Sistemas y Aplicaciones Informáticas

Tema 58. Redes de Área Extensa. Interconexión de Redes Locales.

1. Ámbito de docencia.

- Implantación de aplicaciónes informáticas de gestión (ASI 2).
- Sistemas informáticos multiusuario y en red (DAI 1).
- Instalación y mantenimiento de aplicaciones ofimáticas y corporativas (ESI 1).

2. Redes de área extensa.

2.1. Descripción. Características. Estándares, protocolos y servicios.

- Una red de área extensa (WAN) es una red de datos que interconecta redes de área local que se encuentran separadas por grandes áreas geográficas. Se caracterizan por lo siguiente:
  - Su velocidad de transmisión depende de la tecnología empleada, aunque suele ser menor que las utilizadas en las LAN. Oscila entre 64 Kbps de RDSI-BE y 622 Mbps de ATM.
  - Su tasa de errores (Bit Error Rate, BER) es unas mil veces superior que la de las LAN.
  - Son redes punto a punto, aunque el medio de transmisión puede ser dedicado o compartido.
  - Requieren la utilización de líneas públicas gestionadas por proveedores de servicios de telecomunicaciones mediante un contrato de alquiler con estas entidades.
  - Al tratarse de redes punto a punto, su topología física suele ser en malla.
  - La transmisión de los bits se puede realizar de manera síncrona o asíncrona.
- Las redes punto a punto se construyen por medio de conexiones, denominadas enlaces, entre pares de ordenadores o nodos de la red. Si el nodo tiene un único enlace es un nodo terminal, de lo contrario es un nodo intermedio. Para llegar de un nodo a otro deben atravesarse uno o varios enlaces, y cada nodo intermedio debe decidir dónde dirigir los paquetes que reciba.
- La función de las WAN consiste en establecer una comunicación entre los equipos terminales de circuito de datos (modems, puentes remotos, routers) de las LAN remotas. Operan en los tres primeros niveles del modelo OSI, en los que se definen los siguientes estándares y protocolos:
  - *Nivel físico*. En este nivel se suelen describir los estándares de conexión entre los equipos terminales de datos y los equipos terminales de circuito de datos. Los más importantes son:
    - *RS-232C*. Es el estándar para comunicar directamente un ordenador con otro, o con un periférico o un modem. Consta de 25 patillas (DB-25) distribuidas en conexiones de masa, canal principal y secundario (datos y control) y control de transmisión síncrona, que permiten transmisiones simplex, half-duplex y full-duplex, síncronas o asíncronas.
    - *RS-449*. Consta de 9 patillas (DB-9). Sólo permite la transmisión asíncrona y se corresponde con el canal secundario (datos y control) del conector RS-232C.
    - *V.35*. Estándar de ITU-T para las comunicaciones entre un dispositivo de acceso de red y una red de paquetes. Se recomienda para velocidades de hasta 48 Kbps.
    - *RS-422*. Es una norma definida por la EIA que supone una mejora de RS-232C. Admite velocidades de hasta 2 Mbps y una longitud máxima de cable de 60 metros.
  - *Nivel de enlace*. En este nivel se definen una serie de protocolos de enlace entre los nodos de una WAN. Pueden ser orientados a carácter (la longitud de la trama debe ser un número entero de bytes) u orientados a bit (cada trama puede tener cualquier longitud). Como ejemplos de este tipo de protocolos se pueden citar:

- **HDLC (High-Level Data Link Control)**. Protocolo estándar ISO orientado a bit, es la base de la mayoría de los protocolos de enlace. Puede ofrecer servicio no orientado a conexión y servicio orientado a conexión de ventana deslizante.
- **PPP (Point-to-Point Protocol)**. Protocolo característico de Internet orientado a carácter, soporta simultáneamente varios protocolos a nivel de red. Por defecto ofrece un servicio no orientado a conexión, pero puede negociar transmisión fiable con ACK.

* *Nivel de red*. Se encarga de dirigir los datos desde el origen al destino por una determinada ruta a través de los nodos de la red. Los tipos de servicio que existen son los siguientes:
  - **Orientado a conexión**. Establece un circuito virtual entre los equipos que desean comunicarse a través de los nodos de conmutación en el instante de la conexión. Todos los paquetes van marcados con una etiqueta identificativa y se dirigen por el circuito virtual desde el origen al destino, llegando en el mismo orden con el que han salido. Los nodos de conmutación modifican las etiquetas de los paquetes, asignándoles la interfaz de salida y la nueva etiqueta en función de la interfaz de entrada y la etiqueta vieja de acuerdo a su propia tabla de conmutación. Este tipo de servicio puede ser con acuse de recibo (X.25) o sin él (Frame Relay, ATM).
  - **No orientado a conexión**. Los paquetes pueden ir por caminos físicos diversos, y cada uno debe contener su dirección de destino. Cada nodo de conmutación se encarga de enrutar el paquete por el camino adecuado para que llegue al receptor, sin modificar la dirección de destino. Los paquetes pueden llegar desordenados, de modo que según el tipo de red de comunicación, será misión de ésta o del receptor el ensamblaje correcto de los paquetes. Normalmente este tipo de servicio es sin acuse de recibo (IP).

2.2. Tipos de enlace.

2.2.1. Líneas dedicadas.

- Son circuitos reales formados por un enlace punto a punto permanente entre los ordenadores o los routers que se desean unir. Ningún otro equipo tiene acceso a estas líneas, que pueden ser privadas o públicas, y aportan exclusivamente un medio de transmisión de datos a nivel físico.
- En este tipo de líneas la capacidad contratada está reservada permanentemente en todo el trayecto. Por tanto, su coste elevado sólo justifica su instalación cuando el uso es frecuente.

2.2.2. Líneas conmutadas. Tipos y tecnologías asociadas.

- La conmutación es la solución ante la imposibilidad de conectar todos los nodos de una red a través de líneas punto a punto. Para ello se establece una jerarquía de nodos de conmutación interconectados entre sí, de los que dependen las transmisiones de los nodos terminales.
- Cada nodo terminal se conecta a su nodo de conmutación local. Cuando se intenta una conexión con otro nodo terminal, los nodos de conmutación se encargan de establecer uno o más caminos por los que poder transportar la información de modo transparente a los nodos terminales.
- En transporte de datos hay dos tipos de conmutación:
  * *Conmutación de circuitos*. Establece una conexión física extremo a extremo a través de los nodos de conmutación mediante un procedimiento de llamada entre los equipos que desean comunicarse. Mientras hay conexión, el canal de comunicación está reservado. Por ejemplo:

- **Red de Telefonía Básica (RTB)**. Está formada por las líneas analógicas tradicionales y requiere el uso de módems. La máxima velocidad que puede obtenerse es de 33,6 Kbps.
- **Red RDSI**. Está formada por enlaces digitales de extremo a extremo. El acceso básico proporciona los canales B de 64 Kbps, utilizados para transportar tráfico de voz o datos; y el canal D, que es un canal de control y señalización de 16 Kbps.
- **Red GSM**. Formada por enlaces digitales de extremo a extremo a través de radioenlaces. La capacidad máxima cuando se transmiten datos es de 9,6 Kbps.

* *Conmutación de paquetes*. Es un procedimiento de transferencia de datos mediante paquetes provistos de direcciones, en el que el canal de comunicación no está reservado sino que es compartido por todos los nodos conectados a él. Existen varias tecnologías:
  - **X.25**. Es un servicio orientado a conexión con control de flujo, retransmisión de tramas erróneas y acuse de recibo de los paquetes. Su velocidad típica está entre 9,6 y 64 Kbps.
  - **Frame Relay**. Es un servicio orientado a conexión sin control de flujo, ni retransmisión de tramas erróneas ni acuse de recibo de paquetes. Está pensada para la interconexión multiprotocolo de LANs, y su velocidad típica está entre 64 Kbps y 2 Mbps.
  - **ATM (Asynchronous Transfer Mode)**. Es una evolución de Frame Relay con paquetes de longitud fija. Está orientado a la transmisión de datos, voz y vídeo. Existen varias categorías de servicio y su velocidad típica está entre 34 y 155 Mbps.

3. Interconexión de redes locales.

3.1. A través de redes TCP/IP.

3.1.1. Protocolo IP (Internet Protocol).

3.1.1.1. Direcciones IPv4.

3.1.1.1.1. Descripción. Máscara. Clases. Direcciones especiales.

- Cada interfaz de red de cada host o router en una red IP se identifica mediante al menos una dirección única de 32 bits. Es posible definir varias direcciones IP asociadas a una misma interfaz física. se suelen representar por cuatro números decimales separados por puntos, que equivalen al valor de cada uno de los cuatro bytes que componen la dirección.
- Las direcciones IP tienen una estructura jerárquica: una parte de la dirección corresponde a la red, y la otra al host dentro de la red. Para indicar qué parte de la dirección corrresponde a la red y qué parte al host se suele utilizar una notación denominada máscara, consistente en poner a 1 los bits que corresponden a la parte de red y a 0 los que corresponden a la parte host.
- El espacio de direcciones disponible está organizado en las siguientes clases:
  * *Clase A*. El campo red ocupa los 8 primeros bits y el campo host los últimos 24. Se caracterizan por tener el primer bit de red con el valor 0.
  * *Clase B*. El campo red ocupa los 16 primeros bits y el campo host los últimos 16. Se caracterizan por tener los dos primeros bits de red con el valor 10.
  * *Clase C*. El campo red ocupa los 24 primeros bits y el campo host los últimos 8. Se caracterizan por tener los tres primeros bits de red con el valor 110.d
  * *Clase D*. Es una clase utilizada para definir grupos multicast, no se asigna nunca a hosts. Los primeros cuatro bits valen 1110, y los grupos se definen por los 28 bits siguientes.

    - *Clase E*. Los primeros cuatro bits valen 1111 y está reservada para usos futuros.
- Existen unos convenios que asignan significados especiales a determinadas direcciones IP:
    - Aquellas con el *campo host todo a ceros* identifican redes y no se utilizan para ningún host.
    - Aquellas con el *campo host todo a unos* son la dirección de difusión dentro de la red.
    - Aquellas con el *campo red todo a ceros* identifican a un host en la propia red.
    - *255.255.255.255*. Se utiliza para indicar difusión en la propia red.
    - *0.0.0.0*. Identifica al host que envía el datagrama cuando aún no tiene dirección IP.
    - *127.0.0.1*. Dirección loopback, todas las implementaciones de IP devuelven a la dirección de origen los datagramas enviados a esta dirección sin intentar enviarlos a ninguna parte.
    - Las redes *127.0.0.0* (fin clase A), *128.0.0.0* (principio clase B), *191.255.0.0* (fin clase B), *192.0.0.0* (principio clase C), *224.0.0.0* (principio clase D) y el rango de *240.0.0.0* en adelante (clase E) están reservados y no deben utilizarse.
    - Las redes *10.0.0.0* (clase A), *172.16.0.0* a *172.31.0.0* (clase B) y *192.168.0.0* a *192.168.255.0* (clase C) están reservadas por el RFC 1918. No se asignan a ninguna dirección válida en Internet y por tanto pueden utilizarse para construir redes privadas.

3.1.1.1.2. Subredes. Classless InterDomain Routing (CIDR).

- Las subredes son el resultado de dividir una red de una determinada clase en varias redes más pequeñas que comparten el identificador de red. La división en subredes no ha de hacerse necesariamente de forma homogénea en todo el espacio de direcciones. Esta división se realiza por motivos administrativos, ya que permite establecer una jerarquia de direcciones en una red.
- Para dividir la red en subredes se define una nueva máscara. Por ejemplo, la máscara 255.255.252.0 aplicada sobre una red clase B reserva los primeros 6 bits para la subred y deja 10 para el host, con lo que podría haber hasta 64 subredes con 1024 direcciones cada una.
- La regla mediante la cual se permite que la subred esté toda a ceros o toda a unos se denomina subnet-zero y se adopta para aprovechar mejor el espacio de direcciones disponible.
- El sistema denominado CIDR (Classless InterDomain Routing) dispone que la parte de red de la dirección vendrá especificada por la longitud de la máscara únicamente, no teniendo ya ningún significado la clasificación tradicional en clases A, B y C de acuerdo con el valor de los primeros bits. Sólo se respeta dicho significado en el caso de las clases D (multicast) y E (reservado).

3.1.1.2. El datagrama IPv4. Fragmentación.

- Una red IP es una red de conmutación de paquetes no orientada a conexión. Dichos paquetes se denominan datagramas y constan de cabecera y datos. La longitud total del datagrama puede ser cualquier número entero de bytes con un valor máximo de 65535 (2^{16}) bytes.
- La longitud de la cabecera en bytes siempre ha de ser múltiplo de cuatro, y tiene una parte fija de 20 bytes y una opcional de entre 0 y 40 bytes. Entre otros, tiene los siguientes campos:
    - *Dirección de origen (32 bits)*. Corresponde a la dirección IP de origen.
    - *Dirección de destino (32 bits)*. Corresponde a la dirección IP de destino.
    - *TTL, Time To Live (8 bits)*. Es un contador regresivo que indica el tiempo de vida restante del datagrama medido en segundos. Cada router por el que pasa dicho datagrama está obligado a restar uno del TTL, si llega a valer cero el datagrama debe ser descartado.

- *Campos relacionados con la fragmentación de datagramas:*
  - **Identificación (16 bits)**. El host emisor debe marcar todos los datagramas con un valor único en este campo ante la posibilidad de que sean fragmentados más tarde.
  - **DF, Don't Fragment (1 bit)**. Si está a 1 indica que el datagrama no debe fragmentarse.
  - **MF, More Fragments (1 bit)**. Puesto a 1 especifica que este datagrama es realmente un fragmento de un datagrama mayor, y que no es el último. Si está a 0 indica que este es el último fragmento o bien que el datagrama no ha sido fragmentado.
  - **Fragment offset (13 bits)**. En el caso de que el datagrama sea un fragmento, indica en qué posición del datagrama original se sitúan los datos que contiene. Cuenta los bytes en grupos de 8, ya que los fragmentos siempre se realizan en múltiplos de 8 bytes.
- *Protocolo de transporte (8 bits)*. Especifica a qué protocolo del nivel de transporte corresponde el datagrama. Aparte de los protocolos TCP y UDP, existen protocolos auxiliares que se identifica por un valor diferente en este campo (ICMP, IGRP, OSPF).
- *Checksum de cabecera (16 bits)*. Sirve para detectar errores producidos en la cabecera del datagrama; no es un CRC sino el complemento a uno en 16 bits de la suma complemento a uno de toda la cabecera tomada en campos de 16 bits.

– La fragmentación se produce cuando el tamaño del datagrama es superior al espacio reservado a datos (MTU) de la trama correspondiente a la red utilizada. Puede ser en origen o en ruta, llevada a cabo por el router que hace la transición a la red de MTU menor:
  - Se corta *la parte de datos* del datagrama en trozos tales que cada fragmento con su cabecera quepa en la MTU de la nueva red. La unidad de fragmentación es de 8 bytes, redondeando por abajo si fuese necesario, y todos ellos múltiplos de 8 bytes salvo quizá el último.
  - Todos los campos de la cabecera del datagrama original se replican en los fragmentos excepto aquellos que se emplean para distinguir los fragmentos. Una vez fragmentado un datagrama no se reensambla hasta que llegue al host de destino.
  - Los fragmentos de un datagrama pueden llegar desordenados a su destino; el receptor podrá identificarlos gracias al campo Identificación. El host receptor retiene en su buffer los fragmentos y el nivel de red los reensambla cuando los ha recibido todos.
  - Si alguno de los fragmentos de un datagrama se pierde el resto terminarán desapareciendo a medida que agoten su TTL. Si el protocolo utilizado a nivel superior contempla el reenvío de paquetes perdidos (por ejemplo TCP) se provocará el reenvío del datagrama completo.

3.1.1.3. Nivel de red en Internet. Protocolos de enrutamiento. Sistemas autónomos.

– La red Internet está formada por multitud de redes interconectadas, pertenecientes a diversas empresas y organizaciones, que comparten a nivel de red el protocolo IP y varios protocolos auxiliares que hacen uso de IP para transmitir la información. **La única excepción a esta regla son los protocolos ARP y RARP**. Estos protocolos auxiliares son los siguientes:
  - Protocolos de control: ICMP e IGMP (multicast).
  - Protocolos de resolución de direcciones: ARP, RARP, BOOTP y DHCP.

– Un protocolo de enrutamiento es el que permite a los routers elegir la ruta que debe tomar un datagrama IP hacia un determinado destino. Cada router se encarga de calcular sus tablas de

rutas a partir de la información que recibe de los demás routers de la red. Existen dos tipos de protocolos de enrutamiento: por *vector distancia* y por *estado del enlace*.

- Un sistema autónomo es una subred gestionada por una autoridad común, con un protocolo de enrutamiento homogéneo mediante el cual intercambia información en toda la subred, y que posee una política común para el intercambio de tráfico con otras redes o sistemas autónomos.
- En Internet se dan dos niveles jerárquicos de enrutamiento:
  - *Interno*. El que se realiza dentro de un sistema autónomo. Suelen utilizarse protocolos por vector distancia (RIPv2, IGRP y EIGRP) y por estado del enlace (IS-IS y OSPF).
  - *Externo*. El que se efectúa entre sistemas autónomos. El protocolo utilizado actualmente es la cuarta versión de BGP (Border Gateway Protocol).

3.1.2. Protocolo TCP (Transmission Control Protocol).

3.1.2.1. Características. Puertos. Acuse de recibo y control de flujo.

- TCP es un protocolo de transporte orientado a conexión, fiable (con acuse de recibo y retransmisión de paquetes), con control de flujo y control de congestión. En TCP se utilizan los puertos para que las aplicaciones de un host distingan a cuál de ellas van dirigidos los datos.
- Un puerto TCP es un número entero entre 0 y 65535. Por convenio los números 0 a 1023 están reservados para el uso de servicios estándar, por lo que se les denomina puertos bien conocidos. En UNIX, estas asignaciones de puertos se encuentran en el fichero /etc/services. Cualquier número superior a 1023 está disponible para ser utilizado libremente por los usuarios.
- La combinación de una dirección IP y un puerto identifica un socket. Así pues, una conexión de dos entidades usuarias del nivel de transporte se especifica por la combinación dirección IP host 1 + puerto host 1 (*socket 1*) y dirección IP host 2 + puerto host 2 (*socket 2*).
- TCP divide o agrupa los mensajes recibidos del nivel de aplicación en segmentos según le convenga. Al viajar en datagramas IP, los segmentos pueden perderse, llegar desordenados o duplicados. Es responsabilidad de TCP generar un flujo de bits fiable para el nivel de aplicación.
- Un segmento TCP tiene una cabecera de 20 bytes formada por entre otros los siguientes campos:
  - *Puerto origen (16 bits)*. Identifica el puerto que se va a utilizar en el host origen.
  - *Puerto destino (16 bits)*. Identifica el puerto que se va a utilizar en el host destino.
  - *Número de secuencia (32 bits)*. Indica el número del primer byte transmitido dentro de ese segmento. TCP incrementa el número de secuencia de cada segmento según los bytes que tenía el segmento anterior, con la excepción de los flags SYN y FIN, que cuando están puestos incrementan en uno el número de secuencia. Esto permite que se pueda acusar recibo de un segmento SYN o FIN sin ambigüedad.
  - *Número de ACK (32 bits)*. Indica el número del primer byte que se espera recibir en el siguiente segmento. La presencia del flag ACK no incrementa el número de secuencia.
  - *Flags de control de segmentos:*
    - **ACK, Acknowledgement (1 bit)**. Indica que en este segmento el campo Número de ACK tiene el significado habitual (número del próximo byte que se espera recibir), de lo contrario carece de significado. En la práctica el bit ACK esta a 1 siempre, excepto en el primer segmento enviado por el host que inicia la conexión.

- **RST, Reset (1 bit)**. Se usa para abortar una conexión porque se ha detectado un error.
- **SYN, Synchronize (1 bit)**. Indica que se está estableciendo la conexión y está puesto sólo en el primer mensaje enviado por cada uno de los hosts en el inicio de la conexión.
- **FIN, Finish (1 bit)**. Para que una conexión se cierre de manera normal cada host ha de enviar un segmento con el bit FIN puesto.

* *Tamaño de ventana (16 bits)*. Indica la cantidad de bytes que se está dispuesto a aceptar en cada momento antes de enviar un acuse de recibo. Cuando un receptor tiene lleno su buffer anuncia una ventana de 0 bytes, con lo que el emisor queda bloqueado hasta nueva orden. El intercambio de segmentos en TCP se desarrolla de acuerdo con un protocolo de ventana deslizante de retroceso n, aunque también puede utilizarse repetición selectiva.
* *Checksum (16 bits)*. Sirve para detectar errores en el segmento recibido. El algoritmo utilizado en TCP es el mismo que el de IP. Para el cálculo del checksum se antepone al segmento una pseudocabecera que incluye la dirección IP de origen y destino, el protocolo de transporte utilizado (TCP en este caso) y la longitud del segmento. Esta pseudocabecera permite a TCP comprobar que no ha habido errores en la transmisión a nivel IP.

– Con acuse de recibo, el origen envía la cantidad de bytes correspondiente al número de la ventana, inicia un temporizador y espera un acuse de recibo antes de enviar los bytes siguientes. Si el temporizador expira antes de que el origen reciba un acuse de recibo, el origen retransmite los bytes correspondiente al número de la ventana y reinicia el temporizador.
– TCP proporciona un secuenciamiento de segmentos con un acuse de recibo de referencia de envío. Cada segmento se numera antes de la transmisión. En la estación receptora, el TCP reensambla los segmentos hasta formar un mensaje completo. Si falta algún número de secuencia en la serie, ese segmento se vuelve a transmitir. Si no se recibe un acuse de recibo para un segmento dentro de un período de tiempo determinado, se produce la retransmisión.

3.1.2.2. Proceso de conexión y desconexión TCP.

– El software o proceso TCP de un host puede mantener en un momento dado múltiples conexiones simultáneas con homólogos suyos en otros hosts. El mecanismo utilizado en TCP para establecer una conexión es el de saludo a tres vías, que evita los problemas debidos a segmentos duplicados. Un proceso normal entre el host 1 y el host 2 sería el siguiente:
  * En el primer segmento el host 1 indica al host 2 que desea establecer una conexión (bit SYN puesto) y le informa del número de secuencia que ha elegido aleatoriamente (x).
  * El host 2 le responde con otro segmento en el que acepta la conexión (bit SYN puesto) y le indica el número de secuencia que él ha elegido aleatoriamente para las transmisiones en el sentido contrario (y). Además acusa recibo de su número de secuencia al indicarle en el ACK que el próximo byte que espera recibir de él es x + 1.
  * El host 1 responde con un tercer mensaje en el que acusa recibo del número de secuencia de host 2, indicándole en el ACK que el próximo byte que espera recibir de él es y + 1.
– Para terminar una conexión TCP se utiliza la finalización a tres vías, en el cual cada lado cierra su parte de forma independiente como si se tratara de una conexión simplex. Un proceso normal entre el host 1 (que inicia la desconexión) y el host 2 sería el siguiente:

- El host 1 envía un FIN/ACK y aceptando datos del otro lado.
- El host 2 recibe el FIN/ACK y envía un ACK. La aplicación podría aún enviar más datos.
- El host 1 recibe el ACK, pero no un FIN. Por tanto, se siguen aceptando datos del otro lado.
- En el host 2 la aplicación local cierra la conexión y TCP envía un FIN/ACK.
- El host 1 recibe el FIN/ACK y envía un ACK. La conexión se mantiene en espera ante la posibilidad de recibir datos retrasados. El tiempo de espera es igual al doble del tiempo de vida de un segmento. Después se borra toda la información relativa a esta conexión.
- El host 2 recibe el ACK y se borra toda la información sobre la conexión.

3.2. A través de redes privadas virtuales (VPN).

- Una red privada virtual permite la interconexión de dos routers, conectados a su vez con sus respectivas redes de área local, utilizando una infraestructura pública normalmente compartida para simular una infraestructura dedicada o privada.
- Cuando se quiere intercambiar paquetes entre dos redes que utilizan el mismo protocolo A, pero que están unidas por una red que utiliza un protocolo B diferente, la técnica a utilizar es establecer un túnel en el que dos nodos ubicados en sus extremos serán los encargados de añadir a los paquetes del protocolo A la cabecera del protocolo B. Tambien realizan el proceso contrario, es decir, quitarle la cabecera del protocolo B a los paquetes recibidos.
- Por tanto, los paquetes del protocolo A viajan encapsulados a través del túnel en paquetes del protocolo B, de manera que no sean vistos por la red del protocolo B. Los conceptos de túnel y de encapsulado de paquetes van siempre asociados entre sí.
- La seguridad de las VPN corre a cargo del protocolo IPSec, que define dos funcionalidades:
  - *AH (Autentication Header).* Añade una cabecera al paquete IP que asegura al receptor que no ha sido alterado durante su viaje por la red, ni en su contenido ni en su cabecera.
  - *ESP (Encapsulating Security Payload).* Encripta la parte de datos del datagrama.
- Existen dos modos de funcionamiento de IPSec:
  - *Modo transporte*. La encriptación se realiza extremo a extremo. Requiere todos los hosts implementen IPSec. Intercala la cabecera IPSec entre la cabecera IP y los datos.
  - *Modo túnel*. El encriptado se efectúa únicamente entre los routers de acceso a los hosts implicados. En este caso la información viaja no encriptada en la parte de la red local. Añade la cabecera IP del túnel y la cabecera IPSec delante de la cabecera IP y los datos.
- Existen dos protocolos de VPN, que utilizan PPP para proporcionar una envoltura inicial para los datos y luego guardan las cabeceras adicionales para el transporte a través de la red:
  - *PPTP (Point-to-Point Tunnel Protocol).* Orientado al usuario, permite establecer un túnel de manera transparente al proveedor de Internet. Requiere que la red sea IP y sólo soporta un túnel simple entre dos puntos. Soporta múltiples protocolos de red y puede utilizar IPSec.
  - *L2TP (Layer 2 Tunnel Protocol).* Orientado al proveedor, permite establecer un túnel de manera transparente al usuario (se utiliza junto con IPSec). Puede utilizarse en redes IP, Frame Relay y ATM. Es superior a PPTP, permite la utilización de múltiples túneles entre dos puntos e incorpora compresión de cabeceras y autenticación a nivel de enlace.