descartado lo que hace es mandar un mensaje para que el receptor resetee la conexión y ambos estén sincronizados.



Cierre de conexión

1. Se envía un FIN (flag F a 1) y se envía en el número de secuencia el siguiente byte que el otro espera recibir X.

2. El otro responde con ACK con X+1 y envía un FIN con número de secuencia Y (el siguiente byte que espera recibir el primero).

3. El primero responde con ACK con Y+1.

En este caso, al igual que en el establecimiento de conexión, el que inicia el cierre realiza un cierre activo y el otro un cierre pasivo. Dependiendo de la aplicación el cierre activo puede realizarlo tanto el cliente como el servidor.

La conexión se cierra, pero para liberar los recursos se deja un tiempo de margen por si tienen que llegar datos aún (suelen ser 2 minutos).

MSS (Maximum Segment Size)

El MTU, que es un concepto de capa de enlace (capa 2), especifica la longitud máxima de datos de un paquete de enlace, es decir, cabecera IP + datos IP.

MSS es un concepto de la capa de transporte. Indica lo que puede ocupar como máximo los datos de TCP. Por tanto, al MTU le tenemos que quitar lo que ocupa la cabecera IP y la cabecera TCP para calcular el MSS.

Diagrama de estados de conexiones TCP

Un diagrama de estados es un autómata finito de estados TCP desde los cuales puedo hacer una serie de acciones, en las cuales puedo recibir y transmitir datos: a/b equivale a que recibo a y transmito b.

3.3.4. Control de errores

Los campos que tenemos involucrados en el control de errores son:

- Número de secuencia.
- Campo de acuse.
- Bit de ACK.
- Campo de checksum (incluye cabecera y datos TCP y pseudocabecera IP).

El sistema que se usa para el control de errores es el de confirmaciones positivas y acumulativas. Si el emisor pierde un ACK tiene que reenviar los datos, independientemente de que se haya perdido el dato o el ACK, tienen el mismo efecto ambos sucesos.

Lo que se hace es que el emisor tenga unos timeouts para que si este expira reenviemos el dato si no se ha recibido el ACK. Hay que calcular muy bien los timeouts puesto que si es muy corto se reenviarán datos innecesariamente y si es muy largo tardamos mucho en darnos cuenta del error.

Por otra parte tenemos el buffer del receptor. Se va rellenando con los datos que van llegando y se van colocando en orden gracias al número de secuencia, es decir,

los datos se introducen por la derecha. Hay que destacar que hay un buffer por cada conexión TCP. Cuando la aplicación pide un dato, el SO saca un paquete de más a la izquierda del buffer. Por esto, decimos que el buffer es una ventana deslilzante, una cola FIFO circular.

Generación de ACKs

Vamos a ver situaciones que se dan en el receptor y el comportamiento que sigue a dichas situaciones:

1. Si ocurre una llegada ordenada de segmento, sin discontinuidad, y con todo lo anterior ya confirmado, se retrasa el envío del ACK. Se pone un temporizador a 500ms (este tiempo está estipulado en el correspondiente RFC) y si traspasado ese tiempo no ha llegado otro segmento, en ese momento ya sí se envía el ACK.

2. Si tenemos todo en orden, y ocurre una llegada ordenada, sin discontinuidad y hay pendiente un ACK retrasado, se manda inmediatamente el ACK acumulativo. Vemos por tanto que se manda un ACK cada dos segmentos, si va todo bien.

3. Supongamos que ahora nos llega un segmento con número de secuencia mayor que el esperado, por lo que tenemos una discontinuidad. En este caso se envía un ACK duplicado, indicando el número de secuencia del siguiente byte esperado.

4. Supongamos por último que llega un segmento que completa una discontinuidad total (tapa el hueco entero) o parcialmente (tapa parte del hueco). En este caso se manda inmediatamente un ACK con el número de segmento del siguiente byte que se espera.

En el control de flujo veremos alguna situación más que requiere envío de ACKs.

Estimación de timeouts

Dichos timeouts deben adaptarse al Round Trip Time. Este no es un valor fijo pues hay que tener en cuenta el tiempo de transmisión (tiempo que tarda en enviarse un paquete, que depende de la tarjeta), tiempo de propagación (tiempo que tarda desde que se empieza a enviarse el paquete hasta que se empieza a recibir, que depende de la distancia y de la red), tiempo de procesado en un router (depende de la carga de la red). Y todo esto es solo el tiempo de ida, a lo que hay que sumarle el tiempo de vuelta, que es similar.

Como enviamos un paquete y recibimos un ACK, podemos medir el RTT. A esto lo llamamos RTT_{medido}.

$$RTT_{nuevo} = \alpha \cdot RTT_{viejo} + (1 - \alpha) \cdot RTT_{medido},\ \alpha \in [0, 1]$$

Este es un RTT filtrado, es una media suavizada.

$$Desviacion_{nueva} = (1 - x) \cdot Desviacion_{vieja} + x \cdot |RTT_{medido} - RTT_{nuevo}|,\ x \in [0, 1]$$

Esta es la desviación instantánea respecto a la media, que se utiliza para procurar cubrir todos los casos.

$$Timeout = RTT_{nuevo} + 4 \cdot Desviacion_{nueva}$$

Tenemos un problema con los ACKs repetidos, pero esto se soluciona muy fácilmente (algoritmo de Karn). Se actualiza el RTT solo para los ACKs no ambiguos, pero si hay que retransmitir algún segmento, se duplica el timeout.

3.3.5. Control de flujo

Es un mecanismo de atrás hacia delante: el receptor le dice al emisor que envíe más o menos datos. Los paquetes que lleguen cuando el buffer está lleno se descartan, lo que supone sobrecargar inútilmente la red. Nuestro objetivo es evitar esto. Es un sistema crediticio, el receptor informa al emisor sobre los bytes autorizados a emitir sin esperar respuesta.

Se utiliza el campo de la cabecera ventana, que tiene 16 bits, por lo que esto limita el tamaño de la ventana.

$$ventana\ util\ emisor = ventana\ ofertada\ receptor - bytes\ en\ transito.$$

Es importante que tengamos en cuenta los bytes que ya se han mandado pero de los cuáles no hemos recibido confirmación.

Cuando la ventana está llena, el emisor se bloquea hasta recibir un nuevo ACK que confirme que se ha liberado espacio de la ventana. Aquí está la situación que comentábamos antes de la necesidad de envío de ACKs fuera del control de errores.

Este ACK es importante, dado que si se pierde el emisor se queda bloqueado. Para evitar esta situación se usa un temporizador de persistencia. Cuando expira dicho temporizador se envía 1 byte para que se fuerce el posible reenvío del ACK.

Un problema que puede surgir es el Síndrome de la ventana tonta, que sucede cuando por alguna razón se tiene que mandar un segmento corto, a partir de ahí, lo más probable es que la ventana útil sea similar al tamaño de dicho segmento. Esto hace que se sature la red con muchos segmentos cortos.

Se puede hacer una posible mejora, usar la ventana optimista, no tomamos la ventana útil ni la ofertada, sino una cosa intermedia.

Hay dos medios que nos permiten saltarnos el orden:

- El bit U (urgente) con el campo puntero.
- Solicitar entrega inmediata a la aplicación con el bit P (push).

3.3.6. Control de congestión

La velocidad de TCP depende en gran parte de esto. Se manifiesta en pérdidas y/o retrasos de ACKs. Es un problema diferente al control de flujo, involucra la red

y los sistemas finales.

Tiene una naturaleza adelante-atrás: es el emisor el que decide cuánto se transmite. Por esto, no es necesario ningún campo en la cabecera TCP.

Lo que se hace es en la fuente limitar de forma adaptable el tráfico generado: reduciendo la velocidad de emisión ante congestiones e incrementándola si todo va bien.

Primero vamos a explicar el funcionamiento del control de congestión, y luego pasaremos a juntarlo con el control de flujo, dado que están directamente relacionados.

Funcionamiento del control de congestión:

Hablaremos de varios valores: ventana de congestión, ventana inicial y umbral. Aunque realmente lo que mide es la cantidad de bytes hablaremos de cantidad de segmentos.

En primer lugar se hace el establecimiento de conexión (siempre en TCP). Ahora bien, tras esto, vamos a tener dos fases:

Inicio lento: Al principio la ventana de congestión está puesta en el valor que estipula la ventana inicial (depende del sistema operativo, suele ser 2 para no tener que esperar los 500ms). Se mandan esa cantidad de paquetes, y se espera los ACKs.

Después de cada ACK recibido se le suma a la ventana de congestión anterior la cantidad de paquetes confirmados en dicho ACK. Es decir, si todo va bien, en cada ACK se aumentará la ventana de congestión en 2. Pero si nos damos cuenta, cada RTT la ventana duplicará su tamaño. Por tanto, la velocidad aumenta exponencialmente.

$$CW = CW + n^o\ datos\ confirmados$$

Siempre debemos tener en cuenta que el número de segmentos que podemos enviar es el que nos permite la ventana de congestión menos los segmentos que hay ya en tránsito (al igual que en el control de flujo). Esto va ocurriendo hasta que llegamos a un umbral, y pasamos a la siguiente fase.

Prevención de congestión: En esta fase, después de cada confirmación se aumenta la ventana de la siguiente forma:

$$CW = CW + \frac{1}{CW}$$

Entonces, cuando pasa un RTT aumenta en 1 la ventana de congestión, es decir la velocidad aumenta linealmente.

Ocurre un timeout: esto es por que ha habido algún error, y se asume que es por congestión, por lo que volvemos al valor de la ventana inicial y el umbral se establece en la mitad del valor de la ventana de congestión.

$$\text{umbral} = \frac{CW}{2}, \qquad CW = CW_{inicial}$$

En este caso, la ventana de congestión se va a ir duplicando de nuevo, pero ahora de forma más lenta.

Funcionamiento del control de flujo y congestión: habiendo explicado ambos funcionamientos por separado, solo nos queda juntarlo. En realidad no solo vamos a tener una de las dos limitaciones aisladas, sino que las tenemos las dos a la vez, por tanto los bytes permitidos a enviar son el mínimo de las dos ventanas, la de congestión y la del receptor.

$$Ventana\ util = \text{mín}\{VentanaCongestion, VentanaReceptor\}$$

3.4. Extensiones TCP

TCP se define con múltiples "sabores" o *flavours* en inglés, que no afectan a la interoperabilidad entre los extremos.

- TCP Tahoe: es el que hemos estudiado.
- TCP Reno: es la siguiente versión a TCP Tahoe. Distingue entre los timeout, que opera igual que Tahoe, y ACKs duplicados, que pone a la mitad la ventana de congestión y sigue en prevención de congestión.
- TCP NewReno: la versión anterior tiene un inconveniente. Si se pierden muchos paquetes, en cada uno se reduce la ventana a la mitad, cuando realmente esto no es necesario porque probablemente reduciendo una vez hubiera sido diferente. Esta nueva versión intenta ponerle solución a esto con ACKs parciales.
- TCP Vegas: si el RTT aumenta se disminuye la ventana, y si el RTT disminuye se aumenta la ventana de congestión.
- TCP Cubic: se usa en cualquier versión de Linux con kernel mayor que la 2.6.19. La ventana de congestión depende de los ACKs y del RTT.
- TCP Westwood: hay que tener en cuenta que, si bien en redes cableadas suponer que los errores siempre son por congestión es un buen enfoque; en redes inalámbricas no es ni de cerca el mejor, pues el 10 % de los errores son por el medio. Esta versión tiene en cuenta esto, y está pensada para redes inalámbricas.

4. Seguridad en redes

En el presente tema, dejaremos por un momento de lado la capa de aplicación para centrarnos en la seguridad en las comunicaciones, concepto esencial que iremos detallando a lo largo de las siguientes páginas.

Objetivos

- Comprender la importancia de la seguridad en las comunicaciones y aprender cómo desplegar mecanismos básicos de seguridad en redes de computadores e Internet.
- Conocer los aspectos de seguridad en redes: confidencialidad, autentificación, no repudio, integridad y disponibilidad.
- Entender los conceptos básicos de la seguridad en redes, como el uso de algoritmos de clave secreta, de clave pública, intercambio de claves...
- Comprender qué son los certificados digitales y las autoridades de certificación, y los diferentes mecanismos que se pueden implementar con certificados.
- Conocer algunos de los principales protocolos de comunicación seguros, como TLS e IPSec, y los mecanismos que lo utilizan.

4.1. Introducción

Una red de comunicaciones es **segura** cuando se garantizan todos los aspectos de seguridad, por lo que no hay protocolos ni redes 100 % seguras. No obstante, el objetivo de una red debe ser cubrir todos los aspectos de seguridad posibles. Definamos brevemente los aspectos de seguridad que vamos a estudiar, junto con los métodos que se utilizan para garantizarlos.

- **Confidencialidad / privacidad:** se garantiza que, cuando transmitimos algo a un receptor determinado, tan solo dicho receptor sea capaz de ver el mensaje. Se consigue con el cifrado.
- **Autenticación:** las entidades son quien dicen ser.
  Se consigue con algoritmos de Reto-Respuesta o doble cifrado.
- **No repudio o irrenunciabilidad:** no se permite la renuncia de la autoría de determinada acción, por lo que se convierte en una prueba legal en ante un juez en el caso de ser necesario. Por ejemplo, no podemos renunciar haber

participado en una transacción.
Se consigue con la firma digital o con el doble cifrado con certificado, pero ha de haber una entidad fiable.

- **Integridad:** se garantiza que los datos no sean manipulados por el camino (intencionadamente o no).
  Se consigue con funciones hash o compendios (resúmenes).
- **Disponibilidad:** el sistema mantiene las prestaciones de los servicios independientemente de la demanda[1].

Como hemos mencionado antes, una red es **segura** cuando se garantizan todos los aspectos de seguridad, y esta debe estar presente en todos los niveles de la red. El grado de seguridad lo *fija el punto más débil*, ya que este es el punto más vulnerable y por el que se podría producir un ataque de seguridad. Por tanto, es importante que haya seguridad en todos los niveles de la red.

Definición 4.1 (Ataque de seguridad)**.** Cualquier acción intencionada o no que menoscaba cualquiera de los aspectos de seguridad.

Veamos algunos ejemplos de ataque de seguridad:

- **Sniffing:** escuchar comunicaciones, por ejemplo mediante Wireshark. Se produce una vulneración de la confidencialidad.
- **Snooping (phishing):** suplantación de la identidad de alguna entidad. Se vulnera la autentificación.
- **Man in the Middle:** un atacante se situa en medio de dos equipos que se comunican e intercepta todos los mensajes que se transmiten.
- **Distributed Denial of Service (DDoS):** ataque consistente en enviar muchas peticiones a un servidor para que este no pueda atender a todas, consiguiendo que el servicio deje de funcionar. Se denomina *distributed* si las peticiones provienen de distintos equipos, que suele ser lo más común.
- **Malware:** software malicioso, como troyanos, gusanos, *spyware*, *backdoors*, *rootkits*, *keyloggers*, etc. Un ejemplo es *ransomware*, en el que se encriptan todos o parte de los datos y se pide un rescate a cambio de estos.

Los mecanismos de seguridad que vamos a estudiar, como hemos mencionado antes, son:

- Para garantizar la confidencialidad:
  - Cifrado (simétrico y asimétrico).
- Para garantizar la autentificación:
  - Autentificación con clave secreta (reto-respuesta).
  - Intercambio de Diffie-Hellman (establecimiento de clave secreta).

[1] Este aspecto no se tratará en la asignatura.

Figura 4.1: Proceso de cifrado y descifrado.

  - Firma junto con Certificado Digital.
- Para garantizar la integridad:
  - Funciones Hash.
- Para garantizar el no repudio:
  - Firma digital y Certificados digitales.

4.2. Cifrado

Se trata de un procedimiento para garantizar la confidencialidad, y en muchos casos también la autenticación.

El proceso se ilustra en la Figura 4.1. Inicialmente, se dispone de un texto plano a transmitir (P), que buscamos que tan solo pueda ser leído por el receptor. Para ello, se emplea una función de cifrado E_k que dará lugar a un texto cifrado (C), el cual se mandará a través del canal de comunicaciones (no supone un problema, ya que este texto cifrado no será entendible). Llegará al otro extremo y será descifrado con una función $D_{k'}$, obteniendo así de nuevo el texto plano (P).

Los algoritmos de cifrado y descifrado (E_k y $D_{k'}$) normalmente son conocidos, pero estos dependen de claves k y k' que son secretas. La dificultad reside en hallar estas claves.

Veremos dos tipos de algoritmos de cifrado:

- Cifrado simétrico. La clave es secreta y única ($k = k'$), y se usan distintas funciones para cifrar y descifrar.
- Cifrado asimétrico. Hay dos claves (pública y privada), y se usa la misma función para cifrar y descifrar.

4.2.1. Cifrado simétrico

Este tipo de algoritmos de cifrado se denomina simétrico porque se usa la misma clave para cifrar y descifrar los datos. Por tanto, la clave es secreta y tan solo es conocida por el emisor de los datos y el receptor.

Data Encryption Standard (DES)

Se trata de algoritmo de cifrado simétrico que se basa en realizar permutaciones y funciones `XOR` encadenadas. Se cifran palabras de 64 bits usando una clave de 56 bits.

Como principal ventaja, como estas operaciones se pueden implementar de forma sencilla en hardware, es un algoritmo muy rápido, por lo que se puede usar en tiempo real (por ejemplo para codificar voz). No obstante, presenta una serie de problemas:

- La longitud de la clave es corta (2^{56} posibles claves), por lo que es vulnerable a ataques de fuerza bruta.
- Lo que se termina obteniendo es una sustitución, por lo que con la misma entrada el resultado siempre será el mismo. Usando estudios estadísticos dependiendo del idioma, se puede llegar a descifrar el mensaje.

Para mitigar este segundo aspecto, se utiliza un esquema de cifrado reentrante, donde la salida de aplicar una transformación se usa para el cifrado de la siguiente palabra a cifrar. De esta forma, quien recibe el mensaje codificado necesita conocer la última entrada usada para codificar y podrá así aplicar el proceso inverso.

DES doble y 3DES

Estas son distintas mejoras del algoritmo DES para aumentar su seguridad y robustez. Se toman dos claves k_1 y k_2 (en el caso de 3DES, podrían ser 3 distintas) y para cifrar se toma una función E y su inversa D y se concatenan E_{k_1}, D_{k_2}, E_{k_1} y para descifrar se concatenan D_{k_1}, E_{k_2}, D_{k_1}.

De esta forma, podemos simular una clave de 112 bits (en el caso de 2DES) o de 168 bits (en el caso de 3DES); aunque se reduce la velocidad de cifrado.

International Data Encryption Algorithm (IDEA)

Emplea la misma idea que DES (cifrado empleando permutaciones y funciones `XOR`), pero con claves de 128 bits en vez de 56. De esta forma, hay 2^{128} posibles claves, lo que reduce las posibilidades de un ataque por fuerza bruta. Los bloques que se encriptan siguen siendo de 64 bits.

4.2.2. Cifrado asimétrico

Cada usuario A tiene una clave pública K_{pub_A} y una clave privada K_{pri_A} distintas. Conociendo la pública no es posible conocer la privada, por lo que la pública la conocen todos pero la privada solo la conoce su propietario, A. Además, hay una correspondencia biunívoca entre las claves públicas y privadas.

Veamos ahora la forma de funcionar de estos algoritmos. Supongamos que A quiere enviar un mensaje a B, por lo que cifraremos con la clave pública de B, de forma que sólo B podrá descifrarlo con su clave privada. De esta forma, se garantiza la confidencialidad del mensaje. Si P es el mensaje a enviar y C el mensaje cifrado, se tiene que:

$$C = K_{\text{pub}_B}(P) \longrightarrow P = K_{\text{pri}_B}(C)$$

De cara a la autentificación, si se cifra un documento con la clave privada de A, se garantiza que solo A ha podido cifrarlo, por lo que a priori[2] se garantiza la autentificación de A.

$$C = K_{\text{pri}_A}(P) \longrightarrow P = K_{\text{pub}_A}(C)$$

RSA

Este algoritmo, cuyo nombre se debe a sus creadores, es ampliamente utilizado en la actualidad. Es un algoritmo de cifrado asimétrico que se basa en la factorización de números enteros. Aunque no entraremos en el detalle de por qué es así el algoritmo[3], explicaremos tanto la generación de claves como el cifrado y descifrado de mensajes. Respecto a la generación de claves, se sigue el siguiente procedimiento:

1. Elegimos p, q primos grandes ($p, q > 10^{100}$).
2. $n = p \cdot q \qquad z = (p-1) \cdot (q-1)$.
3. Elegimos d primo relativo de z ($\text{mcd}(d, z) = 1$).
4. Calculamos e tal que $e \cdot d \mod z = 1$.

Las claves serán los siguientes pares:

$$K_{\text{pub}} = (e, n) \qquad K_{\text{pri}} = (d, n)$$

Para cifrar un número entero P en C, y descifrarlo de nuevo en P, se usan las siguientes funciones:

$$\begin{aligned} \text{Cifrado:} \quad & C = P^e \mod n \quad && \text{con } K_{\text{pub}} = (e, n) \\ \text{Descifrado:} \quad & P = C^d \mod n \quad && \text{con } K_{\text{pri}} = (d, n) \end{aligned}$$

Ejemplo. Veamos el siguiente ejemplo de aplicación del algoritmo.

1. Elegimos $p = 3$ y $q = 11$.
2. $n = 3 \cdot 11 = 33 \qquad z = (3-1) \cdot (11-1) = 20$.
3. Elegimos $d = 7$, ya que $\text{mcd}(7, 20) = 1$.
4. Tomamos $e = 3$, ya que $3 \cdot 7 \mod 20 = 1$.
5. Tenemos $K_{\text{pub}} = (3, 33)$ y $K_{\text{pri}} = (7, 33)$.

Suponemos que queremos codificar la palabra "SUZANNE". Para ello, asignamos un número a cada letra (el orden en el alfabeto sin la ñ), y el proceso se ilustra en la Tabla 4.1. Notemos que, por la red, tan solo se envía el número cifrado, C, y no se podría descifrar sin conocer la clave privada.

[2]En el apartado dedicado a la Firga digital se verá que no es suficiente.

[3]Se basa en factorización de números enteros, y se emplea para ello conocimientos mátemáticos, algunos vistos en la asignatura de Álgebra I, como la función de Euler.

Simbólico	Numérico (P)	$C = P^3$ mód 33	$P = C^7$ mód 33	Simbólico
S	19	28	19	S
U	21	21	21	U
Z	26	10	26	Z
A	1	1	1	A
N	14	5	14	N
N	14	5	14	N
E	5	26	5	E

Tabla 4.1: Cifrado y descifrado de la palabra "SUZANNE".

4.3. Autenticación

Pongámonos en el supuesto de que dos equipos, A y B, quieren autenticarse. Lo más sencillo es que cada uno tenga una base de datos con el usuario y la clave que comparten con el otro. Para autenticarse A, este le manda a B su usuario y su clave compartida, y B comprueba si son correctos. De forma análoga, B se autentica con A. Al estar enviándose la clave, este método es vulnerable, pero se usa en muchos servicios, como en el protocolo PAP. Se pueden hacer algunas mejoras, como enviar la información a través de túneles cifrados, pero la vulnerabilidad sigue presente.

Para evitar este problema, se pueden usar algoritmos de reto-respuesta.

4.3.1. Reto-respuesta

Este algoritmo se ilustra en la Figura 4.2. Al igual que antes, supongamos que dos equipos A y B quieren autenticarse. Ambos tienen una base de datos que contiene, para cada usuario, la clave que comparten. Para autenticarse A con B, este envía su identidad (usuario) A (que no es un dato sensible), y B le contesta con un número aleatorio (R_B) denominado reto. Usando la clave compartida K_{AB}, A cifra el reto ($K_{AB}(R_B)$) y se lo envía a B. El quipo B también cifra el reto con la clave compartida que posee en su base de datos, y si coincide con el que ha recibido, A queda autenticado. Además, A habrá enviado ya un reto R_A a B para que este se autentique de la misma forma. De esta forma, se garantiza la autenticación de ambos equipos.

Notemos que por la red no se envía ningún dado sensible, sino que solo se envían números aleatorios cifrados. Aunque parece seguro, este algoritmo tiene algunas vulnerabilidades:

- **Ataque por repetición:** el atacante escucha por mucho tiempo y va guardando las respuestas correctas para cada resto. De esta forma, cuando se repita un reto, ya sabe qué respuesta ha de enviar para identificarse él, suplantando así la identidad. **Solución:** que el reto no se pueda repetir (denominado *nonce*), como puede ser el instante de tiempo junto a un número aleatorio (por ejemplo).

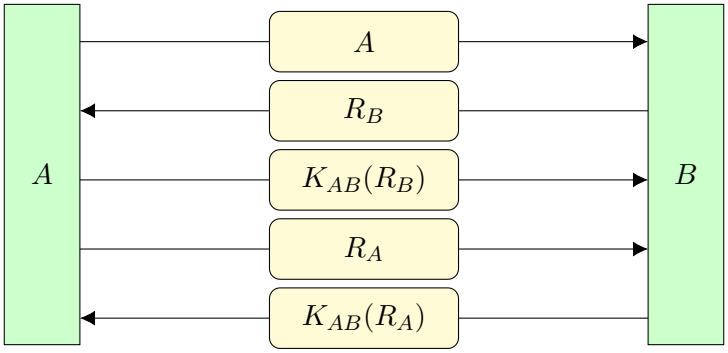


Figura 4.2: Algoritmo de reto-respuesta.

- **Ataque por reflexión:** el atacante, tras escuchar el reto de B, le envía a B su mismo reto, como si este fuese el reto de A. Cuando B le responda, le reenvía dicha respuesta a B como si hubiese sido él quien la ha cifrado. **Solución:** usar dominios de retos disjuntas, para que así no se pueda reenviar el reto de B a B.

4.3.2. Intercambio de Diffie-Hellman

Aunque en el algoritmo de reto-respuesta no se envían claves, estas se han tenido que establecer en algún momento. Además, también es posible que no sea posible almacenar las claves en las bases de datos mencionadas, y que tengamos que calcular una clave secreta y compartida en cada autenticación. Estos dos problemas se resuelven con el intercambio de Diffie-Hellman, ya que este algoritmo permite establecer una clave secreta entre dos entidades a través de un canal no seguro.

El algoritmo se muestra en la Figura 4.3. Aunque tampoco entraremos en detalle en las matemáticas que hay detrás, el algoritmo para crear una clave secreta compartida entre A y B es el siguiente:

1. A elige enteros x, n y g, y B elige el entero y.

2. A envía a B los valores g, n y $g^x \mod n$.

3. B envía a A el valor $g^y \mod n$, que calcula a partir de los valores recibidos.

4. La clave secreta que comparten A y B, que nunca se ha transmitido por la red y, como no se ha transmitido ni x ni y, tampoco la podrá calcular un atacante, es:

$$K_{AB} = (g^y \mod n)^x \mod n = g^{xy} \mod n$$
$$K_{BA} = (g^x \mod n)^y \mod n = g^{xy} \mod n$$

No obstante, este algoritmo también tiene sus vulnerabilidades. Por ejemplo, puede sufrir un ataque del tipo *man-in-the-middle*, en el que un atacante se sitúa entre A y B y se hace pasar por A ante B y por B ante A. De esta forma, hace de mensajero invisible, y las claves compartidas en realidad serán con el atacante.

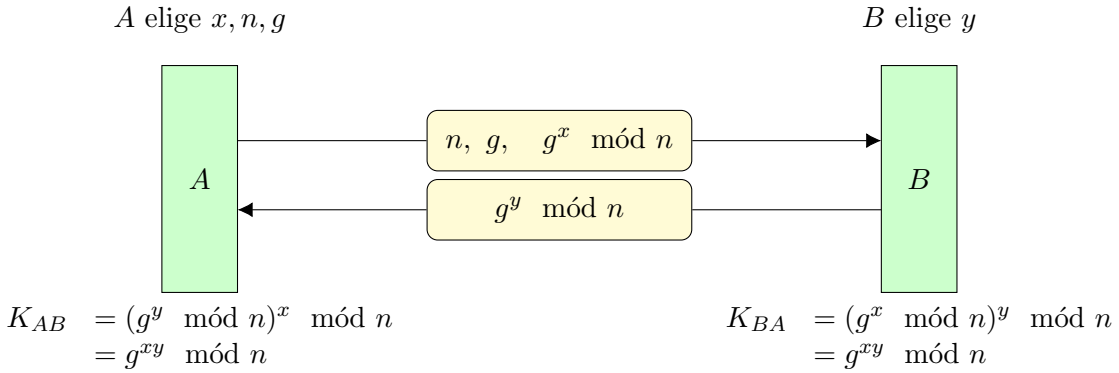


Figura 4.3: Algoritmo de intercambio de Diffie-Hellman.

4.4. Funciones Hash

Las funciones hash son funciones de forma que, dado un texto de entrada M de longitud variable, nos proporcionan un resumen (también llamado compendio) R de longitud fija. Estas funciones son unidireccionales e irreversibles; es decir, a partir de un resumen R no se puede obtener el mensaje original M. Estas deben además ser de cálculo sencillo, pues se usan en muchos protocolos de comunicación y han de poder calcularse rápidamente. Además, son invulnerables a ataques de colisión; es decir, dos mensajes distintos no pueden tener el mismo resumen.

Su principal utilidad es garantizar la **integridad** de un mensaje enviado. Un mensaje M se enviará junto al resumen R de este, y el receptor, tras recibir el mensaje, calculará el resumen del mensaje, R', y comprobará si coincide con el resumen recibido. En tal caso, se garantiza que el mensaje no ha sido modificado en el camino.

No obstante, podría ocurrir que un atacante interceptase el mensaje y lo modificase, cambiando M por M' y $h(M)$ por $h(M')$. Para evitar esto, hay varias alternativas:

- Cifrar el resumen usando la clave compartida, de forma que el atacante no podría cifrar $h(M')$ por no conocer la clave.
- El resumen puede incluir también a la clave compartida entre las entidades. A estos mensajes (M junto a $h(K \mid M)$) se les denomina Hash-based MAC (HMAC).

De ambas formas, también se garantiza la autenticación del emisor del mensaje. La confidencialidad no obstante no se garantiza, pues el mensaje no se cifra, sino que se envía en texto plano.

Message Digest Algorithm 5 (MD5)

Se trata de una función hash que, dado un mensaje, nos proporciona un resumen de 128 bits. Su funcionamiento se muestra en la Figura 4.4, y se desarrolla a continuación.

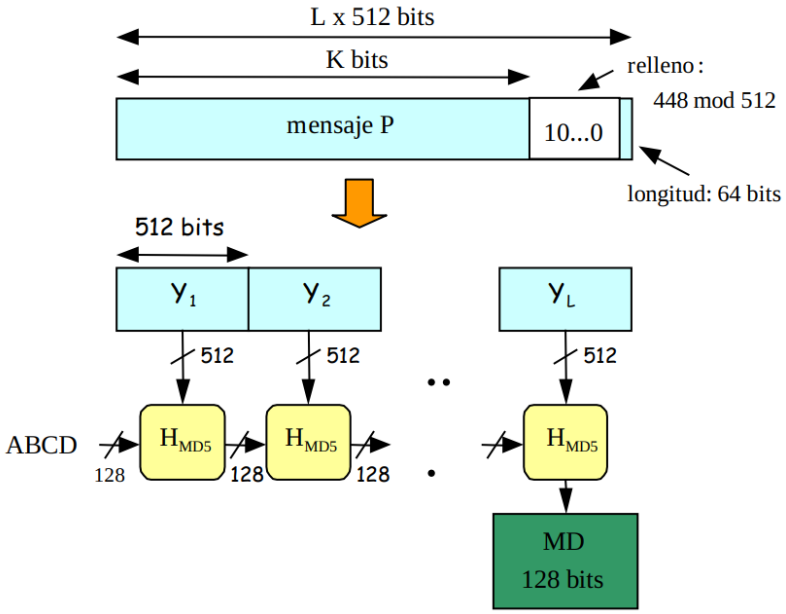


Figura 4.4: Funcionamiento de la función hash MD5.

Como el algoritmo trabaja sobre bloques de 512 bits, el mensaje será *siempre* extendido hasta que su longitud sea congruente con 448 módulo 512 (es decir, notando por K a su longitud, se extiende hasta que $K \equiv 448 \mod 512$, o lo que es lo mismo, hasta que $K - 448 \mod 512 = 0$). Esta extensión se hace añadiendo un 1 seguido de ceros hasta que se cumpla la congruencia, y se hace *siempre* (aunque la longitud del mensaje ya sea congruente con 448 módulo 512).

A continuación, se añade un campo de longitud de 64 bits, que indica la longitud del mensaje original. Si la longitud del mensaje original era mayor a 2^{64}, se toman los 64 bits de menor peso.

Tras añadir este campo de 64 bits, como $448 + 64 = 512$, el mensaje ya tendrá longitud múltiplo de 512, por lo que se divide en bloques de 512 bits, que son a los que les aplicaremos la función hash. Se hace un procesamiento secuencial por bloques, teniendo en cuenta que la salida tras procesar un bloque sirve como entrada para procesar el siguiente. El resumen se obtendrá tras procesar el último bloque.

Secure Hash Algorithm 1 (SHA-1)

El funcionamiento, desde el punto de vista de usuario[4], es análogo al de MD5, ya que también se procesan bloques de 512 bits; aunque en este caso los resúmenes son de 160 bits.

4.4.1. Ataque por Extensión

Supongamos que una entidad A quiere enviarle un mensaje M a otra entidad B. Para garantizar la integridad del mensaje, lo enviará junto a su resumen, y para

[4]No entraremos en detalle en cómo está implementada como tal la función hash, aunque evidentemente son distintas.

evitar que estos sean reemplazados por un atacante, el resumen también se hará de la clave compartida; es decir, se enviará M junto a $h(K_{AB} \mid M)$.

Supongamos no obstante que hay un atacante escuchando, y que intercepta el mensaje M junto al resumen calculado. Aunque no puede cambiar completamente M, sí podrá añadirle información (de ahí el nombre de extensión). Con el mensaje M, puede rellenarlo tal y como se describe en las funciones anteriores, y después de convertirlo a un mensaje con longitud múltiplo de 512, puede añadir al mensaje lo que quiera, obteniendo así un mensaje modificado M'. Para calcular $h(K_{AB} \mid M')$, como desconoce la clave compartida, no podrá hacerlo de forma directa. No obstante, como hemos visto que las funciones hash se basan en realimentación, podría usar el resumen $h(K_{AB} \mid M)$ que ha interceptado como entrada para el primer bloque que él haya añadida. De esta forma, cuando el mensaje llegue a B, este calculará el resumen de M', que coincidirá con el que ha calculado el atacante, creyendo por tanto que el mensaje no ha sido modificado y produciéndose una vulnerabilidad.

Para evitar este problema, el HMAC que en realidad se envía es:

$$h\left(K_{AB} \mid h(K_{AB} \mid M)\right)$$

De esta forma, el atacante podrá modificar el resumen calculado en la función exterior, pero nunca podrá calcular ni modificar el resumen que hay en el interior, ya que no conoce la clave compartida.

4.5. Firma digital y certificados digitales

Una **firma digital** intenta ser un sustituto de una firma escrita para poder garantizar el **no repudio** en nuestras acciones en Internet. Con ellas conseguimos:

- Autenticación del firmante frente al receptor.
- No repudio por parte del firmante.
- El firmante obtiene garantía de no falsificación, proporcionando integridad.
- Se garantiza la confidencialidad del mensaje entre el firmante y el receptor.

Hay dos tipos de firmas digitales, mediante clave secreta o mediante doble cifrado.

4.5.1. Firma digital con clave secreta. *Big Brother.*

Este método se basa el uso de una entidad fiable, denominada *Big Brother* o *BB*, en la que todos los usuarios confían (posiblemente sea del estado). Este comparte una clave con cada una de las entidades, de forma que todos los mensajes pasan por él. De esta forma, si surge algún problema, el Big Brother puede demostrar ante un juez quién ha hecho una transacción, en qué momento, etc.

Supongamos que A quiere enviarle un mensaje P a B firmado digitalmente. La forma de hacerlo se ilustra en la Figura 4.5. En primer lugar, A le envía al Big Brother un mensaje que contiene:

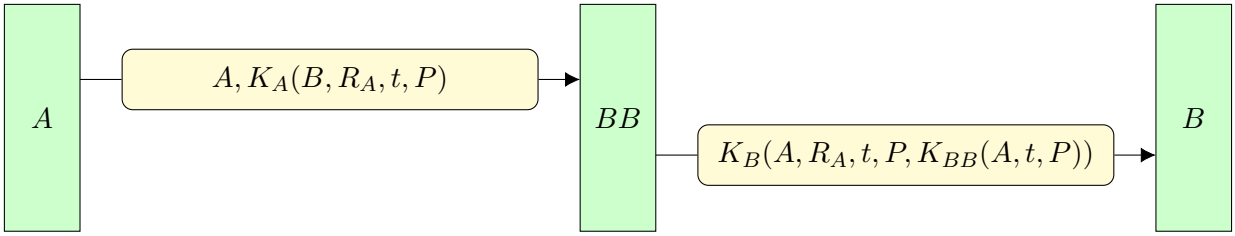


Figura 4.5: Firma digital con clave secreta. *Big Brother*.

- A: Identificador de A.
- B: Identificador de B, el destinatario.
- R_A: Resumen del mensaje para garantizar la integridad.
- t: Instante de tiempo.
- P: Mensaje a enviar, en texto plano.

Notemos que, exceptuando el identificador de A, el resto de campos van cifrados con la clave que comparte A con el Big Brother, proporcinando así confidencialidad con el BB y atenticándose así A. El mensaje es recibido por el BB, que lo descifra, identificando así que tiene que reenviarlo a B. Para ello, añade:

- $K_{BB}(A, t, P)$: Datos de la transacción, cifrados con la clave del BB, que solo él posee y por tanto se convierte en una prueba ante un juez. Se consigue así el no repudio.

Todo esto va cifrado con la clave que comparte B con el BB, garantizando así la confidencialidad del mensaje.

4.5.2. Firma digital con clave asimétrica. Doble cifrado

Supongamos que A le quiere mandar un mensaje a B. La idea se basa en lo siguiente:

- Cifrar con K_{pri_A} garantiza autenticación, ya que solo A ha podido cifrarlo.
- Cifrar con K_{pub_B} garantiza confidencialidad, ya que solo B podrá descifrarlo.

De esta manera, realizando ambos cifrados se garantiza la autenticación y la confidencialidad del mensaje. El orden de los cifrados no importa, pero ha de establecerse previamente para que el destinatario sepa cómo descifrarlo.

$$C = K_{\text{pub}_B}\left(K_{\text{pri}_A}(P)\right)$$
$$P = K_{\text{pub}_A}\left(K_{\text{pri}_B}(C)\right)$$

Sin embargo todo esto no garantiza el **no repudio**, puesto que nada nos garantiza que K_{pri_A} sea realmente de A. Para garantizarlo, necesitamos los **certificados digitales**, que son emitidos por autoridades de certificación.

Certificado digital

Definición 4.2 (Autoridades de certificación)**.** Entidad fiable (posiblemente del estado) que garantiza la asociación entre identidad y claves. En España, por ejemplo, la más extendida es la FNMT, aunque hay otras.

En primer lugar, el usuario obtiene sus claves pública y privada y envía una solicitud firmada digitalmente a la Autoridad de Certificación. Esta, tras comprobar la firma y que el solicitante es quien dice ser, emite el certificado digital solicitado, que contiene (entre otros campos):

- Identidad de la Autoridad de Certificación.
- Identidad del usuario.
- Clave pública del usuario.

Cualquier persona puede consultar este certificado digital, comprobando así que la clave pública que se le proporciona es realmente de la persona que dice ser. Para evitar falsificaciones, el certificado se cifra con la $K_{\text{priv}_{\text{AC}}}$ de la Autoridad de Certificación, de forma que solo esta ha podido ser la emisora del certificado.

El formato de certificados digitales más extendido es el estándar X.509, cuyos campos son:

- Versión del estándar X.509.
- Número de serie único, usado por la Autoridad de Certificación para identificar el certificado.
- Algoritmo empleado para calcular las claves.
- Identidad de la Autoridad de Certificación que ha emitido el certificado.
- Periodo de validez del certificado.
- Usuario al que se le ha emitido el certificado.
- Clave pública del usuario al que se le ha emitido el certificado.

4.6. Protocolos seguros

La seguridad se divide en dos tipos:

- **Perimetral:** consiste en garantizar la seguridad dentro de una misma red. Se usan firewalls, Intrusion Detection System (IDS) o Intrusion Response System (IRS).
- **Seguridad en protocolos:** si no podemos garantizar la seguridad en la red (o aun así, queremos mejorar la seguridad), se usan protocolos seguros para garantizar seguridad. Como vimos, estos han de establecerse en todas las capas, pues la seguridad la fija el punto más débil.

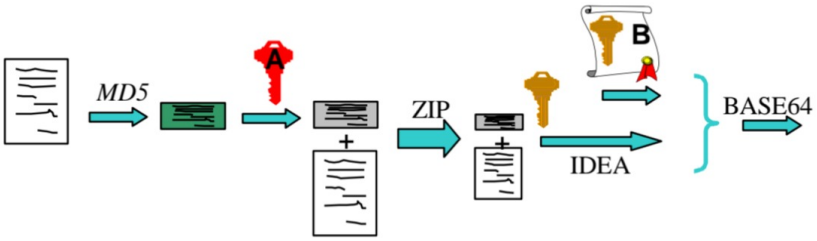


Figura 4.6: Protocolo PGP.

- Capa de aplicación: PGP o SSH.
- Capa de sesión[5]: TLS o SSL.
- Capa de red: IPSec.

4.6.1. Seguridad en la Capa de Aplicación. PGP.

En capa de aplicación deben usarse protocolos distintos para garantizar la seguridad en cada uno de los servicios prestados. Uno de ellos, el protocolo Pretty Good Privacy (PGP), tiene como objetivo garantizar la seguridad en el correo electrónico.

Supongamos que A quiere enviar un mensaje P a B mediante el correo electrónico. El protocolo se ilustra en la Figura 4.6. Al enviar A el correo, el proceso es el siguiente:

1. Se hace un resumen del mensaje mediante el algoritmo MD5, $R = \text{MD5}(P)$.
2. Este se firma digitalmente con la clave privada de A, $FD = K_{\text{pri}_A}(R)$.
3. Tanto el mensaje como resumen cifrado se comprimen (para enviar menos datos) usando para ello el el formato ZIP, $Z = \text{ZIP}(FD + P)$.
4. Se genera una clave privada específica para ese mensaje, K, y se cifra Z con esta clave usando para ello el algoritmo de IDEA, $\text{IDEA}_K(Z)$. A esta clave K se le denomina *clave de sesión*, pues solo se usa en esa sesión. Notemos que, si un atacante la consigue, tan solo podrá descifrar ese mensaje, y no otros.
5. Se cifra también la clave de sesión con la clave pública de B, $K_{\text{pub}_B}(K)$, para que solo B pueda obtener dicha clave y, por tanto, descifrar el mensaje. Por tanto, el mensaje cifrado es $C = K_{\text{pub}_B}(K) + \text{IDEA}_K(Z)$.
6. Este mensaje cifrado se codifica con el sistema Base64[6], $M = \text{Base64}(C)$, y será el que se envíe por internet.

El receptor, por su parte, cuando reciba el mensaje M, hará el proceso inverso:

1. Decodificará el mensaje usando Base64, $C = \text{Base64}^{-1}(M) = K_{\text{pub}_B}(K) + \text{IDEA}_K(Z)$.

[5]Entre aplicación y transporte. Ver Tabla 1.2 correspondiente al Modelo OSI.

[6]No tiene que ver con seguridad y no se verá en la asignatura. Es una forma de codificar mensajes para enviar por internet.

2. Descifrará la clave de sesión con su clave privada, $K = K_{\text{pri}_B}\left(K_{\text{pub}_B}(K)\right)$.

3. Descifrará el mensaje con la clave de sesión, $Z = \text{IDEA}_K^{-1}\left(\text{IDEA}_K(Z)\right)$.

4. Descomprimirá el mensaje, $FD + P = \text{ZIP}^{-1}(Z)$.

5. Se obtiene el resumen recibido, $R = K_{\text{pub}_A}(FD)$.

6. Se calcula el resumen del mensaje recibido, $R' = \text{MD5}(P)$.

7. Para comprobar que no se ha modificado, se comprueba si el resumen calculado es el mismo que el recibido, $R = R'$.

En resumen, tenemos lo siguiente:

Emisor (A)	Receptor (B)
$R = \text{MD5}(P)$	$C = \text{Base64}^{-1}(M)$
$FD = K_{\text{pri}_A}(R)$	$K = K_{\text{pri}_B}\left(K_{\text{pub}_B}(K)\right)$
$Z = \text{ZIP}(FD + P)$	$Z = \text{IDEA}_K^{-1}\left(\text{IDEA}_K(Z)\right)$
Generación K	$FD + P = \text{ZIP}^{-1}(Z)$
$C = K_{\text{pub}_B}(K) + \text{IDEA}_K(Z)$	$R = K_{\text{pub}_A}(FD)$
$M = \text{Base64}(C)$	$R' = \text{MD5}(P)$
	¿ $R = R'$?

Con este proceso conseguimos garantizar los siguientes aspectos de seguridad:

- Confidencialidad: el mensaje va cifrado con K, que va cifrada con la clave pública de B, luego solo B podrá obtener B y, por tanto, solo él descifrar el mensaje.

- Integridad: gracias al resumen, comprobamos que el mensaje no se ha modificado.

- Autenticación: gracias al cifrado con la clave privada de A, B sabe que el mensaje viene de A.

- No repudio: Tan solo si hay un certificado digital de A emitido por una Autoridad de Certificación, B podrá demostrar que el mensaje viene de A.

4.6.2. Seguridad en la Capa de Sesión. SSL y TLS.

Esta capa ofrece servicios de seguridad empleados por gran variedad de protocolos de aplicación, como HTTPS, IMAPS, SSL-POP o VPN. Los principales protocolos de esta capa son SSL y TLS, que en esencia crean túneles cifrados para el intercambio de información.

Secure Sockets Layer (SSL)

En realidad, no es un protocolo sino una familia de ellos que se usan de forma conjunta.

- SSL Handshake Protocol: se negocia el algoritmo de cifrado y la función hash; y el servidor se autentica con un certificado digital del tipo X.509. El cliente genera claves de sesión (de esta forma, si un atacante la consigue tan solo podrá obtener los mensajes de esa sesión), y hay dos opciones para ello:
  - Se generan aleatoriamente y se envían cifradas con la clave pública del servidor (este ya se ha autenticado).
  - Se generan mediante el intercambio de Diffie-Hellman. El problema del "man-in-the-middle" no se tiene en este caso, pues el servidor ya se ha autenticado.
- SSL Assert Protocol: informa sobre errores en la sesión.
- Change Cipher Spec Protocol: usado para notificar cambios en el cifrado.
- SSL Record Protocol: encapsula los protocolos anteriores, y ofrece un canal seguro.

  Para enviar datos, se hace lo siguiente:

  1. Se fragmenta el mensaje en fragmentos denominados *registros*.
  2. Cada registro es comprimido, y al comprimido se le calcula un resumen mediante la función hash acordada.
  3. Se cifra el mensaje comprimido junto con su resumen mediante la clave de sesión.
  4. Esto será lo que trasmite, encapsulado en un paquete TCP.

  Se garantiza *confidencialidad* (pues se cifra), *integridad* (pues se calcula el resumen) y *autenticación* por parte del servidor (pues se ha autenticado con su firma y certificado digital).

Transport Layer Security (TLS)

Inicialmente, el protocolo que había era SSL, desarrollado por la empresa Netscape. No obstante, y basándose en este, se desarrolló el protocolo TLS, al que se le cambió el nombre para indicar que ya no estaba asociado con dicha empresa. Este protocolo solventa distintas vulnerabilidades de SSL, aunque las diferencias inicialmente no eran muy significativas, **impedían la compatibilidad** entre ambos protocolos. En la actualidad el protocolo usado es TLS, aunque es común que, erróneamente y debido a la confusión histórica, la gente se refiera a él como SSL.

En la asignatura, y debido a que nos centramos tan solo en los contenidos básicos sin entrar en detalle en cada uno de los protocolos, hemos estudiado SSL por ser el primero, aunque en lo estudiado no difieren.

4.6.3. Seguridad en la Capa de Red. IPSec.

En la capa de red, se garantiza la seguridad mediante el protocolo IP Security (IPSec). Su objetivo es garantizar autenticación, integridad y (opcionalmente) confidencialidad. Se basa en la creación de túneles unidireccionales seguros[7], para lo cual encapsularemos cada paquete IP en otro paquete IP, con la diferencia de que el paquete encapsulado va cifrado. Se basa en tres procedimientos:

1. Establecimiento de una "Asociación de seguridad":

   Tiene el objetivo de establecer una clave secreta mediante el Intercambio de Diffie-Hellman, y para evitar el ataque de "man-in-the-middle"se establece una conexión entre dos routers. ha de haber autenticación previa mediante certificados.

   Se identifica mediante la dirección IP de origen y un número de 32 bits, denominado *Security Parameter Index*. Se trata for tanto de una comunicación simplex (en un solo sentido).

   Como aspecto negativo, vulnera el carácter NO orientado a conexión del protocolo IP, y por tanto tu aceptación no es universal.

2. Garantizar la autenticación e integridad de los datos:

   Una vez se ha establecido una "Asociación de seguridad", ha de garantizarse la integridad de los datos y la autenticación de sus orígenes. Esto se consigue añadiendo cabeceras denominadas "Cabeceras de autenticación".

3. Garantizar la confidencialidad de los datos:

   Opcionalmente, este aspecto de seguridad se puede garantizar mediante el protocolo de "Encapsulado de seguridad de la carga".

Este protocolo tiene dos modos de funcionamiento, que diferen en qué túneles se establecen:

- Modo transporte: la asociación (túnel) se hace extremo a extremo entre el host origen y destino, por lo que se protege toda la comunicación entre ambos.
- Modo túnel: la asociación se hace entre dos routers intermediarios.

  Como ejemplo para ilustrar su utilidad, supongamos una empresa con varias sucursales. Si se establece una asociación entre los routers de las distintas sucursales, se garantiza la seguridad de la comunicación entre ellas. Dentro de una misma sucursal la red es segura, pues se habrán establecido medidas de seguridad perimetrales para evitar que entren intrusos desde Internet.

[7] Por tanto, para enviar de forma segura y bidireccional hemos de establecer dos túneles.

5. Relaciones de Problemas

5.1. Introducción

Ejercicio 5.1.1. Explique brevemente las funciones de cada una de las capas del modelo de comunicación de datos OSI.

El modelo de comunicación de datos OSI cuenta con 7 niveles o capas:

1. Capa física: Se encarga de la parte física de la transmisión de los datos. Encontramos distintas formas de codificar los bits para su envío.

   Realiza funciones adicionales, como la codificación del canal.

2. Capa de enlace: Se encarga de los mecanismos de acceso al medio. En caso de haber un medio compartido por varios dispositivos, debe encargarse de no transmitir datos cuando otro medio lo está haciendo y de hacerlo cuando el canal se encuentre libre.

   En esta capa nos encontramos con los protocolos MAC y LLC.

3. Capa de red: Se encarga principalmente del direccionamiento de equipos (saber dar una dirección y tener un identificador dentro de la red) y del encaminamiento de datos (saber cómo mandar los paquetes al destinatario).

4. Capa de transporte: Se encarga principalmente de la fiabilidad de las comunicaciones:

   - Corrección de errores.
   - Manejar el congestionamiento de la red.
   - Controlar el flujo de datos (reducir velocidades si el receptor no es capaz de adecuar la velocidad de recibo a la de envío).
   - Realizar la multiplexación de los datos (ya que un mismo equipo puede tener varias aplicaciones que estén recibiendo datos a la vez).

5. Capa de sesión.

6. Capa de presentación[1].

7. Capa de aplicación: Se encarga de decidir qué datos envía a qué equipo, así como de interpretar los datos recibidos por otros equipos.

[1] No se han mencionado en clase las funcionalidades de las capas de presentación ni de sesión.

Ejercicio 5.1.2. Si la unidad de datos de protocolo en la capa de enlace se llama trama y la unidad de datos de protocolo en la capa de red se llama paquete, ¿son las tramas las que encapsulan los paquetes o son los paquete los que encapsulan las tramas? Explicar la respuesta.

Son las tramas las que encapsulan a los paquetes, ya que son las capas inferiores (en este caso, la de enlace) las que encapsulan la información de las capas superiores (en este caso, la de red) para su envío.

De esta forma, los paquetes son el PDU de la capa de red, que se convierte en el SDU de la capa de enlace, la cual añade su cabecera al mismo convirtiéndolo en su PDU.

Ejercicio 5.1.3. Averigüe qué son los sistemas de representación de datos "*Little Endian*" y "*Big Endian*". ¿Puede un host que utilice representación *Little Endian* interpretar mensajes de datos numéricos provenientes de un host que utilice representación *Big Endian* y viceversa? Discuta la respuesta.

Sí que puede, para ello, debe haber un determinado protocolo que permita indicar qué codificación llevan los datos en binario. De esta forma, en alguna parte de la cabecera de los paquetes enviados, debe haber un bit que indique si los valores numéricos que se envían estén en *Big Endian* o en *Little Endian*.

Ejercicio 5.1.4. Cuando se intercambia un fichero entre dos hosts se pueden seguir dos estrategias de confirmación. En la primera, el fichero se divide en paquetes que se confirman individualmente por el receptor, pero el fichero en conjunto no se confirma. En la segunda, los paquetes individuales no se confirman individualmente, es el fichero entero el que se confirma cuando llega completo. Discutir las dos opciones.

Suponiendo que enviamos n paquetes de datos, la primera forma envía de vuelta al emisor n paquetes de confirmación, uno por cada paquete. De la segunda forma, el receptor espera a unir todos los paquetes en un fichero completo (y a verificar que no se ha perdido ningún paquete del mismo) para enviar el mensaje de verificación.

De la segunda forma se envían menos mensajes de verificación al emisor, por lo que la posibilidad de congestión de red por paquetes de verificación es menor. Sin embargo, en caso de que un paquete no consiga llegar o llegue en mal estado, no será hasta el final del envío de todos los paquetes que el receptor no genere el mensaje al emisor, por lo que en caso de errores en la comunicación, hay un mayor tiempo en la comunicación, al tener que esperar a que el receptor tenga todos los paquetes. Además, en el caso de error, el receptor no informará de qué paquete ha llegado mal, por lo que deberá pedir al emisor que reenvíe todos los paquetes de nuevo.

Resumiendo, ambas estrategias de confirmación tienen sus pros y sus contras. Dependiendo de la situación (si queremos mayor velocidad en la comunicación o si queremos menor saturación de red), puede interesarnos una u otra.

Ejercicio 5.1.5. ¿Para qué sirve el programa *ping*? ¿y el programa *traceroute*?

El programa *ping* usa el protocolo ICMP para enviar un paquete a un equipo, el cual tratará de responder con un paquete de confirmación de recepción del primer paquete. Sirve para comprobar la conexión y el buen funcionamiento de la red existente entre dos equipos. También sirve para calcular empíricamente la latencia de la conexión.

Por otra parte, el programa *traceroute* sirve para consultar todos los nodos intermedios por los que pasan los paquetes que salen de un emisor y llegan a un receptor, junto con la latencia de cada salto. Se usan varios paquetes ICMP con un valor creciente del campo TTL (1,2,...) para que cada salto intermedio devuelva un paquete de error ICMP por TTL excedido. De esta forma, el emisor puede saber cuántos saltos intermedios hay entre él y el receptor, así como la latencia de cada uno de ellos.

Ejercicio 5.1.6. ¿Qué protocolos de un paquete puede cambiar un router? ¿En qué circunstancias?

Un router puede cambiar los protocolos situados debajo de la capa de red, siempre que sea necesario debido a que las redes que interconecta tengan dichos protocolos diferentes.

Por ejemplo, una red doméstica típica es aquella basada en Wi-Fi y con acceso a Internet contratado con tecnología ADSL. En este caso, el router inalámbrico deberá modificar el protocolo de las capas físicas y de enlace convenientemente.

Ejercicio 5.1.7. Averigue qué ISP operan en España.

Algunos de los ISP que operan en España son:

- Movistar.
- Vodafone.
- Orange.
- Jazztel.
- MásMóvil.
- Yoigo.
- Digi.

Ejercicio 5.1.8. ¿Qué es una aplicación cliente-servidor? ¿y una aplicación *peer-to-peer*?

Una aplicación cliente-servidor es una aplicación que depende de otra que probablemente esté en un equipo remoto (llamado servidor) para su funcionamiento.

Un ejemplo de aplicación cliente-servidor es una página web: tenemos aplicaciones que se ejecutan en local en cada equipo que accede a una determinada url. Dicha aplicación solicita datos a una aplicación que se encuentra en un equipo remoto, la cual proporciona datos (por ejemplo, accediendo a una base de datos) como respuesta

a los datos solicitados por la aplicación que se ejecuta en cada equipo de forma local.

Por otra parte, una aplicación *peer-to-peer*[2] es una aplicación que se distribuye entre varios equipos (que pueden estar muy lejanos entre sí) de forma que todas las aplicaciones tienen la misma relevancia en el buen funcionamiento del sistema.

Ambos tipos de aplicaciones se estudiarán en el Capítulo dedicado a la Capa de Aplicación.

Ejercicio 5.1.9. Describa brevemente la diferencia entre un *switch*, *router* y un *hub*.

Para responder a la pregunta, usamos además información que hemos aprendido en el Tema 2:

- Un switch es un nodo en una red que permite conectar tantos equipos como deseemos (normalmente, estos tienen 48 bocas de entrada RJ45 en el caso de conectar los equipos por ethernet) a una red. Funcionan a nivel de enlace, luego no tienen una dirección IP asociada.

- Un router es un nodo en una red que permite conectar redes distintas entre sí. Para ello, disponen de distintas tarjetas de red, cada una asociada a una red que se encuentra conectada al router. Disponen por tanto de varias direcciones IP, una por cada red a la que se conecta. Funciona a nivel de red.

  Presenta en su interior la tabla de enrutamientos, que permite el encaminamiento en la capa de red. Cuenta además con el NAT, que permite traducir direcciones de IP privadas a públicas y viceversa.

- Un *hub* es un nodo en una red que permite implementar la difusión. Se trata de un conjunto de bocas ethernet que internamente funcionan como un bus. Cada vez que un paquete se envía por una de las bocas, este es reenviado a todas las demás bocas, por lo que todos los equipos conectados al *hub* reciben el paquete.

Ejercicio 5.1.10. ¿Qué diferencia, en el contexto de una red de computadores, existe entre la tecnología de difusión y la tecnología punto-a-punto?

La tecnología de difusión permite enviar un paquete desde un equipoo y hacer que este sea recibido por el resto de equipos que estén conectados a la misma red (o hacer llegar estos a equipos en distintas redes). Es cada dispositivo el que decide si el paquete es para él o no.

Por otra parte, la teconología punto-a-punto permite el envío de paquetes desde un equipo a otro usando un medio directo, por lo que el destino está implícito desde que se envía el paquete. Esta tecnología es más rápida y segura, pero su escalabilidad es mucho menor.

Ejercicio 5.1.11. Un sistema tiene una jerarquía de protocolos de n capas. Las aplicaciones generan mensajes de M bytes de longitud. En cada capa se añade una cabecera de h bytes. ¿Qué fracción del ancho de banda de la red se llena con cabeceras? Aplique el resultado a una conexión a 512 kbps con tamaño de datos de 1500

[2]En español, podemos pensar en "entre pares".

bytes y 4 capas, cada una de las cuales añade 64 bytes cabecera. ¿Qué velocidad real de envío de datos resulta?

Debemos sumar a los M bytes iniciales que proporcionan las aplicaciones n veces (la capa de aplicación también incluye una cabecera) h bytes, por lo que la longitud de los mensajes que de verdad se envían es de $n \cdot h + M$ bytes. Por tanto, por cada $n \cdot h + M$ bytes enviados, $n \cdot h$ de ellos son de cabeceras:

$$\frac{n \cdot h}{n \cdot h + M} \cdot 100 \ \% \text{ de ancho de banda que se llena de cabeceras}$$

Si ahora partimos de 1500 bytes iniciales y añadimos 4 veces (una por capa) 64 bytes, estamos en realidad enviando mensajes de longitud:

$$4 \cdot 64 + 1500 = 256 + 1500 = 1756 \text{ bytes}$$

Por tanto, el ($^{256}/_{1756} = 0{,}145786$) 14.58 % de la red se emplea para enviar cabeceras, luego se aprovecha el ($1 - 0{,}145786 = 0{,}854214\,\%$) 85.42 % de la red para el envío de datos.

Si enviamos paquetes a una velocidad de 512kbps, en realidad estaremos enviando datos a una velocidad real de:

$$0{,}854214 \cdot 512 = 437{,}357568 \text{ kbps}$$

Ejercicio 5.1.12. Clasifique como de *difusión* o *punto a punto* cada uno de los siguientes sistemas de transmisión:

1. Radio y TV: Difusión, ya que es un emisor (en este caso, una cadena de televisión o radio) que difunde paquetes a cualquiera que tenga sintonizado dicho canal.

2. Redes inalámbricas (WLAN): Difusión, ya que cualquier equipo puede conectarse a la red y recibir los paquetes que se envían de forma inalámbrica.

3. ADSL: Punto a punto, ya que la conexión se establece mediante un cable. Usa en medio único.

4. Redes de cable: Puede implementar ambas tecnologías, ya que puede ser punto a punto (si cada equipo tiene su propio cable) o de difusión (si todos los equipos comparten el mismo cable).

5. Comunicaciones móviles (por ejemplo, GSM, UMTS, ...): Difusión, ya que (de nuevo) cualquier equipo puede recibir los paquetes que se envían por la red.

Ejercicio 5.1.13. Clasifique los siguientes servicios como orientados a conexión/no orientados a conexión y confirmados/sin confirmación. Justifique la respuesta.

Recordamos que los medios orientados a conexión son aquellos que comprueban si el receptor está disponible antes de enviar la información, y que los confirmados son aquellos que confirman la recepción del mensaje.

1. Correo postal ordinario: No es orientado a conexión (ya que no comprobamos anteriormente que el destinatario esté disponible, simplemente enviamos la carta) y es sin confirmación, ya que tras enviar la carta nada nos garantiza que el destinatario nos responda, pese a pedirlo explícitamente.

2. Correo certificado: No es orientado a conexión por la misma razón que el correo normal. Sin embargo, es confirmado, ya que al recibir el destinatario la carta debe firmar para que el emisor sea consciente de que la carta ha sido recibida.

3. Envío y recepción de fax: Orientado a conexión y confirmado.

4. Conversación telefónica. Es orientado a conexión, puesto que no se puede establecer una llamada si la otra persona no coge el teléfono. Además, es confirmado, ya que la otra persona ha de responder para que se produzca una comunicación.

5. Domiciliación bancaria de recibos: No es orientado a conexión, ya que no se comprueba si el destinatario está disponible antes de enviar la información. Además, es confirmado, puesto que el banco envía un mensaje de confirmación al emisor del recibo.

6. Solicitud de certificado de empadronamiento. Es no orientado a conexión, ya que no se comprueba si el destinatario está disponible antes de enviar la solicitud. Además, es con confirmación, ya que el ayuntamiento envía un documento que certifica que el solicitante está empadronado.

Ejercicio 5.1.14. ¿Cuál es el tiempo necesario en enviar un paquete de 1000 Bytes, incluidos 50 Bytes de cabecera, por un enlace de 100 Mbps y 10Km? ¿cuál es el tiempo mínimo desde que se envía hasta que se recibe confirmación? ¿qué relación hay entre este tiempo y los temporizadores en, por ejemplo, las capas de enlace y transporte?

En primer lugar, hemos de calcular el retardo de transmisión T_t, que es el tiempo que se tarda en enviar el paquete por el enlace. Para ello, tenemos que:

$$T_t = 10^3\,\mathrm{B} \cdot \frac{8\,\mathrm{b}}{1\,\mathrm{B}} \cdot \frac{1\,\mathrm{s}}{100 \cdot 10^6\,\mathrm{b}} = 80 \cdot 10^{-6}\,\mathrm{s} = 80\,\mu\mathrm{s}$$

Por otra parte, el retardo de propagación T_p es el tiempo que se tarda en enviar el paquete por los 10Km de cable. Para ello, suponiendo que la velocidad de transmisión es $^2/_3c = 2 \cdot 10^8\,\mathrm{m/s}$, tenemos que:

$$T_p = 10 \cdot 10^3\,\mathrm{m} \cdot \frac{1\,\mathrm{s}}{2 \cdot 10^8\,\mathrm{m/s}} = 50 \cdot 10^{-6}\,\mathrm{s} = 50\,\mu\mathrm{s}$$

Por tanto, el tiempo total que se tarda en enviar el paquete es de $T_t + T_p = 130\,\mu\mathrm{s}$.

Veamos ahora el tiempo mínimo desde que se envía hasta que se recibe confirmación. Además de los tiempos anteriores, hemos de tener en cuenta el tiempo de procesamiento del paquete, el retardo de transmisión del paquete de confirmación y el retardo de propagación del paquete de confirmación. Tenemos que:

- No se proporciona información del tiempo de procesamiento del paquete. No obstante, en los dispositivos modernos, este retardo es de varios órdenes de magnitud menor que los otros, por lo que se puede considerar despreciable.
- El retardo de propagación del paquete de confirmación es el mismo, puesto que la distancia recorrida es la misma.
- El retardo de transmisión sí difiere, puesto que el tamaño del paquete de confirmación difiere. Normalmente, estos solo incluyen una cabecera, por lo que este tiempo, notado por T_{ACK}, es:

$$T_{\text{ACK}} = 50\,\text{B} \cdot \frac{8\,\text{b}}{1\,\text{B}} \cdot \frac{1\,\text{s}}{100 \cdot 10^6\,\text{b}} = 4 \cdot 10^{-6}\,\text{s} = 4\,\mu\text{s}$$

  Un temporizador de control de flujo en capa de enlace o de transporte debe ser suficientemente mayor a este tiempo mínimo para evitar un re-envío inmediato de paquetes ante cualquier eventualidad mínima en la red, como un retardo en las colas (mayor retardo de procesamiento) por un cierto nivel de congestión.

Por tanto, el tiempo total mínimo que se tarda en enviar el paquete y recibir confirmación es de:

$$T_{\text{total}} = T_t + T_p + T_{\text{ACK}} + T_p = 80\,\mu\text{s} + 50\,\mu\text{s} + 4\,\mu\text{s} + 50\,\mu\text{s} = 184\,\mu\text{s}$$

5.2. Capa de red

Ejercicio 5.2.1. Estime el tiempo involucrado en la transmisión de un mensaje de datos para la técnicas de conmutación de circuitos (CC) y de paquetes mediante datagramas (CDP) y mediante circuitos virtuales (CPCV) considerando los siguientes parámetros:

- M: longitud en bits del mensaje a enviar.
- V: velocidad de transmisión de las líneas en bps.
- P: longitud en bits de los paquetes, tanto en CPD como en CPCV.
- H_d: bits de cabecera de los paquetes en CPD.
- H_c: bits de cabecera de los paquetes en CPCV.
- T: longitud en bits de los mensajes intercambiados para el establecimiento y cierre de conexión, tanto en CC como en CPCV.
- N: número de nodos intermedios entre las estaciones finales.
- D: tiempo de procesamiento en segundos en cada nodo, tanto en CC como en CPD y en CPCV.
- R: retardo de propagación, en segundos, asociado a cada enlace, en CC, en CPD y en CPCV.

Ejercicio 5.2.2. Un mensaje de 64 kB se transmite a lo largo de dos saltos de una red. Ésta limita la longitud máxima de los paquetes a 2 kB y cada paquete tiene una cabecera de 32 bytes. Las líneas de transmisión de la red no presentan errores y tienen una capacidad de 50 Mbps. Cada salto corresponde a una distancia de 1000 km. ¿Qué tiempo se emplea en la transmisión del mensaje mediante datagramas?

Ejercicio 5.2.3. Suponga que una red de datagramas usa cabeceras de H bytes y que una red de paquetes de circuitos virtuales utiliza cabeceras de h bytes. Determine la longitud M de un mensaje que se consigue transmitir más rápido haciendo uso de la técnica de conmutación de circuitos virtuales que mediante la de datagramas. Suponga que los paquetes tienen la misma longitud en ambas redes y que los retardos de procesamiento son idénticos

Ejercicio 5.2.4. Una aplicación audiovisual en tiempo real hace uso de conmutación de paquetes para transmitir voz a 32 kbps y vídeo a 64 kbps a través de la conexión de red de la figura **??**. Se consideran paquetes de voz e información de audio con dos longitudes distintas: 10 ms y 100 ms. Cada paquete tiene además una cabecera de 40 octetos.

a. Encuentre para ambos casos el porcentaje de bits suplementarios que supone la cabecera.

b. Dibuje un diagrama temporal e identifique todas las componentes del retardo extremo a extremo en la conexión anterior. Recuerde que un paquete no puede ser transmitido hasta que esté completo y que no se puede retransmitir hasta que no se haya recibido completamente. Suponga despreciables los errores a nivel de bit.

c. Evalúe todas las componentes del retardo de las que se dispone suficiente información. Considere las dos longitudes de paquete aceptadas. Suponga que la señal se propaga a una velocidad de 1 km/5 microsegundos y considere dos velocidades para la red troncal: 45 Mbps y 1,5 Mbps. Resuma el resultado para los cuatro posibles casos en una tabla con cuatro entradas.

d. ¿Cuál de las componentes anteriores implica la existencia de retardos de cola?

Ejercicio 5.2.5. Imagine una situación donde hay cinco routers RA-RE. RA, RB y RC se conectan cada uno a una red local A, B y C, siendo cada router única puerta de enlace de cada red. RA, RB y RD están conectados entre sí a través de un switch. RC, RD y RE están conectados entre sí a través de un switch. RE conecta a Internet a través de la puerta de acceso especificada por el ISP. Especifique tablas de encaminamiento en los routers. Asigne a voluntad las direcciones IP e interfaces necesarias.

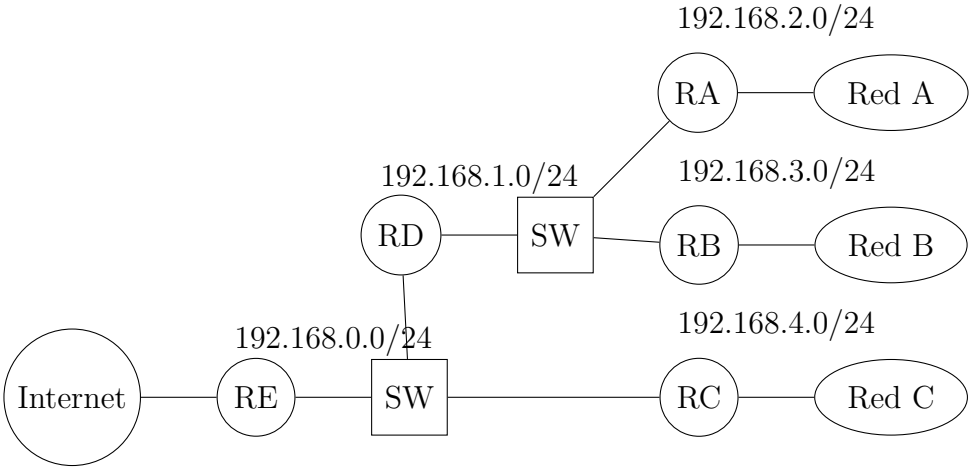


Figura 5.1: Situación del ejercicio 5

En primer lugar, asignaremos las direcciones IP y las interfaces de cada router. Cada router presenta una conexión por la izquierda y otra por la derecha, por lo que sólo usaremos dos interfaces de cada router, luego asociaremos dos direcciones IP a cada router.

Por comodidad, asociaremos las conexiones de la derecha de cada router a la interfaz *ether0*, y las conexiones de la izquierda de cada router a la interfaz *ether1*.

Una vez añadidas las interfaces, procederemos a asocciar direcciones IP a cada interfaz de cada router:

- RA:
  - Tendrá IP 192.168.2.1 en la red 192.168.2.0/24.

    - Tendrá IP 192.168.1.2 en la red 192.168.1.0/24.
- RB:
    - Tendrá IP 192.168.3.1 en la red 192.168.3.0/24.
    - Tendrá IP 192.168.1.3 en la red 192.168.1.0/24.
- RD:
    - Tendrá IP 192.168.1.1 en la red 192.168.1.0/24.
    - Tendrá IP 192.168.0.2 en la red 192.168.0.0/24.
- RC:
    - Tendrá IP 192.168.4.1 en la red 192.168.4.0/24.
    - Tendrá IP 192.168.0.3 en la red 192.168.0.0/24.
- RE:
    - Tendrá IP 192.168.0.1 en la red 192.168.0.0/24.
    - Su IP en la red que le conecta con Internet la proveerá el ISP.
- Suponemos que RE se conecta a Internet a través de un router con IP 33.33.33.33 en la red 33.33.0.0/16.

Procedemos ahora a rellenar las tablas de encaminamiento de cada router:

Red destino	Máscara	Siguiente salto	Interfaz
192.168.2.0	255.255.255.0	*	ether0
192.168.1.0	255.255.255.0	*	ether1
192.168.3.0	255.255.255.0	192.168.1.3 (RB)	ether1
0.0.0.0	0.0.0.0	192.168.1.1 (RD)	ether1

Tabla 5.1: Tabla de encaminamiento para RA.

Red destino	Máscara	Siguiente salto	Interfaz
192.168.3.0	255.255.255.0	*	ether0
192.168.1.0	255.255.255.0	*	ether1
192.168.2.0	255.255.255.0	192.168.1.2 (RA)	ether1
0.0.0.0	0.0.0.0	192.168.1.1 (RD)	ether1

Tabla 5.2: Tabla de encaminamiento para RB.

Red destino	Máscara	Siguiente salto	Interfaz
192.168.4.0	255.255.255.0	*	ether0
192.168.0.0	255.255.255.0	*	ether1
192.168.0.0	**255.255.252.0**	192.168.0.2 (RD)	ether1
0.0.0.0	0.0.0.0	192.168.0.1 (RE)	ether1

Tabla 5.3: Tabla de encaminamiento para RC.

Donde hemos agrupado la Red A (192.168.2.0/24), B (192.168.3.0/24) y la red 192.168.1.0/24 en la superred 192.168.0.0/22. Notemos que dentro de las direcciones de la superred se encuentran las direcciones de la forma 192.168.0.x, que no se encuentran en dicha superred. Sin embargo, tenemos una entrada específica para dichas direcciones, con una máscara de mayor prioridad (más 1s), por lo que no tenemos problema[3]

Red destino	Máscara	Siguiente salto	Interfaz
192.168.1.0	255.255.255.0	*	ether0
192.168.0.0	255.255.255.0	*	ether1
192.168.2.0	255.255.255.0	192.168.1.2 (RA)	ether0
192.168.3.0	255.255.255.0	192.168.1.3 (RB)	ether0
192.168.4.0	255.255.255.0	192.168.0.3 (RC)	ether1
0.0.0.0	0.0.0.0	192.168.0.1 (RE)	ether1

Tabla 5.4: Tabla de encaminamiento para RD.

Red destino	Máscara	Siguiente salto	Interfaz
192.168.0.0	255.255.255.0	*	ether0
33.33.0.0	255.255.0.0	*	ether1
192.168.4.0	255.255.255.0	192.168.0.3 (RC)	ether0
192.168.0.0	**255.255.252.0**	192.168.0.2 (RD)	ether0
0.0.0.0	0.0.0.0	33.33.33.33 (Router ISP)	ether1

Tabla 5.5: Tabla de encaminamiento para RE.

Donde hemos vuelto a usar la superred 192.168.0.0/22 que engloba a Red A, B y 192.168.1.0/24.

Ejercicio 5.2.6. Asigne las direcciones de subred en la siguiente topología a partir de 192.168.0.0 para minimizar el número de entradas en las tablas de encaminamiento, asumiendo que en las redes LAN puede haber hasta 50 PCs.

[3]Si no tuviéramos dicha entrada, tendríamos un problema, ya que si mandamos un paquete a 192.168.0.26, por ejemplo, iría a la superred que hemos definido pero algún router se daría cuenta de que no sabe llegar a 192.168.0.0/24.

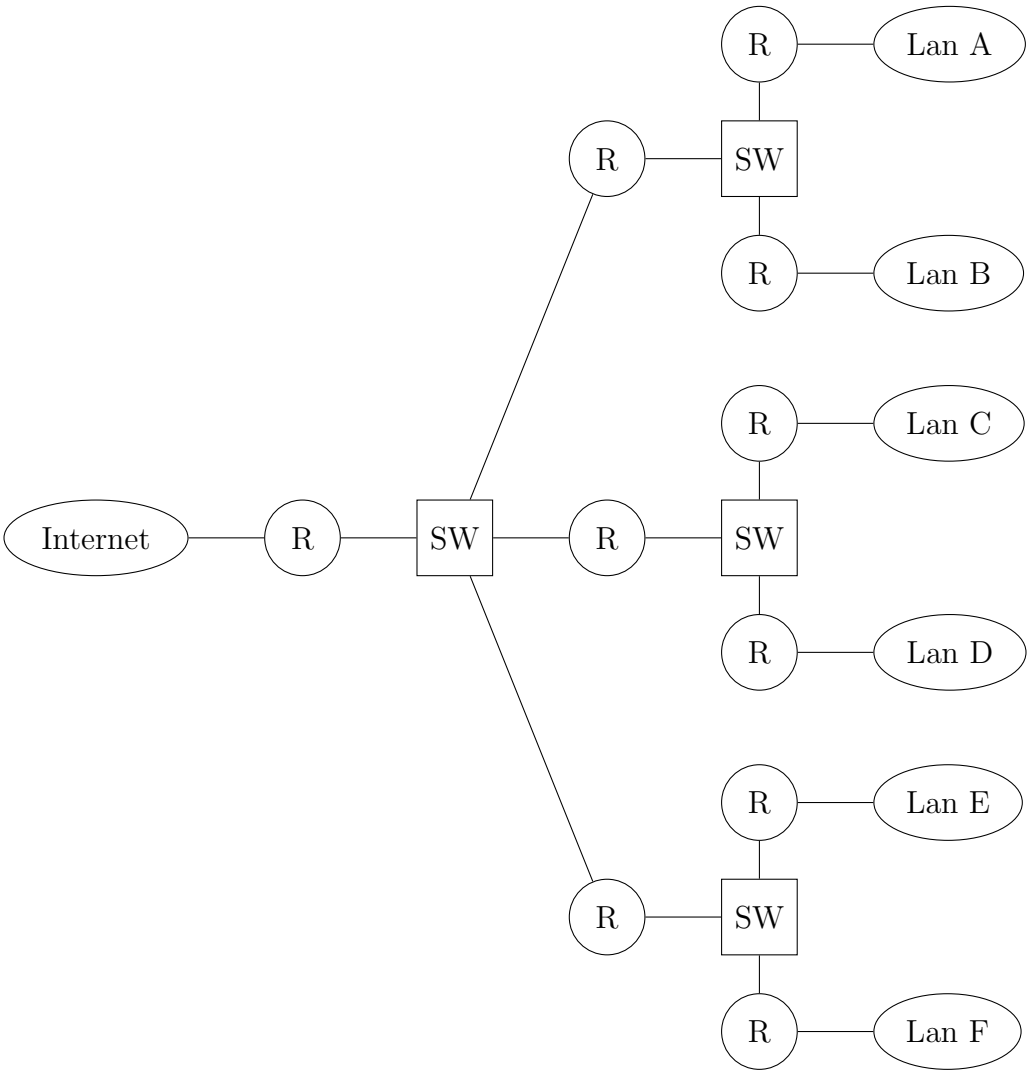


Figura 5.2: Situación del ejercicio 6

Ejercicio 5.2.7. Un datagrama de 4020 bytes pasa de una red Token Ring con THT 8 ms (MTU 4400) a una Ethernet (MTU 1500) y después pasa por un enlace PPP con bajo retardo (MTU 296). Si ese mismo datagrama pasara directamente de la red Token Ring al enlace PPP (sin pasa por la red Ethernet) ¿habría alguna diferencia en la forma como se produce la fragmentación? Especifique en ambos casos los fragmentos obtenidos.

Ejercicio 5.2.8. ¿Cómo podría utilizar ICMP para hacer una estimación de la latencia entre dos entidades finales? ¿Y para estimar la latencia de un enlace en particular entre dos routers?

Ejercicio 5.2.9. Considere la subred de la figura. Se utiliza el algoritmo de encaminamiento de vector distancia, habiéndose recibido en el encaminador C los siguientes vectores de encaminamiento: desde B (5, 0, 8, 12, 6, 2), desde D (16, 12, 6, 0, 9, 10) y desde E (7, 6, 3, 9, 0, 4). Los retardos medidos a B, D y E son, respectivamente, 6, 3 y 5. ¿Cuál es la nueva tabla de encaminamiento de C? Indique la línea de salida y el retardo esperado.

Ejercicio 5.2.10. Considere la red mostrada en la figura 5.3, en la que se representan 4 nodos unidos con enlaces. En cada enlace se indica el retardo sufrido por los mensajes al atravesarlo. Los nodos utilizan un protocolo de encaminamiento dinámico de tipo distribuido en el que la métrica está basada en el retardo. Se pide lo siguiente:

a. Escriba las tablas de encaminamiento para todos los nodos de la red una vez haya pasado el tiempo suficiente para que dichas tablas se construyan de forma estable.

b. Considere que los nodos envían y actualizan sus tablas cada 5 segundos, siendo la primera actualización en $t = 0$ s. Suponga que, en $t = 12$ s., el enlace BD pasa a tener un retardo de 3 s. ¿Cuál será el encaminamiento desde el nodo A hasta el nodo B cuando las tablas se estabilicen de nuevo?

c. ¿En qué instante comenzará dicho encaminamiento a funcionar? Justifique su respuesta explicando qué sucederá desde $t = 12$ s. hasta dicho instante y también después del mismo.

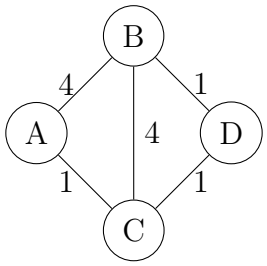


Figura 5.3: Grafo para el ejercicio 10.

Ejercicio 5.2.11. En la topología de red adjunta se indica la capacidad, en Kbps, de las líneas de transmisión entre los distintos nodos intermedios. Considérese al respecto que los enlaces son *full-duplex* y que la velocidad es la misma para cada uno de los sentidos. Por otra parte, la tabla anexa especifica el tráfico, en paquetes/segundo, entre cada par de nodos. Además, en cursiva se indica la ruta (secuencia de nodos) seguida en la transmisión. Teniendo en cuenta todo lo anterior, determine el retardo medio en el envío de un paquete sobre la red global.

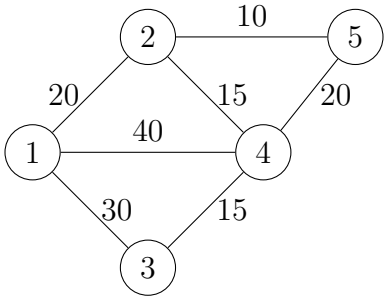


Figura 5.4: Grafo para el ejercicio 11.

		Nodo destino				
		1	2	3	4	5
Nodo origen	1		2-*12*	3-*13*	1-*14*	2-*145*
	2	2-*21*		4-*243*	2-*24*	2-*25*
	3	3-*31*	4-*342*		3-*34*	5-*345*
	4	1-*41*	2-*42*	3-*43*		1-*45*
	5	2-*541*	2-*52*	5-*543*	1-*54*	