

## 7.1 Técnicas de compartición del medio

---

En muchas ocasiones se dispone de un único medio de comunicación que es compartido por distintos equipos y que es empleado para la transferencia de información entre todos ellos. Fundamentalmente se adopta un medio compartido con el objetivo de ahorrar costes de material y hacer más sencillo el mantenimiento e instalación. Véase, por ejemplo, los casos mostrados en la Figura 7-1 donde se ha representado una red basada en bus y otra en anillo. En ambos casos existe un único medio de transmisión que es compartido por cuatro equipos y al cual pueden acceder indistintamente para comunicar información al resto de equipos. Por lo tanto, es necesario que se implemente algún tipo de protocolo para coordinar los equipos con el objetivo de decidir cual de ellos envía información en un instante de tiempo determinado sin que las tramas enviadas “colisionen” con las enviadas por otro equipo. De realizar esta coordinación para el acceso al medio físico compartido se encarga el nivel de enlace de las LAN y se denominan técnicas de compartición del medio (MAC).

El término colisión se emplea para indicar la situación en la que una trama de datos interfiere en el medio de transmisión con la que simultáneamente ha enviado otro equipo. Esto se produce cuando dos equipos transmiten información casi al mismo tiempo. En este caso, las dos tramas pueden interferir entre sí.

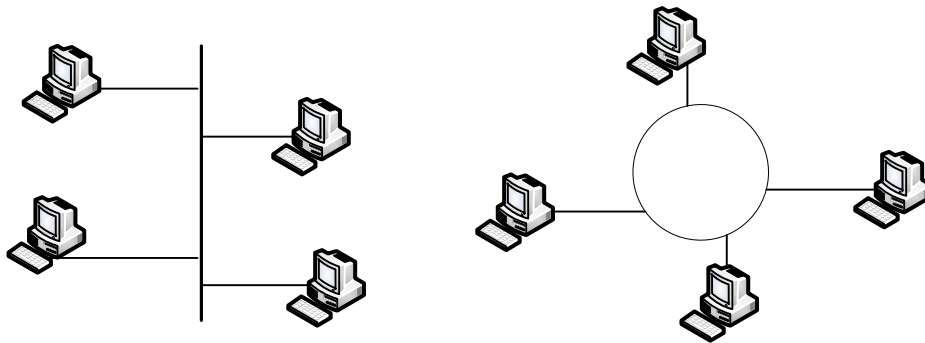


Figura 7-1. Medios compartidos.

Las técnicas de compartición del medio pueden clasificarse en:

- *Contienda o acceso múltiple.* Son las técnicas más fáciles de implementar aunque también las menos eficientes. Se denominan técnicas de contienda debido a que los equipos que pretenden acceder al medio para realizar la transmisión de los datos “compiten” por el medio antes de realizar el envío de los datos. Una de las desventajas de este método es que pueden producirse colisiones en los datos transmitidos por los distintos equipos.
- *Reserva.* El acceso al medio se realiza mediante dos pasos: reserva y envío de datos. Durante la fase de reserva el equipo que quiere acceder al medio solicita la reserva del medio de transmisión. Una vez realizada la reserva podrá realizarse la transmisión de datos sin correr el riesgo de que los datos enviados puedan colisionar con los transmitidos por otro equipo. Aunque se evitan las colisiones al transmitir los datos, aún pueden producirse colisiones en la petición de reserva. Sin embargo, las peticiones de reserva generalmente son más cortas y, por lo tanto, se reduce la probabilidad de que llegue a producirse una colisión. Existen dos tipos de acceso al medio por reserva:

- *Centralizada*. En la que existe un equipo especial en la red que gestiona y atiende las reservas.
- *Distribuida*. Si las reservas se gestionan entre todos los equipos que conforman la red.
- *Selección*. En esta técnica se aplica un determinado algoritmo que va seleccionando los equipos que pueden acceder al medio. Cuando el equipo es seleccionado podrá realizar el envío de los datos. La principal ventaja de este método es que no se producirán colisiones ya que en un momento dado solo podrá realizar envío de datos el equipo que se encuentre seleccionado. Al igual que el acceso por reserva, el acceso al medio por selección puede ser:
  - *Centralizada*. Hay un equipo que va concediendo los turnos al resto de equipos para realizar el envío de datos.
  - *Distribuida*. El turno es gestionado entre todos los equipos.

El método de acceso por selección distribuida es empleado por redes en anillo tipo IEEE 802.5 (Token Ring), sin embargo, quizás los métodos más empleados en la actualidad son los basados en contienda. Estos últimos métodos son los empleados por las redes en bus tipo Ethernet IEEE 802.3, es por ello por lo que en el siguiente apartado se describe con más detalle los distintos tipos y funcionamiento de los métodos de acceso al medio basados en contienda.

## 7.2 Técnicas de contienda

---

Las técnicas de contienda pueden clasificarse en:

- *Transmisión sorda (ALOHA)*. Los equipos que componen la red no tienen en cuenta si hay información en el medio antes de realizar el envío de sus datos.
- *Transmisión con escucha (CSMA, carrier sense multiple access, Técnica de acceso múltiple con detección de portadora)*. Los equipos solo enviarán datos al medio si determinan que no hay información previa enviada por otro equipo. Empleando este método sólo se producirán colisiones cuando dos o más equipos envíen datos a la vez (ya que ambos determinarían simultáneamente que el medio de comunicación está libre). Si una estación determina que el medio está ocupado deberá esperar. El tiempo de espera se establece en una cantidad de tiempo razonable en el cual debería llegar la confirmación del equipo destinatario, teniendo en consideración el retardo de propagación máximo, del trayecto de ida y vuelta y el hecho de que la estación que confirma debe competir también por conseguir el medio para responder. Si no llega la confirmación, la estación supone que se ha producido una colisión. En este caso esperará un tiempo aleatorio y volverá a comprobar si el medio está libre antes de realizar el reenvío de los datos.

A continuación se pasan a describir las distintas técnicas de contienda basadas en la clasificación anterior.

### 7.2.1 ALOHA puro y ranurado.

Empleando esta técnica de acceso al medio una determinada estación puede transmitir una trama siempre que lo necesite. A continuación, la estación pasa a escuchar el medio durante un tiempo igual al máximo retardo de propagación posible de ida y vuelta a través de la red más un pequeño

incremento de tiempo. Se considera que todo ha ido bien si durante este intervalo de escucha, a la estación le llega la confirmación procedente del destino. En caso contrario retransmitirá la trama. La estación desistirá si no recibe una confirmación después de varias retransmisiones.

ALOHA es una técnica muy sencilla de implementar, sin embargo, las colisiones aumentan rápidamente cuando aumenta la carga de la red. Con el objetivo de mejorar el comportamiento del método se implementó el denominado ALOHA ranurado. En ALOHA ranurado el canal se divide en ranuras de tiempo discreto, considerando ranuras uniformes de duración igual al tiempo de transmisión de una trama. De esta manera, la transmisión solo se permite en los instantes de tiempo que coincidan con el comienzo de una ranura. Así, las tramas que se solapan lo harán completamente, lo que incrementa la utilización máxima del sistema desde el 18% en ALOHA puro al 37% en ALOHA ranurado.

Habitualmente ocurre que el tiempo de propagación de una trama es notablemente inferior al tiempo requerido para su transmisión. De esta forma, cuando una estación transmita una trama, el resto de estaciones lo sabrá casi inmediatamente. Así, si las estaciones que componen una red pueden determinar que hay otra que ya está transmitiendo se evitarán que se produzcan colisiones a no ser que dos equipos decidan transmitir datos casi simultáneamente. Esto llevó a la definición de las técnicas de control del acceso al medio denominadas CSMA.

### 7.2.2 CSMA no persistente.

Como se ha indicado con anterioridad en CSMA un equipo antes de enviar datos escucha el medio para determinar si está o no ocupado. Sólo cuando está libre puede transmitir y si está ocupado deberá esperar un tiempo prudencial antes de realizar el reenvío de los datos.

En general, la utilización máxima que se puede conseguir en CSMA puede superar con mucho la de ALOHA ranurado. La utilización máxima depende de la longitud de la trama y del tiempo de propagación. Cuanto mayor sea la longitud de las tramas o cuanto menor sea el tiempo de propagación, mayor será la utilización.

En CSMA se precisa de un algoritmo que determine qué debe hacer una estación si encuentra el medio ocupado. Un posible algoritmo es el implementado por CSMA no persistente en el que una estación que desea transmitir escuchará el medio y procederá según las siguientes reglas (véase Figura 7-2):

1. Si el medio se encuentra libre transmite. Si está ocupado se aplica el paso 2.
2. Si el medio se encuentra ocupado espera una cierta cantidad de tiempo obtenido de una distribución de probabilidad (retardo de transmisión) y repite el paso 1.

El uso de retardos aleatorios reduce la probabilidad de las colisiones. Esto es debido a que si dos estaciones detectan simultáneamente que se ha producido una colisión y ambas esperan el mismo tiempo para realizar la retransmisión de las tramas, se volverá a producir la colisión.

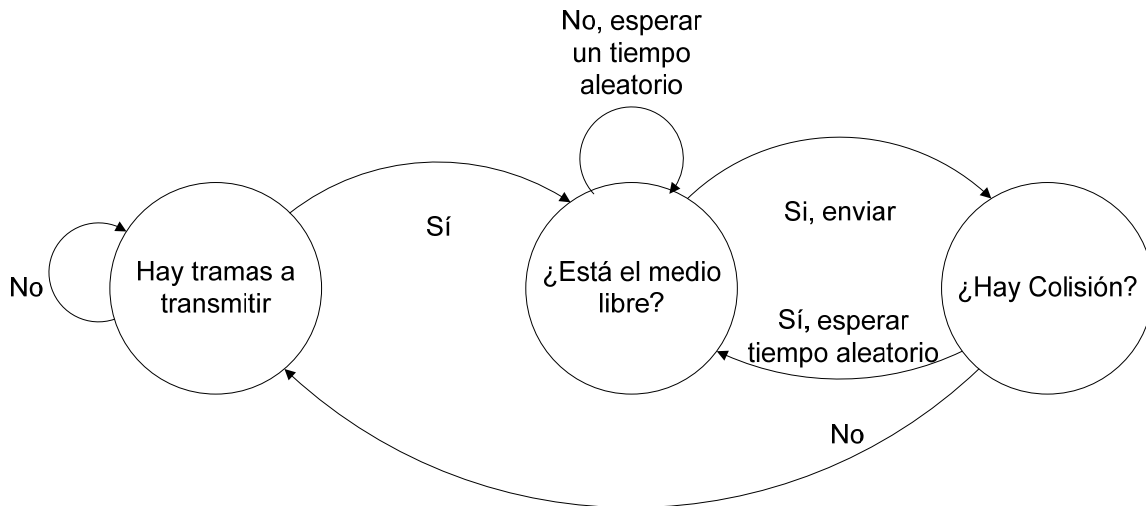


Figura 7-2. CSMA no persistente.

### 7.2.3 CSMA 1-persistente.

Uno de los principales problemas de CSMA no persistente es que se desaprovecha la capacidad debido a que el medio permanecerá libre justo tras el fin de una transmisión, incluso si una o más estaciones se encuentran listas para transmitir. Para aprovechar estos intervalos de tiempo se puede utilizar el protocolo CSMA 1-persistente. En este caso un equipo que desea transmitir escuchará el medio y actuará de acuerdo siguiendo los siguientes pasos (véase Figura 7-3):

1. Si el medio se encuentra libre transmite. Si está ocupado se aplica el paso 2.
2. Si el medio está ocupado, continúa escuchando hasta que el canal se detecte libre, momento en el cual se transmite inmediatamente.

El principal problema de este algoritmo es que si dos estaciones desean transmitir se garantizará que se producirá la colisión entre sus tramas.

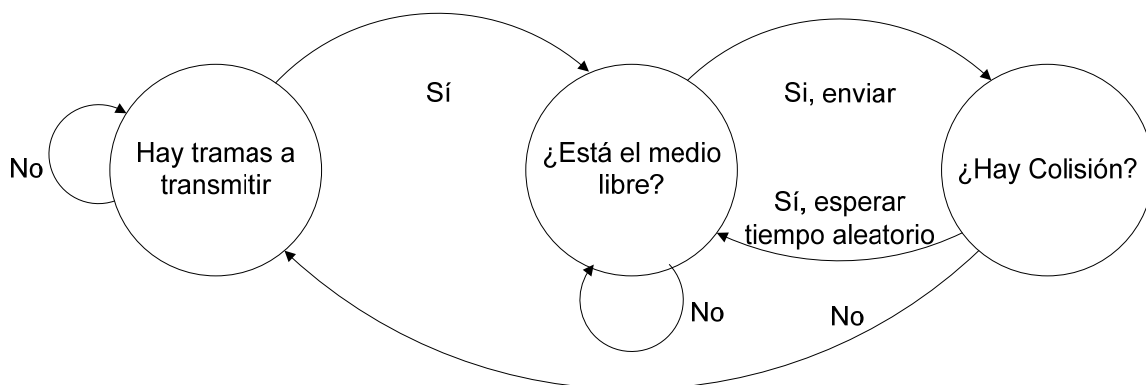


Figura 7-3. CSMA 1-persistente.

### 7.2.4 CSMA p-persistente.

Esta técnica representa un compromiso entre reducir el número de colisiones (como en el caso de no persistente) y reducir el tiempo de desocupación del canal (como en el 1-persistente). Las reglas a aplicar en este caso son las siguientes (ver Figura 7-4):

1. Si el medio se encuentra libre, entonces se transmite con una probabilidad  $p$  y se espera una unidad de tiempo con una probabilidad  $(1-p)$ . La unidad de tiempo es generalmente igual al retardo máximo de propagación.
2. Si el medio está ocupado, se continúa escuchando hasta que se detecte libre y se repite el paso 1.
3. Si la transmisión se ha retardado una unidad de tiempo, se repite el paso 1.

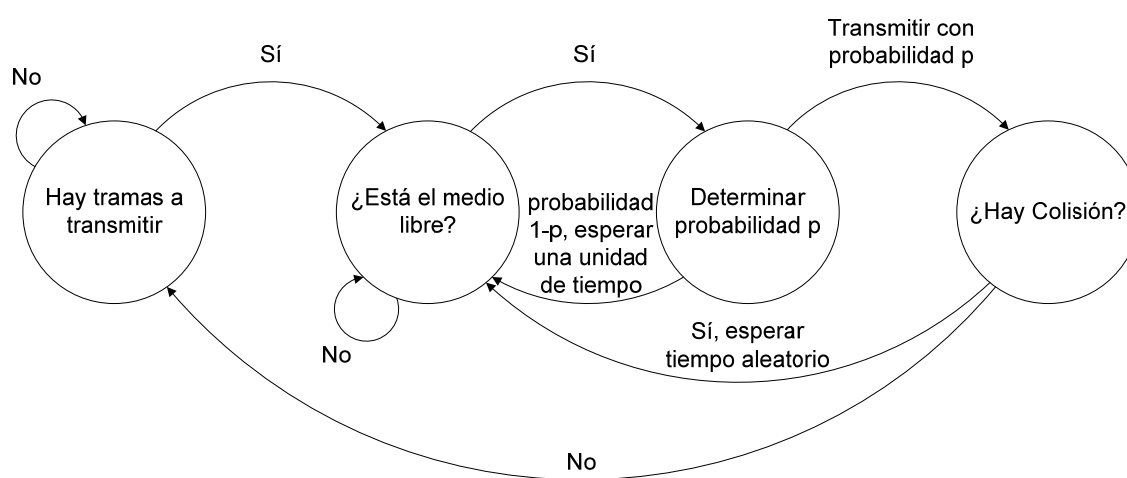


Figura 7-4. CSMA p-persistente.

### 7.2.5 CSMA/CD.

En CSMA, una estación que desee transmitir escuchará primero el medio para determinar si existe alguna otra transmisión en curso. Sin embargo, pueden producirse colisiones si dos estaciones comienzan a transmitir casi al mismo tiempo. Independientemente del método de CSMA (no persistente, 1-persistente o p-persistente) cuando se producen colisiones las estaciones esperan una determinada cantidad de tiempo antes de retransmitir. Por lo tanto, el medio permanece inutilizable mientras dure la transmisión de ambas tramas dañadas. En el caso de que la longitud de las tramas sea elevada comparada con el tiempo de propagación, la cantidad de tiempo desaprovechado puede ser importante. Este desaprovechamiento puede reducirse si una estación continúa escuchando el medio mientras dura la transmisión. Esta característica es empleada por CSMA/CD (acceso múltiple con detección de portadora y detección de colisiones (carrier sense multiple access with collision detection)). En este caso para el acceso al medio se siguen las siguientes reglas (ver Figura 7-5):

1. Si el medio se encuentra libre transmite. Si está ocupado se aplica el paso 2.
2. Si el medio se encuentra ocupado, continúa escuchando hasta que el canal se libere, en cuyo caso transmite inmediatamente.

3. Si se detecta una colisión durante la transmisión, se transmite una pequeña señal de interferencia para asegurarse de que todas las estaciones constaten la colisión. A continuación, se deja de transmitir.
4. Tras la emisión de la señal de interferencia, la estación espera una cantidad aleatoria de tiempo conocida como espera, intentando transmitir de nuevo a continuación (volviendo al paso 1).

Este método de acceso es el empleado por las redes Ethernet IEEE 802.3. Cuando se implementa este método de acceso al medio las tramas a nivel de enlace deben presentar un tamaño mínimo como para permitir la detección de la colisión antes de que finalice la transmisión

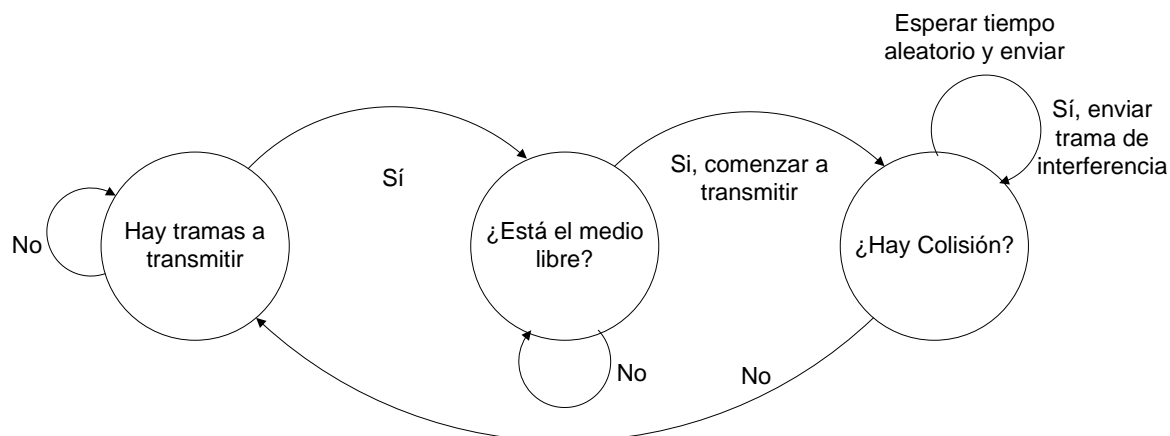


Figura 7-5. CSMA/CD.

Las redes inalámbricas IEEE 802.11 emplean para el acceso al medio una modificación de CSMA/CD denominada acceso múltiple con detección de portadora y prevención de colisiones CSMA/CA. Con este método se evita la aparición de colisiones debido a la dificultad de su detección en el medio inalámbrico. Empleando este mecanismo cada equipo anuncia opcionalmente su intención de transmitir antes de hacerlo para evitar colisiones entre los paquetes de datos. De esta forma, el resto de equipos de la red sabrán cuando hay colisiones y en lugar de transmitir la trama en cuanto el medio está libre, se espera un tiempo aleatorio adicional corto y solamente si, tras ese corto intervalo el medio sigue libre, se procede a la transmisión reduciendo la probabilidad de colisiones en el canal.

## 7.3 Técnicas de control del enlace: Protocolo HDLC

En el capítulo anterior se presentó el protocolo de ventana deslizante como uno de los protocolos más usados para regular el flujo de información entre dos dispositivos. En este capítulo se proporcionan los conocimientos básicos, relacionados con algunos de los protocolos estándar del nivel de enlace, que hacen uso del protocolo de ventana deslizante para regular el intercambio de información y controlar errores. En concreto, se presenta el estándar HDLC (High Level Data Link Control), su estructura de trama, sus modos de funcionamiento y su repertorio básico de instrucciones. El protocolo HDLC está regulado por el estándar ISO 3309 e ISO 4335 y se caracteriza por ser un protocolo de nivel de enlace orientado a bit. Este protocolo es de vital importancia porque ha servido como base para la implementación de otros muchos protocolos (LAPB: Link Access Procedure Balanced para redes X.25, LLC: Logical Link Control para redes 802 o PPP: Point to Point). Este protocolo tiene sus orígenes en el protocolo SDLC (Synchronous Data Link Control) de IBM.

### 7.3.1. Tipos de estaciones y enlaces

El protocolo HDLC define tres tipos de DTEs (Equipos terminales de datos). Los DTEs pueden funcionar como estaciones primarias, secundarias o combinadas.

- *Primarias*: Una estación se dice que funciona como primaria cuando es la responsable de controlar el enlace de datos, por ejemplo, creando o liberando éste.
- *Secundaria*: Una estación se denomina secundaria cuando funciona siempre bajo el control de una estación primaria y sólo se puede comunicar con primarias.
- *Combinada o Balanceada*: Las estaciones combinadas son todas aquellas que pueden funcionar como estaciones primarias y secundarias. Dependiendo de la situación del enlace funcionara como primaria o en su defecto como secundaria.

Las tramas HDLC que envía una estación funcionando como primaria se denominan *órdenes* y las tramas que envía una estación secundaria se denominan *respuestas*. Por lo tanto, una estación combinada puede enviar tramas orden o tramas respuesta.

Además, de acuerdo a la combinación de los tipos de DTE que determinan un enlace de datos, se establecen dos tipos de configuraciones de enlace de datos.

- *No Balanceada*: Es un enlace de datos formado por una estación primaria y una o más estaciones secundarias sobre un canal con transmisión dúplex o semidúplex.
- *Balanceada*: Es un enlace de datos formado por dos estaciones combinadas sobre un canal con transmisión dúplex o semidúplex.

### 7.3.2. Modos de funcionamiento

El protocolo HDLC define tres modos de funcionamiento que determinan el modo en como se realiza el intercambio de datos entre DTEs.

- *Modo normal*: El modo normal o NRM (Normal Response Mode) es siempre utilizado en configuraciones no balanceadas. En este tipo de configuraciones, la estación que funciona como primaria se encarga de iniciar la transmisión y la estación secundaria únicamente puede transmitir respuestas a dichas ordenes.
- *Modo asíncrono*: El modo asíncrono o ARM (Asynchronous Response Mode) es empleado también en configuración no balanceada. La diferencia con respecto a NRM es que con este modo de funcionamiento, la secundaria puede iniciar la transmisión sin tener permiso de la primaria.
- *Modo asíncrono balanceado*: El modo asíncrono balanceado o ABM (Asynchronous Balanced Mode) es empleado con configuraciones balanceadas del enlace. En este caso, cualquiera de las dos estaciones combinadas puede iniciar la transmisión sin solicitar permiso a la otra.

### 7.3.3. Estructura de la trama

Al igual que ocurre en otros protocolos del nivel de enlace (Ethernet, PPP, etc), el intercambio de información entre dos DTEs se realiza organizando los bloques de datos en tramas. El protocolo HDLC para realizar el control de errores y el control de flujo emplea siempre un mismo formato de

tramas (Figura 7.6) numerado con 3 bits, lo que permite numerar las tramas entre 0 (cuando el valor de los bits es 000) y 7 (cuando es 111). El intercambio de datos en HDLC se realiza siempre usando una transmisión síncrona.

DELIMITADOR (8 bits)	DIRECCION (8 ó k-8 bits)	CONTROL (8 ó 16 bits)	INFORMACION (Variable)	FCS (8 ó 32 bits)	DELIMITADOR (8 bits)
-------------------------	-----------------------------	--------------------------	---------------------------	----------------------	-------------------------

Figura 7-6: Formato de trama HDCL.

El formato de una trama HDLC se organiza de la siguiente manera:

- *Delimitador*: Es el campo que se sitúa al principio y al final de la trama y que determina dónde empieza y termina el bloque de datos que se envía. Al ser el protocolo HDLC un protocolo orientado a bit, emplea delimitación por bits especiales. Así, tanto el delimitador de inicio como delimitador de final emplean la secuencia '0111110', y se emplea el mecanismo de bits de relleno para evitar que la secuencia especial de delimitación aparezca en los bits de datos (véase Apartado 5.4.4). La longitud del campo delimitador es fija y de 8 bits.
- *Dirección*: Identifica a la estación secundaria cuando la trama representa una orden enviada por una estación primaria. También, puede identificar a una estación secundaria cuando la trama representa una respuesta enviada hacia una estación primaria. En el primer caso, el campo identifica a una estación secundaria que funciona como receptor, y en el segundo caso a una estación secundaria que funciona como emisor. El campo dirección tiene una longitud cuyo valor corresponde con múltiplos de 8 bits.
- *Control*: Identifica el tipo de trama que se intercambian los dispositivos. Según el tipo de trama que se intercambien dos estaciones, el campo control será distinto. Así, en el campo control, los dos primeros bits se emplean para identificar el tipo de trama, y el resto de bits se suelen dividir en varios subcampos que se organizan de modo distinto dependiendo del tipo de trama. La longitud de este campo suele ser de 1 o 2 bytes.
- *Datos o Información*: Contiene la secuencia de bits de datos que quieren intercambiar los dos dispositivos. La longitud de este campo es variable. Este campo no está presente en cualquier tipo de trama, por lo tanto, su longitud puede ir desde 0 bits hasta cualquier múltiplo entero de 8 bits.
- *FCS o campo de detección de errores*: Almacena la secuencia de bits de CRC necesaria para detectar errores en el campo de datos o información. Para generar la secuencia de ceros y unos que determina el CRC se emplean polinomios generadores del tipo CRC-CCITT de 16 o 32 bits.

### 7.3.4. Tipos de tramas.

El protocolo HDLC emplea tres tipos de tramas. Estas tramas se distinguen unas de otras en función de los dos primeros bits del campo control de la trama. Así en función de que estos dos bits se pueden clasificar las tramas como:

- *Información*: Las tramas de información se emplean para el intercambio de datos del nivel de red entre dispositivos (Figura 7.7a).

- *Supervisión:* Estas tramas se emplean para incorporar mecanismos adicionales que permitan supervisar el control de flujo mediante ventana deslizante y control de errores (Figura 7.7b).
- *No-Numerada:* Estas tramas permiten incorporar otras funciones para controlar el enlace de datos (Figura 7.7c).

a)	0 (1 bit)	N(S) (3 bits)	P ó F (1 bit)	N(R) (3 bits)
b)	10 (2 bit)	S (2 bit)	P ó F (1 bit)	N(R) (3 bits)
c)	11 (2 bit)	M (2 bit)	P ó F (1 bit)	M (3 bits)

Figura 7-7: Formato del campo control de 8 bits. a) Tramas de Información. b) Tramas de Supervisión. c) Tramas No-Numeradas

El campo control en las tramas de Información está formado por 3 subcampos. Un subcampo N(S) que determina el número de secuencia enviada, un subcampo N(R) que indica el número de secuencia recibida y un subcampo de sondeo (P/F), que permite identificar la última trama asociada a una secuencia de paquetes del nivel de red fragmentados. Este bit P/F, cuando la trama HDLC indica una orden se denomina bit P, y se fija a 1 para solicitar (sondear) una respuesta a la entidad HDLC par situada en el otro extremo de la comunicación. Sin embargo, cuando la trama HDLC indica una respuesta, se denomina F, y su valor se pone a 1 para identificar a la trama devuelta tras una recepción de una orden

El campo control en las tramas de Supervisión está formado por 3 subcampos. Un código S que determina el tipo de trama de supervisión, un subcampo N(R) que indica el número de secuencia recibida y un subcampo de sondeo (P/F), que al igual que en la trama de Información, permite identificar la última trama asociada a una secuencia de paquetes del nivel de red fragmentados. Los códigos que puede adoptar S son los mostrados en la figura 7-8.

El campo control en las tramas No-Numeradas, también, está formado por 3 subcampos. Dos subcampos M que indican el tipo de tramas No-Numeradas y un subcampo de sondeo (P/F), que al igual que en las otras tramas, permite identificar la última trama asociada a una secuencia de paquetes del nivel de red fragmentados. Los códigos que puede adoptar M, también se muestran en el apartado 7.3.5, en la figura 7-8.

### 7.3.5.Repertorio básico de instrucciones

El protocolo HDLC tiene un conjunto de órdenes y respuestas que constituyen el conjunto de todo el repertorio de tramas HDLC. En la tabla de la figura 7.8 se han definido las órdenes y respuestas básicas organizadas en función del tipo de trama que se emplea para comunicarlasy. Los distintos tipos de estaciones, enlaces, modos de funcionamiento y tipos de tramas permiten definir diferentes variantes del protocolo HDLC, como se verá a lo largo de los siguientes apartados.

Tipo trama	Instrucción	Orden/Respuesta	Descripción
Información	I	O/R	Información
Supervisión	RR	O/R	Receptor preparado
	RNR	O/R	Receptor no preparado
	REJ	O/R	Rechazo
	SREJ	O/R	Rechazo selectivo
No numeradas	SNRM	O	Fijar modo normal no balanceado
	SARM	O	Fijar modo asíncrono no balanceado
	SABM	O	Fijar modo balanceado asíncrono
	DISC	O	Desconectar
	UA	R	Confirmación no numerada

Tipo trama	Instrucción	Campos 'S' o 'M'	Descripción
Supervisión	RR	00	Se ha recibido correctamente hasta la trama indicada en N(R)-1 y se indica en N(R) la siguiente trama que se espera recibir.
	RNR	10	Se ha recibido correctamente hasta la trama N(R)-1, pero no se pueden recibir más tramas
	REJ	01	Se solicita el reenvío de todas las tramas a partir de la indicada en N(R), incluida ésta.
	SREJ	11	Se solicita el reenvío de la trama indicada en N(R)
No numeradas	SNRM	00 001	Fijar modo normal no balanceado
	SARM	11 000	Fijar modo asíncrono no balanceado
	SABM	11 100	Fijar modo balanceado asíncrono
	DISC	00 010	Desconectar
	UA	00 110	Confirmación no numerada

Figura 7-8: Repertorio simplificado de Instrucciones.

### 7.3.6. Control del enlace en Modo Normal No Balanceado

En un modo de funcionamiento Normal no balanceado (NRM), una de las estaciones se tiene que definir como primaria y la otra como secundaria. De modo, que si se configura la estación A como primaria, será la única que podrá enviar órdenes lo que imposibilita a la estación B para establecer y liberar el enlace de comunicación. Como se muestra en el ejemplo de la figura 7.9, sólo la estación A se encargará de establecer la comunicación, enviando la orden SNRM mediante una trama no numerada. Y la estación B confirmará ese establecimiento con la respuesta UA mediante una trama no numerada.

Posteriormente, si la estación A tiene que enviar datos a la estación B procederá como se indica en la figura 7.9, enviando tantas tramas como permita la ventana deslizante del emisor. Y la estación B, podrá recibir tantas tramas sin enviar asentimiento como permita la ventana del receptor. Para el caso que nos ocupa  $W_e=W_r=2$ . Los datos en este caso se encapsularán siempre en tramas de información, I. Y la confirmación o asentimiento de dichos datos se realizará, por parte de B, con tramas de supervisión RR. En este ejemplo, la primera trama de Información indica que  $N(S)=0$  y  $N(R)=0$ , la segunda trama de Información indica que  $N(S)=1$  y  $N(R)=0$ , y el flag P/F se ha puesto a 1. En ese mismo ejemplo, la trama de supervisión tiene el valor S a 00, indicando que es una trama RR cuyo campo  $N(R)=2$  y cuyo campo P/F adopta el valor 0.

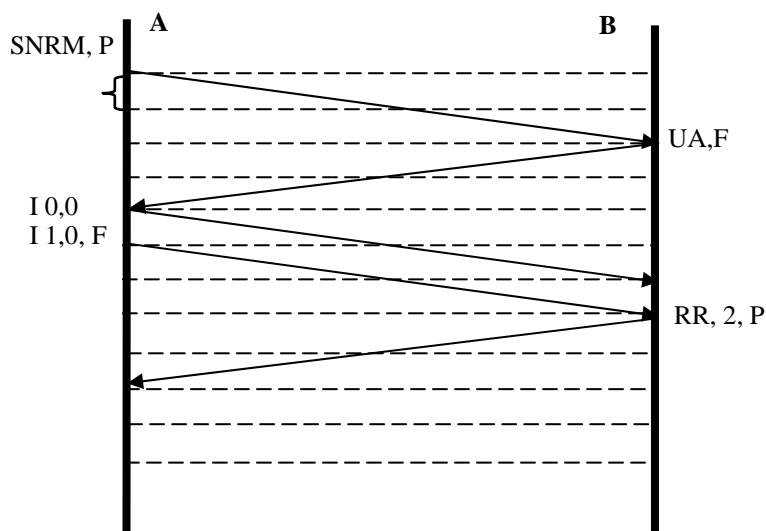


Figura 7-9: Transmisión de datos en Modo Normal no Balanceado.

Supóngase ahora que el modo de funcionamiento y el tipo de estaciones son las mismas que se indicaban en el ejemplo anterior, sin embargo la que necesita enviar datos es la estación B. Es decir, la estación contraria a la que controla el enlace. En tal caso, el protocolo HDLC procede de la siguiente manera (Figura 7.10):

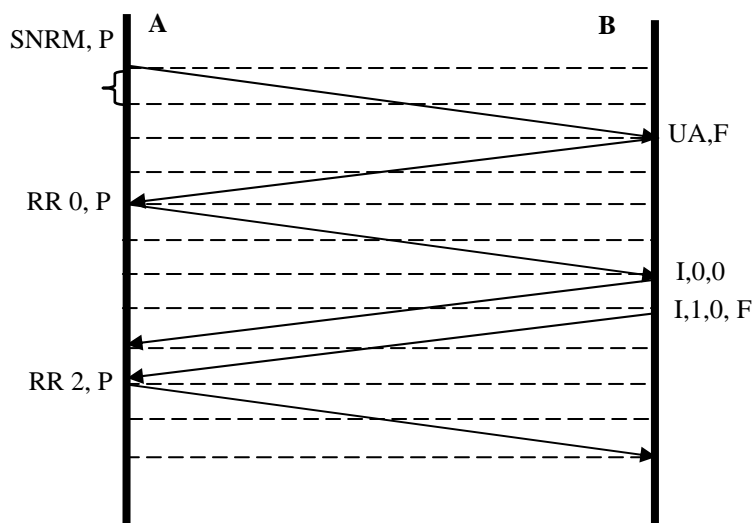


Figura 7-10: Transmisión de datos en Modo Normal no Balanceado.

En este caso, una vez el enlace ha sido establecido, la estación A informa mediante una trama de supervisión RR que está preparada para recibir datos de la estación B. Sino ésta no sabrá cuando la estación A está preparada para recibirlos. Posteriormente, la estación B ya está preparada para enviar datos mediante tramas de información, I. Y la confirmación o asentimiento de dichos datos se realizará, de nuevo, con tramas de supervisión RR.

### 7.3.7. Control del enlace en Modo Asíncrono No Balanceado

En un modo de funcionamiento Asíncrono no Balanceado (ARM), al igual que en el NRM, una de las estaciones se tiene que definir como primaria y la otra como secundaria. De modo que, será la estación A como primaria, la única que podrá enviar órdenes para establecer y liberar el enlace de datos. Para llevar a cabo el control del enlace, la estación A se encargará de establecer la comunicación enviando la orden SARM mediante una trama no numerada. La estación B confirmará ese establecimiento con la respuesta UA mediante una trama no numerada. Sin embargo, a diferencia del modo NRM, en este caso la estación B que es secundaria puede iniciar la transmisión de datos sin necesidad de esperar un permiso explícito de la estación primaria, A.

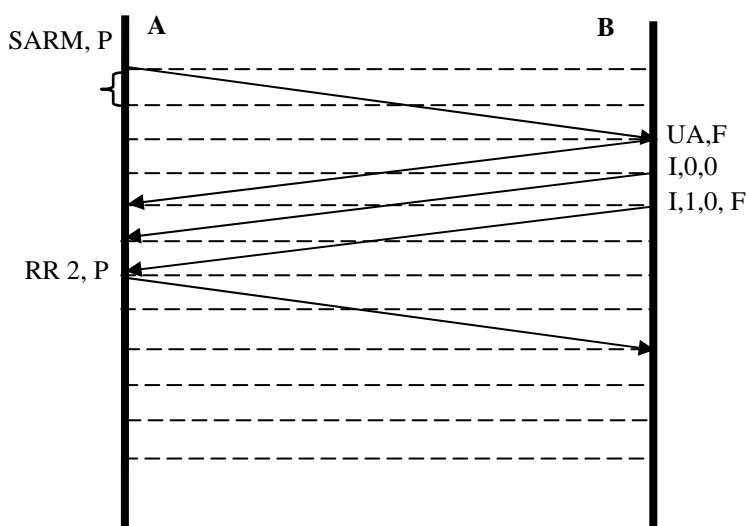


Figura 7-11: Transmisión de datos en Modo Asíncrono no Balanceado.

### 7.3.8. Control del enlace en Modo Asíncrono Balanceado

En el modo de funcionamiento Asíncrono Balanceado (ABM), las dos estaciones que configuran el enlace son balanceadas. Por lo tanto, ambas estaciones, A y B, pueden controlar el enlace e iniciar la transmisión de datos, sin pedir permiso explícito a la otra estación. Por ejemplo, en la figura 7.12, es la estación A la que controla el enlace y comienza la transmisión de datos. Así, comienza creando un enlace enviando la orden SABM mediante una trama no numerada. Y la estación B confirmará ese establecimiento con la respuesta UA mediante una trama no numerada. Posteriormente, A comienza el envío de datos, I, mediante tramas de información y B los confirma con tramas de supervisión RR.

En la figura 7.13, es la estación B la que controla el enlace y comienza la transmisión de datos. Así, comienza creando un enlace enviando la orden SABM mediante una trama no numerada. La estación A confirmará ese establecimiento con la respuesta UA mediante una trama no numerada.

Como se observa en la figura se realiza el mismo intercambio de tramas que en el caso anterior, pero tomando como origen B y como destino A.

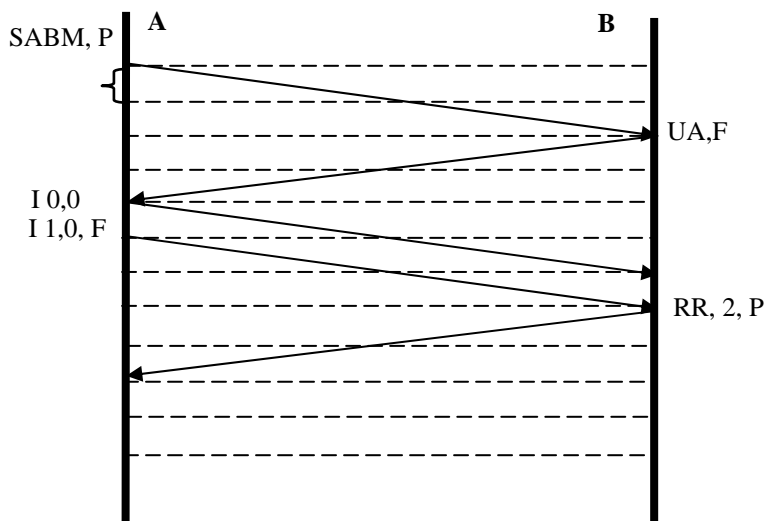


Figura 7-12: Transmisión de datos en Modo Asíncrono Balanceado.

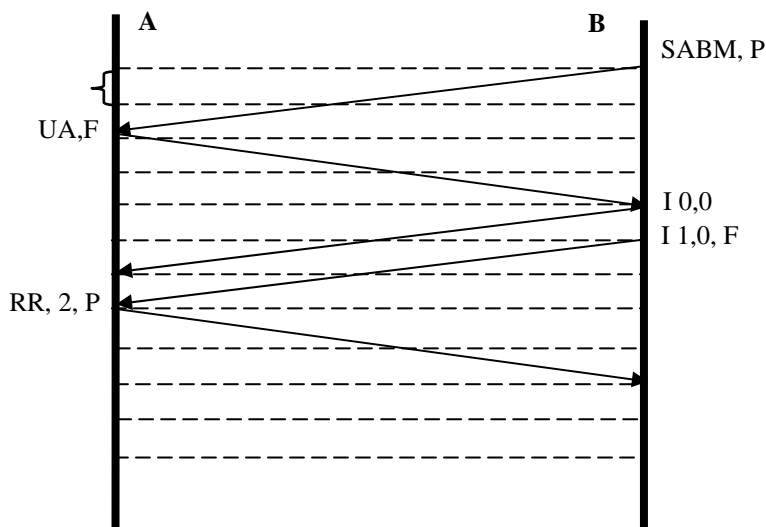


Figura 7-13: Transmisión de datos en Modo Asíncrono Balanceado.

Y en la figura 7.13, es la estación B la que controla el enlace y comienza la transmisión de datos. Así, comienza creando un enlace enviando la orden SABM mediante una trama no numerada. Y la estación A confirmará ese establecimiento con la respuesta UA mediante una trama no numerada. Y se realiza el mismo intercambio de tramas que en el caso anterior, pero tomando como origen B y como destino A.

### 7.3.9. Configuración del medio de Transmisión y transferencia de datos

El medio de transmisión puede estar configurado en modo *simplex*, *semiduplex* (half-duplex) o *dúplex* (full-duplex). Las líneas dúplex permiten enviar varias tramas en ambos sentidos de la transmisión. Esto implica que si una estación transmite datos, la otra estación no tiene que esperar a que se libere la línea para confirmar esos datos. En la figura siguiente se puede observar un intercambio de datos en un medio de transmisión dúplex. La estación A envía 3 tramas de datos y la estación B va confirmando una a una cada una de las tramas de información, I, recibidas utilizando tramas RR. En ningún caso necesita esperar a que la estación A libere la línea.

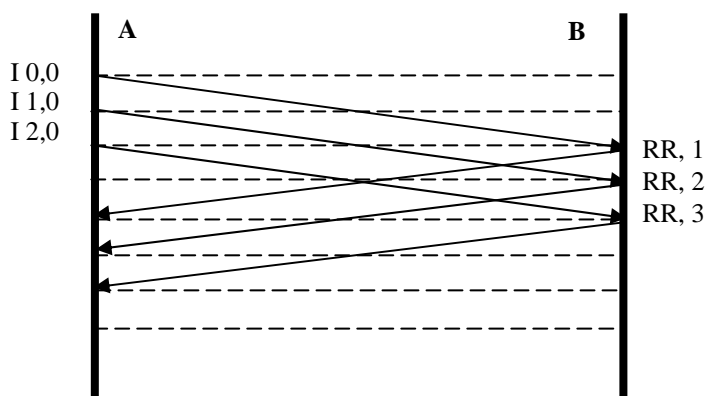


Figura 7-14: Transmisión dúplex.

Sin embargo, si el medio empleado es un medio de transmisión semiduplex. La estación que confirma los datos, no puede confirmar dichos datos hasta que el medio de transmisión queda libre. Así, en la figura 7.15, se observa como la estación A envía una ventana entera de tramas de datos, antes de ceder el turno de transmisión a la estación B para que confirme las tramas enviadas.

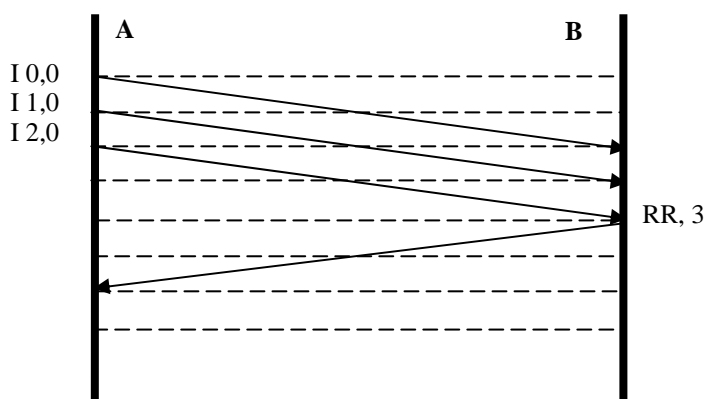


Figura 7-15: Transmisión semiduplex con  $W_t=W_e$ .

En los ejemplos anteriormente mostrados, se puede deducir fácilmente que en muchos casos el tamaño de la ventana y la configuración del modo de transmisión de la línea pueden ser incompatibles. Así, por ejemplo si la estación A tiene una ventana de emisor,  $W_e=3$ , y la ventana de B para recepción es de  $W_r=1$ , nunca podrá emplearse una línea semiduplex. Ya que el receptor, B, necesitaría confirmar cada trama I que recibe con un RR, justo en el momento de recibirla. Sin embargo, al estar el medio ocupado por las otras tramas de datos, no puede confirmarlas. Es decir, en el ejemplo, tras

recibir la trama I,0; B tendría que confirmarla con un RR,1. Sin embargo, no puede enviar esa trama de supervisión porque la línea de transmisión está ocupada aún con las tramas I1 e I2. Hasta que B no reciba I2 y la línea quede liberada, no podrá enviar el RR,1. Si el protocolo HDLC esperara a que llegase la trama I2 y la línea quedase liberada para enviar RR,1 necesitaría poder ir almacenando las tramas recibidas hasta su posterior confirmación. En cuyo caso, el sistema de ventana estaría funcionando como un ventana deslizante selectivo, y puesto que se definió el emisor como  $W_r=1$  estaríamos concurrendo en una incongruencia absurda.

Por lo tanto, HDLC la resuelve descartando los datos cuando la  $W_r < W_e$ , y la línea es semiduplex. Así, el diagrama de transmisión correcto queda contemplado en la figura 7.16.

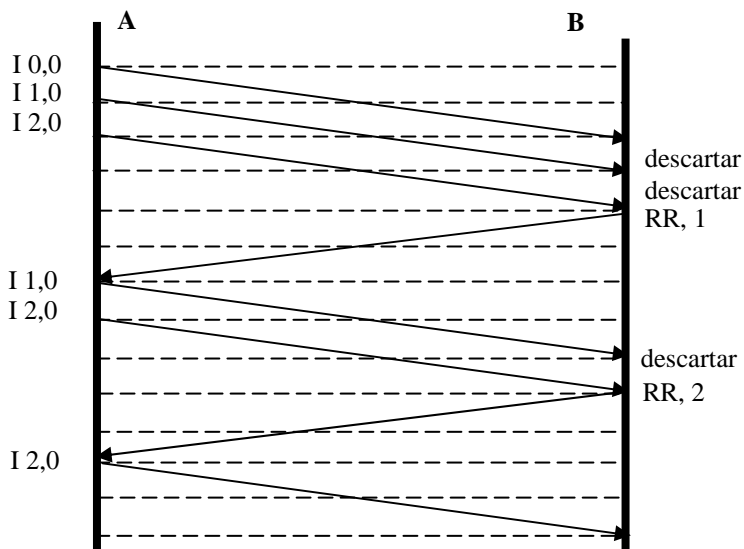


Figura 7-16: Transmisión semiduplex con  $W_r < W_e$ .

Una vez establecida la inicialización del enlace, es decir se haya realizado la conexión y esta haya sido aceptada (ver Apartados 7.3.6, 7.3.7 y 7.3.8) es posible comenzar a enviar datos mediante el empleo de tramas de información, I., empezando por el número de secuencia 0. Los campos N(R) y N(S) contendrán los números de secuencia necesarios para llevar a cabo el control de flujo y de errores.

En los ejemplos vistos en las figuras anteriores, siempre se han usado tramas de supervisión del tipo RR para confirmar las tramas recibidas. La trama RR (campo S=00) mediante el campo N(R) indica el número de secuencia de la siguiente trama que espera recibir.

### 7.3.10. Transferencia de datos con rechazos

Hasta ahora, siempre se ha supuesto que las tramas que intercambian emisor y receptor no tienen errores. Pero, ¿cómo se comportaría el protocolo HDLC en caso de recibir tramas con errores? Para ver este caso se plantean dos situaciones bien distintas. En la primera de ellas, se supone que emisor y receptor funcionan con ventanas de distinto tamaño y además, se sabe que  $W_e > W_r$ . En el segundo caso, se supone que el emisor y receptor trabajan con una ventana deslizante de igual tamaño,  $W_e = W_r$ .

En la figura 7.17 se muestra un medio de transmisión configurado en modo dúplex, y por lo tanto, se pueden enviar tramas en ambos sentidos de la transmisión. En el ejemplo, la estación A envía 3 tramas de datos: I,0,0; I,1,0 e I,2,0; y además la estación B detecta errores en la segunda de estas tramas I,1,0. Si en el control de flujo la ventana del emisor, A, es  $W_e=3$  y la ventana del receptor, B,

es  $W_r=1$ , entonces el protocolo HDLC está haciendo uso de una ventana en modo no selectivo. De ahí, que el receptor B no pueda almacenar las tramas que recibe correctamente, tras la trama de datos que contiene errores. Además el receptor B requiere confirmar todas y cada una de las tramas que le van llegando procedentes de A, una a una.

Por lo tanto, la estación B, confirma la primera trama que le llega correctamente y cuando le llega la segunda trama, es decir la trama con errores I,1,0; la descarta y envía una trama de supervisión de tipo rechazo, REJ, para solicitar el reenvío de tramas a partir de la trama que ha fallado. Esto implica que puesto que la trama que falla es I,1,0, la trama de rechazo no selectivo se haya numerado como REJ,1. Y además, la imposibilidad de aceptar tramas después del rechazo, puesto que  $W_r=1$ , obliga al receptor B a descartar todas las tramas que lleguen a continuación.

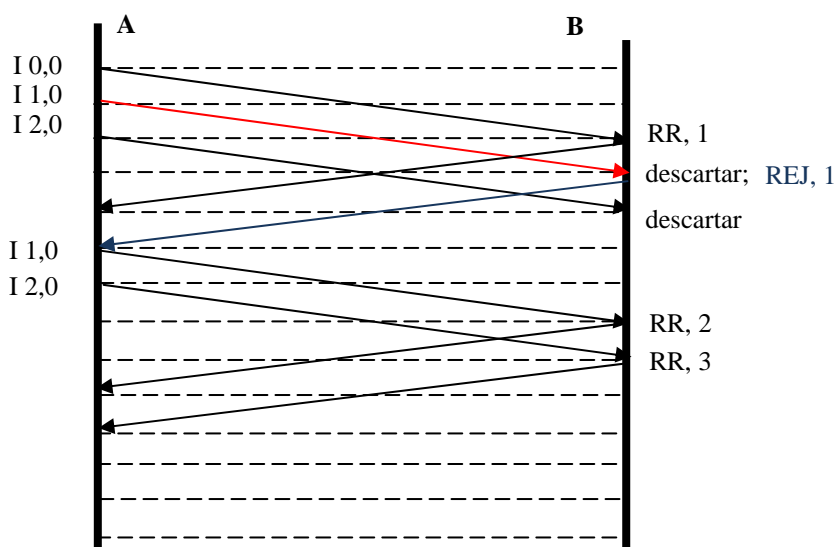


Figura 7-17: Transmisión con rechazo no selectivo.

En la figura 7.18 se muestra un medio de transmisión configurado en modo semidúplex y, por lo tanto, no se pueden enviar simultáneamente tramas en ambos sentidos de la transmisión. En el ejemplo, la estación A envía 3 tramas de datos: I,0,0; I,1,0 e I,2,0; y además la estación B detecta errores en la segunda de estas tramas I,1,0. Si en el control de flujo la ventana del emisor, A, es  $W_e=3$  y la ventana del receptor, B, también es  $W_r=3$ , entonces el protocolo HDLC está haciendo uso de una ventana en modo selectivo. Consecuentemente, el receptor B puede almacenar las tramas que recibe correctamente, tras la trama de datos que contiene errores. Además, el receptor B no requiere confirmar todas y cada una de las tramas que le van llegando procedentes de A, una a una, ya que puede emplear una única trama para confirmar todas las tramas enviadas en la ventana.

Por este motivo, la estación B, no confirma la primera trama sino que espera confirmar las tres tramas enviadas por A. Sin embargo, como la segunda trama, es decir la trama I,1,0 llega con errores; es descartada por B, sin necesidad de descartar las que llegan tras ésta. Así, la estación B, envía una trama de supervisión de tipo rechazo selectivo, SREJ para solicitar el reenvío de la trama que ha fallado y el resto de tramas I,0,0 e I,2,0 se almacenan temporalmente en un buffer a la espera de su confirmación. Esto implica que puesto que la trama que falla es I,1,0, la trama de rechazo selectivo se haya numerado como SREJ,1.

A diferencia de los ejemplos vistos en el apartado 7.3.9, en este apartado, además de emplearse tramas de supervisión del tipo RR para confirmar las tramas recibidas, se han empleado tramas de supervisión REJ (campo S=01) y SREJ (campo S=11) para solicitar el reenvío de datos erróneos.

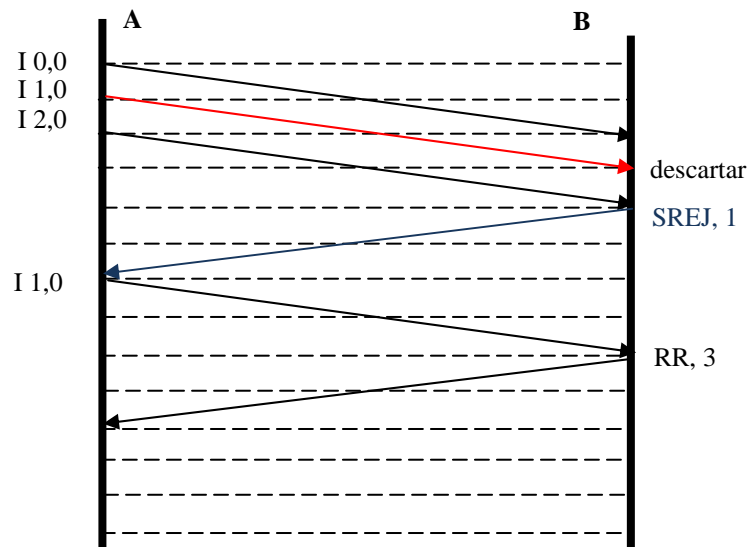


Figura 7-18: Transmisión con rechazo selectivo.

## 7.4 Protocolo PPP

---

El protocolo PPP es quizás el protocolo del nivel de enlace más empleado en cualquier tipo de conexiones punto a punto. Este protocolo se emplea tanto en conexiones por línea alquilada entre dos routers como en conexiones conmutadas entre un DTE y un router, o entre dos DTE. Algunas de estas situaciones son:

- Cuando se quiere establecer una conexión entre un particular y un proveedor de acceso a Internet, a través del empleo de un módem telefónico y la red X.25
- Cuando se quiere establecer una conexión entre un particular y un proveedor de servicios de cablemodem o xDSL. En cuyo caso, el protocolo PPP se encapsula sobre Ethernet formando lo que se conoce como protocolo PPPoE (Point to Point over Ethernet).
- Cuando se quiere establecer una conexión entre un particular y un proveedor de servicios de cablemodem o xDSL empleando un modo de transferencia asíncrona (ATM). En este caso, el protocolo PPP se encapsula sobre ATM formando lo que se conoce como protocolo PPPoA (Point to Point over ATM).

Además, del protocolo PPP, existen otros protocolos de nivel de enlace para conexiones punto a punto, como el protocolo SLIP (Serial Line Internet Protocol). No obstante, aunque el protocolo SLIP es un protocolo que está específicamente diseñado para TCP/IP, la tendencia actual es el empleo de PPP. Las diferencias entre SLIP y PPP radican en que SLIP necesita configurar algunos parámetros de forma estática. Así, SLIP necesita conocer la dirección IP de los dos extremos de la comunicación, por lo tanto se hace difícil su uso cuando alguna de estas direcciones IP se asignan dinámicamente, además de necesitar conocer la unidad máxima de transmisión del nivel de enlace (MTU), etc.

El protocolo PPP fue diseñado y desarrollado por IETF (Internet Engineering Task Force) en 1993 para solventar estas deficiencias, y proporcionar un estándar internacional para las conexiones punto a punto. El protocolo PPP define su estándar en el documento RFC 1661, el PPPoA está definido en RFC 2364 y el PPPoE en la RFC 2516.

Por lo tanto, el protocolo PPP proporciona un método estándar para transportar datagramas IP multiprotocolo (independiente de los protocolos del nivel de red empleado, ya que soporta IP, IPX y Appletalk) sobre enlaces simples punto a punto entre dos máquinas situadas en cada uno de los extremos del enlace de datos. En estos casos, la comunicación es bidireccional (full-dúplex) y los paquetes se entregan en orden.

PPP utiliza el mismo control de enlace de datos de alto nivel que HDLC como base para encapsular datagramas multiprotocolo y llevar a cabo la detección de errores. Además, hace uso de otros dos protocolos LCP (Link Control Protocol) y NCP (Network Control Protocol) para establecer la configuración del enlace de datos, y para establecer la configuración de los distintos protocolos del nivel de red que permite encapsular, respectivamente.

### 7.4.1 Estructura de la trama

La estructura de una trama PPP es la misma que la de una trama HDLC, puesto que PPP toma muchas cosas en común de éste último protocolo. El protocolo PPP emplea el mismo formato de trama comentado en la Figura 7.6. No obstante, algunos de los campos que en HDLC podían adoptar distintos valores, en PPP adquieren valores fijos (Figura 7.19).

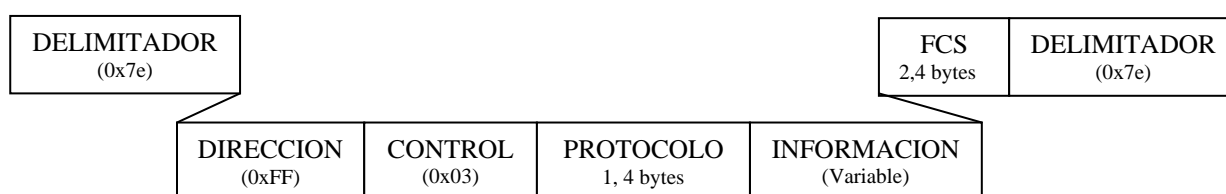


Figura 7-19: Formato de trama PPP.

El formato de una trama PPP se organiza de la siguiente manera:

- *Delimitador*: Todas las tramas comienzan y terminan con el byte ‘01111110’ (0x7e).
- *Dirección*: El campo dirección suele tener asignado el valor broadcast ‘11111111’ (0xFF).
- *Control*: El campo control tiene como valor predeterminado ‘00000011’ (0x03). Este valor indica una trama no numerada. Por lo general, PPP no proporciona numeración de tramas de datos y de asentimientos, aunque es posible numerar tramas y asentimientos cuando el ambiente en el que se transmite es ruidoso y se requiere.
- *Protocolo*: El campo protocolo es de 1 o 2 bytes y su valor identifica el contenido del datagrama almacenado en el campo información. Para que el valor del campo sea válido, el bit menos significativo del byte menos significativo debe ser ‘1’, y el bit menos significativo del byte más significativo debe ser ‘0’. En caso de no ser así, se considerará el paquete almacenado en el campo Información como irreconocible.
- *Información*: Contiene la secuencia de bits de datos correspondiente a un nivel superior cuyo protocolo se especifica en el campo Protocolo. Esta es la información que intercambian los dos dispositivos. La longitud es variable y puede tener un valor mínimo de 0 bytes y un valor máximo determinado por la MTU (por defecto 1500 bytes). A la información se le puede agregar un relleno (‘padding’) con un número arbitrario de bytes para alcanzar el valor de MTU.
- *FCS*: Es un campo de chequeo de errores o verificación. Este campo almacena una suma de comprobación y normalmente ocupa 2 bytes, aunque puede llegar a ocupar 4 bytes.

## 7.4.2 Tipos de tramas

El protocolo PPP encapsula varios tipos de paquetes en función del valor que adopte el *campo Protocolo*. Los identificadores del campo protocolo están especificados en la norma RFC 1661. Los más importantes son:

- *IP*: El campo toma el valor (0x0021).
- *LCP*: El campo toma el valor (0xc021).
- *PAP*: El campo toma el valor (0x0c23).
- *CHAP*: El campo toma el valor (0xc223).
- *NCP*: El campo toma el valor (0x...).

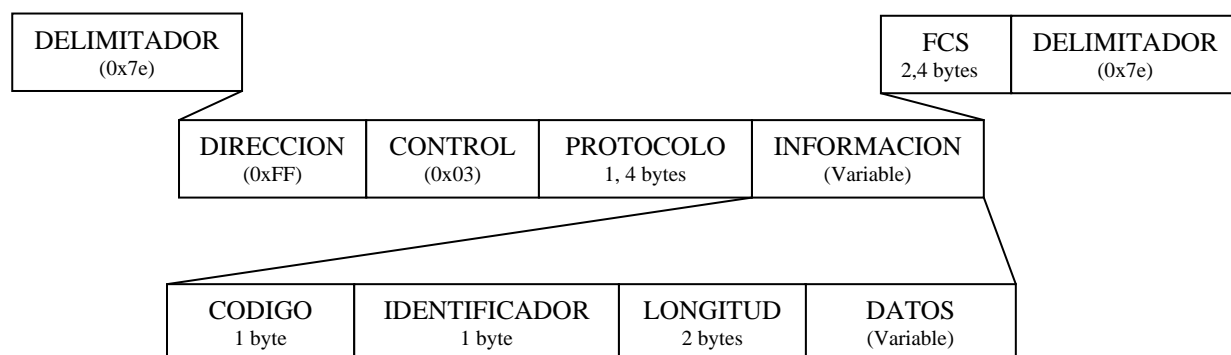


Figura 7-20: Formato de tipos de paquetes para PPP.

Cualquier tipo de paquete PPP tiene el formato que se indica en la Figura 7.20. En función del campo *protocolo* (NCP, CHAP, etc.), el campo de *Información* tendrá encapsulado además de los datos que transporta el paquete, ciertos bits adicionales. Estos bits constituyen 3 campos: *código*, *identificador* y *longitud*. El campo código se emplea para determinar la clase de paquete NCP, clase de paquete CHAP, etc. Esto es así porque dentro de los distintos protocolos que puede encapsular PPP, hay diversas clases de paquetes para cada uno de ellos. Y los otros dos campos permiten definir el número de paquete (identificador) y la longitud que ocupa el paquete (longitud).

### Paquetes LCP

Los paquetes LCP (Link Control Protocol) se emplean para negociar los parámetros del nivel de enlace en el inicio del establecimiento de la conexión. Hay 3 tipos de paquetes LCP:

- Paquetes de establecimiento que son empleados para establecer y configurar el enlace.
- Paquetes de finalización que son empleados para cerrar la conexión.
- Paquetes de testeo que son empleados para mantenimiento del enlace y chequeo de errores.

### Paquetes NCP

Los paquetes NCP (Network Control Protocol) se emplean para negociar opcionalmente parámetros de configuración para poder encapsular multiprotocolos, como por ejemplo la asignación dinámica de dirección IP.

Así, para establecer la comunicación sobre un enlace punto a punto mediante el empleo de PPP, cada extremo del enlace envía primero paquetes LCP para configurar y chequear el enlace de datos. Una vez que el enlace queda establecido, los extremos intercambian mediante el protocolo PPP paquetes NCP encapsulados para elegir y configurar uno o más protocolos de red elegidos. Después, los datagramas de cada protocolo del nivel de red podrán ser enviados a través del enlace. Finalmente, el enlace permanecerá activo hasta que una serie de paquetes NCP y/o LCP cierren la conexión, o hasta que ocurra un evento externo como por ejemplo un temporizador expirado debido a una detección de inactividad.

Más formalmente, los paquetes NCP que se intercambian son los siguientes:

- El servidor manda un NCP con código 1, 'Configure Request', indicando su dirección IP.
- El cliente responde con un NCP con código 2.

- El cliente solicita un NCP con código 1, dándole su IP=0.0.0.0 y pidiendo que se le asigne IP.
- El servidor responde con un NCP con código 3, negando esa IP y ofreciéndole una IP válida.
- El cliente solicita con un NCP con código 1 conectarse con esa IP ofrecida.
- El servidor responde con un NCP con código 2 aceptando la IP ofrecida.

### Paquetes PAP

Los paquetes PAP (Password Authentication Protocol) se emplean para autenticar un usuario que intenta acceder a un servidor de acceso remoto o a un proveedor de servicios a través de una línea alquilada. Los paquetes PAP se emplean sobre PPP para transmitir contraseñas escritas mediante códigos ASCII y además éstas están sin cifrar.

### Paquetes CHAP

Los paquetes CHAP (Challenge Handshake Authentication Protocol), también, se emplean para autenticar un usuario que intenta acceder a un servidor de acceso remoto o a un proveedor de servicios a través de una línea alquilada. La diferencia con PAP es que aquí sí se produce encriptación de la información.

CHAP permite autenticar al usuario de la siguiente manera: Primero, se establece el enlace, y posteriormente, el servidor de acceso manda un mensaje 'Challenge' CHAP para que el usuario se identifique. A continuación, el usuario responde con un valor codificado almacenado en otro paquete CHAP 'Response'. Finalmente, el servidor verifica la respuesta, comprobando el valor codificado. Si este valor coincide con el esperado por el servidor, entonces se informará al cliente de la autenticación, mediante un mensaje CHAP 'Success'. Si el valor no coincide, entonces se cerrará la conexión y se informará con un mensaje CHAP 'Failure'. El mensaje de autenticación que solicita el servidor se realiza y repite de manera aleatoria, durante la conexión.

Los dos extremos del enlace pueden intercambiar distintos paquetes CHAP, los cuales se definen a través del campo *Código* (Figura 7.20). Así, paquetes CHAP con el código a 1 indican que se envía un mensaje 'Challenge'. El mensaje 'Response' del usuario es un paquete CHAP con código 2 que indica el identificador de trama, el password y el mensaje de 'challenge' todo ello concatenado y codificado con un algoritmo de cifrado (por ejemplo MD5), y a esta cadena se le añade, también, el login sin cifrar. El servidor responde con un CHAP 'Success' código 3 si es la respuesta esperada y con CHAP 'Failure' código 4 no es la esperada.

## 7.4.3 Funcionamiento de PPP

Para describir el funcionamiento general del protocolo PPP (Figura 7.21) y cómo hace uso de los distintos paquetes que encapsula (PAP, CHAP, LCP, NCP, etc.) se ha optado ilustrarlo con un ejemplo de conexión a un router de un proveedor de servicios de Internet (ISP), por parte de un DTE de usuario que emplea un modem analógico de 56Kbps.

El funcionamiento de PPP se puede dividir en varias fases o etapas:

- *Establecimiento de la conexión:* Inicialmente, el usuario llama al router del proveedor de servicios, empleando el modem analógico. Así establece el circuito físico. Una vez, se ha establecido el circuito conmutado, el usuario hace llegar al router del proveedor de servicios un paquete LCP para negociar los parámetros del enlace de datos que

empleará PPP en el intercambio de datos. Haciendo uso de paquetes LCP se negocia también el método de autenticación que se empleará (PAP, CHAP o no se requiere).

- *Autenticación:* Si durante la fase de establecimiento se ha negociado PAP, no se requiere autenticación cifrada. Sin embargo, si por el contrario, se ha negociado CHAP se requerirá autenticación cifrada.
- *Configuración de la red:* A continuación, mediante paquetes NCP el protocolo PPP negocia los parámetros de la capa de red. Así, se configura el protocolo de red que se usa de entre todos los que se pueden encapsular sobre PPP. Por ejemplo, para un protocolo de nivel de red IP, se negocia la asignación dinámica de una IP válida. A partir de este momento, el DTE de usuario ya es una máquina de Internet y puede enviar y recibir paquetes.
- *Transmisión de datos:* Es en esta fase cuando se mandan y reciben datagramas de nivel red encapsulados en tramas PPP. Durante esa fase pueden aparecer paquetes LCP encapsulados en tramas PPP para comprobar aleatoriamente si la línea sigue activa o ha quedado inactiva durante algún periodo de tiempo.
- *Finalización:* Finalmente, cuando el intercambio de datos haya finalizado. El DTE del usuario terminará la comunicación, liberando los parámetros del nivel de red con NCP. Posteriormente, enviará paquetes LCP para liberar el enlace de datos. Y ya para concluir, cuando se cuelgue el teléfono mediante una orden del modem, se habrá liberado el circuito que había quedado definido en la capa física.

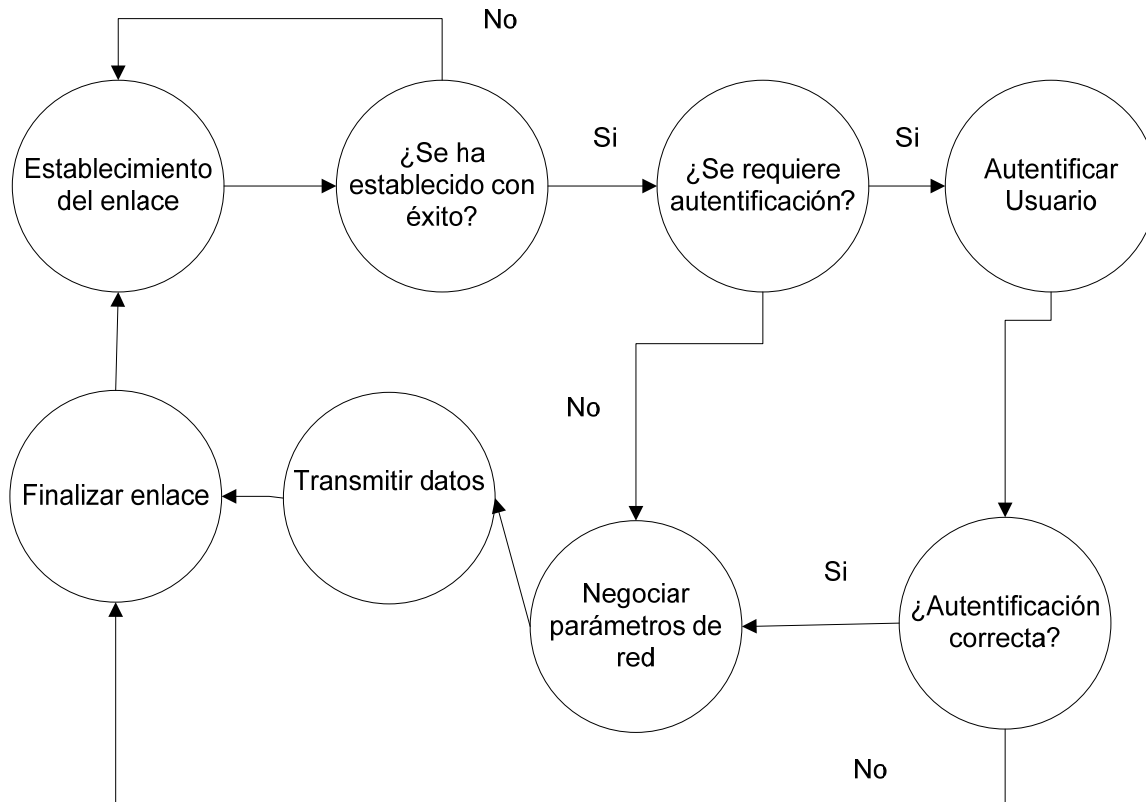


Figura 7-21: Funcionamiento general de PPP