Tema 1

Sistemas de comunicación y redes

Las redes es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y obtener servicios.

Un sistema de comunicación está formado por:
- Fuente: Dispositivo que genera los datos a transmitir
- Transmisor: Transforma y codifica la información generada en forma de señales electromagnéticas
- Sistema de transmisión: Medio a través del cual se produce el envío de información
- Receptor: Transforma las señales de manera que el destino pueda interpretar la información
- Destino: Encargado de tomar los datos procesados del receptor

Se espera que en una red haya autonomía, interconexión e intercambio de información con eficacia y transparencia. Permitiendo compartir recursos, escalabilidad, fiabilidad, robustez (a base de redundancia) y ahorro de costes.

Los componentes de una red son:
- Servidor: Computadora que controla la red y se encarga de permitir o no el acceso de los usuarios a los recursos. También controlan si un nodo puede pertenecer o no a la red.
- Estación de trabajo: Computadora conectada a una red pero que no puede controlarla.
- Nodo de red: Cualquier elemento conectado y comunicado a una red
- Tarjeta de red: Circuito integrado cuya función es recibir el cable que conecta a la computadora con una red informática.

Los medios de transmisión pueden ser:
- Cable coaxial: Hilo de cobre cubierto por una capa de plástico, una malla de hilos metálicos y una capa de hule
- Cable trenzado: 4 pares de cables
  - UTP: Sin pantalla (recubrimiento)
  - STP: Malla metálica sobre cada par de cables
  - FTP: Con pantalla global
- Fibra óptica: Muy resistente, pero de costo elevado. Fabricado a base de vidrio

Se llama topología de una red a la forma en la que están conectados sus nodos. Puede ser tanto física como lógica.
Tipos:
- **En bus**: Camino bidireccional donde la señal se propaga a ambos lados del emisor. Canal de difusión.
- **En anillo**: Camino unidireccional cerrado. Bucle si el acceso está centralizado.
- **En estrella**: Todos los nodos están conectados a un controlador central, encargado de gestionar las comunicaciones. Un fallo en un nodo es fácil de detectar, pero uno en el central desactiva la red al completo.
- **De árbol**: Variante de estrella donde no todos los dispositivos se conectan al central.
- **De malla**: Todas las computadoras están interconectadas entre sí, provee redundancia.
- **Híbrida**: Combinación de dos o más topologías anteriores. Si un solo equipo falla no afecta al resto de la red.

Las redes se pueden clasificar, según su tamaño:
- **LAN**: Redes de área local, para oficinas, colegios y empresas pequeñas. Suelen usar tecnología broadcast.
- **MAN**: Redes de área metropolitana, con el tamaño de una ciudad.
- **WAN**: Redes de área amplia. Colección de redes LAN conectadas por una subred
- **Internet**: Red de redes.
- **Inalámbricas**: Redes cuyos medios físicos no son cables, sino que transmiten a través de ondas.

Según la tecnología de transmisión:
- **Broadcast**: Por un solo canal de comunicación, compartido por todas las máquinas.
- **Point-To-Point**: Muchas conexiones entre parejas de máquinas. A veces los paquetes pasan por máquinas intermedias, siendo obligado un trazado de rutas.

Según el tipo de transferencia:
- **Transmisión simple**: Los datos solo viajan en un solo sentido
- **Half-Duplex**: Pueden viajar en ambos sentidos, pero no al mismo tiempo
- **Full-Duplex**: Pueden en ambos sentidos y a la vez.

Diseño y estandarización de redes

El modelo OSI está compuesto por siete capas donde cada una de ellas define las funciones que deben proporcionar los protocolos con el propósito de intercambiar información entre sistemas. Cada nivel depende de los que están por debajo de él, y ofrece funcionalidad a los de los niveles superiores. Estos solamente se comunican con los equivalentes en el lado del emisor, cada una añadiendo cabeceras, sin sobreescribir. Capas (de abajo a arriba):
- **Física**: Se encarga de las conexiones físicas de la computadora hacia la red, características del medio y la forma en la que se transmite la información. Transforma una trama de datos proveniente del nivel de enlace en una señal adecuada para el medio físico. Garantiza la conexión, aunque no la fiabilidad de esta.
- **Enlace**: Proporciona una transmisión sin errores. Crea y reconoce los límites de las tramas y resuelve los problemas derivados del deterioro, perdida o duplicidad de tramas. Encargada del direccionamiento físico, la topología, el acceso, la notificación de errores…
- **Red**: Hace que los datos lleguen del origen al destino, aunque no estén conectados directamente. Controla la congestión en red, el direccionamiento lógico y la determinación de la ruta.
- **Transporte**: Divide los datos en paquetes si es necesario.
- **Sesión**: Gestiona las conexiones entre usuarios, ofreciendo control de sesión, de concurrencia y mantenimiento de puntos de verificación.
- **Presentación**: Encargada de la representación de la comunicación, cifrado y compresión de datos.
- **Aplicación**: Protocolos para intercambiar datos como POP y SMTP

TCP/IP es el conjunto de protocolos común para la comunicación en Internet, es compatible con cualquier SO y tipo de HW. Está formado por las capas:
- **Aplicación**: Agrupa los niveles de aplicación, presentación y sesión de OSI. Protocolos destinados a proporcionar servicios (FTP, TELNET, HTTP)
- **Transporte**: Manejo de datos en el transporte (TCP y UDP)
- **Internet**: Nivel de red en OSI. Incluye a IP.
- **Acceso al medio**: Corresponde a la capa de enlace y física.

Terminología y servicios

Los elementos activos HW y SW de la capa N en una comunicación OSI reciben el nombre de entidades de nivel N. Existen dos tipos de comunicación:
- **Real o vertical**: Entre capas adyacentes en sentido descendente en el emisor y ascendente en el receptor.
- **Virtual u horizontal**: Comunicación observada entre las mismas capas en cada lado de la comunicación.

Un protocolo es un conjunto de reglas a utilizar en una comunicación entre 2 entidades paritarias (mismo nombre) para llevar a cabo un servicio. Junto al conjunto de capas los protocolos forman una arquitectura de red (TCP/IP).

Maximun Transfer Unit: Tamaño máximo de la trama que se puede transmitir. Cuanto más grande más se reduce la sobrecarga en la red y en las CPUs, pero implica mayores buffers, mayor pérdida de información y posibilidad de bloqueo de paquetes.
Para evitar estos errores los datagramas se fragmentan, puede ser en origen o en ruta.
Con el Path MTU Discovery se envía un paquete grande al router para que devuelva un error y el tamaño máximo que acepta.

Los servicios pueden ser:
- **Orientados a la conexión**: Antes de transmitir los datos se ha realizado una conexión.
- **Confirmados**: Cuando el emisor tiene constancia de la recepción

- **Retardos en la comunicación**
  - Tiempo de Propagación al siguiente salto (Tprop.)
    - Depende de la distancia y del medio de transmisión.
  - Tiempo de procesamiento en los routers (Tproc.)
    - Tiempo que se tarda en decidir que hacer con el paquete. Depende del router y de la carga.
  - Tiempo de espera en la cola salida (Tesp.)
    - Depende del tráfico en la red.
  - Tiempo de transmisión (Ttx.)
    - Depende de la velocidad del enlace y tamaño del paquete

$$T_{prop} = \frac{D\ (\text{Distancia a Recorrer})}{V\ (\text{Velocidad Propagación})}$$

$$T_{tx} = \frac{L\ (\text{Longitud del Paquete})}{V\ (\text{Velocidad Transmisión})}$$

El **Round Trip Time** es el tiempo para enviar un paquete y recibir su respuesta asociada. Ignorando los retardos, es el doble del tiempo de propagación)

Internet: Arquitectura y direccionamiento

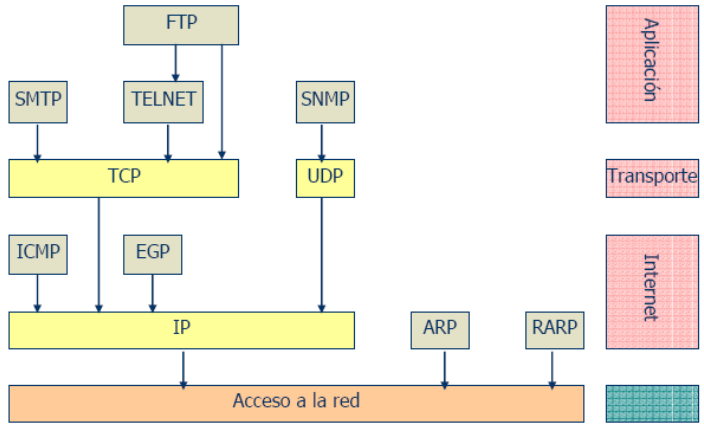
La estructura actual de Internet está basada en la conexión de redes de forma jerárquica, separada en 3 Tiers. Las conexiones se pueden hacer de dos formas:

- **De tránsito**: Entre operadores de igual jerarquía
- **De peering**: Para el intercambio de tráfico sin coste entre dos operadores. Cada operador publica sólo sus rutas. Pueden ser:
  - Públicos: Utilizando IXP, una infraestructura física para el intercambio de tráfico.
  - Privados: Conexión directa.

El método de identificación se realiza mediante direcciones IP de forma jerárquica. Existen dos versiones (IPv4 y IPv6), cada dirección puede ser pública (no se pueden repetir) o privada, y fijas o dinámicas.

Tema 2

Estructura de protocolos



Sockets

Proceso Cliente: El que inicia la comunicación desde su socket (identificador que cuenta con una IP y un puerto)
Proceso Servidor: El que espera a ser contactado (IP permanente y pública).

Protocolos

Tipos:
- De dominio público VS propietarios
- In-band VS Out-of-band: Si se controla o no el flujo de datos
- Stateless VS State-full: Si se trata cada petición como una transacción independiente o no
- Persistentes VS no-persistentes: Envío de varios objetos o no

La tendencia es a hacer una cabecera fija con unos parámetros TLV (Type-Length-Variable)

Características de las aplicaciones en red
Tolerancia a la pérdida de datos
Requisitos temporales, por si se necesita un retardo acotado
Rendimiento, ancho de banda
Seguridad

Protocolos de transporte
TCP es:
- Orientado a la conexión
- De transporte flexible
- Con control de flujo y de congestión

UDP en cambio:
- No orientado a la conexión
- Con transporte no fiable
- Sin control de flujo ni congestión

Ninguno de los dos garantiza por pertenecer a la capa IP:
- Retardo acotado
- Fluctuaciones acotadas
- Mínimo rendimiento
- Seguridad

Servicio de nombres de dominio (DNS)
Porque es más sencillo memorizar nombres que direcciones IP.
Cuenta con estructuro jerárquica en dominios: *parte-local.dominio0.dominio1…*

Las preguntas formuladas por los clientes DNS pueden ser:
- **Recursivas**: Obliga al servidor DNS a que responda aunque tenga que consultar a otros servidores
- **Iterativa**: El servidor contesta si tiene o no la información, en el caso de que no también indica la dirección de otro servidor capaz de resolver.

Para la gestión de la base de datos DNS, cada zona de be tener **al menos** un servidor de autoridad, teniendo cada zona servidores **primarios** (copia de la BD) y **secundarios** (obtiene la BD por transferencia). Además, existe un servicio caché para mejorar prestaciones.

La respuesta del servidor puede ser:
- CON autoridad: El servido tiene autoridad sobre la zona en la que se encuentra el nombre solicitado
- SIN autoridad: No tiene autoridad, pero si lo tiene en la caché.
- No conoce la respuesta: Se preguntará de forma iterativa o recursiva.

Navegación Web
Una página Web es un fichero HTML formado por objetos, cada objeto direccionado por una URL.
El protocolo HTTP sigue el modelo cliente-servidor, en base a los *browsers* y a los *servers*

Características HTTP:
- TCP al puerto 80
- "Stateless", el servidor no mantiene información sobre las peticiones de los clientes (las *cookies* van aparte)
- Puede ser **no persistente** si se envía un único objeto en cada conexión TCP, o **persistente** si permite varios.

Proceso HTTP:
1. Cliente inicia la conexión al puerto 80 del servidor
2. Servidor acepta y notifica
3. Cliente envía solicitudes de objetos
4. Servidor envía los mensajes
5. Si es persistente se envían más objeto, en otro caso se cierra la conexión.

Existen dos tipos de mensajes:
- **Request**: Con solicitud GET, POST o HEAD
- **Response**: Con código de estado de la operación anterior, versión de HTTP e información solicitada.

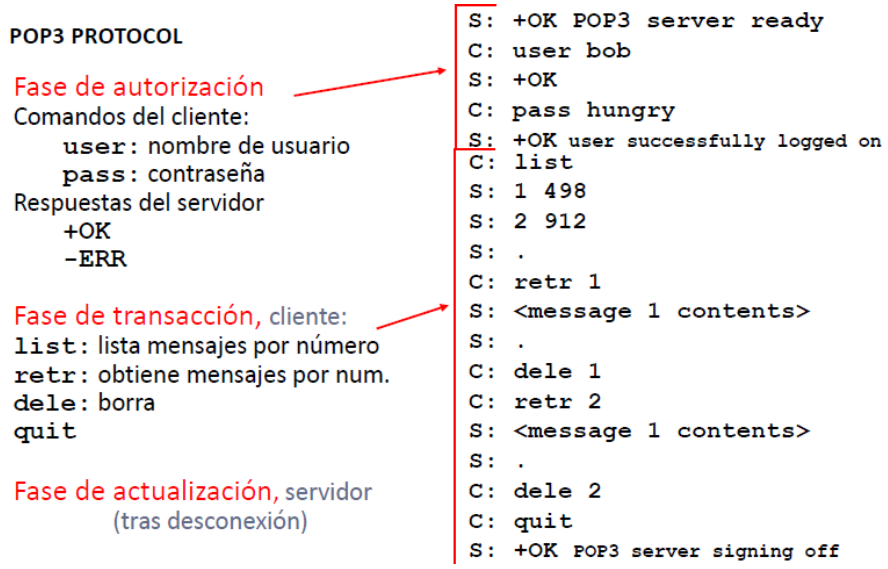
La caché satisface el requerimiento del cliente sin involucrar al servidor de destino. A veces solicita al servidor preguntando si el objeto se ha actualizado (conditional GET)

<u>Correo electrónico</u>
Basado en 4 componentes principales:
- Cliente de correo: Compone, edita y lee
- Servidor de correo: Donde se almacenan los mensajes salientes y entrantes
- Simple Mail Transfer Protocol SMTP
- Protocolos de descarga POP3, IMAP, HTTP

Pasos del envío/recepción de correo:
1. El usuario compone mediante su Agente de Usuario un mensaje dirigido a la dirección de correo del destino
2. Se envía con SMTP o HTTP el mensaje al servidor de correo origen que lo sitúa en la cola de mensajes salientes
3. El cliente SMTP abre una conexión TCP con el servidor de correo del usuario destiino
4. El cliente SMTP envía el mensaje sobre la conexión TCP
5. El servidor de correo del usuario destino ubica el mensaje en la mailbox del usuario destino
6. El usuario invoca a su Agente para leer el mensaje utilizando POP3, IMAP o HTTP

SMTP utiliza 3 fases (handshaking, transferencia y cierre); sus mensajes se realizan mediante comandos y códigos de respuesta en ASCII

MIME permite extender el correo al envío de otro tipo de objetos (no solo texto)



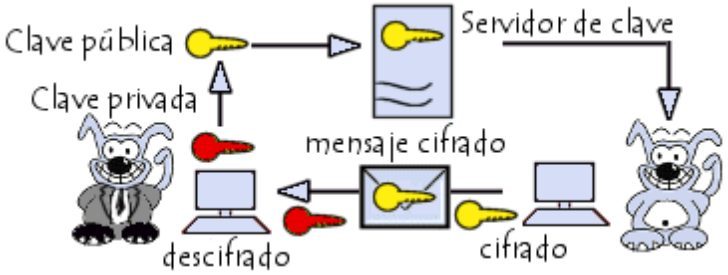
Ventajas de IMAP:
- Permite organización en carpetas en el lado del servidor
- Mantiene información entre sesiones
- Permite la descarga de partes de los mensajes
- Posible acceder con varios clientes

Ventajas de Web MAIL:
- Organización total en el servidor, accesible desde cualquier cliente con HTTP
- Seguridad mediante HTTPS

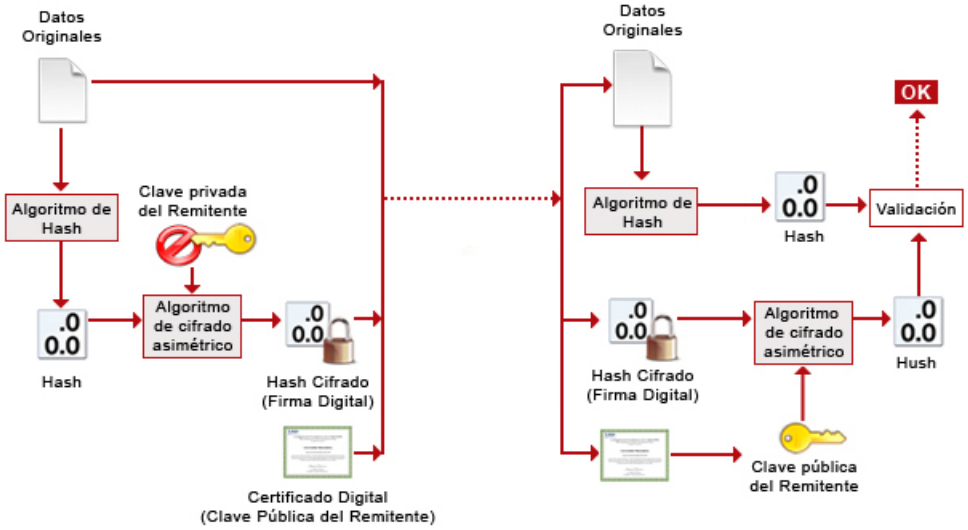
Puertos:
- POP3: 110
- IMAP: 143
- SMTP: 25

<u>Seguridad y protocolos seguros</u>
Primitivas de seguridad:
- **Confidencialidad**: Solo accede a la información quien debe hacerlo
- **Responsabilidad**
  - Autenticación: Los agentes de la comunicación son quien dicen ser
  - No repudio: No se puede negar el autor de una determinada acción
  - Control de accesos: Garantía de identidad para el acceso
- **Integridad**: La información no ha sido manipulada
- **Disponibilidad**: Acceso a los servicios

Mecanismos de seguridad:
- **Cifrado de clave privada**: Las claves de cifrado y descifrado son la misma, se utiliza en el intercambio de información una vez establecida la sesión. La clave se debe transmitir de forma segura.
- **Cifrado de clave pública**: Se basa en el uso de dos claves, una puede descifrar lo que la otra ha cifrado.
  La pública es usada por el propietario para cifrar los mensajes y la cifrada para descifrar, logrando **confidencialidad** en el envío.
  Si el propietario usa su clave privada para cifrar, cualquiera puede descifrarlo con la pública, consiguiendo **autentificación e identificación**.



- **Firma Digital**: Proceso que permite garantizar la autenticidad del remitente y verificar la integridad del mensaje recibido.



- **Certificado Digital**: Permite asociar una clave pública con una entidad para garantizar su validez, puesto que el cifrado asimétrico no garantiza que la clave pertenezca al usuario con el que está asociada.
  La entidad firma un certificado y esto implica que una función hash crea una huella digital y luego este hash se cifra con la clave privada de la entidad. La clave pública se distribuye antes de tiempo para permitir a los usuarios verificar la firma de la entidad.

<u>Aplicaciones multimedia</u>
La **calidad de servicio** es la capacidad de ofrecer el rendimiento requerido para una aplicación.
El **mejor esfuerzo** no garantiza la calidad de servicio.

Tipos de aplicaciones:
- Flujos de audio y video almacenado
- Flujo de audio y video en vivo
- Audio y vídeo interactivo

Características:
- Elevado ancho de banda
- Tolerantes a la pérdida de datos
- Delay acotado: Medida del tiempo en la que un paquete tarda en viajar desde el origen hasta un destino
- Jitter acotado: Variabilidad temporal durante el envío de señales digitales (ruido)
- Uso de multicast

<u>Aplicaciones para interconectividad de redes locales</u>
DHCP: Configuración dinámica de direcciones IP

<u>Tema 3</u>

Introducción

Las funciones de la capa de transporte son asegurar la comunicación **extremo a extremo** y la **multiplexación/demultiplexación** de aplicaciones (a través del puerto)

Protocolo de datagrama de usuario (UDP)

Con funcionalidad *best-efford*: no orientado a la conexión, no fiable, sin garantías de entrega ordenada ni control de congestión.

Se utiliza frecuentemente en aplicaciones multimedia, tolerantes a fallos y sensibles a retardos. Cada segmento UDP se encapsula en un datagrama IP.

Protocolo de control de transmisión (TPC)

Servicio orientado a la conexión, con entrega ordenada y full-duplex, fiable ya que cuenta con mecanismo de control de congestión y de control de flujo basado en:

- Confirmaciones positivas (ACKs) y acumulativas
- Incorporación de confirmaciones
- "Timeouts" adaptables
- Ventanas adaptables

Cada segmento TCP se encapsula en un datagrama IP, y la conexión TCP se identifica por el puerto e IP origen junto al puerto e IP destino

Control de conexión TPC

Cuenta con tres fases:

- **Establecimiento de la conexión (reserva de recursos)**: Puede ser una apertura tanto activa (cliente) como pasiva (servidor)
- **Intercambio de datos**
- **Cierre de la conexión (liberación de recursos)**: Puede ser tanto un cierre activo como pasivo

Los nº de secuencia son un campo de 32 bits inicializado a un contador (ISN del sistema) que ayuda a identificar la conexión, este nº protege de coincidencias, pero no de sabotajes. Se incrementa en base a los bytes de la carga útil.

Control de errores y de flujo en TCP

Se utiliza una ventana deslizante que ayuda a mejorar el rendimiento, y un sistema con confirmaciones positivas y acumulativas para controlar los errores.

La generación de ACKs funciona de la siguiente manera:

Evento	Acción del TCP receptor
Llegada ordenada de segmentos, sin discontinuidad y todo lo anterior confirmado	Retrasar el ACK. Esperar recibir el siguiente segmento hasta los 500 ms, en caso de que no llegue, enviar ACK
Llegada ordenada de segmento, sin discontinuidad pero hay pendiente un ACK retrasado	Enviar inmediatamente un ACK acumulativo
Llegada desordenada de segmentos con un nº de secuencia mayor que el esperado, discontinuidad detectada	Enviar un ACK duplicado, indicando el nº de secuencia del siguiente byte esperado
Llegada de un segmento que completa una discontinuidad parcial o totalmente	Confirmar ACK inmediatamente si el segmento comienza en el extremo inferior de la discontinuidad.

Para estimar los timeout, se debe tener en cuenta de que debe ser mayor que el RTT. Si es demasiado grande habrá una reacción lenta a la pérdida de segmentos, y si es muy pequeño habrá timeouts prematuros. Se considera mejor opción la solución adaptable. Se actualizan los RTT sólo para los segmentos no repetidos.

La pérdida y/o retrasos en los ACKs es la que permite el control de congestión. Procedimiento:

- En el emisor se utilizan una ventana y un umbral
- Inicialmente *Ventana = MSS (Maximum segment size)* y *Umbral* a un cierto valor

- Si *Ventana < Umbral* por cada ACK recibido *Ventana += Ventana* (**Inicio lento**)
- Si *Ventana > Umbral* por cada ventana completada *Ventana += MSS* (**Prevención de la congestión**)
- Si hay timeout entonces *Umbral = Ventana/2* y *Ventana = MSS* (**Tahoe**) o *Ventana = Ventana/2* (**Reno**)

Tema 4

Funciones y servicios en TCP/IP

Encaminamiento, conmutación, interconexión de redes y (en OSI) control de congestión.

Protocolo IP

Permite la interconexión de redes y el direccionamiento en Internet, siguiendo la retransmisión salto a salto entre hosts y routers. Protocolo no orientado a la conexión y no fiable (*best-efford*). Gestiona la fragmentación, y la unidad de datos (paquete) se denomina datagrama.

Para determinar las subredes, se debe separar cada interfaz de los hosts y routers, creando redes aisladas.

La dirección IP cuenta con dos partes: Subred y dispositivo (no cubierta por la máscara)
La máscara se elige según el nº de dispositivos: $Nº\ dispositivos = 2^{nº\ ceros} - 2$

Encaminamiento

Consiste en llevar los paquetes de un origen a un destino en una red. El encaminamiento per sé se llama **routing** (decisión de rutas), la retrasmisión **forwarding**

Asociación con Capa de Enlace: El protocolo ARP

Las direcciones MAC son usadas en redes Ethernet y Wifi, son únicas.
El protocolo ARP sirve para obtener la MAC de un dispositivo a partir de su IP, RARP para la inversa.

Protocolo ICMP (Internet Control Message Protocol)

Sirve para informar sobre situaciones de error, encapsulándose en IP