Unidad de Trabajo 4

La arquitectura de las comunicaciones

Lo que caracteriza a las redes de área local es el conjunto de **servicios** que proporcionan a sus usuarios. Estos servicios fundamentan su actuación en el intercambio de datos entre niveles lógicos semejantes en distintas máquinas o terminales de la misma o de distinta red.

Todas esta estructura de comunicación está organizada jerárquicamente formando una **arquitectura**. En esta unidad de trabajo nos proponemos comprender conceptualmente esta arquitectura y prepararnos así para conocer los diferentes servicios que puede ofrecer.

1. Conceptos previos

Las palabras "protocolo" y "arquitectura" tienen una especial importancia en comunicaciones. Estos términos serán utilizados frecuentemente a partir de ahora; por tanto, merece la pena aclarar con precisión qué deberemos entender cuando nos refiramos a estos términos.

1.1 La organización de los ordenadores en red

Cuando se habla de comunicaciones existe una gran confusión entre los diferentes tipos e sistemas de organización de las redes, confusión que se ha extendido incluso en la literatura técnica. Vamos a aclarar algunos de estos conceptos. Para ello tomaremos ejemplos informáticos donde los equipos emisores y receptores serán ordenadores con capacidad de mantener una comunicación. En una primera aproximación, llamaremos ***host*** o **nodo** a un ordenador con capacidad de interactuar en red, capaz de alojar algún tipo de servicio de red. Técnicamente no es preciso afirmar que *host* y nodo sea lo mismo, pero se hace así en el lenguaje coloquial de la Telemática. Más adelante se precisarán estos conceptos.

1.1.1 Sistemas aislados y temporalmente remotos

Un sistema aislado es un ordenador incapaz de comunicarse con el exterior por vía telemática. A cada sistema se le añade el software y el hardware necesario para poder operar en red, aunque actualmente muchos fabricantes los proporcionan de serie. Un ordenador con recursos telemáticos de comunicación es mucho más flexible y adquiere una mayor capacidad de acción que un sistema totalmente aislado.

En ocasiones, los sistemas aislados pueden efectuar conexiones temporales, normalmente a través de redes públicas, para efectuar intercambios de información con el exterior. De este modo, el sistema está conectado sólo temporalmente y se dice que este sistema está realizando conexiones remotas (RAS: Remote Access Services). Este tipo de sistema remoto de red está proliferando actualmente, por ejemplo, en las conexiones remotas particulares a Internet a través de empresas que ofrecen estos servicios telemáticos. Las estaciones de los usuarios sólo pertenecen a la red cuando se produce la conexión.

1.1.2 Redes de ordenadores

Un segundo modo de interconectar ordenadores es la solución de red. Según esta solución, distintos equipos se conectan a través de redes de datos, pero sin perder su identidad propia. Si un usuario solicita un servicio a una red de ordenadores debe presentarse en una máquina concreta y solicitar un servicio concreto. La red distingue todos y cada uno de los equipos. Esta es la situación más normal en la actualidad desde el punto de vista del modo de instalación de los equipos en la red.

1.1.3 Sistemas distribuidos

Un sistema distribuido está compuesto por una red de ordenadores, pero tiene una peculiaridad especial: la existencia de múltiples ordenadores en la red es totalmente transparente al usuario. Por ejemplo, se puede ejecutar una operación en la red y ésta nos devuelve los resultados sin saber a ciencia cierta (y tampoco nos interesa) qué ordenador de todos los de la red ha atendido nuestra petición. En este caso la red se comporta como un sistema que gestiona todos los recursos de los ordenadores que posee.

1.2 El protocolo de comunicaciones

Un protocolo es un conjunto de reglas perfectamente organizadas y convenidas de mutuo acuerdo entre los participantes en una comunicación y su misión es regular algún aspecto de la misma.

Es habitual que los protocolos se ofrezcan como *normativas* o *recomendaciones* de las asociaciones de estándares. Los fabricantes que se ajustan a estas normativas tienen la seguridad de ser compatibles entre sí en aquellos aspectos regulados por el protocolo.

1.3 El concepto de capa o nivel

Con el fin de simplificar la complejidad de cualquier red, los diseñadores de redes han convenido estructurar las diferentes funciones que realizan y los servicios que proveen en una serie de niveles o capas.

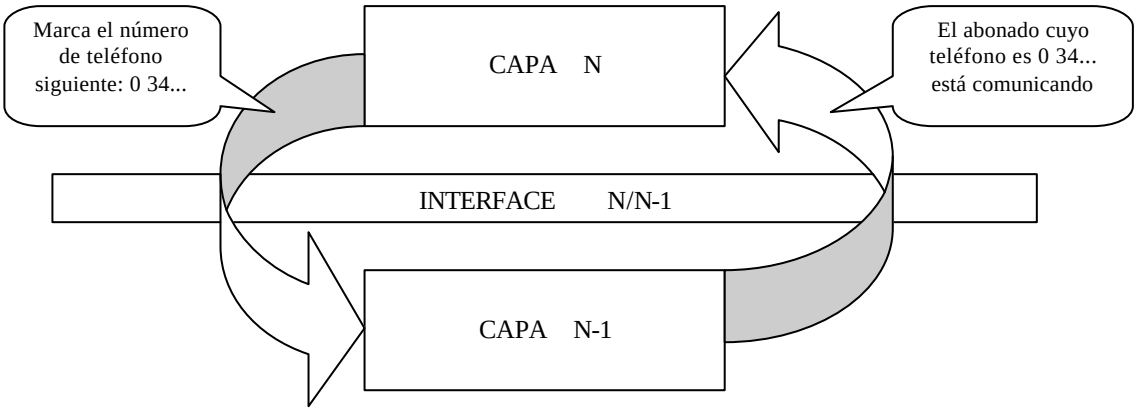
Las capas están jerarquizadas y cada una se construye sobre su predecesora. El número de capas y sus servicios y funciones son variables según el tipo de red. Sin embargo, en cualquier red, la misión de cada capa es proveer servicios a las capas superiores haciendo transparente el modo en que esos servicios se llevan a cabo. De esta manera, cada capa debe ocuparse exclusivamente de su nivel inmediatamente inferior, a quien *solicita servicios*, y del nivel inmediatamente superior, a quien *devuelve resultados.*

Pongamos un ejemplo. Imaginemos un viaje en tren. El viajero debe adquirir un billete, utiliza un servicio concreto. Pero para llegar a su destino no basta con adquirir el billete, la compañía ferroviaria debe conducirle al tren y situarle en su asiento. A su vez, el tren requiere fluido eléctrico procedente de la compañía eléctrica para que se pueda producir el fenómeno de transporte. Cada uno de estos acontecimientos pertenece a una capa. Sólo pueden solicitarse servicios entre sí las capas adyacentes, por ejemplo, el viajero no puede pedir a la compañía eléctrica el fluido, el tren es el único que está capacitado para alimentarse eléctricamente de los tendidos de tensión eléctrica.

1.4 La interfaz entre capas

Hemos afirmado que dos capas consecutivas mantienen relaciones, es más, estas relaciones son las únicas que existen en las redes estructuradas como sucesión de capas. Esto nos lleva a definir el modo en que cada capa negocia los servicios y se comunica con las capas adyacentes. Llamamos interface de capa a las normas de intercomunicación entre capas.

En el ejemplo del epígrafe anterior existe una forma concreta de solicitar un billete: hay que dirigirse a la ventanilla, esperar un turno, solicitar un destino, etc. Para subirse al tren hay que averiguar el número de andén, desplazarse hasta el mismo, buscar el asiento, etc.



La interface, entendida como la definición de los servicios y operaciones que la capa inferior ofrece a la superior, se gestiona como una estructura de **primitivas**. Las primitivas son llamadas entrantes o salientes en cada una de las capas que sirven para solicitar servicios, devolver resultados, confirmar las peticiones, etc. Estas primitivas siguen una estricta regla sintáctica que estudiaremos más adelante.

1.5 La arquitectura de una red

La arquitectura de una red es el conjunto organizado de capas y protocolos de la misma. Esta organización de la red debe estar suficientemente clara como para que los fabricantes de software o hardware puedan diseñar sus productos con garantía de que funcionarán en comunicación con otros equipos que sigan las mismas reglas.

Como se puede observar, no se han incluido en la arquitectura las interfaces. Ello es debido a que la estructura de capas los oculta totalmente. Una interface concreto requiere ser conocido exclusivamente por las dos capas adyacentes a las que separa.

1.6 Los sistemas abiertos

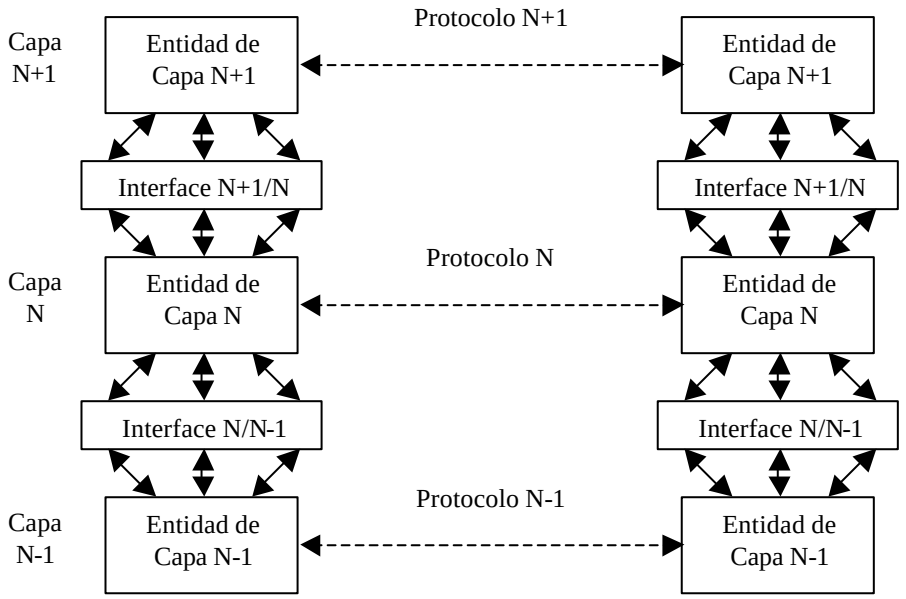
El concepto de sistema abierto fue propuesto inicialmente por la ISO *(International Standards Organization)* como el que está compuesto por uno o más ordenadores, el software asociado, los periféricos, los procesos físicos, los medios de transmisión de la información, etc., que constituyen un todo autónomo capaz de realizar un tratamiento de la información.

En un segundo estadío, más avanzado, lo volvió a redefinir como un sistema capaz de interconectarse con otros de acuerdo con unas normas establecidas. Por tanto, la interconexión de sistemas abiertos OSI *(Open Svstems Interconnection)* se ocupará del intercambio de información entre los mismos. Su objetivo será la confección de una serie de normas que permitan la intercomunicación de estos sistemas.

2 El modelo arquitectónico de capas de red

A continuación procederemos a describir brevemente los componentes de cualquier arquitectura de red basada en el modelo de capas.

En la figura siguiente observamos que las interfaces proporcionan los puntos de acceso a los diferentes servicios que cada capa provee y se diferencian entre sí por las funciones que desempeñan en el proceso de la comunicación. La capa N puede solicitar servicios a la capa N - 1. Del mismo modo, la capa N + 1 sólo puede solicitar servicios de la capa N. La primera es una excepción, pues no tiene ninguna otra por debajo a quien solicitar servicios: fundamentalmente se encarga de operar con los medios de transmisión.



Si se cambia algo en la capa N, ninguna otra capa se sentirá afectada siempre que se conserven las estructuras de las interfaces N / N - 1 y N + 1 / N. Esta es la gran ventaja de la arquitectura de capas: es muy poco sensible a los cambios tecnológicos que se producen por evolución en las funciones y en los servicios de las redes.

Esto hace que las redes configuradas, según un modelo de capas, sean enormemente flexibles.

El proceso de comunicación se produce entre las capas equivalentes de dos hosts distintos. La información y, con ella, la petición de servicios, va descendiendo por la estructura de capas del host emisor hasta que en el nivel más bajo (transmisión física de la señal de la que ya nos ocupamos en la Unidad de Trabajo 2), la información pasa al host receptor. A partir de aquí se inicia el viaje ascendente hasta llegar a la capa equivalente en el host de destino de la capa que inició el servicio en el host emisor.

A1 nodo emisor le parece que la comunicación se ha producido en un nivel alto, quiere pensar que ha entablado una conversación utilizando unas reglas de alto nivel para enlazar con la capa equivalente (de alto nivel) en el nodo destinatario. Sabemos que no es así, que realmente la comunicación ha descendido hasta el nivel más bajo. Pero, tanto para el emisor como para el receptor, todo este proceso ha sido transparente y esto era lo que se pretendía.

Por ejemplo, al utilizar servicios de disco remoto desde un servidor de discos en una red, las unidades remotas se abren virtualmente: al usuario le parece que los discos están situados en su propia máquina, cuando realmente están al otro lado de la red. El software de red se encarga de efectuar esta transparencia.

Se dice que la capa N de un host emisor se comunica con la capa N de un receptor a través de un protocolo de capa N. El protocolo de capa N enmascara el proceso desencadenado en las capas de nivel inferior: no nos interesa lo que ocurre en esas capas; el procedimiento es transparente para la capa N.

Ahora estamos en mejores condiciones para entender el punto en el que se insistió en la Unidad de Trabajo 1, cuando distinguíamos entre transmisión y comunicación: la capa 1 opera con transmisiones en el nivel físico, es decir, con señales; el resto de las capas opera con comunicaciones, es decir, señales interpretadas de acuerdo con unas normas protocolarias.

3 El modelo de referencia OSI

OSI es el nombre del modelo de referencia de una arquitectura de capas para redes de ordenadores y sistemas distribuidos que ha propuesto la ISO como estándar de interconexión de sistemas abiertos.

3.1 Conceptos previos en el modelo OSI

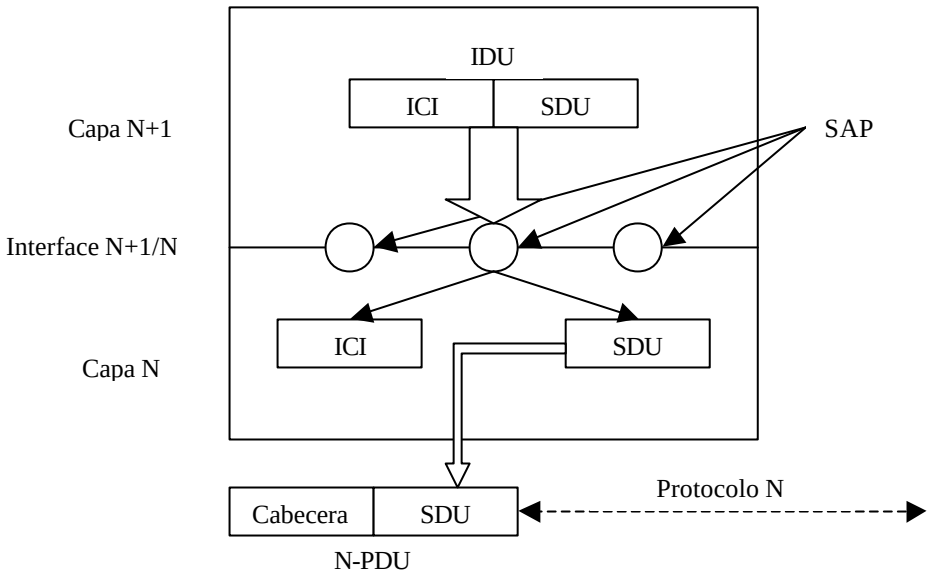
- **Entidades.** Se llama así a los elementos activos que se encuentran en cada una de las capas. Hay entidades software como procesos y entidades hardware como chips encargados de hacer la entrada y salida de datos. A las entidades de la misma capa, residentes en distintos nodos, se les llama entidades pares o iguales.

- **Punto de acceso al servicio SAP (*Service Access Point*).** Los **SAP** son los puntos en los que una capa puede encontrar disponibles los servicios de la capa inmediatamente inferior. Cada SAP tiene una *dirección* que le identifica y por la que se invoca el servicio. Por ejemplo, en el sistema postal, los SAP serían equivalentes a las direcciones postales de cada uno de los domicilios.

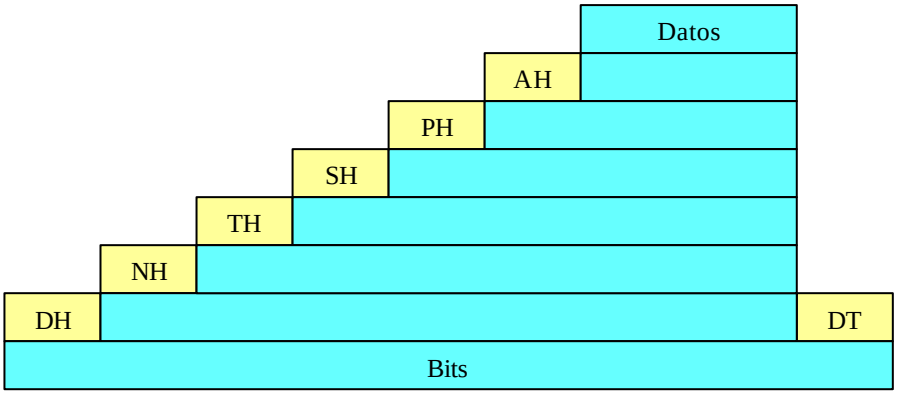
- **Unidad de datos del interfaz IDU (*Interface Data Unit*).** Es el bloque informativo que la entidad de capa N pasa a la entidad correspondiente de la capa N-1 a través de la interface N/N-1.

- **Unidad de datos del servicio SDU (*Service Data Unit*).** Cada IDU está compuesto de un campo con información para el control de la interface (campo ICI; *Interface Control Information*) y de un segundo campo llamado SDU, que es la información que se pasa a través de la red a la entidad par, es decir, a su equivalente en el host destinatario.

- **Unidad de datos del protocolo PDU (*Protocol Data Unit*).** La información del SDU no siempre se puede transmitir en directo. A veces hay que fraccionarlo porque su tamaño no es adecuado para la transmisión directa y además siempre habrá que ponerle alguna cabecera con información de control. A este campo SDU más la cabecera de control se le llama PDU. Si estamos operando en la capa N, el PDU recibe el nombre de N-PDU, aunque en algunas capas de OSI se utilizan sinónimos mnemotécnicos, algunos de los cuales aparecerán más adelante. Los N-PDU son las unidades de intercambio entre las entidades pares de capa N de dos nodos utilizando su protocolo de capa N.



Las cabeceras que cada capa añade a los datos que le llegan de su capa inmediatamente superior llevan la información de control necesaria para la interface y para la propia capa. Por ejemplo, si deseamos enviar un mensaje en papel y es necesario segmentarlo en diversas porciones, cada trozo deberá ir acompañado de una etiqueta identificativa con el fin de poder reconstruir el mensaje original en destino. La información de numeración de estas etiquetas podría ser la cabecera de cada porción.



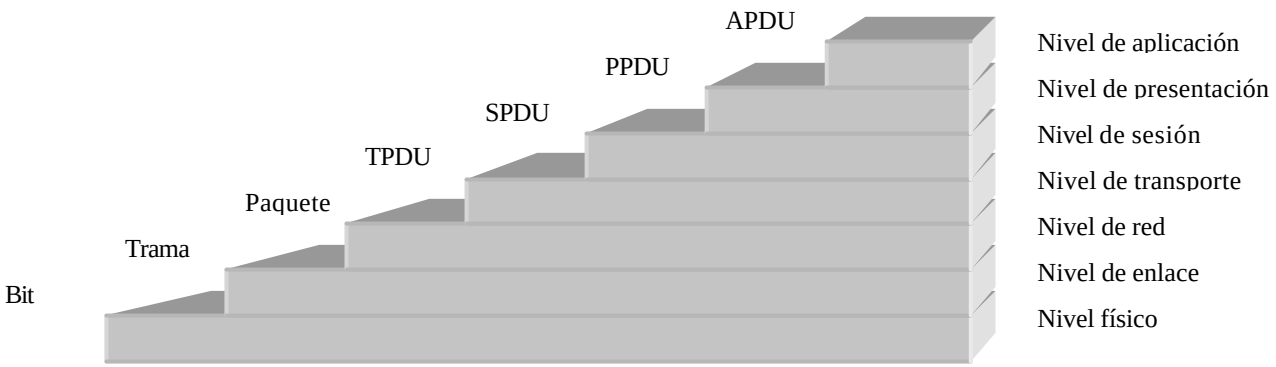
Cabeceras asociadas a cada nivel O.S.I.

3.2 La estructura de capas en OSI

El modelo de referencia OSI propone una arquitectura de siete capas o niveles, cada una de las cuales ha sido diseñada teniendo en cuenta los siguientes factores:

- Una capa se identifica con un nivel de abstracción, por tanto, existen tantas capas como niveles de abstracción sean necesarios.
- Cada capa debe tener una función perfectamente definida.
- La función de cada capa debe elegirse de modo que sea posible la definición posterior de protocolos internacionalmente normalizados.
- Se disminuirá al máximo posible el flujo de información entre las capas a través de las interfaces.
- Las capas serán tan numerosas como sea necesario para que dos funciones muy distintas no tengan que convivir en la misma capa.

Los nombres que reciben estas siete capas son, de menor a mayor nivel: física, enlace, red, transporte, sesión, presentación y aplicación.



Como puede advertirse, el modelo OSI no especifica cómo son los protocolos de comunicaciones, no es una verdadera arquitectura, sencillamente recomienda la manera en que deben actuar las distintas capas. No obstante,

la ISO ha recomendado normas para protocolos en cada una de las capas. Estrictamente hablando, estas normas o realizaciones concretas de los protocolos no pertenecen al modelo OSI; de hecho, se han publicado como normas internacionales independientes.

El diálogo entre las diferentes capas se realiza a través de la interface existente entre ellas. Esta comunicación está perfectamente normalizada en forma de un sistema de llamadas y respuestas que OSI denomina **primitivas**. De este modo, cada servicio está nominado por un SAP que le identifica unívocamente dentro de cada interface y un conjunto de operaciones primitivas, al servicio de la capa superior, utilizadas para solicitar los servicios a que se tienen acceso desde cada SAP.

OSI define cuatro primitivas fundamentales detalladas en la siguiente tabla:

Primitiva	Nombre OSI	Significado
Solicitud	.request	Una entidad solicita que un servicio realice un trabajo para ella.
Indicación	.indication	Una entidad es informada de que ha ocurrido un evento, por ejemplo, que otra entidad solicita sus servicios.
Respuesta	.response	Una entidad responde con esta primitiva a un evento producido anteriormente.
Confirmación	.confirm	Una entidad es informada acerca de una solicitud efectuada anteriormente.

El nombre de cada primitiva fundamental consta de un literal precedido por un punto. La primitiva de un servicio se construye escribiendo el nombre del servicio o función (normalmente en mayúsculas) seguido por un punto y por la primitiva fundamental. No todos los servicios tienen necesidad de las cuatro primitivas fundamentales. Veamos el caso particular de una comunicación de datos por teléfono:

Paso	Primitiva	Significado
1	CONNECT.request	Petición de marcada al número de abonado del destinatario.
2	CONNECT.indication	El teléfono del abonado destinatario produce la señal de llamada.
3	CONNECT.response	El destinatario descuelga el teléfono.
4	CONNECT.confirm	El abonado que originó la llamada escucha que el teléfono destinatario dejó de sonar porque alguien lo descolgó para atender la llamada.
5	DATA.request (desde origen hacia el destino)	Flujo de datos desde el origen al destino.
6	DATA.indication (en el destino)	El destinatario escucha los datos que le llegan por la línea telefónica.
7	DATA.request (desde el destino hasta el origen)	Como el teléfono es full dúplex, el destinatario también puede emitir su mensaje.
8	DATA.indication (en el origen)	El primer abonado escucha en su auricular lo que su destinatario habló por el micrófono.
9	DISCONNECT.request	Quien originó la llamada cuelga el teléfono.
10	DISCONNECT.indication	El destinatario escucha que han colgado y cuelga también

En esta tabla se puede observar el orden de ejecución de diez primitivas para la realización de una conversación telefónica bidireccional. Se han utilizado las primitivas CONNECT, DATA y DISCONNECT en conjunción con las primitivas fundamentales **.request**, **.indication**, **.response** y **.confirm**. No todas las primitivas necesitan todas las fundamentales, por ejemplo, la primitiva DATA sólo requiere **.request** e **.indication** en este ejemplo.

Hay que ser conscientes de que no todas las primitivas se ejecutan en el mismo ordenador: algunas lo hacen en el ordenador origen y otras en el destino. Así, en el ejemplo anterior la primitiva CONNECT.request se opera en el origen y se convierte en CONNECT.indication en el destino.

De modo semejante, algunas primitivas se dirigen desde la capa superior a la inferior y otras al revés: la CONNECT.request es una petición de servicio a la capa inmediatamente inferior, mientras que la CONNECT.indication es una información que le pasa el sistema de marcado (capa inferior) a la capa superior para indicarle que están llamando.

No hay que confundir el concepto «servicio» con el de «protocolo». El servicio es el conjunto de primitivas que cada capa ofrece a través de su interface a la capa superior. En cambio, el protocolo es el conjunto de reglas que normalizan cómo deben ser los formatos de las tramas, paquetes, mensajes, etc., que se intercambian las entidades pares de emisor y receptor.

3.3 Tipos de servicios definidos en OSI

En OSI se definen dos tipos de servicios claramente diferenciados y cada uno provee a la red de una funcionalidad concreta.

3.3.1 Servicios orientados a la conexión

Son servicios que requieren el establecimiento inicial de una conexión y la ruptura o liberación final de la misma. Entre la conexión y la liberación de la misma se produce el intercambio de datos de usuario. Los bloques de datos se reciben en el destino en el mismo orden en que se emitieron en el origen. Todos los paquetes siguen la misma ruta, la conseguida en el establecimiento de la conexión. Por tanto, los paquetes de datos no necesitan especificar la dirección de destino.

Los servicios orientados a la conexión tienen dos variantes:

- **Secuencia de mensajes.** En estos servicios se establecen fronteras que definen y determinan cada mensaje. Por ejemplo, en la transmisión de las páginas de un libro, cada página se podría transmitir secuencialmente con la siguiente intercalando en medio una marca de fin de página. La secuencia de mensajes es equivalente a la sincronización de bloque estudiada en la Unidad de Trabajo 1.

- **Secuencia de bytes.** En estos servicios no hay contornos entre los mensajes. Cada mensaje es una secuencia de caracteres dejando al receptor la responsabilidad de su interpretación.

Un ejemplo de servicio orientado a la conexión es el telefónico: se produce la llamada al abonado destinatario, se intercambian datos una vez realizada la conexión y se libera la conexión cuando ha acabado la transmisión, dando por concluida la comunicación.

3.3.2 Servicios sin conexión

Estos servicios ofrecen la capacidad de comunicación sin necesidad de realizar una conexión con el destinatario. El emisor envía paquetes de datos al receptor confiando en que la red tendrá suficiente inteligencia como para conducir los datos por las rutas adecuadas. Cada paquete debe llevar la dirección de destino y, en algunos casos, el receptor debe enviar acuse de recibo al emisor para informarle sobre el éxito de la comunicación.

Un ejemplo de servicio sin conexión sería el correo postal. Cada mensaje -carta- lleva su dirección y es encaminado a través del sistema postal hasta su destino.

También hay varios tipos de servicios sin conexión:

- **Servicio de datagrama sin confirmación.** El emisor no necesita confirmación por parte del receptor de que los paquetes de datos le llegan correctamente. Por ejemplo, el protocolo IP *(Internet Protocol)*.

- **Servicio de datagrama con confirmación.** El receptor envía confirmaciones al emisor. Por ejemplo, el correo electrónico con acuse de recibo.

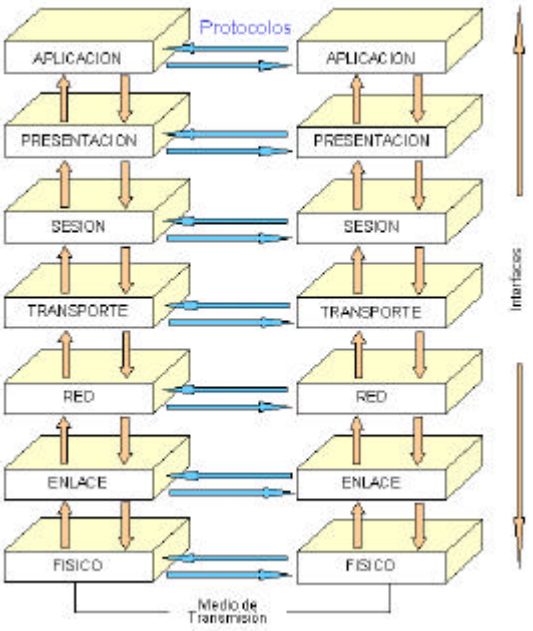
- **Servicio de petición** y **respuesta.** Es un servicio propio de gestión interactiva basado en que a cada petición le sigue una respuesta. Por ejemplo, a cada petición de una base de datos le sigue un mensaje de respuesta que contiene los datos solicitados.

4 Los niveles OSI orientados a la red

En la jerarquía de capas de OSI los niveles superiores están más próximos al usuario y tienen un nivel de abstracción mayor. Se dice que estas capas (aplicación, presentación y sesión) están orientadas a la aplicación o al usuario.

En cambio, los niveles inferiores están más próximos a la red; de hecho, la capa física se ocupa del hardware. Se dice que las capas física, de enlace y de red están orientadas a la red. Al subconjunto de estas tres capas inferiores se le llama subred.

La capa de transporte es muy especial y merece una mención aparte, como veremos más adelante.



4.1 El nivel físico

La capa física se ocupa de definir las características *mecánicas, eléctricas, funcionales* y de *procedimiento* para poder establecer y destruir conexiones entre dos equipos de la red. Es la capa de más bajo nivel; por tanto, se ocupa de las transmisiones de los bits.

Entre otras funciones, debe garantizar la compatibilidad de los conectores, cuántos pines tiene cada conector y la función de cada uno de ellos, el tipo de sistema de cableado que utilizará, la duración de los pulsos eléctricos, la modulación, si hubiera, el número de voltios de cada señal, el modo de explotación del circuito, etc.

4.2 El nivel de enlace

La misión de la capa de enlace es establecer una línea de comunicación libre de errores que pueda ser utilizada por la capa inmediatamente superior: la capa de red.

Como el nivel físico opera con bits, sin detenerse en averiguar su significado, la capa de enlace debe fraccionar el mensaje en bloques de datos de nivel 2 (2-PDU) o tramas. Estas tramas serán enviadas secuencialmente por la línea de transmisión a través de los servicios de transmisión que ofrece la capa física y quedará a la escucha de las tramas de confirmación que genere la capa de enlace del receptor.

Aspecto general de una trama

Por tanto, el nivel de enlace se ocupará del tratamiento de los errores que se produzcan en la recepción de las tramas, de eliminar tramas erróneas, solicitar retransmisiones, descartar tramas duplicadas, adecuar el flujo de datos entre emisores rápidos y receptores lentos, etc.

4.3 El nivel de red

La capa de red se ocupa del control de la subred. La principal función de este nivel es la del *encaminamiento*, es decir, cómo elegir la ruta más adecuada para que el bloque de datos del nivel de red (3-PDU) o **paquete** llegue a su destino. Cada destino está identificado unívocamente en la subred por una dirección.

Otra función importante de esta capa es el tratamiento de la congestión. Cuando hay muchos paquetes en la red unos obstruyen a los otros, generando cuellos de botella en los puntos más sensibles. Un sistema de gestión de red avanzado evitará o paliará estos problemas.

Otro problema que debe resolver es el que se produce cuando el destinatario de un paquete no está en la misma red, sino en otra, en el que el sistema de direccionamiento es distinto que en la red origen. Además, es posible que la segunda red no admita paquetes de las mismas dimensiones que la primera. En general, *la resolución de problemas generados por redes heterogéneas debe resolverse en esta capa*.

5 El nivel OSI de transporte

La capa de transporte es una capa de transición entre los niveles orientados a la red (subred) y los orientados a las aplicaciones. Su misión consiste en aceptar los datos de la capa de sesión (S-PDU), fraccionarlos adecuadamente de modo que sean aceptables por la subred (capa de red e inferiores) y asegurarse de que llegarán correctamente al nivel de transporte del destinatario, esté o no en la misma red que la fuente de los datos. Proporciona, por tanto, el servicio de transporte, abstrayéndose del hardware y software de bajo nivel que utiliza la subred para producir el transporte solicitado.

Se puede confundir el transporte de las tramas en el nivel de enlace con el transporte de datos en el nivel de transporte: no tienen ningún parecido. Por ejemplo, el flujo de tramas se opera en el nivel de cada tarjeta de red, de cada puerto de entrada y salida de datos. El flujo de transporte puede llegar a multiplexar conexiones distintas por cada solicitud de la capa inmediatamente superior (sesión), utilizando uno o más puertos de salida para la misma comunicación: al usuario (o a la capa de sesión o superior) le es transparente la utilización de múltiples circuitos físicos, él lo experimenta como una única sesión que se ha resuelto como múltiples conexiones de transporte que atacan a la misma o a distintas subredes. Si, por ejemplo, tuviéramos un nodo con varias tarjetas

de red, con salida a distintas redes, la capa de sesión las vería como una sola red gestionada por la capa de transporte de modo transparente.

Del mismo modo, la capa de transporte selecciona el tipo de servicio que se le debe dar a la capa de sesión y en último término a los usuarios de la red, situados en la capa superior.

La capa de transporte lleva a cabo las comunicaciones entre ordenadores *peer to peer*, de igual a igual, es decir, es el punto en el que emisor y receptor cobran todo su sentido: un programa emisor puede conversar con otro receptor. En las capas inferiores esto no se cumple. Por ejemplo, en el nivel inferior hay transporte de tramas pero puede ser que entre emisor y receptor haya que pasar por varios ordenadores intermedios que redirijan las comunicaciones o que cambien de red los diferentes paquetes, etc. En el nivel de transporte estos sucesos se hacen transparentes: sólo se consideran fuente, destino y tipo de servicio solicitado.

6 Los niveles OSI orientados a la aplicación

Un ordenador puede soportar múltiples aplicaciones simultáneas que solicitan servicios de comunicación a la capa de transporte. A su vez, la capa de transporte debe solicitar servicios de subred con el fin de elegir la que sea necesaria, la ruta más conveniente y el fraccionamiento de datos adecuado. Por tanto, tenemos que muchas comunicaciones de alto nivel pueden ser ejecutadas por múltiples transmisiones de bajo nivel.

Sin embargo, hay un nivel que tiene que ser común, porque tanto el ordenador fuente (el emisor) y el ordenador destino (el receptor) son únicos y unitarios, el transporte se realiza de extremo a extremo, abstrayéndose de lo accesorio: éste es el nivel de la capa de transporte.

Las capas situadas por encima de este nivel de abstracción del transporte están orientadas a las aplicaciones y, por tanto, la terminología utilizada está exenta de todo lo que tiene que ver con el transporte de datos, se centra exclusivamente en las funciones de aplicación.

6.1 El nivel de sesión

Permite el diálogo entre emisor y receptor estableciendo una sesión, que es el nombre que recibe las conexiones en esta capa. A través de una sesión se puede llevar a cabo un transporte de datos ordinario (capa de transporte). La capa de sesión mejora el servicio de la capa de transporte. Por ejemplo, si deseamos transferir un fichero por una línea telefónica que por su excesivo volumen tardará una hora en efectuar el transporte, y la línea telefónica tiene caídas cada quince minutos, será imposible transferir el fichero.

La capa de sesión se podría encargar de la resincronización de la transferencia, de modo que en la siguiente conexión se transmitieran datos a partir del último bloque transmitido sin error.

En el establecimiento de una sesión se pueden diferenciar dos etapas:

El establecimiento de la sesión y creación de un buzón en donde se recibirán los mensajes procedentes de la capa de transporte y de la subred.

El intercambio de datos entre los buzones del emisor y del receptor siguiendo unas reglas para el control del diálogo.

La capa de sesión determina si la comunicación será bidireccional o simultánea. Además, establece el sistema en que los interlocutores de la comunicación toman la iniciativa para la utilización de los recursos de la red, normalmente a través de la utilización de testigos electrónicos.

6.2 El nivel de presentación

La capa de presentación se ocupa de la **sintaxis** y de la **semántica** de la información que se pretende transmitir, es decir, investiga en el contenido informativo de los datos: Esto es un indicativo de su alto nivel en la jerarquía de capas.

Por ejemplo, si el ordenador emisor utiliza el código ASCII para la representación de información alfanumérica y el ordenador receptor utiliza EBCDIC, no habrá forma de entenderse, salvo que la red provea algún servicio de conversión y de interpretación de datos. Esta es una prestación propia de la capa de presentación.

Otro ejemplo común es el de la representación de la información gráfica. Un emisor puede querer representar un texto en negrita y lo hace a través de una determinada secuencia (secuencia de escape). Es posible que el receptor no interprete esa secuencia como «poner en negrita» y necesite de algún intérprete de datos que le traduzca la secuencia a su código nativo.

Cuando desde un ordenador personal realizamos una conexión (sesión) contra algún servicio telemático y nos aparecen en el monitor caracteres extraños, teniendo certeza de que los parámetros de transmisión son correctos (velocidad, paridad, bit de start y stop, etc.), lo que realmente está ocurriendo es que fallan o no tenemos los servicios de la capa de presentación.

Otra función de la capa de presentación puede ser la de **comprimir los datos** para que las comunicaciones sean menos costosas o la de **encriptación** de la información que garantiza la privacidad de la misma.

6.3 El nivel de aplicación

Es la capa superior de la jerarquía OSI. En esta capa se definen los protocolos que utilizarán las aplicaciones y procesos de los usuarios. La comunicación se realiza utilizando protocolos de diálogo apropiados. Cuando dos procesos que desean comunicarse residen en el mismo ordenador, utilizan para ello las funciones que le brinda el sistema operativo. Sin embargo, si residen en ordenadores distintos, la capa de aplicación disparará los mecanismos adecuados para producir la conexión entre ellos, sirviéndose de los servicios de las capas inferiores.

La ISO inicialmente hizo referencia a cinco grupos de protocolos en el nivel de aplicación. Aunque en la actualidad se han simplificado bastante, resulta instructivo conocer algunos detalles:

· **Grupo l.** Protocolos de gestión del sistema. Están orientados a la gestión del propio sistema de interconexión de los ordenadores en la red.

· **Grupo 2.** Protocolos de gestión de la aplicación. Llevan el control de la gestión de ejecución de procesos: bloqueos, accesos indebidos, asignación y cómputo de recursos, etc.

· **Grupo 3.** Protocolos de sistema. Gestionan las tareas del sistema operativo como el acceso a ficheros, la comunicación entre tareas o procesos, la ejecución de tareas remotas, etc.

· **Grupos 4** y **5.** Protocolos específicos para aplicaciones. Son absolutamente dependientes de las necesidades de las aplicaciones para las que se utilizan.

7 Ejemplo funcional de la arquitectura OSI

En esta Unidad de Trabajo estamos trabajando con protocolos y arquitecturas, capas e interfaces, servicios y primitivas: todos los conceptos utilizados son extremadamente abstractos. Llegados a este punto conviene poner un ejemplo funcional basado en la vida corriente y hacer una analogía con el modelo arquitectónico propuesto por OSI.

El ejemplo consistirá en descomponer, en fases, el transporte de una mercancía desde el lugar de producción hasta el lugar de venta. Supongamos que una cooperativa agrícola tiene como cliente habitual un mercado de

abastos de fruta situado en una ciudad de otro país. Las frutas deben ser recogidas en la cooperativa y trasladadas al mercado.

Vamos a descomponer el proceso de transporte tal y como es visto por la cooperativa en forma de, clasificando los eventos producidos en las diferentes capas de OSI. Los datos que aparecen en la tabla son orientativos y tienen un fin exclusivamente didáctico, puede sernos útil para clarificar los conceptos abstractos.

CAPA	EVENTO	OBSERVACIONES
Aplicación	La cooperativa recoge los frutos que aportan los agricultores, negocia un precio de venta con el mercado de abastos y decide proceder al transporte de la mercancía.	Este evento está en contacto directo con los usuarios de la comunicación: el comprador y el vendedor. La aplicación sería una operación comercial de compraventa, que no se puede llevar a cabo sin un fenómeno de transporte.
Presentación	Una vez recogidas las frutas deben empaquetarse y presentarse como cestas con un peso bruto determinado. Además hay que colocar las cestas de modo que ocupen un espacio mínimo con el fin de facilitar el transporte. Las cajas con las cestas van precintadas.	Este evento se ocupa de que las frutas tengan un aspecto (presentación) determinado de cara al consumidor. Además, lleva incorporado un proceso de compresión para facilitar el transporte. El precinto de cada caja sirve de encriptación, hace que la carga tenga privacidad.
Sesión	El comprador y el vendedor se ponen de acuerdo en enviar todos los lunes, miércoles y viernes 10 tm de fruta, sin embargo, la próxima semana habrá una excepción: el viernes es festivo y la fruta se transportará en lunes, miércoles y jueves. Los pagos se harán con letras de cambio con un vencimiento a treinta días.	En este evento se abre una sesión en que se especifica cómo serán los envíos, es decir, se establece el diálogo sobre cómo proceder para efectuar el transporte. Además se negocia el sistema de pago.
Transporte	Ya es lunes. Hoy hay que efectuar un transporte de fruta. Llamamos a la compañía de transportes para que recoja la fruta. Se compromete a entregar la fruta en el mercado de abastos en el plazo fijado de antemano y en las debidas condiciones de salubridad. Comprueba que el terminal de descarga del mercado de abastos tiene previsto que llegará una carga de fruta de 10 tm en pocas horas.	En este evento se efectúa una conexión. Se negocia la calidad de servicio con parámetros como el plazo de entrega de la carga, el buen estado de la misma, etc. Para cumplir el plazo de entrega la capa inmediatamente inferior deberá elegir medios de comunicación apropiados, suficientemente rápidos (avión o vías terrestres amplias y poco congestionadas, etc.). Además, comprueba que el destinatario puede ofrecer este servicio: en el mercado hay un lugar para la fruta.
Red	La compañía de transportes determina las rutas posibles para efectuar el traslado de la carga, así como el sistema de transporte más adecuado. Elige el siguiente: 5 tm viajarán en avión y las otras 5 tm por carretera en camión. Además se decide el rumbo que debe seguir el avión para evitar una zona de borrasca y las carreteras apropiadas para evitar atascos de tráfico. La carga que irá en avión debe empaquetarse en un contenedor especial para la bodega del avión. La carga que viaja por carretera se empaqueta en cajas de cartón acinturadas con plástico. Tanto el contenedor aéreo como cada una de las cajas llevas adheridas etiquetas identificativas del aeropuerto de destino o de la dirección del terminal de descarga destinatario.	En este evento se estudian las rutas. A partir de esta capa ya se tienen en cuenta las tecnologías físicas o lógicas de bajo nivel que serán utilizadas para producir el fenómeno de transporte. Se seleccionan las rutas más adecuadas. Hay un fraccionamiento de la carga por necesidades del servicio de transporte. La carga se encapsula de un modo apropiado para la tecnología de transporte. Además, cada unidad de carga (contenedor o caja) lleva la dirección de origen y destino (aeropuerto o mercado, que es donde llegan los medios de transporte). Además, las rutas han sido elegidas de acuerdo con ciertos criterios de eficacia: poca congestión de tráfico, mejora en las condiciones de vuelo, etc.
Enlace	Al contenedor de avión se le añade un control de seguridad, se observa que tienen un peso excesivo y se reparte en dos contenedores más pequeños. Se instalan uno a cada lado de la bodega de la aeronave para distribuir proporcionalmente la carga. La otra mitad de la carga, la que viaja por carretera, se distribuye en 10 camiones frigoríficos que se precintan por seguridad. Todas las unidades de carga llevan un etiquetado de origen y destino y cada camión registra la temperatura habida en el viaje. Si no es la prevista, el termómetro del camión frigorífico servirá de prueba para declarar inservible la carga y pedir una nueva.	En este evento se expresa el equivalente a los controles de errores: el termómetro, los precintos de seguridad, etc. La carga ha de repartirse para hacer posible el transporte en ese avión concreto en el que viajará o en los camiones frigoríficos, que tienen una tara y un peso máximo autorizado, es decir, debemos ajustarnos a la tecnología concreta de bajo nivel que se utilizará. Si se ha producido error se pedirá una devolución y reposición de la carga (retransmisión).
Físico	Tanto el avión, por vía aérea, como los camiones, por vía terrestre, transportarán la carga al lugar de destino.	Aquí es donde se produce realmente el transporte de la carga.

Además de los eventos señalados en la tabla anterior, debemos considerar que en el camino podrían haber ocurrido los sucesos que aparecen en la tabla siguiente. El concepto "máquina de red" que aparece en esta tabla se refiere al dispositivo conectable a una red que se encargaría de realizar la función del suceso descrito en la primera columna.

SUCESO	MAQUINA DE RED	OBSERVACIONES
La compañía aérea propietaria del avión que recogió la carga no vuela hasta la ciudad de destino. El avión debe hacer escala en un aeropuerto intermedio en donde la carga es recogida por el avión de otra compañía aérea, que subcontrata el servicio, y que elige una nueva ruta en el espacio aéreo que tiene reservado para alcanzar el destino de la carga.	**Encaminador o *Router***	La ruta que sigue la carga sufre una modificación. Se produce un cambio en la red de transporte, se pasa de una compañía aérea a otra que sí tiene vuelos hasta la ciudad de destino. La capa 2 sólo puede hacer enlaces locales: se mueve dentro de la misma compañía aérea. Un cambio de compañía aérea exige servicios de capa 3.
Como en el suceso anterior, la compañía aérea propietaria del avión que recogió la carga no vuela hasta la ciudad de destino. El avión debe hacer escala en un aeropuerto intermedio en donde la carga es recogida por un tren, porque la ciudad de destino no tiene aeropuerto. La carga debe ser fraccionada para que quepa en los contenedores del tren. Hay que rehacer los etiquetados para que cumplan con la normativa ferroviaria.	**Pasarela o *Gateway***	En este caso hay un cambio de red, se pasa de una red aérea a una red ferroviaria. Las condiciones de transporte son totalmente diferentes. Hay una conversión de protocolo y, por supuesto, hay que cambiar el sistema de direcciones: el destino ya no es un aeropuerto, sino una estación ferroviaria.
Los camiones que transportan la carga tienen prohibido traspasar las fronteras del país al que pertenece la cooperativa agrícola. En la frontera hay un paso de la carga a otros camiones semejante del país destinatario. Se comprueba que la carga sigue en buen estado.	**Puente o *Bridge***	El destino no se alcanza en el ámbito geográfico posible para los camiones que iniciaron el transporte. Deben traspasar la carga a otra red de transportes internacional que sí alcanza el destino. Además, se comprueba que la información es correcta.
Los camiones reponen combustible periódicamente y vigilan el termómetro del contenedor frigorífico. Si la temperatura sube, entonces elevan la potencia del refrigerador para asegurar que no se perderá la carga.	**Repetidor o *Repeater***	Periódicamente se deben restituir las señales originales; en nuestro ejemplo, el estado de la carga. Se deben poner los medios necesarios para corregir las deficiencias.

8 Otras arquitecturas y redes

El modelo de referencia OSI es un modelo teórico. No hay ninguna red que sea OSI al cien por cien. Los fabricantes se ajustan a este modelo en aquello que les interesa y, de hecho, se observa una evolución de las redes existentes para compatibilizarse con OSI. En este epígrafe vamos a considerar otras arquitecturas que nos interesan por su extensión o por el contexto histórico en que se sitúan.

8.1 La arquitectura SNA de IBM

SNA (*Systems Networks Architecture*) es el nombre de la arquitectura de redes propia de IBM. El modelo OSI se configuró a partir de SNA, de la que toma el número y funciones aproximadas de sus capas.

SNA vino a resolver la complejidad producida por la multitud de productos de comunicaciones de IBM. Una vez que SNA se concretó en un producto de red, sirvió para resolver la casi totalidad de las situaciones en que fueran necesarias las comunicaciones de ordenadores en el entorno o de IBM.

8.1.1 La historia de la SNA

La primera versión de SNA apareció en 1974 y sólo tenía capacidad para gestionar redes centralizadas en forma de árbol con un solo host al que se conectaban sus terminales.

La segunda versión es de 1976, en ella se permitían varios hosts con sus respectivos árboles, pudiendo establecer comunicaciones entre ellos.

Se fueron añadiendo sucesivas mejoras en 1979 y 1985, año este último en el que se incluyeron el resto de las topologías y cualquier relación entre hosts y otras redes de área local.

8.1.2 Organización de la SNA

Una red SNA está constituida por un conjunto de máquinas, que pueden conectarse a la red, denominadas nodos. SNA define cuatro tipos de nodos: terminales, controladores (máquinas que supervisan el funcionamiento de los terminales u otros periféricos), procesadores frontales (*front-ends*; encargados de reducir la carga de CPU de los procesadores principales, encargándose de las labores de red) y los hosts.

Cada uno de estos nodos tiene al menos una NAU *(Network Address Unit),* unidad direccionable de red, que es el software por el que un proceso puede utilizar la red. Para entenderlo mejor podríamos decir que una NAU en SNA es equivalente a un SAP en OSI. Para poder utilizar la red, debe conectarse un proceso directamente a una NAU, a partir de aquí podrá utilizar los recursos de la red. Por tanto, las NAU son los puntos de entrada a la red para los procesos de usuario.

Hay varios tipos de NAU, la primera, llamada LU *(Logical Unit,* unidad lógica), es la más común; la segunda se llama PU *(Physical Unit,* unidad física), se encarga de la gestión del nodo (por ejemplo, ponerlo en línea), y la tercera se llama SSCP *(Systems Services Control Point,* punto de control en los servicios de sistemas), que tiene un conocimiento completo de los procesadores frontales, controladores y terminales. El conjunto de hardware y software controlado por una NAU de tipo SSCP es lo que se llama dominio en SNA.

8.1.3 Estructura de capas de la SNA

Aunque el número de capas en SNA es el mismo que en OSI, no hay una correspondencia exacta entre ellas, difieren especialmente en las capas 3, 4 y 5.

- **Capa 1 o física.** Tiene a su cargo el transporte físico de las señales que representan los bits.

- **Capa 2 o de control de enlace.** Construye tramas de bits y además detecta y recupera errores de transmisión. El protocolo de comunicación de datos de capa 2 en SNA se llama SDLC *(Synchronous Data Link Control,* control de enlace de datos síncrono). El protocolo HDLC *(High Level Data Link Control*, control de alto nivel para el enlace de datos) de OSI es semejante al SDLC de SNA, de hecho, deriva de él. Esta capa también soporta el acceso a la red por testigo (Token Ring), lo que se estudiará en la Unidad de Trabajo 5.

- **Capa 3 o de control de ruta.** Se encarga de establecer una ruta apropiada entre la NAU origen y la NAU destino. Las subredes de SNA se llaman subáreas. Cada subárea tiene un nodo especial que actúa como pasarela entre las distintas subáreas. Más adelante se precisará el concepto de pasarela *o gateway*.

- **Capa 4 o de control de transmisión.** Es la encargada de la creación, gestión y liberación de las conexiones de transporte, que en SNA se llaman sesiones. Como en OSI, la capa 4 se encarga de hacer transparente a las capas superiores la tecnología concreta en que está construida la red.

- **Capa 5 o de control de flujo de datos.** Determina el sistema de diálogo en una comunicación.

- **Capa 6 o capa de servicios NAU.** Ofrece dos tipos de servicios, los de presentación, semejantes a los de OSI y los de sesión, que sirven para el establecimiento de conexiones.

- **Capa 7 o de usuario terminal.** Es la capa equivalente a la de aplicación en OSI.

8.2 La arquitectura DNA de DEC

DNA *(Digital Network Architecture)* es la arquitectura de red propuesta por DEC *(Digital Equipment Corporation).* Consta de una estructura jerárquica de siete capas semejantes en gran parte a las de OSI.

- **Capa 1 o física.** Se encarga de la transmisión de señales, como en OSI. Tiene bajo su gobierno todo el hardware de comunicaciones: interfaces, módems y líneas de comunicaciones.

- **Capa 2 o de enlace de datos.** Se encarga de lo necesario para establecer una comunicación libre de errores entre dos nodos adyacentes de la red.

- **Capa 3 o de transporte.** Define los mecanismos para transportar unidades de datos de un nodo a otro, independientemente de su posición en la red.

- **Capa 4 o de control de sesión** y **servicios de la red.** Define lo necesario para que dos procesos se comuniquen entre sí, independientemente de si están situados o no en el mismo nodo de la red. Para ello, si fuera necesario, establece lo que llama enlaces lógicos *(logical links),* que actúan como vía lógica de intercomunicación de los procesos. A veces, en la literatura técnica aparece esta capa separada en dos: de sesión y de servicios de red.

- **Capa 5 o de aplicación de la red.** Permite el acceso remoto a ficheros, gestores remotos de órdenes, terminales virtuales, etc.

- **Capa 6 o de gestión de la red.** Define las funciones necesarias para gestionar, planificar y controlar la red.

- **Capa 7 o de usuario.** Posibilita que los programas de usuario puedan tener acceso a los recursos de la red.

OSI	SNA	DNA
Aplicación	Servicios de transacción	Usuario
Presentación	Administración de funciones	Gestión de red
Sesión	Control de flujo	Sesión y control de red
Transporte	Control de transmisión	Extremos de comunicaciones
Red	Control de rutas	Encaminamiento
Enlace	Enlace	Enlace
Físico	Física	Física

8.2.1 La arquitectura de ARPANET

ARPANET es una red que no sigue el modelo OSI, entre otras razones, porque nació una década antes. ARPANET tiene protocolos equivalentes a lo que en OSI sería la capa de red y de transporte.

Los protocolos más conocidos son:

- **IP** *(Internet Protocol),* protocolo entre redes. Es protocolo sin conexión, especialmente diseñado para la interconexión de numerosas redes WAN y LAN.

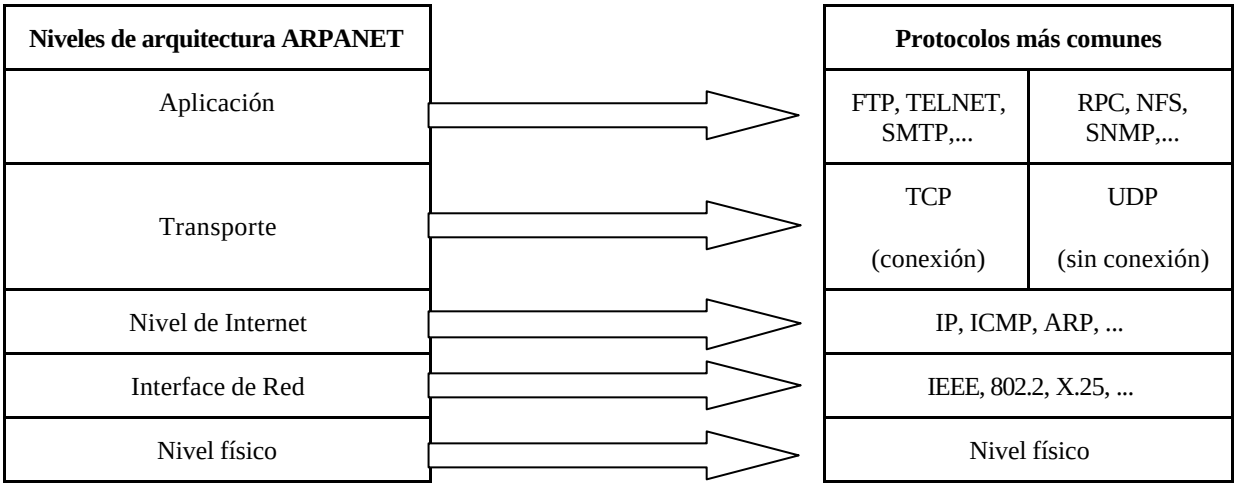
- **TCP** *(Transmission Control Protocol)*, protocolo de control de transmisión. Es un protocolo orientado a la conexión muy semejante a su equivalente (en la capa de transporte en cuanto a su función, aunque difiere notablemente en cuanto a su formato).

En las capas de presentación y sesión, ARPANET carece de protocolos, pero en la de aplicación sí hay varios. Los más conocidos son:

- **FTP** *(File Transfer Protocol)*, protocolo de transferencia de ficheros. Se utiliza para efectuar la transferencia de ficheros de un ordenador a otro.

- **SMPT** *(Simple Mail Protocol Transfer)*, protocolo simple de transferencia de correo. Sirve para gestionar los envíos de una oficina postal de correo electrónico a través de la red.

- **TELNET,** protocolo de conexión remota. Es utilizado para efectuar conexiones remotas gestionadas como terminales virtuales.



Aunque la familia de protocolos de ARPANET está alejada de la estructura de OSI, tiene una gran repercusión. Se han convertido en un estándar *de facto* multiplicando extraordinariamente su utilización, debido a que Internet se sirve de ellos.

9 La estructura de las redes de área local

Si tomamos el ordenador como punto de referencia, caben dos modos de enfocar su estudio. El primero consiste en fijarse en las características del ordenador hacia adentro: su arquitectura, su composición, sus reglas de funcionamiento, etc. De este estudio se ocupa la **Arquitectura de Ordenadores**.

El segundo enfoque considera el ordenador como una entidad que se relaciona con otros ordenadores o dispositivos de comunicación. De esto se ocupa la **Telemática**.

Cuando las comunicaciones entre equipos se extienden en una zona geográfica limitada, se exige una elevada velocidad de transmisión de datos y una tasa de error mínima, nos encontraríamos en el campo de las LAN *(Local Area Network)* o redes de área local.

En la Unidad de Trabajo 1 ya se estudiaron algunos conceptos previos y los principales servicios que puede proporcionar una LAN. Ahora consideraremos las redes de área local desde el punto de vista técnico. En este epígrafe estructuraremos gran parte de los conocimientos adquiridos hasta ahora al hilo de las necesidades de diseño de una LAN.

Una LAN puede incorporar protocolos de múltiples capas, aunque el mayor número de protocolos pertenecerá siempre a las capas inferiores. De hecho, siempre tiene que haber una capa física, de lo contrario sería imposible la transmisión, no habría comunicación y ello inhabilitaría la red como dispositivo de comunicación.

Es normal que una LAN tenga funciones y servicios propios de capas superiores de OSI, pero lo propio de las LAN son las capas inferiores. Por ejemplo, una WAN requiere técnicas de encaminamiento, que son propias de la capa de red (nivel 3 de OSI). No todas las redes de área local pueden encaminar paquetes. Sin embargo, todas las LAN son capaces de entregar tramas de bits (nivel 2) a la capa física (nivel 1) para que sean transmitidas en forma de señales por las líneas de comunicación. Esta es la razón por la que en esta estructuración de las redes de área local estudiemos los niveles 1 y 2 de OSI, aclarando que la LAN abarca más que estos niveles.

9.1 El nivel físico

El nivel físico está regido por la física de la comunicación estudiada en la Unidad de Trabajo 2. Los medios de transmisión tienen unas características y unas limitaciones propias de las propiedades del medio con que son construidos. Ya hemos visto que una de las dificultades más importantes en comunicaciones de datos se debe a la limitación del ancho de banda de los equipos, que si es pequeño sólo permite transmisiones de baja velocidad.

Otro problema importante es el ruido. Cuando la razón señal/ruido es baja, es decir, el ruido adquiere niveles importantes respecto de la señal, aparecen dificultades en la interpretación de la señal y desciende más aún el caudal de información, hasta el punto de hacer la comunicación imposible.

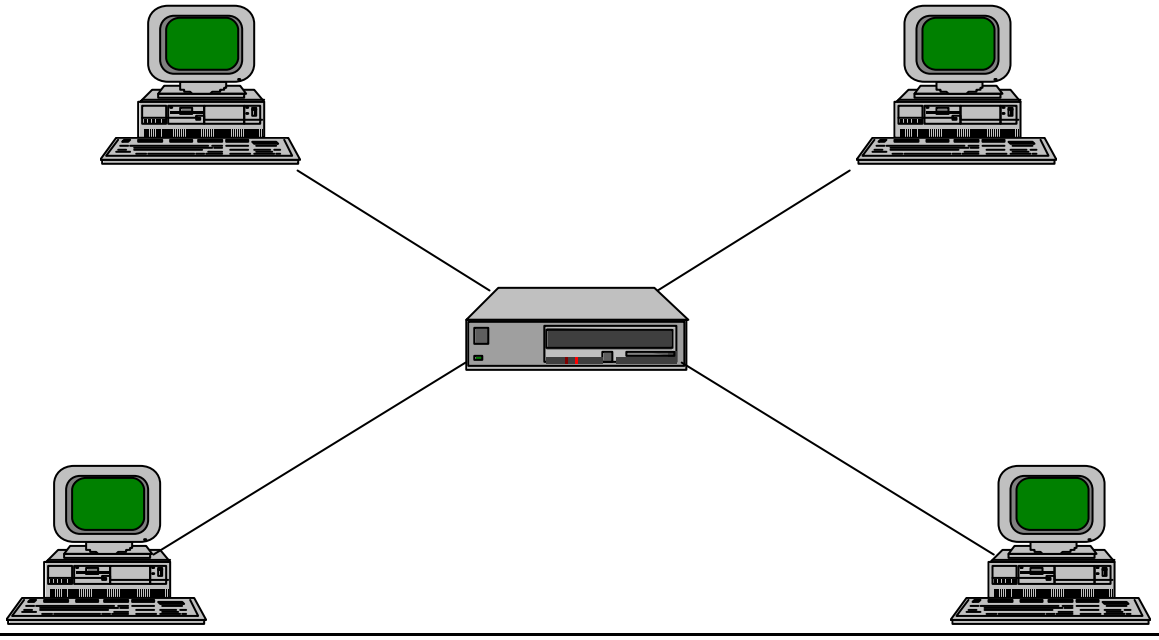
La mayor parte de las redes de área local utilizan codificación ***Manchester diferencial*** para señalizar cada bit del mensaje.

9.1.1 Topologías básicas

La topología de una red es la forma que toma. Por ejemplo, una red en anillo tiene una topología constituida por un anillo transportador al que se conectan todos los equipos que pertenecen a la misma red. Los fabricantes organizan sus productos de acuerdo con unas normas previamente establecidas, que son los estándares propuestos por ellos mismos o por asociaciones internacionales. Un estándar muy común para redes de área local es el propuesto por el IEEE 802.X.

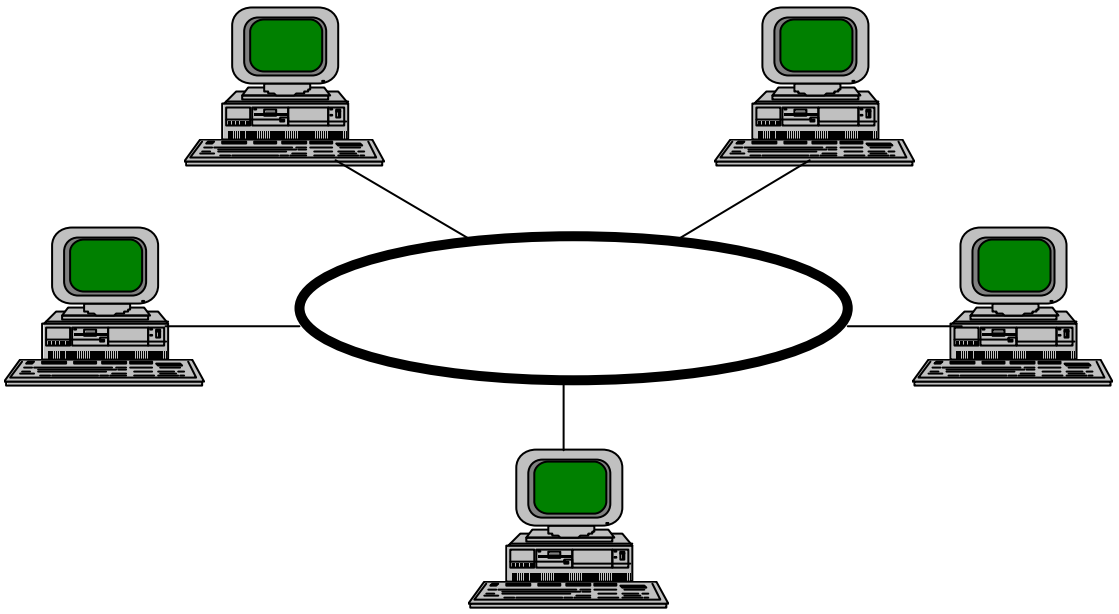
9.1.1.1 Topología en estrella

En una red con topología en estrella todos los puestos se conectan a un puesto central a través de líneas de transmisión individuales. Bajo esta topología, las comunicaciones no presentan ningún problema; sin embargo, tienen un grave inconveniente: si falla el nodo central de la red, que centraliza todas las comunicaciones, no funcionará nada en la red. La conexión de un ordenador central con sus terminales puede ser un buen ejemplo de red de comunicaciones con topología en estrella.



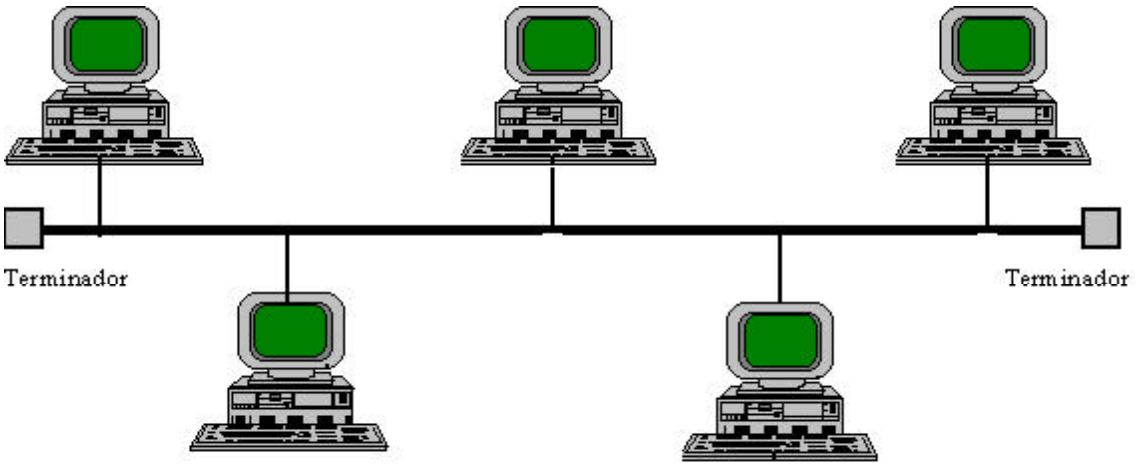
9.1.1.2 Topología en anillo

Una red en anillo conecta todos sus equipos en torno a un anillo físico. Tampoco presenta problemas de tráfico; sin embargo, una rotura del anillo produce el fallo general de la red. Un ejemplo concreto de red en anillo es la red *Token Ring*, que sigue el estándar IEEE 802.5.



9.1.1.3 Topología en bus

Los puestos de una red en bus se conectan a una única línea de transmisión (bus) que recorre la ubicación física de todos los ordenadores. Esta red es muy simple en su funcionamiento, sin embargo, es muy sensible a problemas de tráfico o a las roturas de los cables. Un ejemplo de red con topología en bus es *Ethernet* sobre cable coaxial. Sigue el estándar IEEE 802.3.



9.1.2 Los medios de transmisión

Los medios de transmisión utilizados en las redes de área local son múltiples y variados. En general, deben permitir altas velocidades de transferencia de datos y con tasas de error mínimas. Las características de estos medios de transmisión se pueden encontrar en la Unidad de Trabajo 2.

9.1.3 Funciones del nivel físico

El nivel físico define las características mecánicas, eléctricas, funcionales y de procedimiento necesarias para conseguir que las tramas de bits que la capa física recibe del nivel de enlace, su capa inmediatamente superior, puedan ser emitidas por los medios de transmisión adecuados en forma de señales.

Para ello la capa física utiliza una gran cantidad de recursos propios de las transmisiones de señales, que en gran parte ya hemos estudiado en anteriores unidades de trabajo. Esquematicemos un breve repaso:

- Los medios de transmisión de señal: cables de pares, cables coaxiales, fibras ópticas, transmisión vía satélite, etc.
- Transmisiones analógicas a través de líneas telefónicas utilizando módems con diferentes técnicas de modulación.
- Transmisiones digitales a través de redes digitales de transmisión de datos utilizando técnicas de modulación digital: impulsos codificados, modulación delta, etc.
- Técnicas de multiplexación en el tiempo y en la frecuencia.
- Técnicas de concentración de canales.
- Técnicas de conmutación: de circuitos, de mensajes y de paquetes (se verá en la Unidad de Trabajo 8).
- Transmisión en serie o en paralelo.
- Transmisión síncrona o asíncrona.

También hemos estudiado una buena parte de las normas de conexión en el nivel físico. Las exponemos brevemente:

- Conectores telefónicos de la serie RJ, especialmente el RJ-12.
- Norma EIA RS-232 y su equivalente CCITT V.24.
- Norma RS-449.
- Interface digital X.21, para líneas digitales.
- Otros conectores, como las T coaxiales o los conectores DB25.

9.2 El nivel de enlace

Como ya estudiamos en su momento, la capa de enlace asegura una conexión libre de errores entre dos ordenadores de la misma red. Fundamentalmente organiza los bits en forma de tramas y los pasa a la capa física para que sean transmitidos al receptor.

Cabe distinguir dos funciones en esta capa:

- Como en muchas redes de área local los canales están compartidos por muchos nodos, ¿cómo se puede saber que el canal está libre? Y si lo está, ¿cómo sabe un nodo si se puede o no apropiar de los recursos de la red?

- Puesto que los bits deben ser agrupados en tramas, ¿cómo confeccionarlas? Además, ¿cómo saber si las tramas recibidas son correctas?

Cada una de estas funciones da origen a una subcapa, la primera función es propia de la subcapa de control de acceso al medio o MAC *(Media Access Control),* la segunda lo es de la subcapa de control de enlace lógico LLC *(Logical Link Control),* aunque normalmente toma el nombre de la capa OSI que la incluye: enlace de datos o DLC *(Data Link Control).*

9.2.1 La subcapa MAC (Media Access Control)

La subcapa de control de acceso al medio es muy importante en las redes de área local, ya que la mayoría de ellas utiliza un canal común (canal de acceso múltiple) como base de sus comunicaciones, a diferencia de las redes de área extendida que suelen utilizar enlaces punto a punto.

La principal función de esta subcapa consiste en cómo determinar quién tiene derecho de acceso sobre ese canal compartido por todos los equipos conectados a la misma red. Se establecen cinco hipótesis posibles:

1. *Modelo de estación*. Este modelo consta de N estaciones independientes. Una vez que se ha generado la trama, la estación se bloquea hasta que no se haya transmitido con éxito. Esta hipótesis proporciona un modelo en el que las estaciones son independientes y en las que e1 trabajo se genera a un ritmo constante.

2. *Hipótesis de un solo canal*. En este caso se supone que hay un solo canal que utilizan todas las estaciones, aunque se les puede asignar prioridades a la hora de transmitir y dar así más peso a unas estaciones que a otras.

3. *Hipótesis de colisión*. Si dos estaciones transmiten sendas tramas simultáneamente en el mismo canal se producirá una colisión que provocará una interferencia de la señal. Todas las estaciones pueden detectar las colisiones habidas en el canal. Sí una trama ha colisionado con otra, ambas deben ser retransmitidas por las estaciones que las generaron.

4. *Tiempo continuo y ranurado*. En tiempo continuo, la transmisión de la trama puede comenzar en cualquier instante. No hay ningún organizador del tiempo de la red. En el caso de tiempo ranurado, el tiempo de la red se divide en intervalos o ranuras y las estaciones emplean las ranuras a las que tienen derecho para transmitir sus tramas.

5. *Detección de portadora*. En la detección de portadora cada estación puede escuchar en el canal si hay o no señal portadora. Si no la hay, podrá transmitir si así lo desea, en caso contrario deberá esperar hasta que se desocupe el canal. En el caso de que no haya detección de portadora, la estación que emite la trama sólo puede saber si el canal estaba libre una vez que la trama ha sido puesta en el canal.

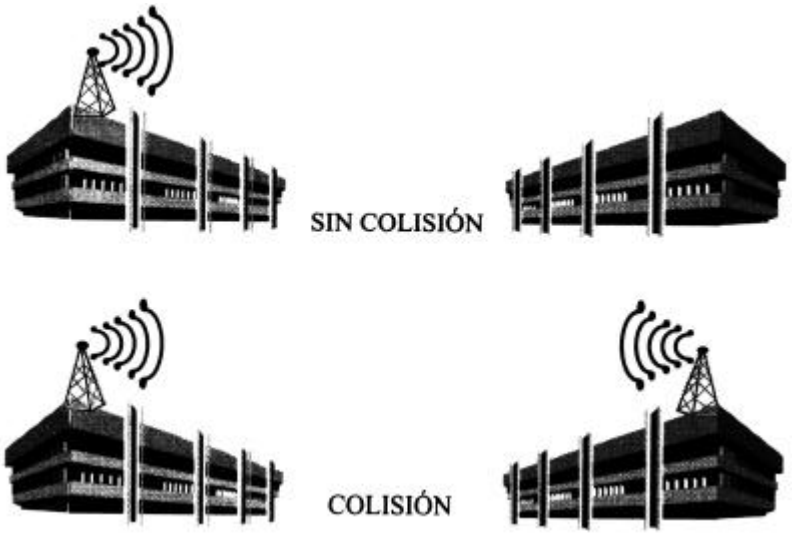
Distintas combinaciones de estas hipótesis proporcionan sistemas distintos de establecimiento de las características de acceso al medio de transmisión. Una vez elegida una solución concreta, se dice que se ha establecido un sistema de contienda. Vamos a estudiarlo con algunos ejemplos.

9.2.1.1 El protocolo Aloha

Aloha es un protocolo que nació en la década de los 70 para la difusión radioterrestre de varias fuentes de datos en la Universidad de Hawai.

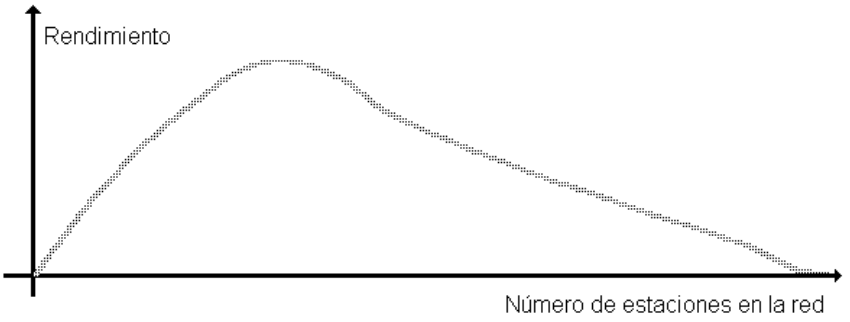
Con Aloha cualquier estación que tenga datos que transmitir lo hace inmediatamente y esto puede provocar colisiones con otras estaciones que también iniciaron la transmisión. Cuando se produce una colisión, la estación

la descubre simplemente escuchando el canal: si lo que escucha no es lo que ella puso, es que alguien más ha puesto señal y, por tanto, se ha producido una colisión.



En este caso las estaciones esperan un tiempo al azar y vuelven a intentar la transmisión de las tramas que colisionaron. De este modo se establece un sencillo sistema de contienda.

El rendimiento de este protocolo de capa 2 es muy bajo



y especialmente crítico cuando se incrementa el número de estaciones de la red, ya que aumenta en gran medida la probabilidad de colisión.

9.2.1.2 Protocolo CSMA p-persistente

Los protocolos CSMA *(Carrier Sense Multiple Access)* permiten el acceso múltiple a un único canal y averiguan si el canal está libre por detección en él de señal portadora.

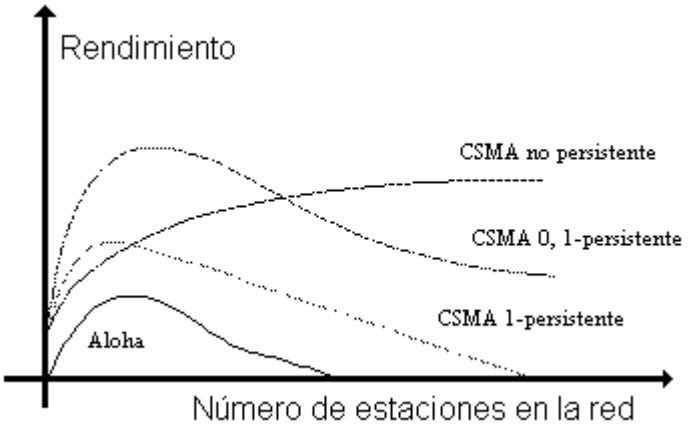
Los protocolos CSMA llevan asociado un índice de persistencia *p*, que es un número real comprendido entre 0 y 1 que indica una probabilidad de envío. Vamos a ver, de manera simplificada, cómo funciona un protocolo CSMA p-persistente.

Cuando una estación desea transmitir se pone a la escucha del canal para determinar si está libre o no. Si el canal está libre, puede efectuar la transmisión. En cambio, si está ocupado, deberá esperar a que se libere, lo que detectará automáticamente si permanece a la escucha. Cuando efectivamente se libere, la estación emitirá su trama con probabilidad *p*. Por ejemplo, si el protocolo fuera 1-persistente, enviará su trama inmediatamente.

¿Cuál es la razón de que algunos CSMA tengan índices de persistencia menores que la unidad? Para contestar a esta pregunta debemos fijarnos en que si dos estaciones estuvieran esperando la liberación del canal a la vez, con

un protocolo 1-persistente, las dos iniciarían su transmisión simultáneamente, puesto que ambas ven el canal libre a la vez, momento en que se produciría una colisión. Si la probabilidad de emisión no es 1 (suceso seguro probabilístico) sino que es menor, entonces la probabilidad de colisión también descenderá, puesto que será más improbable que ambas estaciones comiencen sus emisiones en el mismo momento.

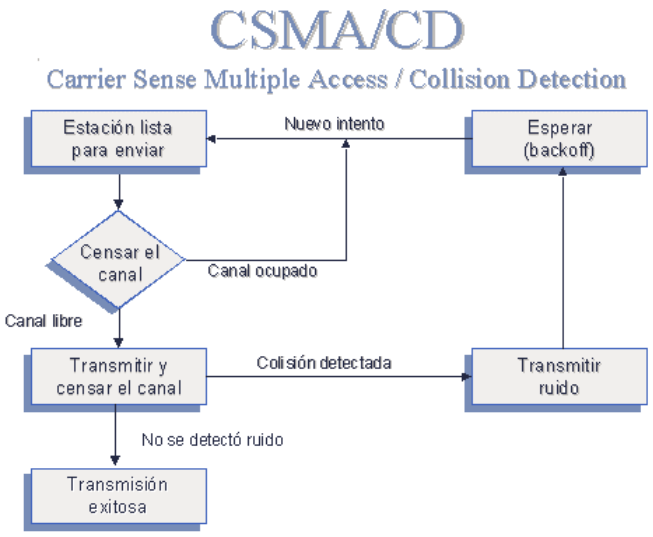
También existe un protocolo CSMA no persistente. Cuando la estación escucha el canal y está ocupado, deja de escucharlo y vuelve a intentar después de un tiempo aleatorio. De esta manera, si dos estaciones están a la escucha con el canal ocupado será más difícil que coincidan en leer el canal, ya libre, en el mismo instante de tiempo, pues es altamente probable que los retardos generados sean diferentes. Este método, por tanto, tiene una menor probabilidad de colisión.



9.2.1.3 El protocolo CSMA /CD

Los protocolos CSMA, tanto persistentes como no persis tentes, representan una mejora sustancial con respecto al protocolo Aloha. Además, se ocupan de disminuir el número de colisiones tanto como sea posible. Sin embargo, las colisiones son inevitables con las técnicas CSMA.

La técnica CD *(Collision Detect)* del protocolo CSMA implica que las estaciones permanezcan a la escucha mientras transmiten sus tramas. Si reconocen una colisión en el canal, es decir, lo que emiten no es lo que escuchan en el canal, entonces suspenden inmediatamente la transmisión: es inútil seguir enviando las tramas sabiendo que no se reconocerán en el destino. Con esto se ahorra tiempo y ancho de banda del canal.



En algunas redes las estaciones llegan incluso a transmitir una señal especial cuando detectan la colisión para advertir a todas las estaciones que se produjo una colisión en la red.

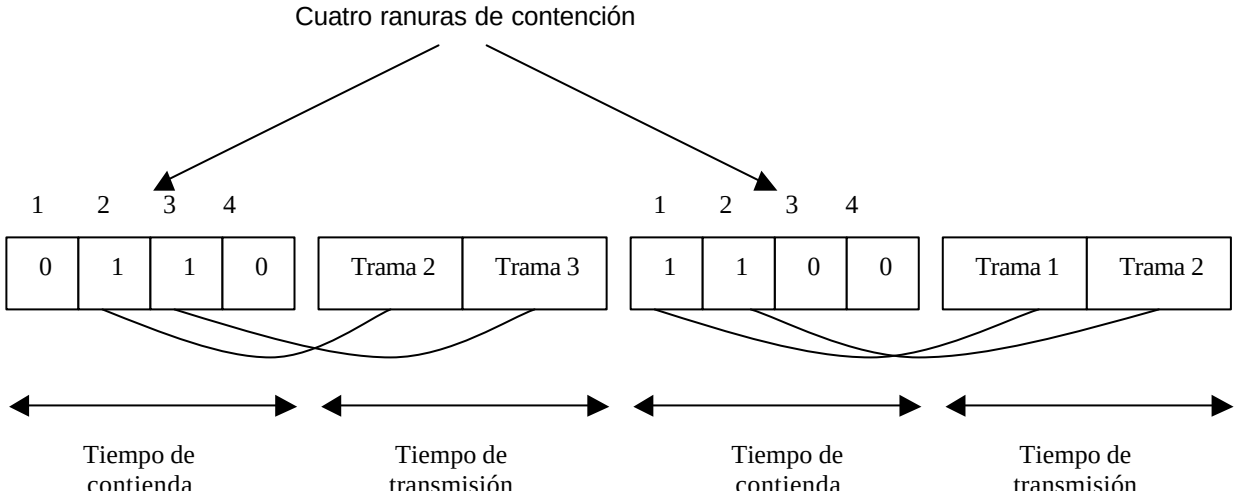
9.2.1.4 Protocolos sin colisión

Con el método CSMA/CD las colisiones se reducen al máximo. De hecho, una vez que una estación se ha apropiado del canal sin error será imposible que se produzca una colisión. Sin embargo, el problema no queda resuelto en el tiempo de contienda, es decir, cuando dos estaciones que desean transmitir esperan a que el canal se libere y vuelcan su información simultáneamente en el canal.

Es posible la creación de protocolos carentes de posibilidad de colisión. Aquí vamos a estudiar algún ejemplo. Imaginemos una red compuesta por cuatro ordenadores (el estudio es válido para cualquier otro número). Cada uno de ellos está identificado unívocamente por una dirección, aquí supondremos que esta dirección es un número; así, el primer ordenador llevará el número l, el segundo el 2, etc.

Para establecer la contienda, la red divide su tiempo de contienda en ranuras, una ranura de tiempo por cada estación conectada a la red, en nuestro caso cuatro. En la red habrá estaciones que necesiten transmitir y otras que no. Cada ranura se identifica con un número equivalente al de una estación. Así, a la estación *n* se le asocia la ranura *n*.

En la contienda, de duración cuatro ranuras, cada estación puede escribir en el canal durante el tiempo que dura la ranura que tiene asociada un bit 1, indicando así a la red que necesita transmitir, o bien un 0, para indicar que no necesita competir por los recursos de la red.



Una vez transcurrido el período de contienda se habrán rellenado los bits de contienda correspondientes a todas las estaciones de la red. Sólo necesitarán recursos de red aquellas estaciones cuyos representantes en las ranuras de contienda estén a 1. Inmediatamente después de la contienda, las estaciones enviarán sus tramas en el mismo orden en que aparecen los 1 en las ranuras de contención. Ninguna estación se adelantará a otra, pues todas siguen el mismo criterio.

Una vez que todas las estaciones que lo solicitaron han efectuado sus transmisiones, se genera un nuevo período ranurado de contienda y se vuelve a repetir el proceso. A esta tecnología que proporciona un acceso múltiple sin colisión se le llama método básico del mapa de bits.

Hay otros muchos protocolos sin colisión; de hecho, las redes en anillo también tienen protocolos sin colisión, pero su tecnología será estudiada más adelante.

9.2.2 La subcapa superior del nivel de enlace

La principal función de esta subcapa es garantizar, en colaboración con la subcapa MAC, la comunicación libre de errores de las tramas construidas con la información recibida del nivel de red, su inmediatamente superior.

9.2.2.1 Servicios de la capa de enlace

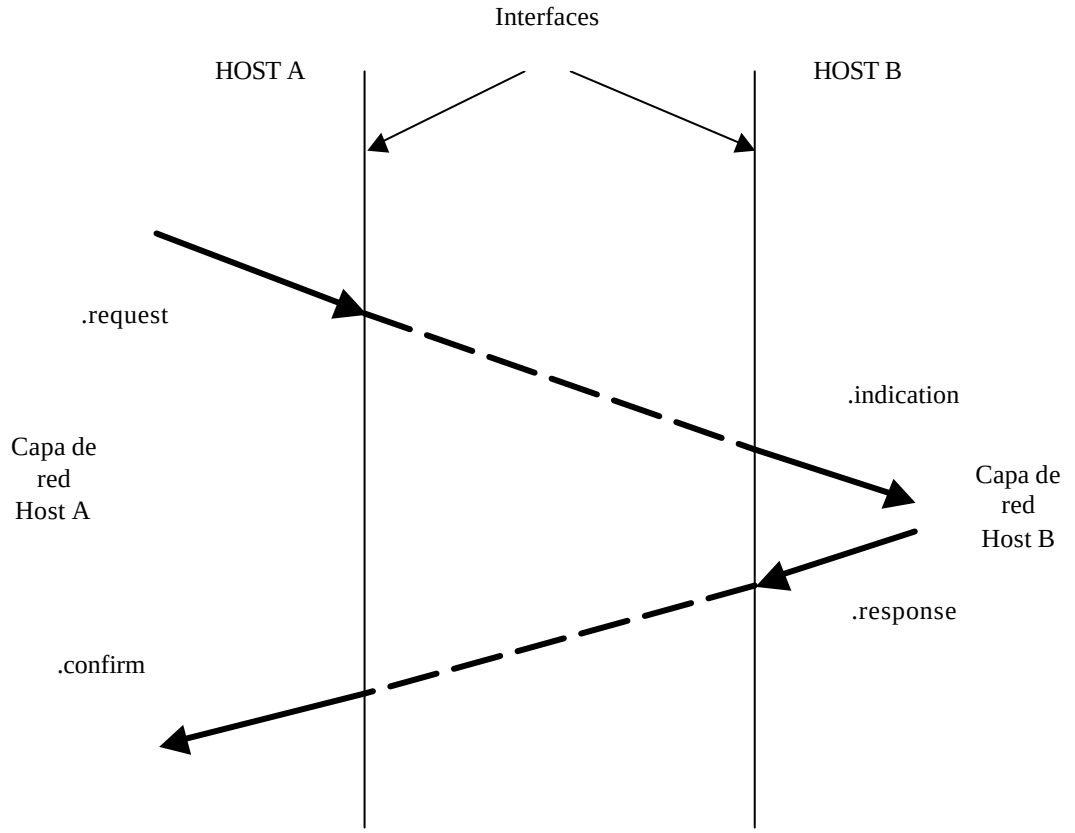
Provee tres tipos de servicios:

- **Servicio sin conexión** y **sin confirmación.** Envía tramas sin esperar confirmación del destino. Si se produce algún error, la responsabilidad de corregirlo estará en las capas superiores, puesto que este servicio no puede recuperar errores. Es un servicio propio de redes con una tasa de error muy baja y con aplicaciones en tiempo real, puesto que la comunicación es muy rápida.

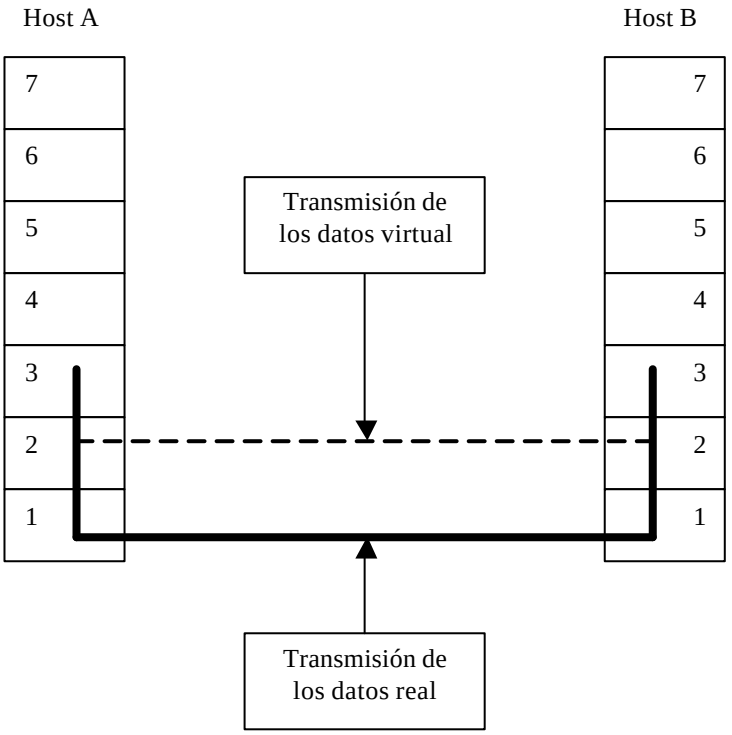
- **Servicio sin conexión** y **con confirmación.** No se establece conexión entre emisor y receptor pero por cada trama transmitida por el emisor se espera una trama de confirmación procedente del receptor. Si la confirmación no llegara en un tiempo determinado o se confirma que la transmisión fue errónea, se retransmite la trama.

- **Servicio con conexión.** Antes de producir el intercambio de tramas, que serán numeradas, se establece una conexión entre emisor y receptor. La red se ocupará de que las tramas lleguen en el mismo orden en que fueron enviadas.

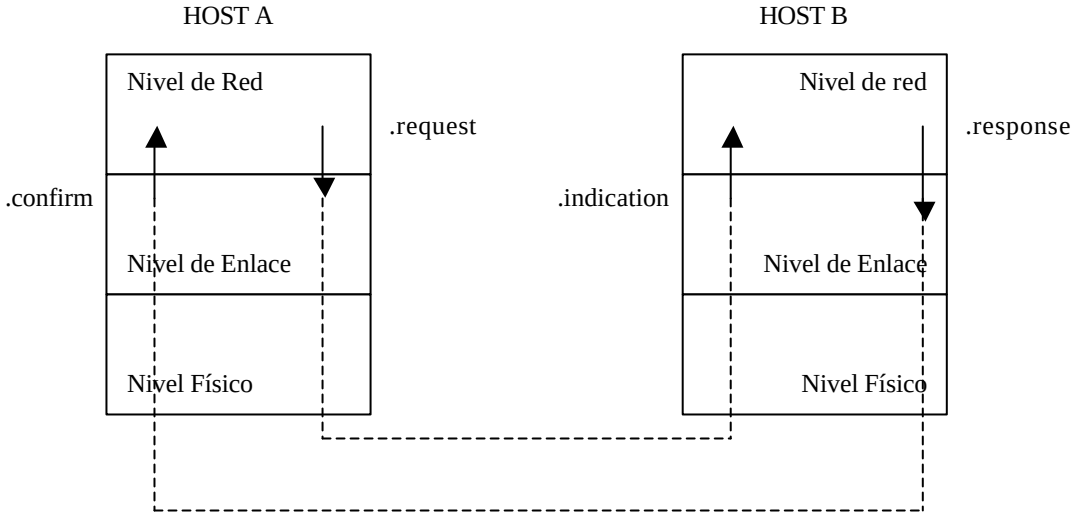
Como en todas las demás capas, los servicios son invocados a través de primitivas, algunas de las cuales se resuelven en la jerarquía del emisor (petición y confirmación) y otras en el receptor (indicación y respuesta) como aparecen en el siguiente gráfico.



Así, la capa de red (nivel 3) solicita servicios a la capa de enlace (nivel 2). La capa 3 cree que la comunicación se opera en la capa 2 (protocolo virtual de nivel 2). Se puede ver claramente en la figura siguiente.



Aunque lo que realmente hace la capa 2 es solicitar servicios de transmisión de señal a la capa física (nivel 1), de modo que las primitivas de servicio se invocan así:



9.2.3 Confección de las tramas

Las unidades de datos (PDU) de nivel 2 se llaman **tramas**. La capa de enlace debe proporcionar un flujo de bits a la capa física para que ésta los transmita una vez convertidos en las señales adecuadas al canal de transmisión. Cada una de las tramas constituye una asociación de bits, tanto de información de usuario como de control. Las técnicas de asociación por la que los bits se agrupan formando tramas se llaman técnicas de entramado o ***framing***.

La primera función de entramado de la capa DLC (*Data Link Control*; Control de Enlace de Datos) o de enlace es delimitar perfectamente dónde comienzan y acaban las tramas, es decir, cómo sabe el receptor cuáles son las

fronteras de las tramas. En segundo lugar, habrá que averiguar si se produjeron errores en la transmisión de los bits. Para delimitar las tramas se pueden emplear diversos métodos, los más comunes son los siguientes:

1. ***Cómputo de caracteres transmitidos según un código de transmisión***. Para ello, cada trama incorpora un campo inicial en donde se escribe el número de caracteres que componen la trama, es decir, su longitud, permitiéndose, por tanto, tramas de longitud variable. El receptor, al leer la información, lee primero el campo de longitud de trama y así averigua cuántos caracteres vienen detrás. Los siguientes caracteres pertenecerán al campo de longitud de una nueva trama.

2. ***Técnica de inserción de carácter y caracteres delimitadores***. Cada trama comienza y termina con un carácter o conjunto de caracteres especiales, normalmente los caracteres ASCII <DLE><STX>[1] para el inicio y <DLE><ETX>[2] para el final. Cuando la información contenida en la trama posee algún carácter <DLE>, éste se puede confundir con un inicio de trama. Para evitarlo se escribe <DLE> <DLE>, es decir, se inserta un carácter <DLE> que indica al intérprete de la comunicación que el siguiente carácter es informativo, no de control. A esta técnica se le llama de inserción de carácter o ***character stuffing***. Éste es el método empleado por la sincronización de bloque ya estudiada en la Unidad de Trabajo 1.

3. ***Técnica de inserción de bit y banderas delimitadoras***. Las banderas o *flags* son secuencias de bits a modo de patrones que delimitan las tramas. Una bandera muy común es la secuencia «01111110». Con ella se quiere significar que cuando lleguen seis unos seguidos, y sólo seis (delimitados por sendos ceros), llega el final o el inicio de una trama. Pero, ¿qué sucederá cuando la información de la trama tenga también seis unos seguidos en estas mismas condiciones? El código empleado utiliza una técnica de inserción de bit o ***bit stuffing***, que inserta un «0» después del quinto bit a 1. Esto tendrá que tenerse en cuenta en el receptor con el fin de restablecer la información original. El receptor determinará un comienzo o final de trama cuando lea en la línea de datos seis unos seguidos: tiene la seguridad de que el contenido de la trama nunca tendrá más de cinco unos seguidos.

4. ***Alteraciones del código en la capa física***. En esta técnica, los delimitadores de comienzo y final de trama consisten en enviar una secuencia de señales -nivel físico- que no pertenecen al código de emisión. Por ejemplo, es común en algunas redes de área local, que los «1» se señalicen como la transición de tensión alta a tensión baja y los «0» a la inversa. Un buen código delimitador consistiría en que durante todo el tiempo que dura el bit la tensión permaneciera alta o baja, es decir, sin transiciones: no se codificaría ni un 0 ni un 1, por tanto, nos saldríamos del código permitido.

9.2.4 Control de errores

Lo normal en las redes de área local es enviar al emisor alguna información de retroalimentación *o feedback* en donde se especifique el estado en que llegó la trama.

Si un protocolo de comunicaciones tiene prevista la recepción de una trama de confirmación y no llega, podría suspender la emisión de nuevas tramas por tiempo indefinido. Esto sucedería si se produjera, por ejemplo, la ruptura del enlace de la línea de datos, si se pierde la confirmación, si el receptor no está en línea, etc.

Para estos casos está previsto un *sistema de temporizadores*. Cuando el emisor envía una trama, dispara un temporizador. Si cuando caduca el temporizador no se ha recibido la confirmación, entonces se entiende que la trama pudo no llegar o llegar mal al destino y se procede a la retransmisión.

Si lo que se perdió fue la confirmación, entonces hay posibilidades de que el receptor reciba varias veces la misma trama, puesto que el emisor la transmitirá por segunda vez al observar que su temporizador ha caducado sin haber obtenido una confirmación. Para poder gestionar esta multiplicidad de la misma trama se numeraran las tramas en el emisor. De este modo, el receptor las identificará como copias de la misma información y no almacenará información redundante, filtrará las duplicidades y así se harán imperceptibles a las capas superiores.

[1] El carácter ASCII <DEL> significa *Data Link Escape* y el <STX> *Start of Text*.
[2] El carácter ASCII <ETX> significa *End of Text*.

9.2.5 Control de flujo

El control de flujo es la solución más simple al problema que se genera cuando las velocidades de transmisión o de aceptación de datos del emisor y del receptor son diferentes. Con un buen control de flujo se puede regular la cadencia con la que se envían las tramas en la red, dependiendo de quiénes sean el emisor y el receptor. Es un sistema, por tanto, que regula el tráfico de la red.

Normalmente, las técnicas de control de flujo necesitan información de feedback intercambiable entre emisor y receptor. Lo más común es que no se transmitan tramas al receptor hasta que éste no haya dado su permiso para que le sean transmitidas, y, cuando lo hace, expresa cuántas tramas está dispuesto a recibir hasta que se conceda un nuevo permiso.

9.2.6 Gestión del enlace de datos

Cuando se tienen dos ordenadores unidos por una línea punto a punto, la gestión del enlace es muy simple: hay un emisor y un receptor, y, en el mejor de los casos, pueden intercambiar sus papeles (semidúplex o dúplex).

El problema se complica cuando se tienen múltiples ordenadores que comparten el canal, especialmente en el caso de que los servicios estén orientados a la conexión puesto que habrá que gestionar quién, cuándo, cómo y con quién.

Algunos sistemas de gestión de enlace requieren la definición de una estación primera que lleve el peso de la gestión, haciendo que el resto sean secundarias. Se crea un sistema de sondeo o *polling* por el que la estación primaria pregunta a las secundarias por sus necesidades de transmisión, estableciendo de este modo un mecanismo de permisos para gestionar la utilización del enlace.

Hay sistemas en que se permite que las estaciones secundarias transmitan a la estación primaria sin necesidad de permiso: es responsabilidad de la red la gestión de los problemas que se pudieran ocasionar.

En las redes de área local, lo más común es que todas las estaciones sean iguales desde el punto de vista de la funcionalidad en el nivel de enlace, es decir, todos los nodos de la red tienen los mismos derechos de transmisión, estableciéndose la competición en los términos de los sistemas de contienda que se han estudiado anteriormente.

9.2.7 Protocolos de la capa de enlace

El número de los protocolos de la capa de enlace es enorme y además crece continuamente. La Unidad de Trabajo 4 se ocupará con detenimiento de los más utilizados. Aquí haremos una mención de los más importantes para que sirvan como referencia.

En las redes públicas se suele utilizar el protocolo HDLC y todos sus derivados: SDLC, LAPB, LAPM, LAPX, etc.

Otro protocolo de capa 2 es el LLC, utilizado en las redes que siguen la norma IEEE 802 en sus múltiples variantes. Este protocolo está íntimamente ligado al HDLC de OSI.

En la jerarquía de protocolos de ARPANET no existe un auténtico protocolo de capa de enlace (ya estudiamos que ARPANET no tenía la arquitectura OSI), pero el protocolo más cercano equivalente es el de su capa de red. Se trata del IMP-IMP. Las redes ARPANET suelen utilizar protocolos de capa 2 tomadas de otras arquitecturas, por ejemplo, LLC, LAPB, etc.

9.3 Las capas de red y de transporte

Evidentemente existen protocolos en éstas capas que se utilizan en las redes de área local, pero su misión principal es intercomunicar ordenadores distantes o la interacción entre ordenadores de distintas redes locales.

Esta es la razón por la que explicaremos aquí brevemente la funcionalidad de la capa, dejando para más adelante un estudio más profundo.

Fundamentalmente, en la capa de red se operan las funciones de las subredes, es decir, aquello que hace transparente la tecnología de la red al resto de los servicios de alto nivel. Por ejemplo, en la transmisión remota de fichero la operación de red para el usuario es independiente de la constitución física de la red e, incluso, del formato de las tramas utilizadas.

También puede ofrecer servicios con conexión, llamados circuitos virtuales, o sin conexión, llamados datagramas. Unos y otros serán estudiados en la Unidad de Trabajo 8. Las unidades de datos PDU de esta capa se llama paquetes. Fundamentalmente proporciona un modo nombrar los nodos -realmente, los IMP *(Interface Message Processor) y* los hosts (nodos que poseen función de la capa de transporte)- para su uso desde la capa de transporte. Un IMP es un dispositivo lógico o físico que actúa de intercomunicador; por ejemplo, se encarga de la conmutación o de la distribución de paquetes. Cada IMP lleva una dirección que le identifica unívocamente en la red.

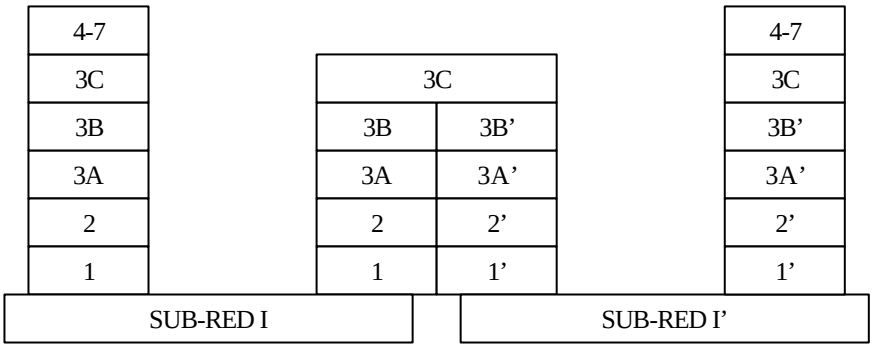
Lo que es el IMP en el nivel de red lo representa el host en la capa de transporte. Un host puede tener más de un IMP, por ejemplo, se pueden asociar a un host varias direcciones: el ordenador es el mismo, pero puede tener asociadas varias redes o varias direcciones dentro de la misma red.

Entre los procedimientos asociados a las funciones de la capa de red vamos a destacar los siguientes:

- **Encaminamiento**. Es la verdadera función de la capa de red. Se encarga de que los paquetes lleguen a s destino eligiendo la ruta apropiada.

- **Tratamiento de la congestión**. Se encarga de detectar, diagnosticar y, en lo posible, corregir los problemas generados por sobrecarga de paquetes en la red.

- ***Internetworking* o interconexión entre redes**. Trata de resolver el problema creado cuando emisor y receptor no están en la misma red. Un cambio de red puede suponer algo tan sencillo como dar un paso intermedio más en la transferencia de la información o algo tan complejo como un cambio en el formato de las tramas o en los protocolos de comunicación. En algunos servicios la interconexión se hace imposible.



Sobre los algoritmos y la maquinaria de red apropiada para llevar a cabo estas funciones trataremos en la Unidad de Trabajo 9.

Algunos de los protocolos utilizados en las redes de área local para la capa de red son los siguientes:

- Redes públicas: X.25 (se estudiará en la Unidad de Trabajo 8).

- Red ARPANET: el protocolo por excelencia es IP (Internet Protocol), al que ya nos hemos referido anteriormente.

La capa de transporte es el núcleo de la jerarquía de capas. Su misión es garantizar la seguridad y proveer un transporte de datos a un coste efectivo independiente de la red en uso. En la tabla siguiente se muestran las características de diseño para los servicios OSI en la capa de red.

CARACTERÍSTICAS DE DISEÑO	ORIENTADOS A LA CONEXIÓN	SIN CONEXIÓN
Setup inicial	Requerido	No es posible
Dirección de destino	Sólo necesario en el setup	Se necesita en cada paquete
Secuenciamiento de paquetes	Garantizado	No garantizado
Control de errores	Por la capa de red	Por la capa de transporte
Control de flujo	Provisto por la capa de red	No provisto por la capa de red
¿Cabe negociación opcional?	Sí	No
¿Identificadores de conexión?	Sí	No

Puesto que los usuarios (capas superiores) no tienen el control de la subnet (capas 1, 2 y 3), no tienen otra forma de corregir los problemas de falta de calidad en el servicio que habilitar una capa intermedia (la de transporte) que se encargue de esta función.

Por ejemplo, nos puede interesar la transmisión de un fichero de datos de gran volumen, sólo si la red nos proporciona una velocidad por encima de un mínimo, se efectuará o no la conexión en función de una serie de parámetros que regulan la calidad del servicio ofrecido por la red.

Algunos de estos parámetros son el retraso en el establecimiento de la conexión, la probabilidad de fallo en la conexión, el nivel de flujo de datos, la probabilidad de fallo en las transferencias de datos, etc. Al producirse la conexión se establece una negociación de estos parámetros en los que el host (entidad de capa 4) origen y el host destino determinan qué posibilidades de comunicación tienen. Por ejemplo, se podría negociar que si la calidad de la línea baja por debajo de un mínimo se rompa la conexión y se establezca de nuevo (reset de capa 4).

OSI ha aconsejado un protocolo de transporte con cinco variantes o clases dependiendo de: su seguridad, si una sola sesión de red puede o no soportar varias conexiones de transporte, si la conexión se puede o no recuperar de un reset, etc.

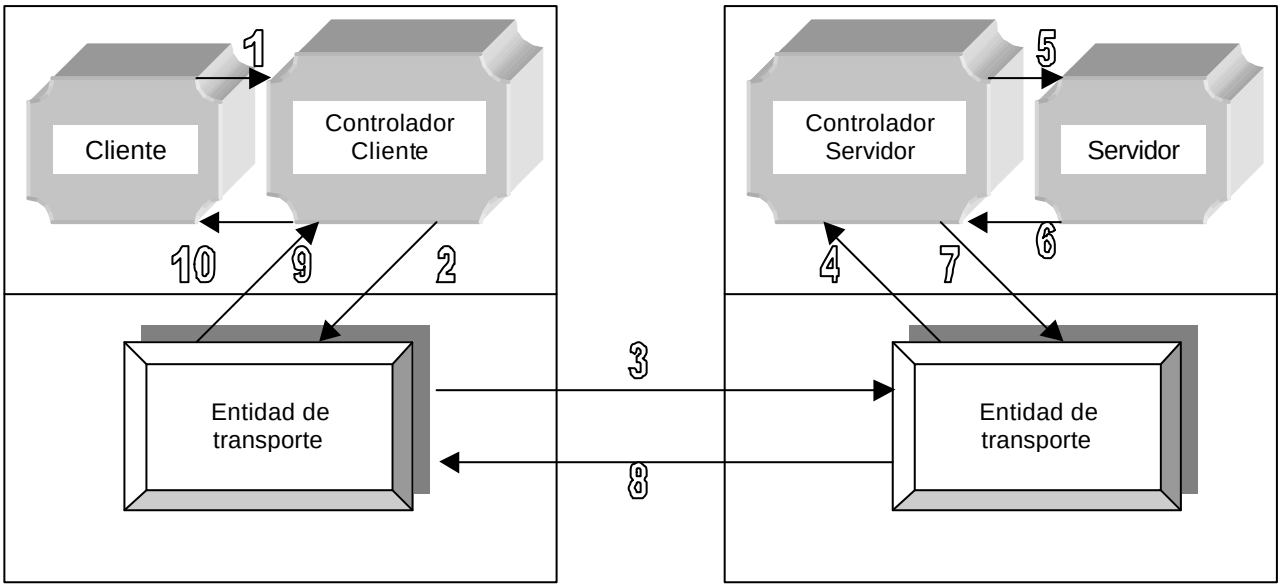
El protocolo más utilizado *de facto* equivalente en OSI a la capa 4 es TCP (Transmission Control Protocol), proporcionado por la red ARPANET.

9.4 Los niveles orientados al usuario

Hasta ahora hemos estudiado las características más importantes de la arquitectura de los protocolos más utilizados en las redes de área local: hemos llegado al nivel de confección de tramas, regulación de la velocidad, transmisiones libres de errores, métodos de acceso al canal, etc.

Pero sabemos que estas funciones deben ser invocadas por entidades de orden superior a la 2. En efecto, cuando deseamos transmitir un fichero de un ordenador a otro, sabemos que en último extremo aquel fichero será convertido de alguna manera en un conjunto de señales que se transmitirán por una o varias líneas de comunicación. Estas peticiones de servicios a la red, que simplifican la tarea de los usuarios, son los protocolos de alto nivel.

En la capa de sesión aparecen protocolos tan utilizados como el RPC *(Remote Procedure Call)*. Éste es un protocolo orientado a la ejecución remota de tareas, ampliamente extendido en aplicaciones cliente servidor y en accesos a bases de datos distribuidas.



En la capa de presentación, OSI propone la resolución de la representación de los datos, la compresión de los mismos, la seguridad y privacidad en la red, etc. La ISO ha desarrollado como parte de OSI un lenguaje de representación, codificación y transmisión de estructuras de datos para una amplia variedad de aplicaciones. Este lenguaje se llama ASN.1 *(Abstract Syntax Notation 1)* y sus reglas de codificación vienen dadas por el estándar 882.5.

Los tipos de datos que ASN.1 puede codificar son los siguientes: *integer, boolean, bit stream, octet stream, any, null y object identifier*. Se puede ver que casi todos son tipos de datos comunes para ser manejados desde los lenguajes de programación.

La expansión de Internet ha hecho que se desarrolle rápidamente los protocolos de compresión y de encriptación de datos propios de las funciones de esta capa de presentación. Algunos de ellos serán estudiados cuando tratemos de Internet.

La capa de aplicación es la más próxima al usuario por tanto, sus servicios tendrán que ver con las aplicaciones que ejecuta sobre el sistema operativo. Así, servicios comunes que puede proporcionar son la transferencia, acceso y manipulación de ficheros (protocolo FTP), correo electrónico con o sin confirmación, conexiones de terminales virtuales y otros simuladores, servicios de directorio electrónico (equivalentes a las páginas amarilla de los servicios telefónicos), ejecución remota de trabajos, etc.

Los protocolos utilizados en la capa de aplicación se han multiplicado extraordinariamente, porque son muy dependientes de los fabricantes de software; sin embargo actualmente se observa un esfuerzo considerable por parte de estos fabricantes para hacer compatibles sus productos, especialmente a partir de la extensión masiva de las redes de área extendida, que interconectan equipos de características muy diversas.

10 Tema 5: Arquitectura de Windows 9x en Red. Controladores

Cliente: conjunto de funciones que permite al sistema operativo interpretar la organización de un determinado sistema de red. P.ej. el de la Novell (p.ej. Netware), de la red Microsoft, etc.

Adaptador: es el driver de la tarjeta de red.

Protocolos: definen la forma que tienen los paquetes de información que generan los programas relacionados con la red. También se puede definir como las normas a seguir en una cierta comunicación; esto es, el formato de los datos que debe enviar el emisor, como deben ser las respuestas del receptor, etc. Por supuesto, para que dos ordenadores puedan comunicarse deben tener instalado el mismo protocolo.

Servicios: Permiten realizar operaciones en la red.

10.15.1. Modelo de referencia OSI y arquitectura de Windows 9x

La arquitectura modular de la red de Windows 95 está basada en dos modelos estándares de la industria: El modelo de la Organización Internacional de Estandarización (ISO) denominado modelo de Referencia de Sistemas Abiertos Interconectados (OSI: *Open System Inerconect*), y el 802 del IEEE.

Ambos modelos definen las características que debe poseer un sistema de red, distribuyendo todos los componentes de la misma en capas interrelacionadas y perfectamente definidas. Se contemplan desde los programas que maneja el usuario, hasta el cableado que une los adaptadores y elementos de la red.

En la práctica, no se encuentran implementados en ningún sistema, pero se utiliza como medida del grado de compatibilidad entre dos sistemas de red diferentes. El modelo de referencia OSI define 7 niveles o capas. Los más inferiores son los más cercanos a la máquina:

7. Capa de aplicación: representa el nivel en el que se encuentran las aplicaciones que acceden a los servicios de red. El usuario maneja estas aplicaciones en esta capa cuando trabaja con programas clientes de correo electrónico, acceso a datos de otros equipos, etc.

6. Capa de presentación: en este nivel el sistema operativo traduce la información que el usuario generó en el nivel anterior. Se encripta la información (si fuese necesario) o se comprime, con el objetivo de disminuir el tráfico de la red y de la forma más fiable.

5. Capa de sesión: permite a dos aplicaciones de diferentes ordenadores establecer, usar y terminar una comunicación. A este nivel se establece el diálogo de control entre dos ordenadores regulando cuál transmite, cuándo y cuánto.

4. Capa de transporte: Maneja los errores de reconocimiento y la recuperación. También empaqueta grandes mensajes cuando es necesario transmitirlos en pequeños paquetes o reconstruye los originales en el lado de la recepción. También envía reconocimiento de la recepción.

3. Capa de red: Dirige mensajes y traduce traducciones lógicas, y nombres de direcciones físicas. También determina la ruta desde el origen al destino, y gestiona problemas de tráfico como conmutar, encaminar y controlar la congestión de paquetes de datos.

2. Capa de enlace. Aquí se empaquetan en bruto los bits de la capa física en tramas (paquetes de datos estructurados y lógicos) Es la responsable de transferir tramas de una computadora a otra sin errores. Después de enviar una trama se espera una expresión de reconocimiento del ordenador receptor.

1. Capa física. Transmite bits de un ordenador a otro, y regula la transmisión de cadenas de bits sobre el medio físico. En esta capa se define cómo se une el cable al adaptador de red, y qué técnica de transmisión se emplea para enviar datos por el cable.

La Red Windows 9x funciona a los siguientes niveles:

7. aplicación

6. Proveedores de red

5. Administradores IFS

4. Redirector red Microsoft/compatible NetWare

3. Protocolo de transporte

2. NDIS.YXD

1. Controlador de la tarjeta de red

NIC (tarjeta de red)

10.25.2. Reexpedidores y Administradores IFS

Un reexpedidor proporciona los mecanismos para localizar, abrir, leer, escribir y borrar archivos; así como mandar trabajos de impresión. También permite localizar y manejar servicios como buzones. Cuando un ordenador necesita comunicar con otro, hace una llamada a un reexpedidor y éste proporciona los servicios necesarios.

Los reexpedidores se sitúan en las capas de aplicación y presentación del modelo OSI.

En Windows 9x, se encuentran implementados en los controladores siguientes:

- VREDIR.VXD: Para redes Microsoft.
- MWREDIR.VXD: Para redes Novell NetWare.

Aunque también se pueden instalar otros reexpedidores.

Los reexpedidores se contemplan como si fueran sistemas de archivos, de forma que a través de un elemento administrador (el IFS) se manejan de forma similar al de un sistema como FAT.

El Administrador IFS (*Instalable File System*) es el administrador de sistemas de archivo instalables. El reexpedidor intercambia información con el IFS para asignar nombres locales a recursos de red y decidir si se necesita acceder a un dispositivo local o remoto.

El IFS se encarga de tramitar todas las transferencias de E/S (entrada-salida) sobre cualquier sistema de archivos (unidades locales o reexpedidores).

En el caso de que se utilice una comunicación con otro sistema Microsoft, la petición se presenta en un paquete de datos SMB (*Session Message Block*), conocido también como NetBIOS, y se envía éste al driver para que le añada la información de control pertinente. Si se utiliza NetWare, el paquete se prepara en formato NCP (*Netware Comunnication Packet*). El protocolo reencamina el paquete para su transmisión al control del adaptador de red. Cuando Windows 9x actúa como servidor utiliza los servicios que proporcionan los controladores VSERVER.VXD para redes Microsoft y NWSERVER.VXD para redes Novell.

jueves 15 de julio de 1999

10.35.3. Soportes para distintos tipos de red

La interface del suministrador modular de Windows 9x le permite mantener conexiones simultáneas con recursos provenientes de distintos tipos de red. Es posible mantener una comunicación con otro equipo que trabaje sobre Windows mientras se utiliza un recurso de una red NT o Netware, y a la vez se transfiere información a través de Internet.

Entre los clientes de red incluidos en Windows 9x tenemos ArtiSoft Lantastic, Banyan Vines, Novell NetWork, SunSoft, PC-NFS, etc. Los componentes de red que permiten el uso de estos clientes son el API (*Aplication Programming Interface*), y la interface Win32/WinNet, el Encaminador de Proveedor Múltiple y los Proveedores de Red.

10.3.1 5.3.1. Interface Win32/WinNet para aplicaciones

Permite a los desarrolladores crear aplicaciones con independencia del tipo de red que exista. Es una ampliación de WinNet 36, utilizada hasta Windows 3.11.

10.3.2 5.3.2. Encaminador de Proveedor Múltiple

Se encarga de encaminar las peticiones de red entrantes hacia el proveedor de adecuado, de forma que se utiliza el mismo interface independientemente del número de suministradores de red que existan.

Las características comunes a todas las redes son implementadas una sola vez en el encaminador, asegurando un comportamiento común para todas.

El encaminador se comunica con los suministradores de red mediante la interface del suministrador de servicio, el cual se encarga de realizar las funciones de peticiones de servicios de red, examinación de servidores, etc.

10.3.3 5.3.3. Proveedores de red

Windows 9x utiliza un suministrador de red modular y abierto que permite múltiples conexiones de red distintas, siendo posible admitir una red de cualquier fabricante mientras se trabaja con recursos y elementos de Windows 9x. Las aplicaciones de usuario realizan peticiones a los proveedores de red, y Windows 9x pasa la petición al proveedor específico.

Viernes 16 de julio de 1999

Los proveedores de red que incluye Windows 9x son:

- MSNP32.DLL para redes Microsoft.
- MWNP32.DLL para redes Netware.
- WINNET16.DLL para suministradores de red de 16 bits.

Además, soporta cualquier proveedor de red de 32 bits suministrado por otro fabricante.

Cada proveedor puede tener su propio cuadro de dialogo, según su modelo de seguridad, y después de conseguir el acceso, el proveedor devuelve el control a Windows.

Cuando el usuario hace doble clic en el icono de red:

1. La interface de usuario de Windows 9x llama al API de red Win32 para enumerar los recursos de red.
2. El Encaminador Suministrador Múltiple, recibe la llamada API, y llama a todos los suministradores de red disponibles.
3. Cada suministrador de red examina sus redes y devuelve la lista a Windows 9x.

El Suministrador de Red de Windows 9x permite conectarse a un recurso de red siguiendo la sintaxis de la red correspondiente. A la hora de indicar el nombre del recurso, en redes Microsoft se utiliza el formato UNC. En las redes Netware la sintaxis es : <Nombre del servidor> /<Nombre del recurso>. Por ejemplo, Pc12/d:\Carpetas.

- Proveedor de red para redes Netware: El proveedor que admite redes Netware proporciona acceso a los recursos de redes Netware a través de las herramientas habituales de Windows. El suministrador permite examinado de redes Netware, acceder y salir de la red, agregar y quitar conexiones, tanto a discos como a impresoras.
- Proveedor de red para redes Microsoft: El proveedor de red para redes Microsoft proporciona acceso a recursos de redes Microsoft a través de las distintas utilidades de Windows. El suministrador de red permite opciones como Examinado de Redes Microsoft, Examinar y Salir de Windows NT o dominios LAN Manager, agregar o quitar conexiones a unidades e impresoras.
- La interface WinNet16: Es el conjunto de API´s utilizadas en Windows 3.x para conectarse a una unidad o impresora de red, y es simplemente una copia de la versión existente en Windows 3.1 del programa o fichero WINNET16.DLL.

Martes, 20 de julio de 1999

10.45.4. Interfaces de dispositivos de red

Hasta hace poco, sobre un adaptador de red sólo se podía montar un único protocolo. Se denominaban arquitecturas de tipo monolítico. Esto quiere decir que para conectar un equipo simultáneamente a una red Novell y a una red de Microsoft, era necesario dotarle de dos tarjetas, una por cada tipo de red.

Con el fin de permitir que sobre una tarjeta se pudiese montar más de un protocolo surgieron dos especificaciones:

- ODI: *Open Device Interface* de Novell.

- NEDIS: *Network Device Interface Specification* de Microsoft.

En Windows 9x, tanto la tarjeta de red como cada uno de los protocolos que se montan sobre ella deben de admitir la especificación NEDIS. Así, entre los controladores que acompañan a las tarjetas en los disketes, se incluyen los que soportan tanto NEDIS como ODI.

Los adaptadores NEDIS 3.1, se gestionan a través de un controlador que se divide en dos partes. La primera es un mini-controlador que realiza detalles como el establecimiento de comunicaciones con el adaptador, el apagado o encendido del aislamiento eléctrico para dispositivo P&P y la activación de cualquier propiedad añadida que tenga el adaptador. La segunda es una envoltura que implementa las funciones NDIS.

10.55 5.5. Arquitectura para protocolos

Windows 9x incluye soporte para protocolos IPX/SPX, NetBeui y TCP/IP. NetBIOS no es un protocolo, es como una capa entre los protocolos y las aplicaciones. Permite conectarse a la red utilizando nombres sencillos, sin importar el protocolo que se esté utilizando.

10.5.1 5.5.1. Protocolo para IPX/SPX

El driver encargado de dar soporte IPX/SPX es el NWNBLINK.VXD, el cual permite NetBIOS sobre IPX, además de permitir la interface de programación NetBIOS. El protocolo compatible IPX/SPX es compatible NEDIS 3.1. De esta forma, permite comunicarse con servidores Novell-Netware configurados como encaminadores para transferir paquetes sobre una LAN y acceder incluso a otros equipos como Windows 9x.

Este es el protocolo más adecuado para una red pequeña que no se conecte a Internet. Por supuesto, debe tener NetBIOS por encima de él. Como desventaja, en este protocolo no pueden redireccionar subredes.

10.5.2 5.5.2. Protocolo NetBeui

El módulo NETBEUI.VXD implementa el protocolo de tramas NetBIOS. Es un protocolo de Microsoft. Puede ser utilizado por cuestiones de compatibilidad con sistemas antiguos, aunque en general es conflictivo, por lo que no es aconsejable en una red con más de diez equipos, por ejemplo.

10.5.3 5.5.3. Protocolo TCP/IP

El protocolo TCP/IP se encuentra en el módulo VTCP.VXD, que es accesible a través de la interface de conexiones lógicas de red de Windows, o a través de la interface NetBIOS.

El problema es que la información no está codificada, por lo que la seguridad no es la mejor. Para ello se ha desarrollado el protocolo Punto a Punto Apantallado PPTP. También es más difícil de configurar.

10.66 5.6. Arquitectura para clientes de redes

Tanto el cliente de redes Microsoft como el de Netware pueden ser instalados en modo protegido de 32 bits.

10.6.1 5.6.1. Cliente para la arquitectura de redes Microsoft

Para poder utilizar todos los productos de red de Microsoft que empleen el protocolo de compartición de archivos NetBIOS, Windows 9x proporciona un controlador en modo protegido de 32 bits. Esto incluye LAN Manager, IBM LAN Server y 3Com 3+Open. El cliente de redes Microsoft permite la conexión sobre cualquier protocolo NEDIS que admita la interface NetBIOS.

Los protocolos en Modo Protegido de Windows 9x que admiten la interface NetBIOS son los siguientes:

- NetBeui mediante el controlador NETBEUI.VXD.
- NetBIOS sobre TCP/IP con los controladores VTCP.VXD y VIP.VXD
- NetBIOS sobre IPX-SPX con el NWBLINK.VXD y el NWLINK3.VXD

El cliente de redes Microsoft también permite la conexión sobre IPX/SPX mediante el controlador NWLINK.VXD sin la interface NetBIOS.

10.6.2 5.6.2. Cliente para arquitectura de redes NetWare

El cliente de Microsoft para redes NetWare permite conectarse a servidores Novell-Netware en modo bindery. Se trata de un cliente de 32 bits, aunque no aprovecha todas las características de este tipo de redes. Por ello, es recomendable utilizar el cliente Novell32 o el cliente IntraNetWare suministrado por Novell sin coste.

10.7 5.7. Arquitectura para compartición de recursos pares

La compartición de archivos e impresoras en la red Microsoft la lleva a cabo el módulo VSERVER.VXD, que es el servidor SMB y permite que todos los servicios de Windows 9x utilicen este protocolo.

Cuando está instalada la red NetWare, el módulo NWSERVER.VXD se encarga de hacer las funciones de servidor NCP, que es un modo de servir NetWare.

En ambos tipos de clientes para los servicios de compartición de archivos e impresoras con seguridad a nivel usuario, el suministrador de seguridad (que según los casos será el MSSP.VXD o NWSP.VXD) ayuda a la validación del acceso de los usuarios para la administración del servidor. Además, el componente de seguridad de archivo FILESEC.VXD proporciona el control de acceso basado en la información del registro.

Por último, el libro de direcciones de red traduce las listas de cuentas del servidor y proporciona el cuadro de dialogo "Agregar usuarios" para seleccionar qué usuarios consiguen derechos de acceso.

10.8 5.8. Mecanismos de comunicación interprocesos IPC

El procesamiento distribuido permite que una tarea se desarrolle en dos partes: Una ejecutándose en el ordenador cliente, consumiendo pocos recursos, y otra en el servidor consumiendo gran cantidad. También permite que determinados dispositivos residan en el ordenador servidor permitiendo que los clientes hagan uso de él.

Otro tipo de procesamiento distribuido permite que la carga de determinadas operaciones se distribuya entre varios ordenadores. De esta forma una tarea que exija de grandes cálculos y que llevaría varios días en un ordenador se puede repartir entre varios equipos de forma que estos tarden menos tiempo en realizarla.

El procesamiento distribuido permite la conexión a nivel proceso-proceso, estableciéndose un flujo de datos en ambas direcciones. Windows 9x incluye los siguientes mecanismos de comunicación y de procesos para permitir la computación distribuida:

- Conexiones lógicas de red,
- Llamadas a procedimientos remotos (RPC)
- NetBIOS.
- Canales identificativos
- Buzones.

10.8.1 5.8.1. Conexiones lógicas de red en Windows 9x

Las conexiones lógicas de red, también llamadas WinSockets, están diseñadas basadas en las API (Aplication Program Interface) de conexión lógica de red U.C.Berkeley, el estándar de facto para acceder a servicios de datagrama y sesión sobre TCP/IP.

Las aplicaciones escritas para la interface de conexiones lógicas de red incluyen FTP y SNMP. En Windows 9x las conexiones lógicas de red también admiten IPX/SPX. Las conexiones lógicas de red Windows son una especificación pública que permiten proporcionar un API familiar de red para programadores Windows o UNIX, establecer compatibilidad binaria entre proveedores heterogéneos de utilidades TCP/IP Windows, y soporte para protocolos sin conexión y orientados a conexión.

Un protocolo de red en Windows debe soportar NetBIOS o WinSockets. El protocolo NetBeui de Microsoft hace uso exhaustivo de NetBIOS. A los protocolos que no soportan NetBeui, TCP/IP o IPS/SPX se les puede activar una interface NetBIOS en la hoja de propiedades del panel del control de la red.

Es importante saber que si pretendemos tener instalado un ordenador con soporte de red, Windows debe tener instalado algún protocolo NetBIOS o activada la interface NetBIOS en algún protocolo, porque NetBIOS es el corazón de una red Windows. La activación de la capa NetBIOS supone que los paquetes de datos generados en el formato del protocolo en cuestión sean modificados por el sistema operativo añadiendo a la cabecera de los mismos información NetBIOS.

Esto repercute en el rendimiento de los equipos, ya que supone un tiempo extra de procesamiento por cada paquete de datos.

Como principal inconveniente, cuando se activa el soporte NetBIOS, el añadir información supone que los ordenadores que ejecutan solamente TCP/IP no podrán ver dichas tramas y no podrán comunicar.

miércoles 21 de julio de 1999

Programas como FTP y TELNET utilizan conexiones lógicas de red Windows.

Los ficheros que permiten las conexiones lógicas de red Win16 y Win32 sobre TCP/IP y las conexiones de Win32 sobre IPX/SPX son:

ARCHIVO	CONEXIONES LÓGICAS	COMENTARIO
WINSOCK.DLL	Red de 16 bits	Proporciona compatibilidad hacia abajo con las aplicaciones de conexiones lógicas de red Win16 (p.ej. Windows 3.11)
WSOCK.VXD	Red Windows virtual	Soporte de conexiones lógicas de red Win16 y conexiones lógicas de red Win32 TCP/IP.
WSOCK32.DLL	Red Windows de 32 bits	Soporte de aplicaciones con conexiones lógicas de red TCP/IP de 32 bits y aplicaciones con conexiones lógicas de red Windows IPX/SPX de 32 bits.
VSIPX.VXD	Red sobre IPX/SPX	Soporte de conexiones lógicas de red Windows IPX/SPX de 32 bits.

10.8.2 5.8.2. Llamada a Procedimientos Remotos

(RPC: *Remote Procedure Call*) El componente RPC de Microsoft es compatible con la especificación de intercambio de comunicación de datos DCE de *Open Software Foundation* (OSF) para llamadas a procedimientos remotos, y por tanto funciona con sistemas compatibles DCE, como sistemas HP y AIX.

RPC emplea mecanismos tales como canales identificativos NetBIOS o conexiones lógicas de red para establecer comunicaciones entre el cliente y el servidor. Con el componente RPC la lógica de programación básica y el código relacionado pueden funcionar en diferentes ordenadores, lo que es muy importante para aplicaciones distribuidas.

10.8.3 5.8.3. NetBIOS

El sistema básico de entrada y salida de red (NetBIOS) es el conjunto de funciones de bajo nivel que dan soporte a todos los servicios de la red Windows.

NetBIOS puede ser usado para comunicación entre protocolos y el software de alto nivel como el reexpedidor y el servicio de servidor. Proporciona compatibilidad hacia abajo para aplicaciones desarrolladas para versiones anteriores de Windows.

NetBIOS define la interface entre las capas reexpedidor y protocolo. La interface NetBIOS es un conjunto de llamadas a funciones que permiten el que una aplicación como el reexpedidor en el cliente de red en modo protegido de Windows 9x pueda utilizar los servicios del suministrador de la capa de transporte.

Muchas aplicaciones de red utilizan NetBIOS para enviar órdenes al controlador de protocolo. La interface NetBIOS del Windows 9x (NETBIOS.DLL, VNETBIOS.386) está admitida por los protocolos enviados con Windows 9x.

Semana 27-30 julio

10.95.9. Instalación de la red en Windows 9x

Como ya hemos visto, la red de Windows 9x está basado en cuatro tipos de elementos:

- Adaptadores de red (Tarjetas)
- Clientes
- Protocolos
- Servicios.

El primer y fundamental elemento a instalar será el adaptador o tarjeta de red. Normalmente, la tarjeta es detectada en tiempo de instalación, y se nos da la oportunidad de configurarla. Si se instala posteriormente y es un dispositivo P&P en el primer arranque es detectado y configurado (a nivel de hardware).

Los pasos a seguir para integrar Windows 9x en red son:

1. Preparar el medio físico: Adquirir el cable necesario, conectarlo, etc., de forma que se adapte a la topología existente o que pretendamos implantar (Bus, anillo).
2. Configurar la tarjeta de red.
3. Agregar los clientes correspondientes.
4. Configurar los protocolos adecuados/necesarios.
5. Introducir o modificar la información de identificación del equipo.
6. Agregar los servicios necesarios.

10.9.1 6.9.1. Integración en una red Microsoft

Se considera una red Microsoft a una red punto a punto compuesta por dos o más equipos dotados de un sistema operativo Microsoft (MS-DOS, Windows NT, Windows 9x, Win3.x), un dominio de Windows NT o una combinación de ambos.

En las redes de Microsoft, los ordenadores se pueden agrupar formando dominios o grupos de trabajo.

10.9.1.1 Grupo de trabajo

En un grupo de trabajo, cada ordenador se hace cargo de sus recursos compartidos, y establece las restricciones para el acceso a dichos recursos. Es una organización que realmente no existe en ningún sitio. No hay ningún ordenador que se encargue de gestionar los miembros del mismo, o que almacene información del grupo al que pertenece. Para integrar un ordenador en un grupo de

trabajo, simplemente lo indicaremos en el campo correspondiente de la solapa identificación en la configuración de la red. Cuando encendemos un ordenador en el que figura que pertenece a un grupo de trabajo, suceden los siguientes eventos:

- Se envía un mensaje de requerimiento a toda la red (*Broadcast*), interrogando si existe algún explorador de equipos al que pertenezca su grupo de trabajo. El explorador de equipo de cada grupo es el encargado de mantener la lista de equipos en sesión, dentro del mismo, y se actualiza cada tres minutos.

- Si se recibe respuesta afirmativa, se le requiere la lista de equipos pertenecientes al mismo grupo de trabajo. También se le suministra la lista de otros grupos de trabajo detectados que estén en la misma red física.

- Si no se recibe dicha respuesta, el equipo en cuestión debe de encargarse de realizar la función de exploración de equipos para el grupo de trabajo.

10.9.1.2 Dominio

Un dominio es una organización de equipos en la que existe un ordenador con Windows NT Server configurado como controlador primario de dominio. Éste hace las funciones de servidor de dominio y se encarga de mantener la base de datos de seguridad, que incluye la lista de equipos pertenecientes al dominio y la lista de usuarios que pueden iniciar sesión en dicho dominio.

Un dominio es por tanto una estructura perfectamente organizada de equipos, recursos y usuarios, mantenida de forma centralizada por un único servidor. Para que un ordenador con Windows 9x pueda establecer conexión con otros sistemas operativos de Microsoft, ya sea Punto a Punto o mediante el dominio, es necesario que tenga instalado el cliente para redes Microsoft.

En una red Microsoft, puede utilizarse tanto el protocolo NetBeui como cualquier otro protocolo que permita instalar la interface NetBIOS (TCP/IP, IPX/SPX).

10.9.2 5.9.2. Integración en una red Novell/NetWare

El sistema operativo del Novell/NetWare es el típico ejemplo de red basada en un servidor dedicado.

En una red de este tipo, los servidores ejecutan el mismo sistema operativo, dedicándose exclusivamente a dar servicio a los clientes. Los clientes, en cambio, pueden trabajar con distintos sistemas operativos.

Para Windows 9x existen tres clientes para redes NetWare:

- Cliente Microsoft para redes NetWare: es un componente de la red disponible en Windows 9x que permite conexiones plenas a redes Novell inferiores a la versión 4 y conexiones limitadas a versiones superiores.

- Cliente NetWare de 32 Bits: es un software disponible en los CD's del sistema operativo NetWare, y también está disponible en la red de Novell. Su instalación implica la modificación de algunas características del explorador de Windows, para adaptarlo a los requerimientos de las redes NetWare de tipo NDS.

- Cliente IntraNetWare: es una versión ampliada de la anterior, y permite la conexión y administración de varios servidores NetWare, entre otras características.

Para integrar un equipo Windows 9x en una red Novell se debe de utilizar el protocolo IPX/SPX, a no ser que el servidor tenga instalado el módulo NetWare/IP.

Si un equipo debe comunicarse con los sistemas operativos Microsoft y NetWare y en consecuencia tener instalados ambos clientes, es recomendable que el primer inicio de sesión lo realice en NetWare, con el fin de que se monte primero la pila de protocolos NetWare, debido a la robustez que esta pila ofrece en cuanto a tráfico por la red.