ÍNDICE

PREFACIO

Dentro del ámbito informático, las certificaciones constituyen uno de los títulos más importantes y reconocidos a nivel mundial. Gracias a ellas, empresas líderes en el sector acreditan que sus poseedores disponen de los conocimientos y habilidades necesarias para ejercer laboralmente las funciones de una determinada rama profesional. Microsoft, Cisco, HP, VMWare, Juniper, Fortinet, Oracle, IBM, CheckPoint o Citrix son solo algunos ejemplos de compañías que basan su formación en torno a certificaciones.

En cuanto a redes y seguridad se refiere, el CCNA es una de las más valoradas, primero, porque abarca desde los conceptos más básicos de *routing* y *switching* hasta protocolos realmente avanzados, y segundo, porque su título es acreditado por Cisco, compañía líder en el sector de redes y comunicaciones.

El objetivo principal de este libro consiste en dotar a sus lectores de los conocimientos necesarios para afrontar con éxito el examen de certificación del CCNA. Su contenido, dividido en 12 capítulos, incluye la totalidad del temario oficial, destacando las siguientes características como las más significativas.

- Contenido estructurado: el contenido se desarrolla de menor a mayor dificultad, no requiriendo ningún conocimiento previo sobre los conceptos tratados.
- Facilidad de aprendizaje: el lenguaje utilizado para desarrollar cada capítulo resulta de comprensión sencilla, lo que, junto a los numerosos ejemplos incluidos en cada apartado, facilita el aprendizaje de cada uno de los fundamentos tratados en el libro.
- Enfoque práctico: toda teoría es acompañada de ejemplos y supuestos prácticos de configuración en aquellas materias que lo requieran. En este aspecto, se recomienda hacer uso de la aplicación "*Packet tracer",* desarrollada por Cisco.

- Preguntas tipo test: al finalizar cada capítulo, el estudiante podrá poner a prueba los conocimientos adquiridos gracias al test incluido en cada uno de ellos. Estos también sirven como preparación para el examen real de certificación, ya que tiene el mismo formato de cuestiones.

Gracias a todo ello, y tras finalizar el estudio y las prácticas incluidas, el lector adquiere los conocimientos necesarios para administrar y asegurar una red corporativa de tamaño medio, aplicando sobre la misma los protocolos y configuraciones más adecuadas en relación con la topología y el propósito final.

El autor

Daniel Pérez Torres nació en Santa Cruz de Tenerife en 1983. Basó sus estudios en la administración de sistemas informáticos, especializándose a posteriori en la rama de redes y seguridad, en cuyo campo posee las certificaciones Cisco CCNP, CCNA, CCNA Security, Juniper JNCIA y CompTIA Security+, entre otros muchos títulos. Propietario del blog http://desdelacli.blogspot.com y cooperador en diferentes portales web, así como instructor de CCNP, CCNA y CCNA Security desde el año 2010.

Su trayectoria profesional ha estado vinculada desde el año 2006 al servicio de la administración pública, donde actualmente pertenece al área de redes y comunicaciones, trabajando a diario con las tecnologías más avanzadas del sector como Cisco, Extreme Networks, FortiNet, ForcePoint o F5.

1 REDES INFORMÁTICAS. CONCEPTOS BÁSICOS

INTRODUCCIÓN A LAS REDES INFORMÁTICAS

El objetivo principal del CCNA consiste en que sus aspirantes obtengan los conocimientos necesarios para crear y administrar una red de tamaño medio de manera segura y eficiente. Para lograrlo, Cisco basa su estudio en análisis detallados de cada uno de los elementos que la conforman, abarcando desde las nociones más básicas hasta los protocolos más avanzados, comenzando por el concepto más esencial. ¿Qué es una red?

Una red puede ser definida como la comunicación entre un conjunto de miembros que hacen uso del mismo medio compartido con el fin de intercambiar información y recursos entre sí. Este concepto, aplicado al ámbito informático, se lleva a cabo mediante la interconexión de dispositivos, donde cada uno de ellos tomará un rol y la totalidad de los mismos definirá el tamaño y el propósito final. Dicha comunicación resulta posible gracias a la aplicación de diferentes medios, tanto físicos como lógicos. Los primeros hacen referencia a elementos de hardware, como cableado y tarjetas de red, mientras, los segundos, al software y protocolos necesarios para poder llevar a cabo la comunicación.

En cuanto al tamaño, la red más básica se compone de dos equipos, físicamente en el mismo lugar y conectados entre sí mediante un simple cable. Mientras, la más compleja puede albergar millones de host ubicados a lo largo del planeta, comunicándose gracias a multitud de dispositivos intermediarios como routers,

switchs, o firewalls, entre muchos otros. Un ejemplo bastante claro de ello es Internet.

Evidentemente, este nivel de complejidad nace como fruto de la evolución llevada a cabo a lo largo del tiempo. Así mismo, una de las primeras redes de computadoras creadas y que sin duda establece el origen de las actuales fue ARPANET, desarrollada en 1968 por el departamento de defensa de EE.UU. y utilizada para la comunicación privada entre diferentes instituciones del país. A raíz de ella, el estudio y avance de esta tecnología ha sufrido un crecimiento exponencial, hasta la actualidad, donde cualquier dispositivo puede acceder a información ubicada en cualquier parte del planeta.

Por último, una red puede ser apreciada de diferentes maneras. Para un usuario simplemente significa obtener acceso a determinados recursos o servicios, como aplicaciones corporativas o Internet. Sin embargo, desde el punto de vista de un administrador resulta más complejo, incluyendo aquellos dispositivos encargados de la comunicación, configuraciones, seguridad, diseño, protocolos, servidores, etc.

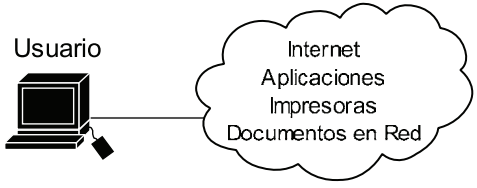

Fig. 1-1 Concepto de red para un usuario.

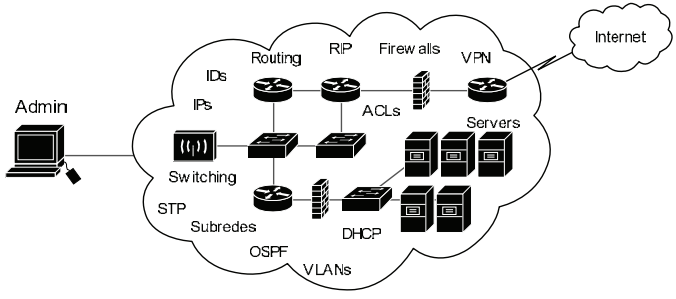

Fig. 1-2 Concepto de red para un administrador.

Como aspirante al CCNA el objetivo consiste en tomar el rol de administrador, para lo cual resulta imprescindible conocer los modelos de comunicación TCP/IP y OSI, en relación con los cuales operan la red y los diferentes protocolos aplicados en la misma.

ESTÁNDARES DE COMUNICACIÓN: TCP/IP Y OSI

La finalidad de una red informática consiste en habilitar la comunicación entre todos los dispositivos que la componen, pero ¿cómo es posible llevarla a cabo? Para lograrlo, resulta imprescindible cumplir una serie de "reglas", gracias a las cuales los datos generados por cualquier host puedan ser interpretados por el receptor de los mismos. Con dicho objetivo nacen los modelos de comunicación TCP/IP y OSI, los cuales definen los estándares, procedimientos y protocolos a aplicar para que la creación, el transporte y la entrega de datos se lleven a cabo de igual manera en cada dispositivo, sin importar ni el fabricante ni los elementos de hardware presentes en el mismo. OSI fue desarrollado por la agencia ISO *(International Organization for Standarization)* mientras que TCP/IP por voluntarios de varias universidades, siendo ambos modelos abiertos, es decir, sin coste económico ni limitaciones sobre su implementación.

Hoy día resulta prácticamente imposible encontrar dispositivos que no los soporten. Todos los sistemas operativos, incluyendo aquellos presentes en smartphones o tablets, lo implementan. Entonces, ¿cuál utilizar? Normalmente dependerá de la aplicación o sistema, pero, de ambos, el más común resulta TCP/IP, primero, porque se estandarizó con mayor rapidez, y segundo, porque la productividad de los datos es considerada más eficiente que en OSI.

A lo largo de la historia se han desarrollado diversos estándares con el mismo propósito, como SNA *(System Network Architecture)*, creado por IBM en el año 1974. Sin embargo, no han tenido éxito ni continuidad por tratarse de modelos propietarios de dichas compañías, debido a lo cual su utilización supone un coste económico, y lo que es peor, las modificaciones y actualizaciones del mismo solo pueden ser llevadas a cabo por la compañía en cuestión.

Modelo TCP/IP

TCP/IP es considerado el estándar por excelencia para llevar a cabo la comunicación en redes informáticas. Su función consiste en definir el procedimiento necesario para que los datos generados en el origen sean entregados y legibles en el destino. Para lograrlo hace uso de diferentes protocolos, cada uno de ellos con una función específica, las cuales serán analizadas a lo largo del capítulo.

Una manera de comprenderlo mejor es comparándolo con la telefonía. Si en nuestro hogar disponemos de un teléfono antiguo y lo sustituimos por otro de última generación, al conectarlo a la línea telefónica permitirá realizar y recibir llamadas de

la misma manera que el anterior, no serían necesarias ni configuraciones especiales ni la sustitución del cableado. Ello es posible gracias a que ambos hacen uso de los mismos protocolos de comunicación, los cuales han sido definidos y aprobados para su aplicación a nivel mundial. Lo mismo ocurre con TCP/IP, cualquier dispositivo que haga uso de él podrá comunicarse con otros que también lo hagan sin importar el fabricante, el modelo o el lugar donde se encuentren.

Como otros estándares de red, TCP/IP basa su modo de operar en capas, cada una de ellas con una función específica e incluyendo los protocolos necesarios para poder llevar a cabo diferentes tipos de comunicación. Estas son:

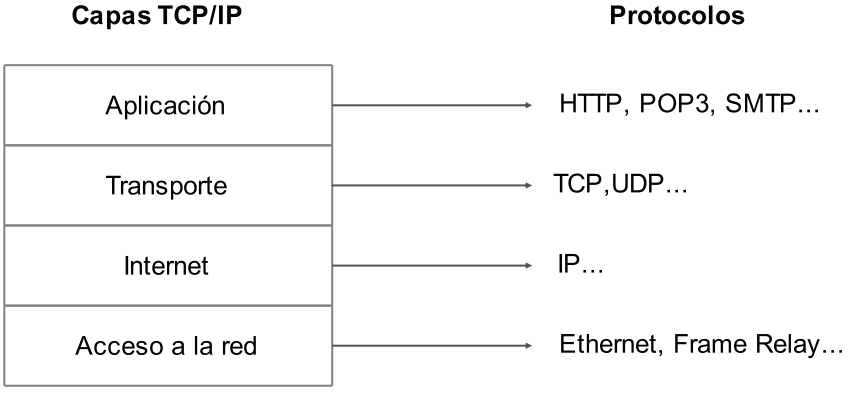

Fig. 1-3 Asociación de capas TCP/IP y sus protocolos.

En relación con las mismas queda definida la comunicación entre dos sistemas, llevando a cabo siempre el mismo procedimiento, donde los datos son generados en la capa de aplicación y enviados sucesivamente hacia las capas inferiores, aplicando cada una de ellas el protocolo correspondiente. Una vez finalizado el proceso, dichos datos son enviados al medio y recibidos por el destinatario.

Una de las grandes ventajas de TCP/IP es que es un estándar abierto, de tal manera que, si fuera necesaria la inclusión de algún nuevo protocolo, podría llevarse a cabo sin problema. Un claro ejemplo de ello fue la aparición de Word Wide Web (www), hecho que conllevó agregar HTTP en la capa de aplicación, cuyo propósito consiste en enviar solicitudes a servidores web para que estos respondan con el contenido requerido.

El proceso y las funciones llevadas a cabo en cada una de las capas son los siguientes.

CAPA DE APLICACIÓN

Es la encargada de brindar los protocolos necesarios a servicios o aplicaciones para que estos puedan iniciar el proceso de comunicación en red. Para una mejor comprensión, tomaremos como ejemplo el intercambio de mensajes entre un cliente y un servidor web, con el fin de analizar cómo son manipulados los datos en cada una de las capas para luego ser enviados al medio.

En este caso el proceso lo inicia el cliente a través de un navegador, por ejemplo, Firefox, haciendo uso del protocolo HTTP en la capa de aplicación. ¿Qué sucede cuando un dispositivo desea enviar una solicitud a un servidor web? Realmente lo que se generan son una serie de mensajes definidos por el propio protocolo, con el fin de que ambos sistemas se "entiendan", logrando con ello que la comunicación concluya con éxito. En el lado del cliente se generan mensajes GET, mientras que el servidor responde a estos mediante algún código (como el 200, con significado OK), además entra en juego otro protocolo, HTML, que define el formato de la página que se enviada.

La comunicación a nivel de capa de aplicación sería la siguiente…

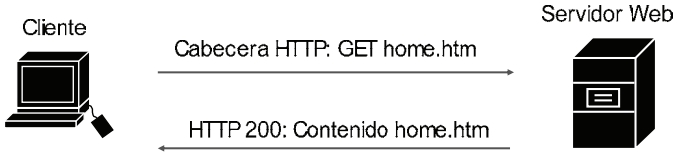

Fig. 1-4 Proceso inicial de comunicación HTTP, capa de aplicación.

Donde el navegador ha solicitado el documento "home.htm" y ha obtenido como respuesta el código 200. Ello significa que efectivamente dicho documento se encuentra almacenado en el servidor, que será enviado posteriormente. Cualquier otra circunstancia daría como resultado la generación de otro código, siendo el más común el 404, utilizado para indicar que el contenido solicitado no se encuentra disponible *(Page not Found)*.

En HTTP, el cliente genera una cabecera, que incluye información y datos propios de la capa de aplicación. Esta será recibida, analizada y respondida por su homóloga en el destino. Este modo de operar también se aplica a las diferentes capas, es decir, los datos agregados por cada una de ellas solo serán analizados y comprendidos por la misma en ambos sistemas (cliente y servidor).

La capa de aplicación no identifica al software en sí, sino los protocolos que se ejecutan en él.

CAPA DE TRANSPORTE

Una vez la capa de aplicación ha generado sus datos estos son enviados a la capa de transporte, la cual provee diferentes funciones, entre las que se encuentra identificar la aplicación a la que va dirigida la comunicación. Para ello hace uso de dos protocolos, TCP *(Transmission Control Protocol)* y UDP *(User datagram Protocol)*, ambos analizados en profundidad en este mismo capítulo.

Continuando con el ejemplo web. ¿Qué ocurriría si la solicitud enviada por el cliente no es recibida por el servidor, o viceversa? ¿Cómo sabe un dispositivo que sus datos han sido recibidos por el destinatario? TCP/IP necesita un mecanismo que garantice la entrega de datos de manera fiable de extremo a extremo. Este servicio es requerido por gran parte de las aplicaciones de red y de ello también se encarga la capa de transporte, más concretamente el protocolo TCP, que provee recuperación de errores mediante el uso de paquetes ACK (*acknowledgments*), basándose en una lógica bastante sencilla para lograrlo:

- Cuando el origen hace uso de TCP, para cada paquete enviado se espera una respuesta de confirmación de recepción por parte del destinatario, la cual se lleva a cabo mediante un mensaje ACK.
- Si transcurrido un tiempo no es recibido dicho ACK, el origen reenvía los datos.

Aplicado al ejemplo:

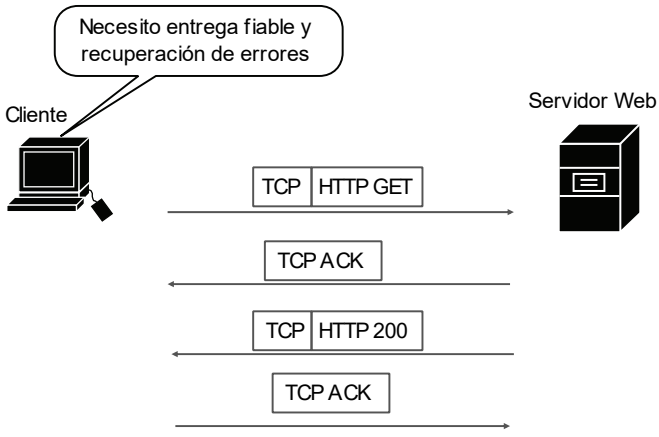

Fig. 1-5 Comunicación TCP, capa de transporte.

Si tanto cliente como servidor no hubieran recibido alguno de los ACK de confirmación, TCP reenviaría los datos nuevamente.

En este proceso se demuestra cómo un protocolo de la capa de aplicación como HTTP puede servirse de otro de la capa de transporte para agregar fiabilidad y control sobre la comunicación. Ello establece una interacción entre capas adyacentes, de tal manera que todas ellas se complementan.

Hasta ahora han sido mencionados dos conceptos que no pueden confundirse: interacción entre la misma capa en diferentes dispositivos e interacción entre capas adyacentes. La primera hace referencia a que los protocolos e información generada en una capa en el origen tan solo será analizada y comprendida por su homóloga en el destino. Mientras, la segunda se refiere a que las distintas capas en un mismo dispositivo se complementan, agregando entre todas ellas las cabeceras necesarias para que la comunicación pueda llevarse a cabo.

CAPA DE INTERNET

La capa de Internet, que se basa mayormente en el protocolo IP, es la encargada de agregar la información necesaria a los datos para que estos puedan ser enviados al destino correcto. Esta tarea se lleva a cabo gracias a las direcciones IP, las cuales identifican a cada uno de los miembros ubicados en la red.

Imagina que deseas establecer una llamada telefónica, pero desconoces el número de destino. Sin él sería imposible realizarla. Lo mismo ocurre con los datos, requieren una dirección para que la comunicación concluya con éxito.

Continuando con el ejemplo anterior, supongamos que el cliente dispone la IP 10.10.10.10 y el servidor la 20.20.20.20.

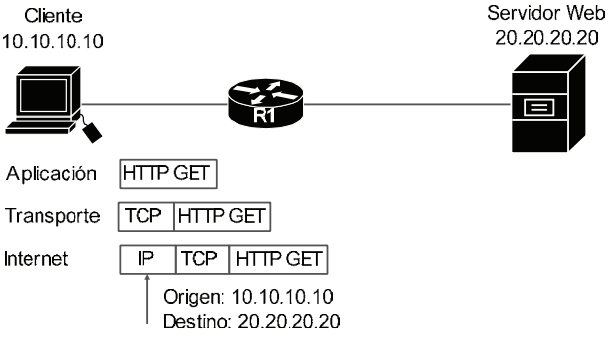

Fig. 1-6 Direccionamiento IP, capa de Internet.

En relación con la información incluida en esta capa, el router (en este caso R1) llevará a cabo el proceso de enrutamiento, mediante el cual toma la decisión de reenvío más adecuada para que los datos sean recibidos por el destinatario de la comunicación.

CAPA DE ACCESO A LA RED

Por último, el acceso a la red define el procedimiento y hardware necesario para que la entrega de datos de un extremo a otro pueda llevarse a cabo a través del medio físico disponible. Esta capa incluye una gran variedad de protocolos, que dependerán del tipo de red y conexiones, por ejemplo, para entornos LAN lo más común es aplicar Ethernet, sin embargo, en WAN resulta necesario PPP o HDLC, entre otros.

Es la última capa que atraviesan los datos antes de ser enviados al medio, por lo que debe definir el formato final de estos. Para ello, además de agregar una nueva cabecera al inicio, también incluye un tráiler al final.

Aplicado al ejemplo, y haciendo uso de una red LAN Ethernet (ETH):

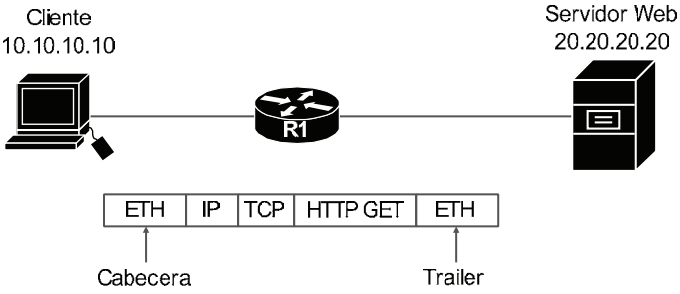

Fig. 1-7 Envío de datos, capa de acceso a la red.

Diferentes libros y webs de documentación dividen la capa de acceso a la red de TCP/IP en dos subcapas, enlace de datos (LLC) y física. Ello es debido a la comparación con el modelo OSI, el cual será objeto de estudio a continuación.

PROCESO DE ENCAPSULACIÓN Y ENVÍO DE DATOS

Como se ha analizado, cada capa agrega una cabecera con información específica a los datos. Este proceso es conocido como encapsulación, y puede ser resumido de la siguiente manera:

- *Paso 1:* Los datos generados por el software son recibidos por la capa de aplicación, que ejecutará el protocolo necesario sobre los mismos. En el ejemplo de comunicación web, HTTP.
- *Paso 2:* Una vez concluido son enviados a la capa de transporte, que agrega una nueva cabecera con información propia del protocolo aplicado. TCP, en el caso del ejemplo anterior.
- *Paso 3:* En la capa de Internet se identifican las direcciones de origen y destino, incluidas en una nueva cabecera IP.
- *Paso 4:* Por último, la capa de acceso a la red establece el formato final de los datos gracias a la cabecera y tráiler correspondientes. Comúnmente Ethernet (ETH) en redes LAN.
- *Paso 5:* Tras todo ello, son generadas las señales necesarias para su posterior transmisión a través del medio físico correspondiente (cobre, fibra, wireless…).

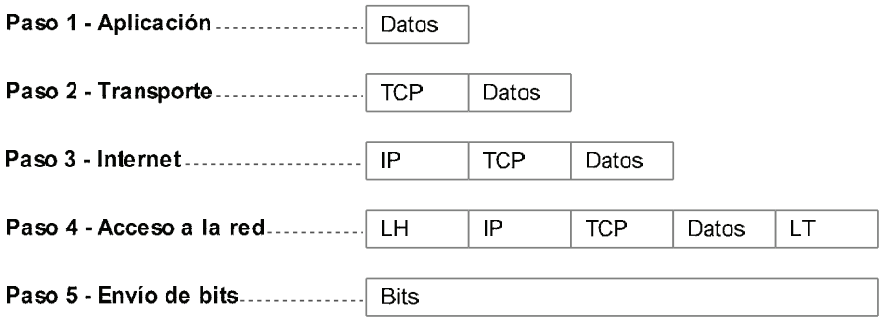

Fig. 1-8 Proceso de encapsulación en TCP/IP.

LH *(Link Header)* y LT *(Link Trailer)* corresponden a la cabecera y al tráiler.

Además, los datos, a medida que atraviesan las diferentes capas, reciben un nombre específico, siendo los siguientes:

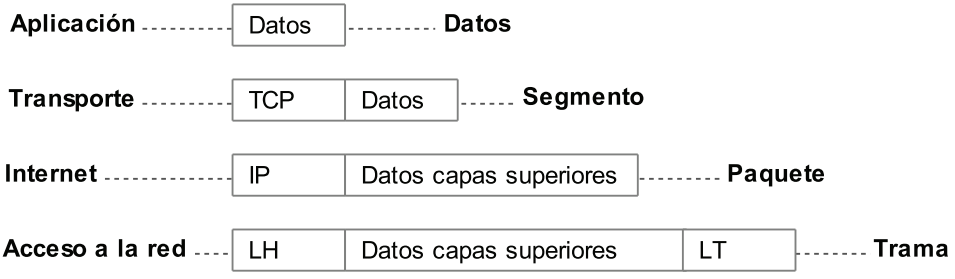

Fig. 1-9 Asociación entre capas y nombre de PDU en TCP/IP.

De ahora en adelante, cuando se haga mención a un segmento automáticamente debe ser asociado con la capa de transporte, paquete con la capa de Internet y trama (o *frame*) con la capa de acceso a la red.

Modelo OSI

OSI *(Open System Interconnection)*, creado en 1984 por ISO *(Organización Internacional para la Estandarización)*, es otro de los estándares definidos para llevar a cabo la comunicación a nivel de red. Este coincide en su finalidad con TCP/IP, es decir, definir el proceso necesario para que los datos generados en un origen sean transportados, recibidos y legibles por el destinatario de los mismos.

Una de las principales diferencias entre ambos modelos consiste en el número de capas utilizadas para lograr su objetivo, mientras que TCP/IP hace uso de 4, OSI implementa 7, siendo las siguientes:

Fig. 1-10 Capas presentes en el modelo OSI.

El emisor genera los datos en la capa de aplicación y son enviados de manera sucesiva hacia las capas inferiores, en las cuales se aplicará el encapsulamiento necesario, agregando la cabecera correspondiente en cada una de ellas para posteriormente ser enviados al medio.

En el destino, el receptor analiza la información de manera ascendente, des-encapsulando la información previamente agregada por el origen. Este proceso concluye en la capa 7 obteniendo los datos originales generados por el emisor.

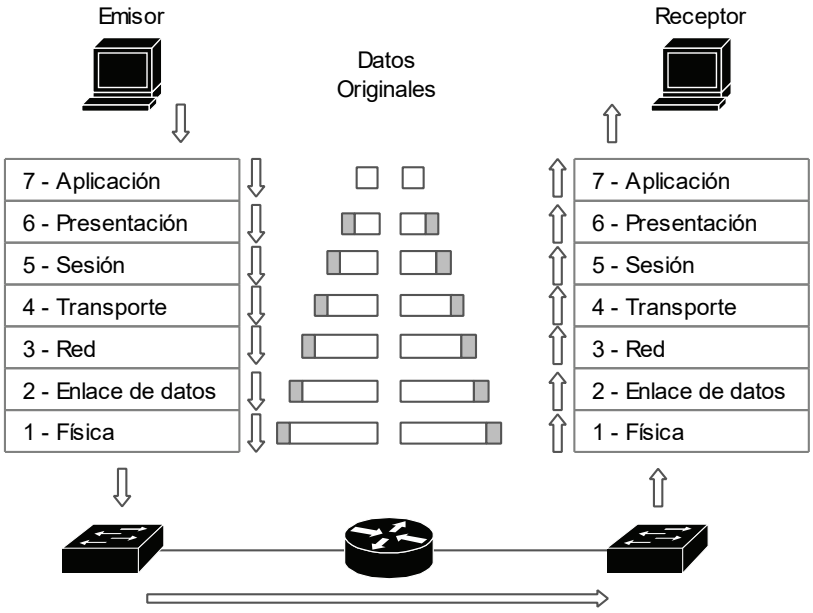

Fig. 1-11 Proceso de comunicación en el modelo OSI.

Además, y al igual que ocurre en TCP/IP, a medida que los datos atraviesan las diferentes capas son reconocidos mediante su propia PDU (*Protocol Data Unit*), siendo, en el modelo OSI, las siguientes:

Capa	**PDU**
7 Aplicación	Datos
6 Presentación	Datos
5 Sesión	Datos
4 Transporte	Segmento
3 Red	Paquete
2 Enlace de datos	Trama (o *Frame*)
1 Física	Bits

Una PDU simplemente es la nomenclatura utilizada para identificar la capa en la que se están procesando los datos, y con ello, la información manipulada.

En OSI, las capas de transporte, red, enlace de datos y física son consideradas "capas de red", mientras que aplicación, presentación y sesión, "capas de host". Cada una de ellas desarrolla una finalidad única, complementándose entre sí y realizando prácticamente las mismas funciones que en TCP/IP.