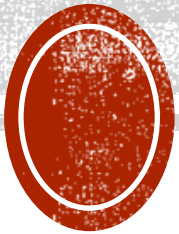
CONCEPTOS BÁSICOS DE TCP/IP

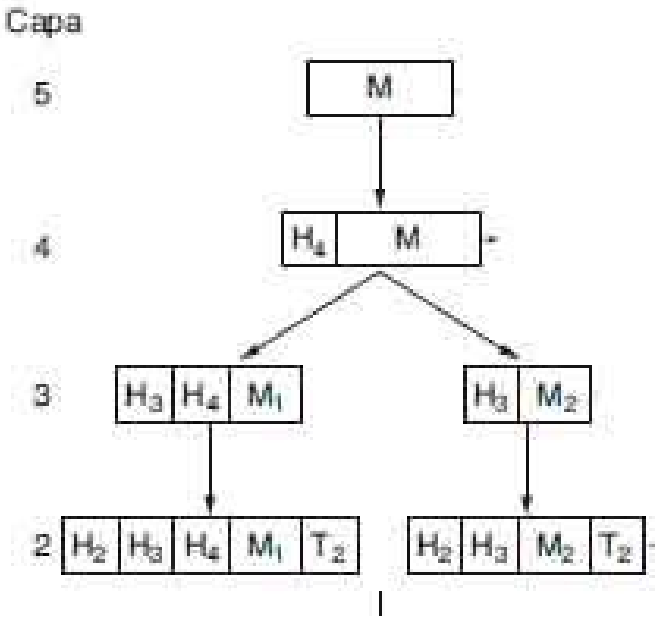


CONCEPTO

- ¿Qué es? ¿A qué nos referimos con una Arquitectura de Red?
  - Conjunto de protocolos organizados por niveles que trabajan de forma conjunta para la transferencia de datos y ofrecer servicios de forma segura y fiable.
  - Es el diseño de una red de comunicaciones
  - Viene definida por tres características fundamentales
    - Topología: establece la configuración básica de interconexión de estaciones
    - Método de acceso a red: regular el orden en que transmiten los equipos
    - Protocolos de comunicación: reglas y procedimientos utilizados en una red para realizar la comunicación

CÓMO FUNCIONA

- Dentro de una máquina
  - Cada nivel utiliza los servicios del nivel inferior
  - Un servicio se define como un conjunto de operaciones que una capa proporciona a la capa superior o al usuario.
    - Ej: servicio web
  - En el emisor la información viaja hacia abajo (del usuario al medio) y cada nivel del emisor añade su propia información en forma de cabecera
  - En el receptor la información viaja hacia arriba (desde medio hacia el usuario) y cada nivel del receptor extrae la información de cabecera que le corresponde y entrega el resto al nivel superior



CÓMO FUNCIONA

- Entre máquinas distintas
  - El nivel n de una máquina A se comunica con el nivel n de la otra máquina B mediante un protocolo
  - Los procesos del mismo nivel que se comunican se llaman procesos pares
    - Ej: Servidor web httpd.exe y cliente chrome.exe
  - Protocolo: conjunto de reglas que regulan el formato y significado de los paquetes que intercambian dos procesos pares
    - Ej: HTTP

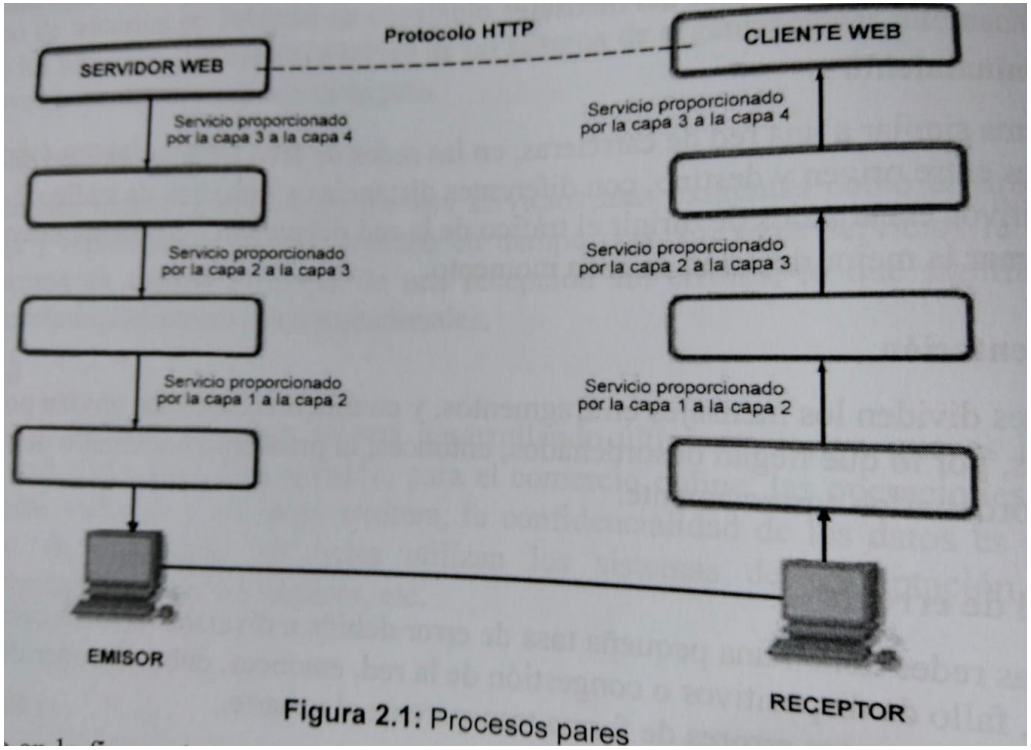


Figura 2.1: Procesos pares

MODELO OSI

- Estándar desarrolla la Organización Internacional de Estandarización (ISO) en 1983
- Cubre todos los aspectos de las redes de comunicaciones
- Está compuesto por niveles

- ¿Recuerdas cuántos niveles, su nombre y función de cada uno?

MODELO OSI

- Está compuesto por 7 niveles

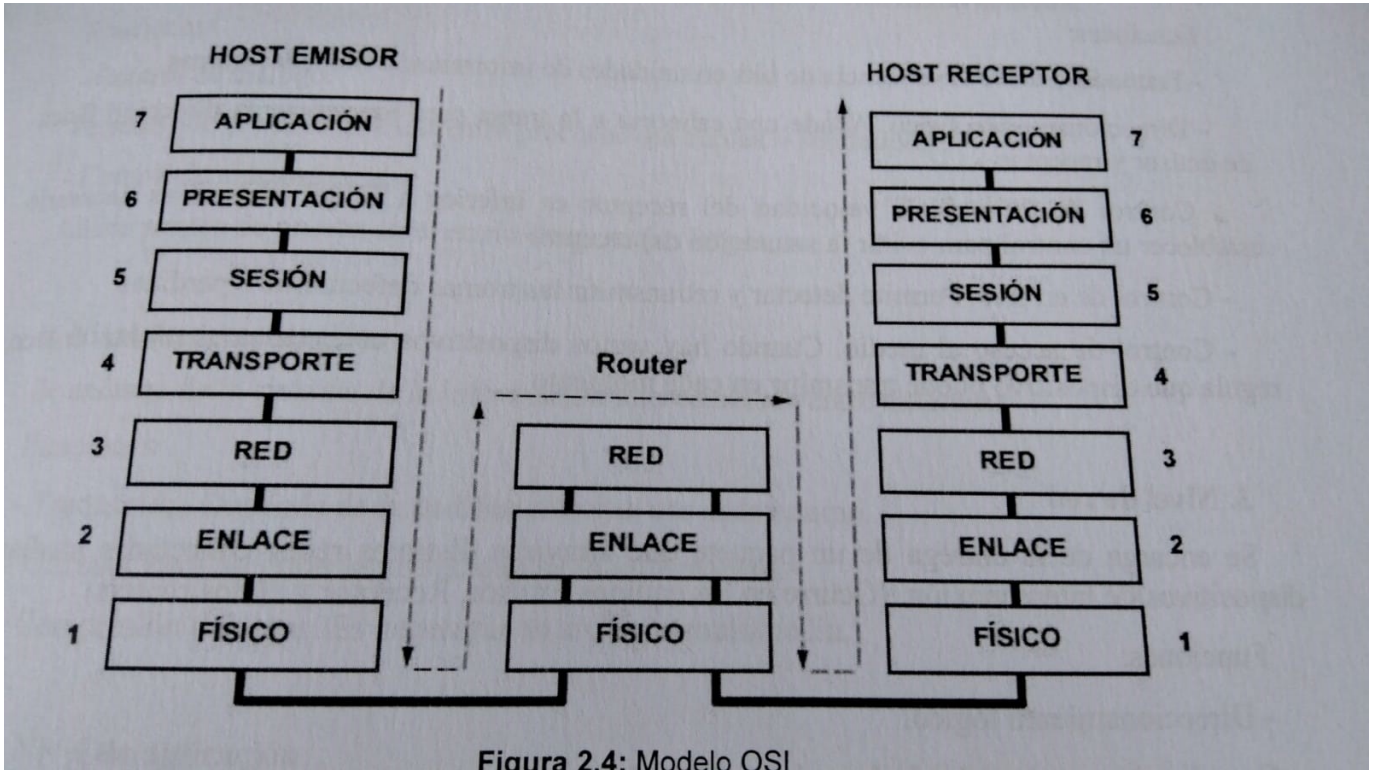


Figura 2.4: Modelo OSI

MODELO OSI

- Funciones de cada nivel

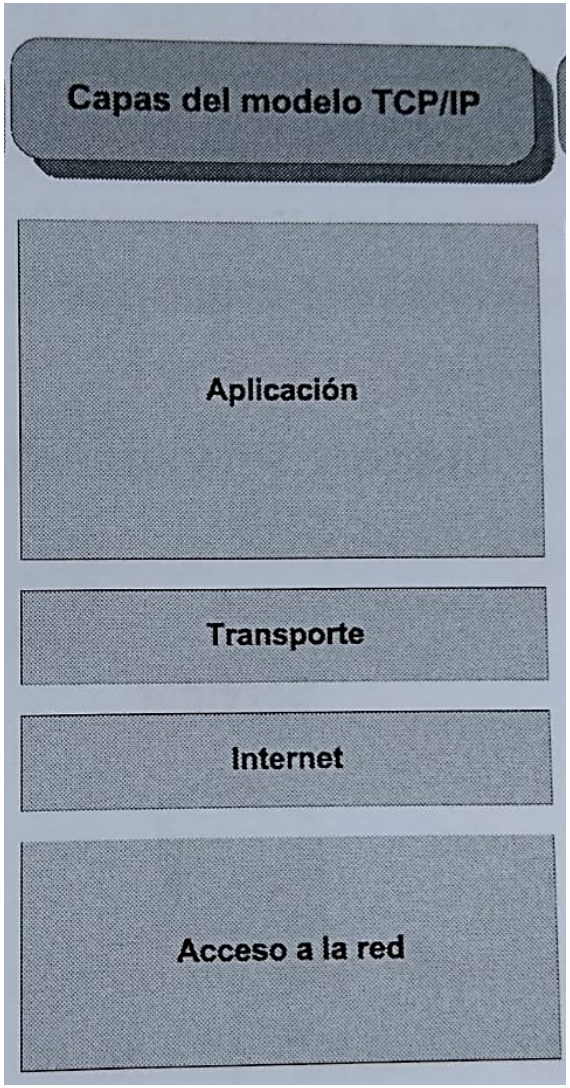
Capa	Se encarga de…
Nivel Físico	Transmitir el flujo de bits a través del medio físico (cable/aire)
Nivel Enlace de Datos	La entrega de los datos de un equipo a otro de manera fiable
Nivel de Red	La entrega de un paquete que atraviesa distintas redes conectadas mediante dispositivos de interconexión
Nivel de Transporte	Entregar el mensaje completo. Reúne todos los paquetes que constituyen el mensaje
Nivel de Sesión	Establecer el diálogo de la red, estableciendo y terminando sesiones
Nivel de Presentación	La sintaxis de la información intercambiada entre sistemas (Cifrado, Compresión datos)
Nivel de Aplicación	Permitir al usuario y al S.O el acceso a la red (Web, DNS, FTP, Mail, Chat, etc…)

ARQUITECTURA TCP/IP

- Se desarrolló antes que el modelo OSI
- Proporciona una estructura y una serie de normas de funcionamiento para poder interconectar sistemas
- TCP/IP es un conjunto de protocolos organizados jerárquicamente con una función determinada y una cierta independencia entre sí.
- ¿Recuerdas cuántos niveles, su nombre y función de cada uno?

ARQUITECTURA TCP/IP

- Está compuesto por 4 niveles

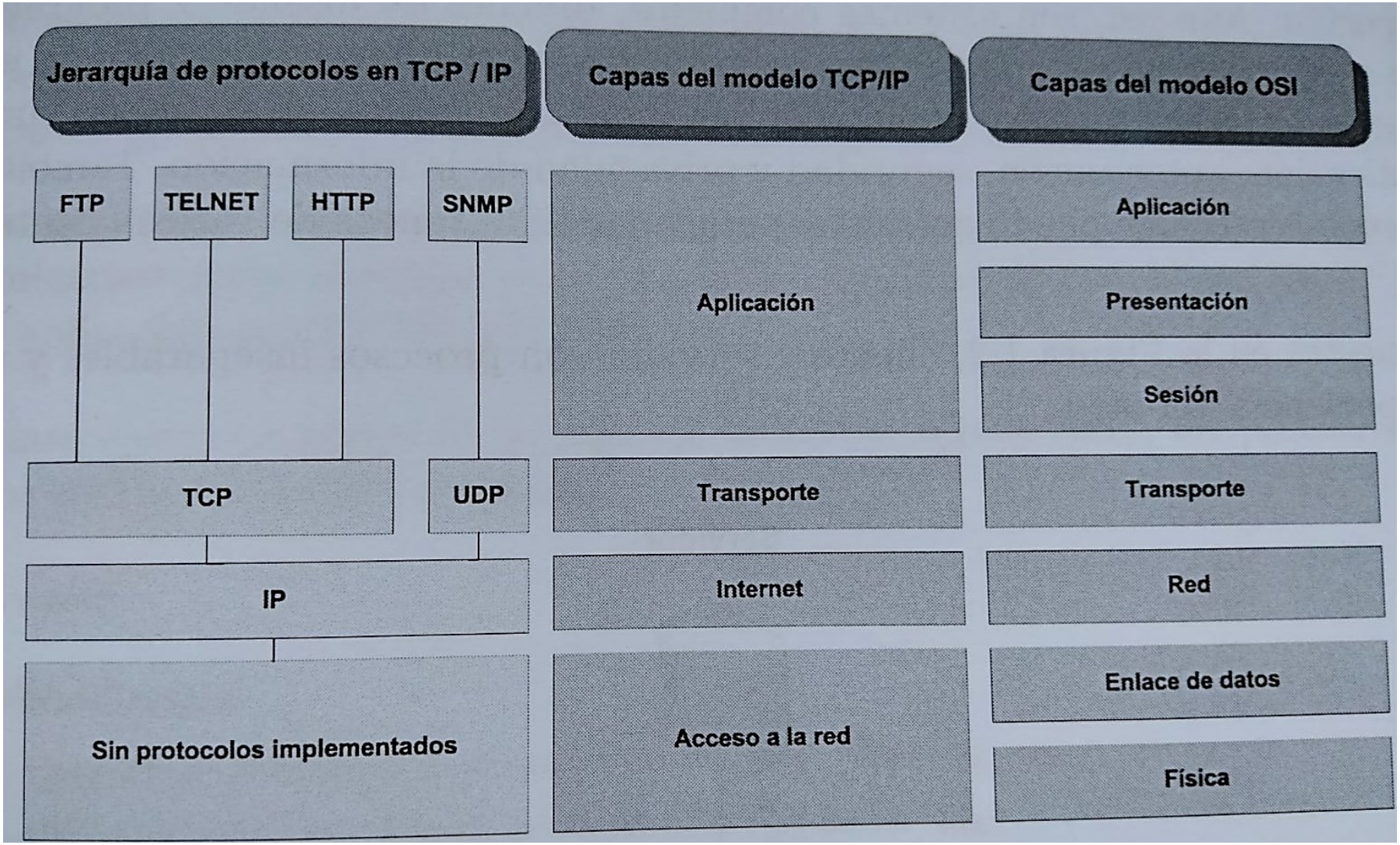


ARQUITECTURA TCP/IP

- Funciones de cada nivel

Capa	Se encarga de…
Acceso a Red	Utiliza protocolos estándar de cada red. Protocolos: SLIP, PPP, HDLC, Ethernet,etc.
Internet	Permitir el envío de paquetes por caminos independientes mediante direccionamiento lógico y enrutamiento Protocolos: IP, ICMP, etc
Transporte	La segmentación de los datos en el origen, la ordenación de paquetes en destino y control errores Protocolos **TCP** y **UDP**
Aplicación	Proporciona la interfaz con el usuario y contiene los protocolos de alto nivel Protocolos: DHCP, DNS, FTP, HTTP, SMTP, POP3, IMAP, etc

COMPARATIVA TCP/IP - OSI



MODELO CLIENTE/SERVIDOR

- Está formado por dos procesos: el proceso cliente y el proceso servidor
- El cliente
  - Inicia comunicación -> papel activo
  - Envía petición a un proceso servidor
  - Queda a la espera de respuesta
- El servidor
  - Permanece a la espera escuchando → papel pasivo
  - Envía una respuesta al cliente
  - Complejos: autentificación, autorización, seguridad y privacidad

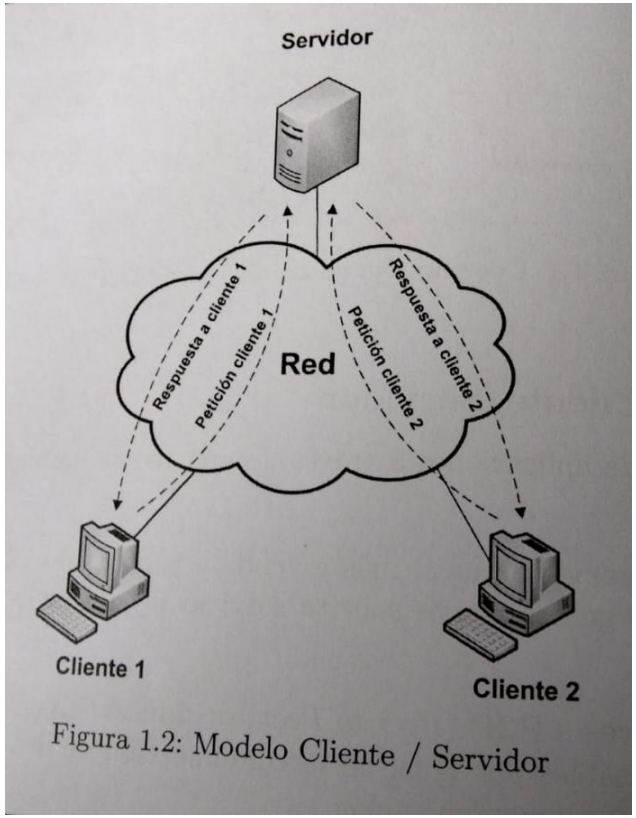


Figura 1.2: Modelo Cliente / Servidor

SERVICIOS DE RED

SERVICIOS DE RED

- Función o prestación que ofrecen las aplicaciones y los protocolos a los usuarios o a otras aplicaciones.
- Las aplicaciones son sistemas de sw que se comunican e intercambian información con otras aplicaciones con la ayuda de los protocolos de la **arquitectura TCP/IP**
  - **OJO: no confundir los protocolos del nivel de aplicación con las aplicaciones que lo utilizan**

DEFINICIONES

- **Aplicación**: Programas de los usuarios o del sistema operativo que se sirve de los protocolos de la arquitectura TCP/IP para comunicarse

  Thunderbird, Apache

- **Protocolo**: Normas concretas que detallan cómo se produce la comunicación entre sistemas para ofreces los servicios de red.

  IMAP, HTTP

Hay protocolos en todas las capas, y los protocolos de una capa, utilizan los protocolos de la capa inferior.

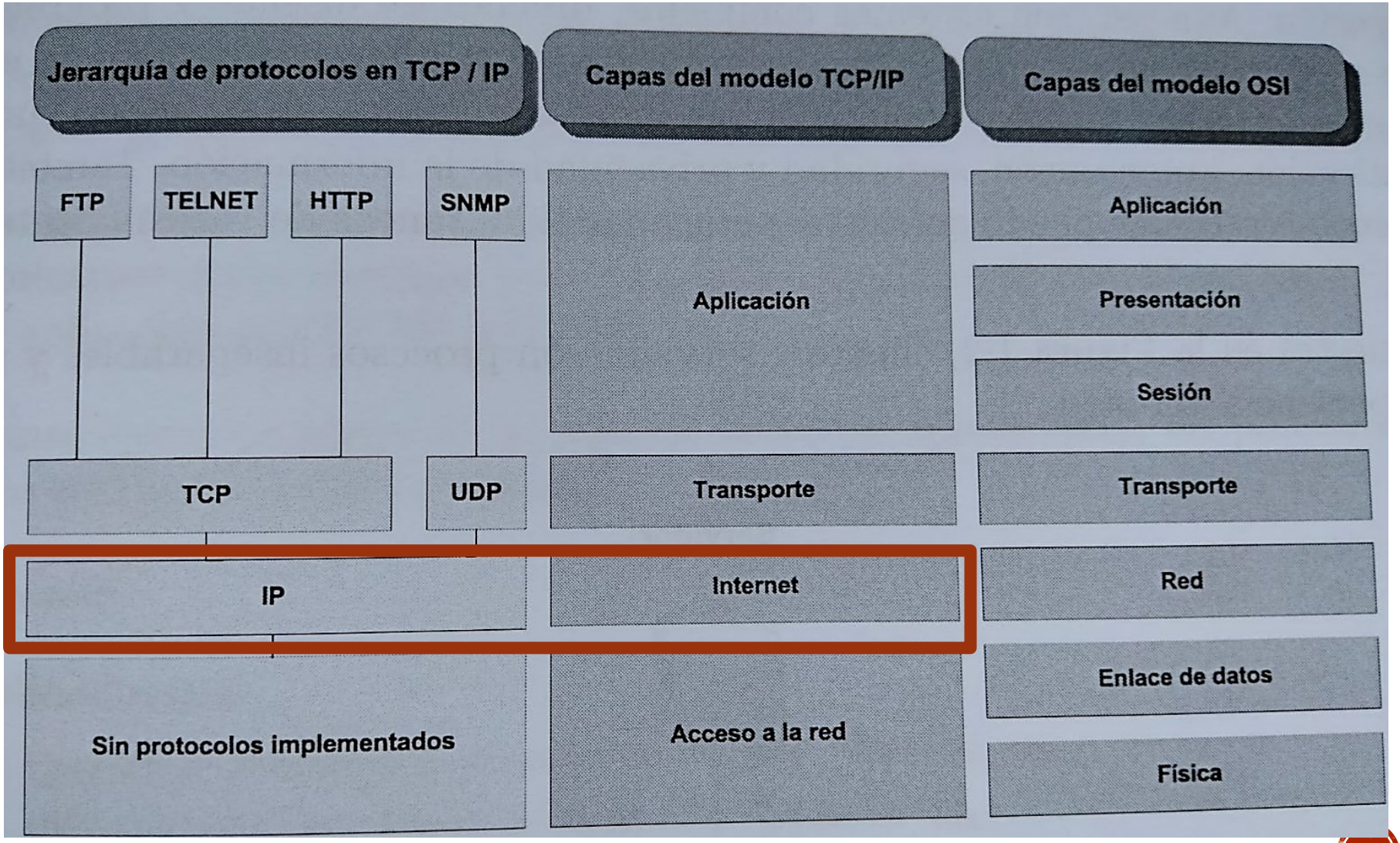
EJEMPLOS REALES

- SERVICIO WEB
  - Aplicaciones:
    - **Servidor:** IIS, Apache, etc.
    - **Cliente:** Firefox, Chrome, etc.
  - **Protocolos:** HTTP, HTTPS

- SERVICIO CORREO ELECTRÓNICO
  - Aplicaciones:
    - **Servidor**: Exchange, Sendmail, etc.
    - **Cliente:** Outlook, Thunderbird
  - **Protocolos**: IMAP, POP, SMTP

Para entender el funcionamiento del servicio de red hay que prestar atención a los niveles de red y transporte de la arquitectura TCP/IP

NIVEL DE RED – EL PROTOCOLO IP



PROTOCOLO IP

- A nivel de Red se realiza el direccionamiento de los dispositivos y el encaminamiento de la información a través de la red.
- La comunicación a nivel IP se hace mediante unidades de datos llamadas datagramas.
- Actualmente se emplea la versión 4 (IPv4), pero ya está implementada la versión IPv6.
- El protocolo IP proporciona conectividad extremo a extremo en la comunicación.
- Cada dispositivo está identificado por una (dirección) IP.

PROTOCOLO IP

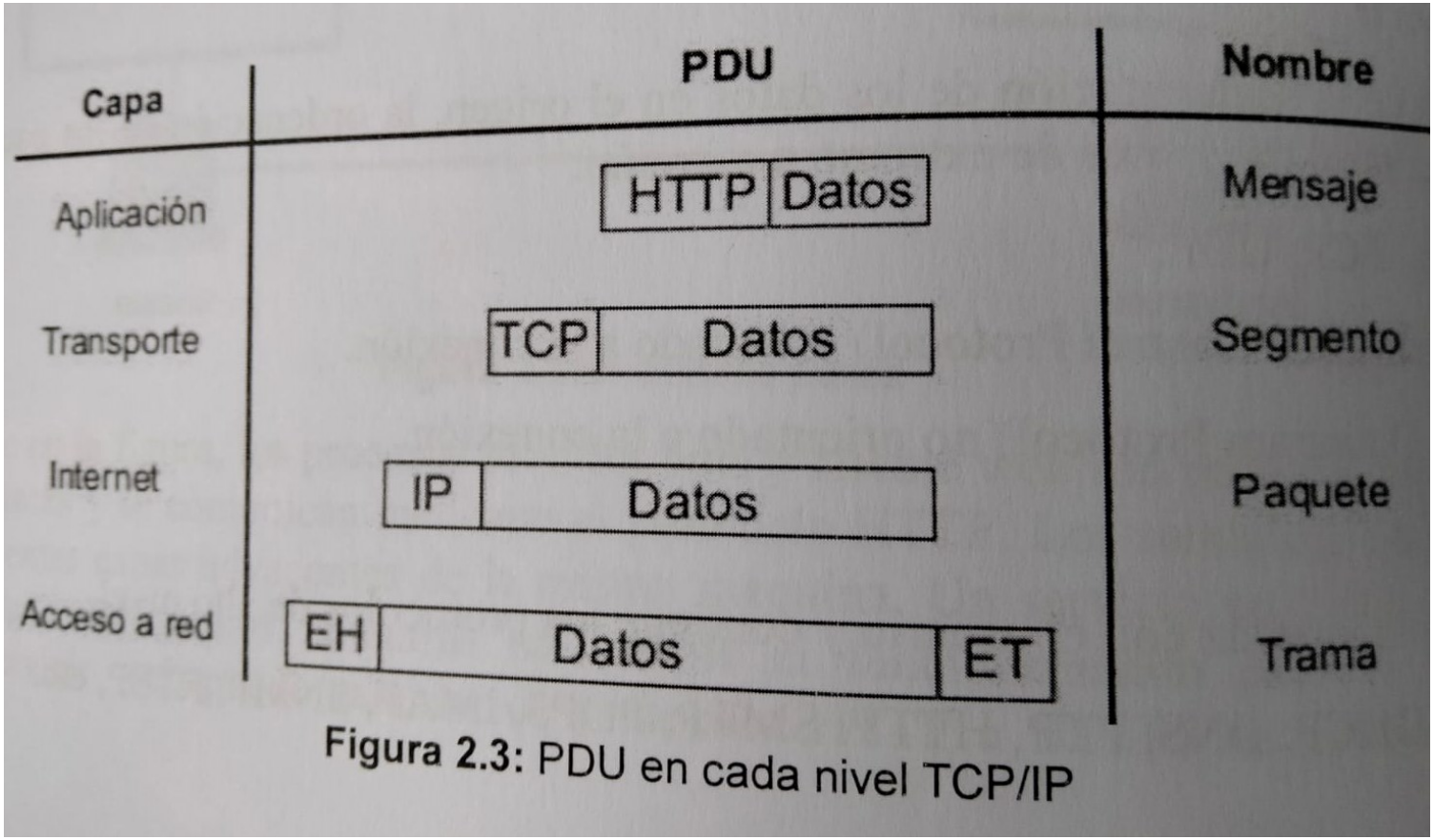


Figura 2.3: PDU en cada nivel TCP/IP

ENCAMINAMIENTO IP

- Proceso de llevar un datagrama de una máquina origen a la máquina destino.
- El responsable es el protocolo IP
- Si las máquinas no están en la misma red, se utilizan encaminadores

ENCAMINADOR O ROUTER

- Dispositivos de nivel 3 (internet o red) que enlazan las diferentes redes
- Conectan al menos 2 redes
- Encaminan todo el tráfico de datagramas que pasa por ellos, mediante tablas de encaminamiento

ENCAMINAMIENTO

- Todos los componentes a nivel de red (host, routers,…) tiene tablas de encaminamiento o enrutamiento.
- Cuando un equipo va a enviar un datagrama comprueba la tabla de enrutamiento. Simplificando:
  - Si el destino está en su misma red, hace un envío directo.
  - Si el destino está en una red distinta, lo dirige al encaminador (puerta de enlace).
- Cuando un router recibe un datagrama comprueba su tabla de enrutamiento.
  - Si va a una dirección que pertenece a una red conectada directamente, envío directo.
  - Si no, lo redirige a otro encaminador, siguiendo su tabla de encaminamiento. Este proceso puede ser recursivo y termina cuando se agota el tiempo de vida (TTL)

TABLA DE ENRUTAMIENTO

- Almacena información necesaria para el encaminamiento de datagramas y están implementadas tanto en los routers como en los hosts
- Campos más importantes
  - Destino (D): Dirección IP de una red o host.
    - Ruta de red: Referencia una red
    - Ruta de host: Referencia un host
    - Ruta por defecto: Cuando no es ninguna de las anteriores.
  - Máscara de Red (MR): Asociada al destino y sirve para conocer todas las direcciones IP que incluye.
  - Dirección de salto (DS): Dirección IP a la que se enviará el datagrama si su dirección IP de destino coincide con la especificada por Destino y Máscara de Red
  - Interfaz: dirección IP de encaminador por la que hay que enviar el datagrama a la dirección de salto.

TABLA DE ENRUTAMIENTO

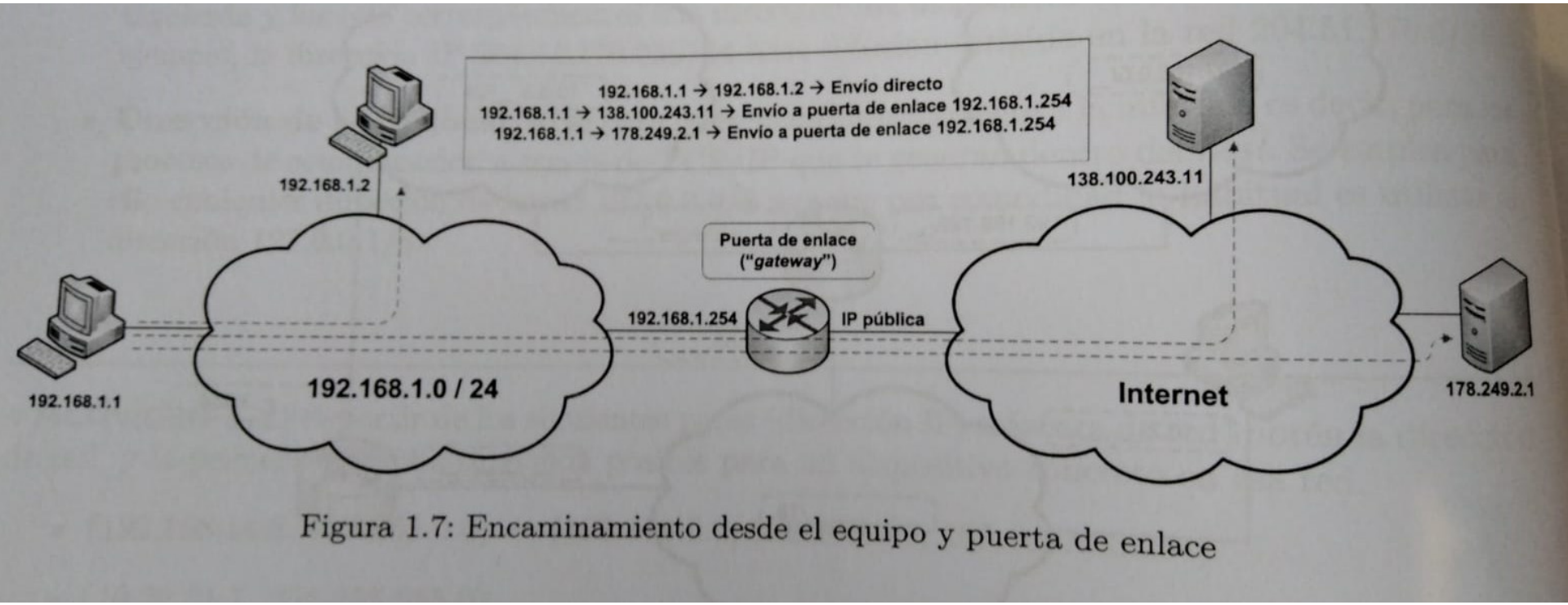


Figura 1.7: Encaminamiento desde el equipo y puerta de enlace

PROTOCOLOS DE ENCADENAMIENTO

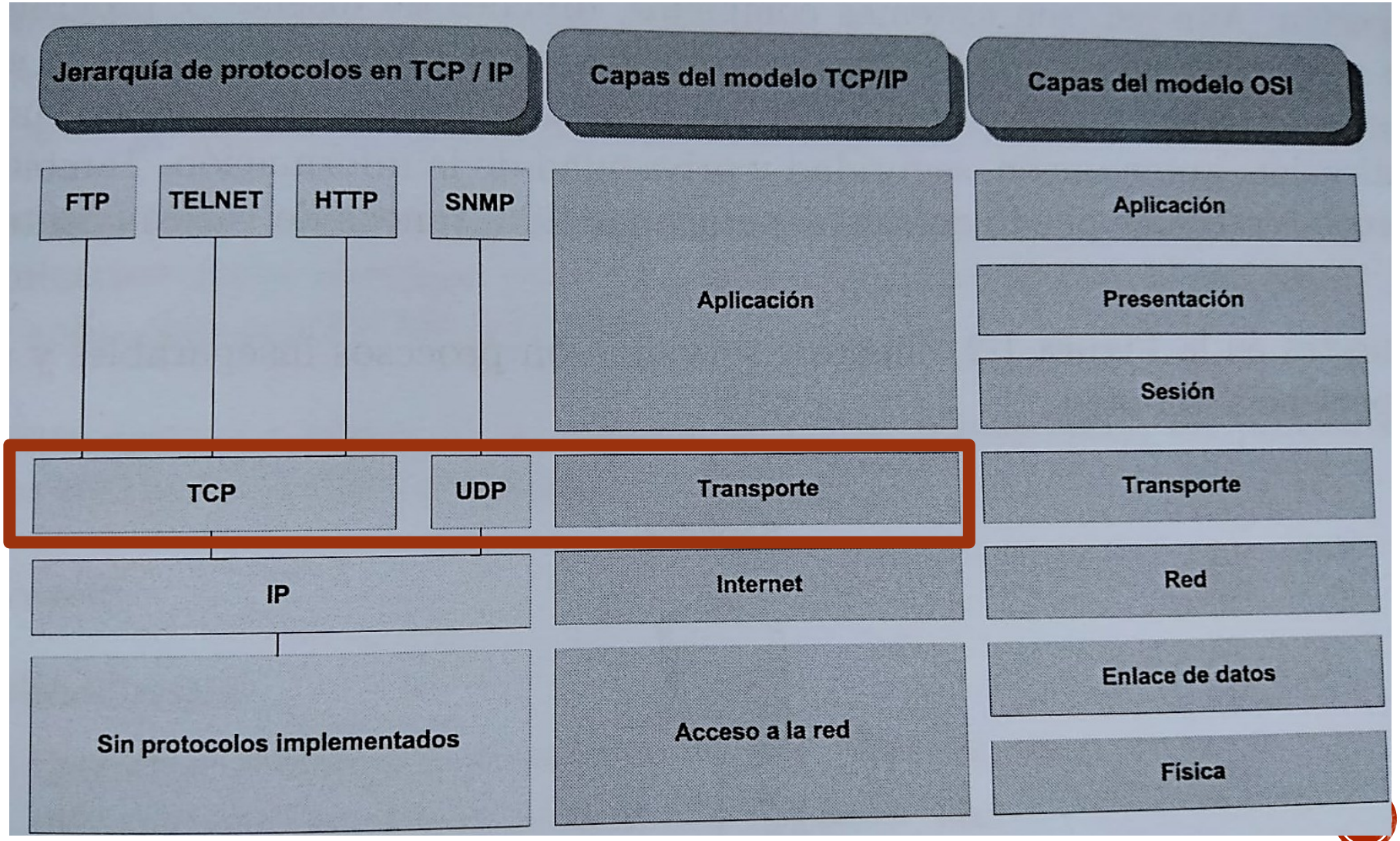
- **Encadenamiento estático:** La configuración de las tablas de rutas es de forma manual.

- **Encadenamiento dinámico:** El encaminador actualiza sus tablas de ruta gracias a protocolos específicos:
  - RIP (Routing Information Protocol)
  - OSPF (Open Shortest Path First)
  - BGP (Border Gateway Protocol)

TAREA

- Consulta la tabla de enrutamiento de tu PC.
- Indica todos los sitios por los que circula un datagrama que se envía desde tu ordenador a la dirección www.google.es
- Y si el datagrama fuera de www.google.es hacia tu equipo. ¿Circularía por los mismos sitios?
- ¿Qué comando has utilizado? ¿Qué información muestra ese comando? ¿Cómo funciona el comando?

NIVEL DE TRANSPORTE: PROTOCOLOS TCP Y UDP



NIVEL DE TRANSPORTE: PROTOCOLOS TCP Y UDP

- El protocolo IP permite comunicar dos máquinas, pero si dos o más aplicaciones requieren comunicación entre esas dos máquinas, el protocolo IP no permite diferenciar de qué aplicación son los datagramas.

- El nivel de transporte provee elementos para diferenciar y gestionar múltiples orígenes y destinos en una comunicación, y múltiples comunicaciones en cada equipo de forma simultánea.

PUERTOS DE COMUNICACIONES

- Los protocolos del nivel de trasporte implementan el concepto de **puerto de comunicaciones que permite identificar los procesos del nivel de aplicación** entre los que se establece la comunicación.

- Cada proceso del nivel de aplicación tiene asociado uno o varios puertos a través de los cuales es accesible.

- Los puertos se identifican con un número de 16 bits. (0 – 65535)

PUERTOS DE COMUNICACIONES

- Puertos conocidos (0 - 1023): se conocen como *well known ports* y están reservados para aplicaciones y servicios estándar (HTTP, FTP,…)

- Puertos registrados (1024 – 49151): para aplicaciones no estándar instaladas por el usuario que no tienen un puerto well known preasignado. Estos puertos pueden asignarse dinámicamente a clientes, si ningún servicio está haciendo uso de ellos.

- Puertos dinámicos (49152-65535): habitualmente se emplean para iniciar conexiones desde el cliente. No suelen emplearse en procesos servidores.

PUERTOS DE COMUNICACIONES

- La correspondencia entre procesos y puertos se hace de dos formas distintas:
  - Asignación estática: Los puertos conocidos están reservados para aplicaciones estándar y solo pueden ser empleados por estos procesos. Algunas aplicaciones se configuran para arrancar sobre algún puerto no conocido, pero si la aplicación está apagada, no hay reserva de puerto.
  - Asignación dinámica: Cuando un proceso necesita un puerto y este no se asigna estáticamente, el sistema operativo le asigna uno que esté disponible.
- En el nivel de transporte tenemos dos protocolos (TCP y UDP). Ambos manejan sus 64k puertos de forma independiente. Por ejemplo, el puerto 80 de UDP es distinto al puerto 80 de TCP.

PROTOCOLO UDP

- El protocolo UDP (User Datagram Protocol) proporciona un servicio no orientado a la conexión.
  - No se establece la conexión previo a la transmisión
  - No hay control de flujo: Pueden enviarse segmentos duplicados o desordenados

- Se emplea en casos donde es más importante la velocidad de la transmisión que la fiabilidad, o bien en aplicaciones sencillas del tipo petición respuesta, como DHCP, DNS, streaming y voz IP

PROTOCOLO TCP

- El protocolo TCP (Transmission Control Protocol) proporciona un servicio orientado a la conexión.
  - Hay establecimiento previo de la conexión
  - Hay control de flujo y de errores.
  - Es un servicio fiable.
- Establecimiento de la conexión: una vez que se ha establecido la conexión, cualquiera de los dos extremos puede empezar a transmitir. Cualquiera puede terminar la conexión.
- Una conexión TCP se define por:
  - Dirección IP origen, Puerto Origen
  - Dirección IP destino, Puerto Destino.
- No puede haber dos conexiones TCP que tengan en común estos 4 datos.

TRADUCCIÓN DE DIRECCIONES DE RED: NAT Y PAT

- El número de dispositivos conectados a Internet crece exponencialmente.
- El número de direcciones IP tiende a agotarse.
- Solución:
  - IPv6
  - Aprovechar más eficientemente el espacio de direcciones:
    - CIDR: Classless Inter-Domain Routing
    - Supernetting.
    - Traducción de direcciones de red - NAT

NAT: NETWORK ADDRESS TRANSLATION

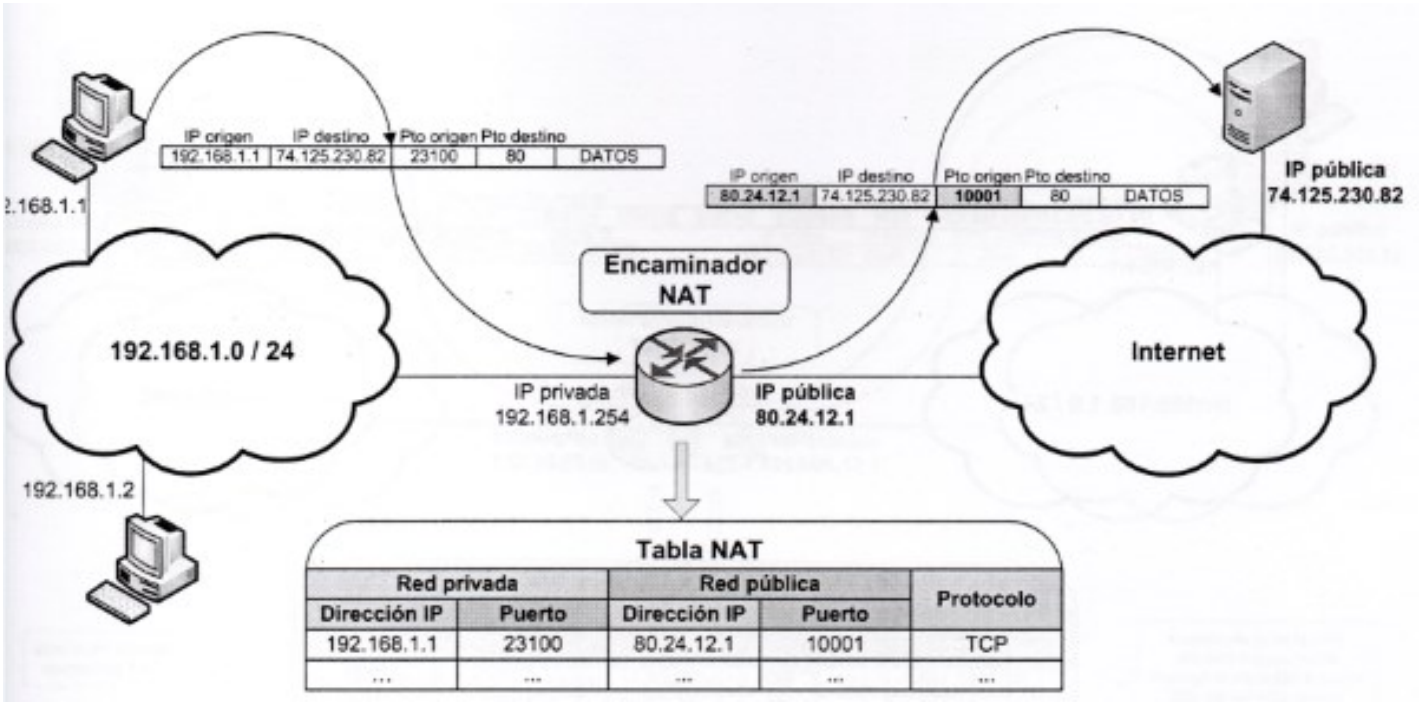
- Permite que direcciones IP privadas puedan acceder a Internet a través de una dirección IP pública
- El router reescribe algunos datos del datagrama que encamina. En función de lo que modifique:
  - NAT básico: Únicamente se modifica la dirección IP
  - NAPT (Network Address Port Translation) / PAT (Port Address Translation): Se modifica la IP, y los puertos empleados en la comunicación.
- Actualmente lo que se usa es NAPT, y lo podemos ver escrito tanto como NAPT como NAT (utilizaremos este término).

NAT: MODIFICACIÓN DE DATAGRAMAS

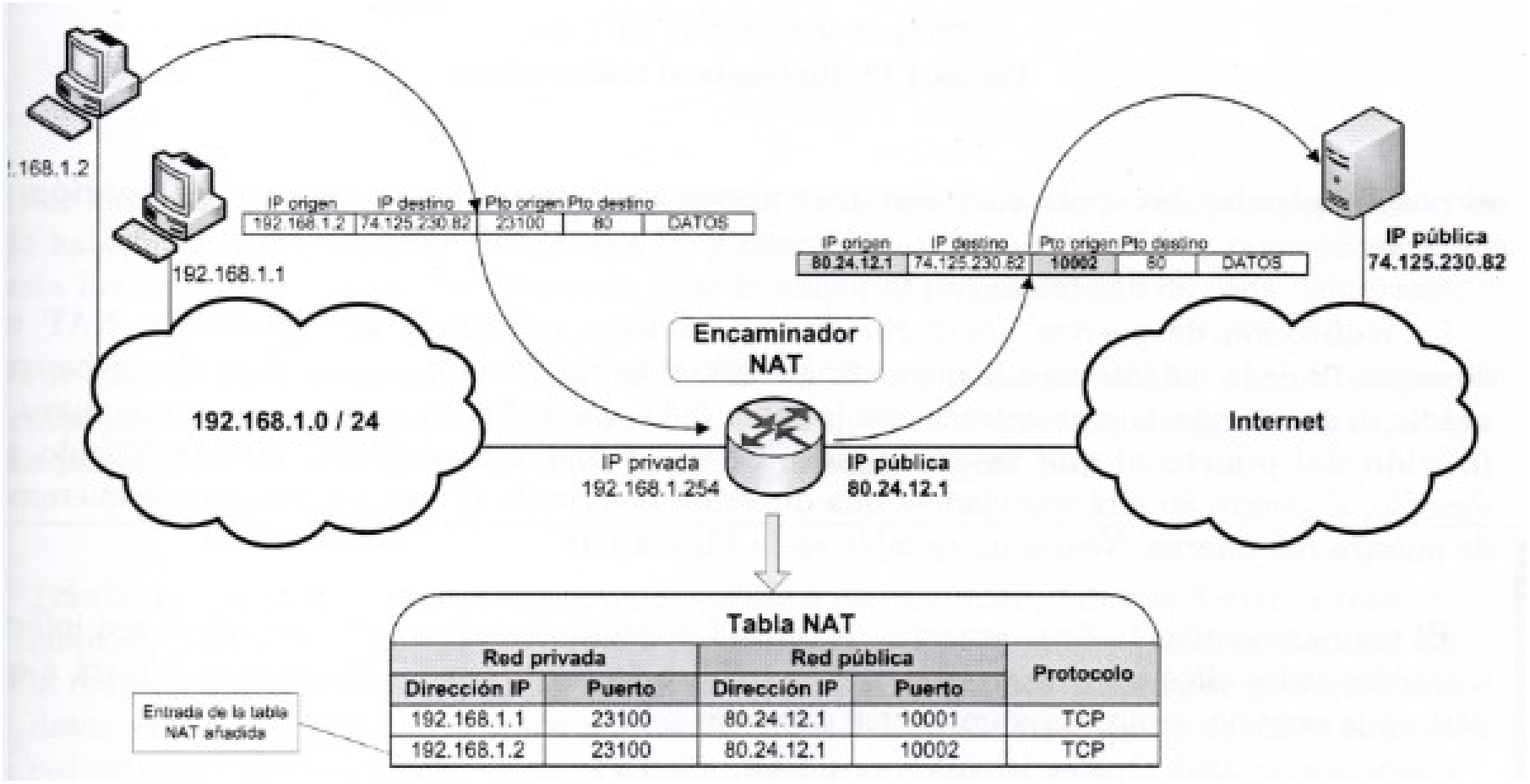
- Se modifican las IP y los puertos al pasar el datagrama por el router:
  - Se modifican la IP de origen y el puerto de origen en el tráfico saliente por los datos del router.
  - Se modifican la IP de destino y el puerto de destino en el tráfico entrante por los datos del destino.
- Para ello, se mantienen una tabla con la siguiente información:
  - Dirección IP interna (privada)
  - Puerto interno
  - Dirección IP externa (pública)
  - Puerto externo
  - Protocolo de nivel de transporte (TCP o UDP)

NAT: TRÁFICO SALIENTE

- Se reemplaza la dirección IP origen y el puerto origen por la dirección IP de salida, y por un puerto disponible en el router.
- En la tabla NAT se guarda esta equivalencia.



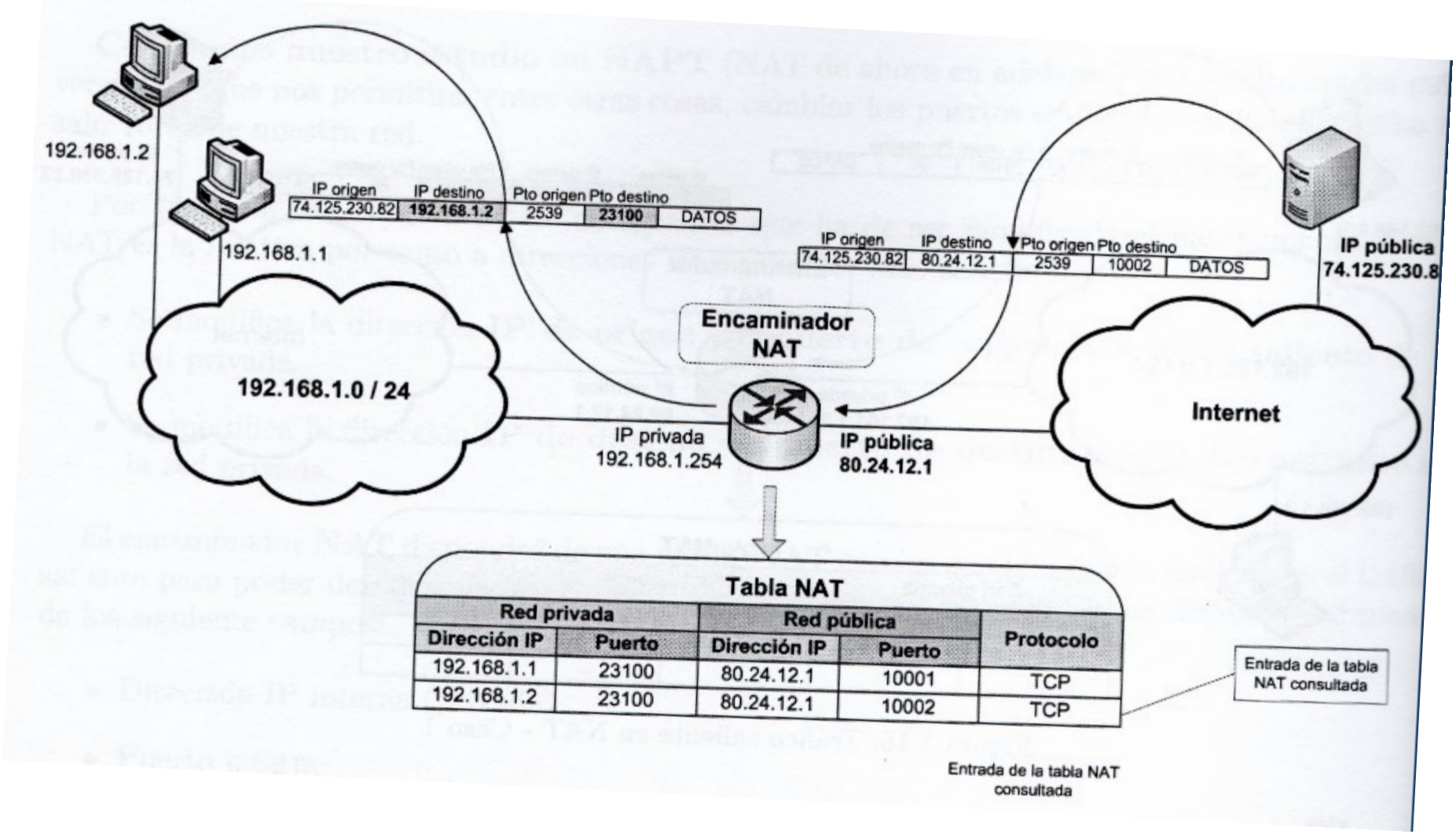
NAT: TRÁFICO SALIENTE



NAT: RESPUESTA AL TRÁFICO SALIENTE

- Cuando al router le llega un datagrama del exterior, comprueba si la dirección IP de destino y el puerto de destino del datagrama entrante coinciden con alguna fila de su tabla NAT en los campos IP externa y Puerto externo.
- Cuando coinciden, modifica el datagrama, modificando la dirección IP destino y el puerto destino, con los datos de la red interna de esa fila de la tabla NAT
  - Redirige el datagrama a esta IP.
- Si no hay coincidencia, por lo general, descarta el datagrama. Solo si el propio router tiene un servidor escuchando en ese puerto, procesa el datagrama.

NAT: RESPUESTA AL TRÁFICO SALIENTE



NAT: TRAFICO ENTRANTE NUEVO

- Como los datagramas que no encuentran equivalencia en la tabla NAT se descartan, en nuestra red interna no podemos tener ningún servidor.
- Para solucionar este problema, se permite la redirección de puertos (Port Forwarding).
- Port Forwarding: Consiste en indicar al router NAT una dirección interna a la que redirigir todo el tráfico entrante nuevo. También se puede hacer para solo un puerto concreto.
- Para ello, hay que añadir manualmente una entrada en la tabla NAT.
- Esto permite tener varios servidores en la misma IP pública, pero cada uno con un puerto distinto.

NAT: TRAFICO ENTRANTE NUEVO

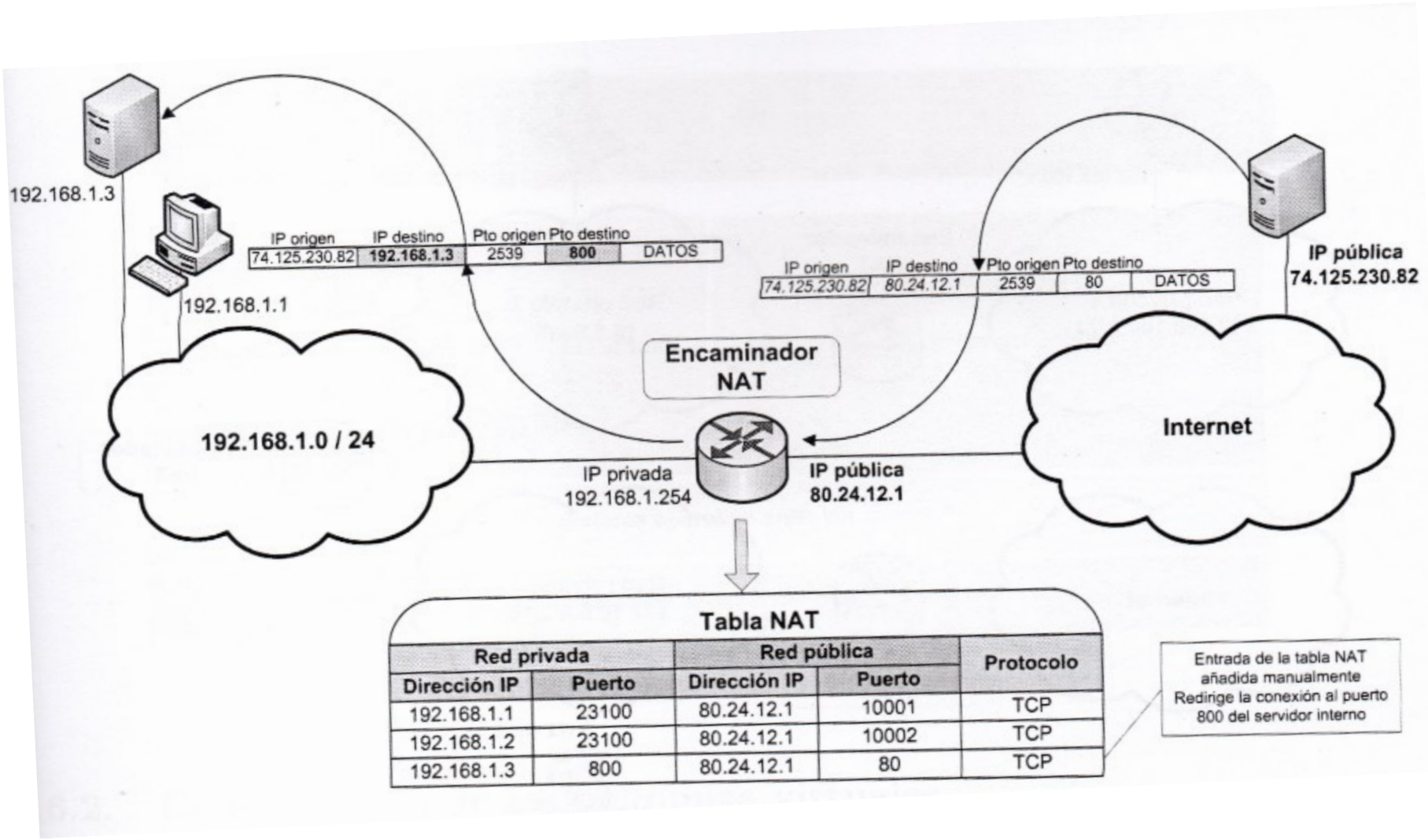


Tabla NAT

Red privada		Red pública		Protocolo
Dirección IP	Puerto	Dirección IP	Puerto	
192.168.1.1	23100	80.24.12.1	10001	TCP
192.168.1.2	23100	80.24.12.1	10002	TCP
192.168.1.3	800	80.24.12.1	80	TCP

Entrada de la tabla NAT añadida manualmente
Redirige la conexión al puerto 800 del servidor interno

NAT: LIMITACIONES

- Hay protocolos del nivel de aplicación que incluyen las direcciones IP.
- El encaminador NAT solo actúa sobre las cabeceras IP, por lo que no modifica la parte de datos del datagrama, y por tanto, no habrá correspondencia entre estas aplicaciones y las direcciones IP que aparecen en las aplicaciones.
- Las últimas implementaciones de NAT incorporan conocimiento de los protocolos más habituales de encapsulamiento de direcciones, y modifican también los datos.

CONCEPTOS BÁSICOS DE TCP/IP