



Router Teldat

Interfaz PPP

Doc. DM510 Rev. 8.31

Mayo, 2000

ÍNDICE

Capítulo 1 Interfaz PPP	1
1. Descripción	2
2. Estructura de la trama PPP	3
2.1. Adaptación PPP asíncrono	4
3. Control del establecimiento del enlace (LCP)	5
4. Formato de paquetes LCP	6
5. Protocolos de Autenticación	8
5.1. Password Authentication Protocol (PAP)	8
a) <i>Formato de paquetes PAP</i>	8
5.2. Challenge Authentication Protocol (CHAP)	9
a) <i>Formato de paquetes CHAP</i>	9
6. Protocolos de Control de Red (NCP)	11
7. Referencias	12
Capítulo 2 Configuración del Interfaz PPP	13
1. Asignación de interfaz PPP	14
2. Configuración del interfaz PPP-RDSI	17
3. Configuración del interfaz PPP sobre E1/PRI ISDN	21
3.1. Dial	21
a) <i>LIST</i>	21
b) <i>SET</i>	22
• SET BASE INTERFACE	22
• SET NAME-CIRCUIT	22
c) <i>EXIT</i>	22
3.2. PPP	22
3.3. EXIT	23
3.4. Configuración del interfaz E1/PRI ISDN	23
a) <i>Enlace PPP sobre canal del interfaz E1</i>	23
b) <i>Enlace PPP sobre canal Semipermanente del interfaz primario ISDN</i>	23
c) <i>Enlace PPP sobre canal Conmutado del interfaz primario ISDN</i>	23
4. Configuración del interfaz AT-PPP	24
5. Configuración del interfaz PPP	26
Capítulo 3 Configuración del interfaz MPPP	42
1. Configuración de los interfaces	43
2. Configuración de los parámetros MPPP	46
Capítulo 4 Ejemplos de configuración para acceso por RDSI	49
1. Conexión a Internet por RDSI	50
2. Conexión por RDSI en modo permanente	54
Capítulo 5 Ejemplo de configuración (Internet-Acceso por RTB)	57
1. Ejemplo de configuración (Internet-Acceso RTB)	58
Capítulo 6 Monitorización del Interfaz PPP	64
1. Estadísticos del interfaz PPP	65
2. Consola PPP	67
Capítulo 7 Eventos del Protocolo PPP	69
1. Monitorización de eventos del protocolo PPP	70
2. Ejemplo de eventos del protocolo PPP	91

Capítulo 1

Interfaz PPP



1. Descripción

El protocolo PPP (Point-to-Point Protocol) proporciona un mecanismo para transmitir datagramas de diversos protocolos sobre un enlace punto a punto. Este protocolo está especificado en la RFC-1661. El PPP soporta transmisión de datos tanto de forma síncrona como de forma asíncrona, y proporciona los siguientes servicios:

- Control de establecimiento del enlace LCP (Link Control Protocol) para establecer, configurar y comprobar el enlace.
- Encapsulado para transmitir datagramas sobre el enlace.
- Protocolos de autenticación para exigir que el extremo remoto del enlace PPP se autentique antes de poder transmitir datos por el enlace. En la implementación actual se soportan los protocolos PAP (Password Authentication Protocol) descrito en la RFC-1172 y CHAP (Challenge Handshake Authentication Protocol) definido en la RFC-1994.
- Protocolo Multilink PPP según la RFC-1990. El protocolo Multilink PPP permite dividir, recombinar y secuenciar datagramas a través de múltiples enlaces de datos. La implementación actual permite agregar canales B de RDSI a uno o varios canales lógicos MPPP. También es posible agregar interfaces PPP sobre WAN (tanto síncrono como asíncrono) a un canal MPPP, aunque en este caso únicamente se deberá agregar una interfaz PPP en cada canal MPPP.
- Protocolos de control de red NCP (Network Control Protocols) para establecer y configurar los distintos protocolos de red que viajen sobre el PPP.

Nota. En la implementación actual, el protocolo de red soportado sobre el PPP es IP (Internet Protocol), con su correspondiente protocolo de control IPCP (Internet Protocol Control Protocol) descrito en la RFC-1332.

Para realizar el establecimiento de la conexión sobre el enlace punto a punto el PPP originador enviará paquetes LCP para configurar y comprobar el enlace. Una vez que esté establecido el nivel de enlace (data-link layer) el PPP enviará los paquetes NCP correspondientes a los protocolos soportados, en este caso sólo IPCP, para configurar y establecer el nivel del red en el enlace (Network layer). Una vez que estos protocolos han sido configurados el PPP transmitirá los datagramas de cada protocolo sobre el enlace.

La adaptación para implementar el PPP de forma asíncrona se realiza según lo indicado en la RFC-1662.

En la implementación actual existen cuatro posibilidades:

1. Definir un interfaz PPP sobre línea serie en formato síncrono que mediante un cable o dispositivo externo, módem o adaptador de terminal, permita establecer un enlace con otro extremo.
2. Agregar un interfaz PPP sobre un acceso básico, para poder conectarse mediante RDSI con otro extremo. En este caso el formato de los datos en la transmisión es síncrono
3. Definir un interfaz PPP sobre línea serie en formato asíncrono que mediante un cable o dispositivo externo, módem o adaptador de terminal, permita establecer un enlace con otro extremo.
4. Agregar un interfaz PPP sobre un interfaz de comandos AT, para poder conectarse a través de un módem con otro extremo. En este caso el formato de los datos en la transmisión es asíncrono



2. Estructura de la trama PPP

El PPP transmite tramas que tienen la misma estructura que las tramas HDLC. El PPP emplea el método de transmisión síncrono orientado a bit con la siguiente estructura de trama:

FLAG	ADDRESS	CONTROL	PROTOCOLO	INFORMACION	FCS	FLAG
------	---------	---------	-----------	-------------	-----	------

FLAG

Indica el comienzo y final de cada trama con un patrón único: 01111110. Permite el sincronismo de tramas. Dentro del resto de datos de la trama se implementa la transparencia, bit-stuffing, para que no aparezca este carácter. La transparencia consiste en que en transmisión después de cinco 1 consecutivos se transmite un 0. En recepción este 0 es excluido de los datos.

ADDRESS

Campo de dirección de la trama HDLC. En el protocolo PPP siempre se emplea 11111111. No hay asignada dirección individual.

CONTROL

Campo de control. Todas las tramas PPP son tramas HDLC de Información No Numerada (UI) con este campo a valor 00000011.

PROTOCOLO

Campo de 2 bytes que diferencia a los distintos protocolos que son transmitidos sobre el enlace punto a punto. Así todos aquellos que contengan en este campo el valor Cxxx se referirán a protocolos de configuración del enlace (LCP, PAP). Los que tengan el valor 8xxx se referirán a protocolos de control de red (NCP). El valor 0xxx corresponderá a la transmisión de datagramas específicos sobre el enlace.

INFORMACIÓN

Cero o más bytes que contienen el datagrama para el protocolo transportado. En caso de que el protocolo sea LCP o NCP este campo contendrá parámetros para la configuración del enlace.

FCS

Campo empleado para incluir el mecanismo de detección de error, en este caso un código de redundancia cíclica (CRC) para detección de errores de 2 bytes.



2.1. Adaptación PPP asíncrono

Cuando el formato de transmisión de datos es asíncrono se realiza el mismo entramado que en el caso sincrónico, según se indica en la RFC-1662. Los bytes que se transmiten son encapsulados dentro de la trama descrita anteriormente, pero se emplea un carácter de transparencia, 0x7D, para implementar el bit-stuffing.

En el sentido de transmisión, después del cálculo del FCS, se examinan todos los caracteres que se van a enviar. Cada flag, carácter de control (inferior a 0x20), carácter de escape (0x7D) o cualquier otro definido en el ACCM, es sustituido por el carácter de transparencia y un carácter adicional que es el resultado del OR-exclusivo del mismo con 0x20.

En recepción, previamente a la comprobación del FCS, se examinan todos los bytes de la trama. Cuando aparece el carácter de transparencia, es eliminado, y el siguiente carácter es sustituido por su OR-exclusivo con 0x20.

El cálculo y posterior comprobación del CRC (FCS) de la trama se realiza mediante un polinomio definido en la RFC-1662, y su posterior transmisión también es afectada por la transparencia.

Así, por ejemplo, el carácter 0x11 (XON) es codificado dentro de la trama en transmisión como 0x7D + 0x31. En recepción se elimina 0x7D y el siguiente byte se sustituye por su OR exclusivo con 0x20, resultando de nuevo 0x11.



3. Control del establecimiento del enlace (LCP)

El LCP del PPP permite el establecimiento, configuración, mantenimiento y finalización de un enlace. Este proceso consta de cuatro fases:

1. Antes del intercambio de datagramas IP sobre el enlace, el LCP abre la comunicación entre los extremos mediante el intercambio de paquetes LCP del tipo CONFIGURE-REQUEST. Una vez que ha sido aceptada la configuración entre los dos extremos con paquetes del tipo CONFIGURE-ACK el enlace entra en estado "OPEN".
2. Una vez que el LCP ha determinado que el enlace está OPEN, se determina si éste tiene la calidad suficiente para arrancar los protocolos de red. Durante este proceso es donde se puede realizar, si se requiere, el procedimiento de autenticación del enlace.
3. Una vez que el LCP ha determinado que la calidad del enlace es suficiente, se arrancan los protocolos de control del nivel de red (NCP).
4. Finalmente, una vez que estos hayan sido establecidos, el LCP se encargará del mantenimiento del enlace mediante la transmisión de paquetes ECHO-REQUEST y ECHO-REPLY. Si desea finalizar la conexión (por ejemplo por tiempo de inactividad), el LCP se encarga de terminar el enlace mediante la transmisión de paquetes TERMINATE-REQUEST y TERMINATE-ACK.



4. Formato de paquetes LCP

Los paquetes LCP viajan con el mismo formato que hemos descrito anteriormente. El campo de protocolo los diferencia (C021) y en el campo de Información va codificado el tipo de paquete y los datos que lleva asociados:

CÓDIGO	IDENTIF	LONG	DATOS
--------	---------	------	-------

CÓDIGO

Campo de un byte que identifica el tipo de paquete LCP de acuerdo a la siguiente tabla:

CÓDIGO	TIPO PAQUETE LCP
1	CONFIGURE-REQUEST (Establecimiento)
2	CONFIGURE-ACK (Establecimiento)
3	CONFIGURE-NAK (Establecimiento)
4	CONFIGURE-REJECT (Establecimiento)
5	TERMINATE-REQUEST (Finalización)
6	TERMINATE-ACK (Finalización)
7	CODE-REJECT (Mantenimiento)
8	PROTOCOL-REJECT (Mantenimiento)
9	ECHO-REQUEST (Mantenimiento)
10	ECHO-REPLY (Mantenimiento)
11	DISCARD-REQUEST (Mantenimiento)

IDENTIFICADOR

Campo de un byte que permite identificar sobre el enlace peticiones y respuestas.

LONGITUD

Dos bytes que indican la longitud total de la trama LCP. En caso de que se este empleando el modo asíncrono, no se incluyen los posibles caracteres de transparencia que existan dentro de la trama.

DATOS (Opcional)

Cero o más bytes cuyo formato está relacionado con el tipo de paquete LCP sobre el que viajan. Como hemos visto en la tabla, los paquetes LCP los podemos agrupar en tres tipos:

- Paquetes para el establecimiento del enlace

- **CONFIGURE-REQUEST**

Paquete que se transmite cuando se desea abrir un enlace. En él viajan las opciones de configuración del mismo. Después de su recepción se debe de enviar una respuesta apropiada, con alguno de los siguientes paquetes.

- **CONFIGURE-ACK**

Las opciones de configuración recibidas son aceptadas. El campo de identificador de trama debe de coincidir con el del configure-request aceptado. Una vez que los dos extremos han recibido el ACK del extremo remoto el enlace entra en estado OPEN

- **CONFIGURE-NAK**



Alguna de las opciones de configuración recibidas en la trama con el identificador empleado no son aceptadas, pero se envía el valor recomendado o aceptado por el extremo. Cuando se recibe un NAK, el receptor debe de generar un nuevo CONFIGURE-REQUEST que contenga los valores aceptados indicados.

- **CONFIGURE-REJECT**

Alguna de las opciones de configuración recibidas en la trama con el identificador empleado no son aceptadas ni reconocidas. Cuando se recibe un REJECT, el receptor debe de generar un nuevo CONFIGURE-REQUEST que no contenga los valores rechazados.

- Paquetes para la finalización del enlace

- **TERMINATE-REQUEST**

Paquete que se transmite cuando se desea finalizar, cerrar, un enlace.

- **TERMINATE-ACK**

Paquete que se transmite después de la recepción de un TERMINATE-REQUEST. La recepción de un paquete TERMINATE-ACK no esperado indica que el enlace ha sido cerrado.

- Paquetes para el mantenimiento del enlace

- **CODE-REJECT**

Indica que se ha recibido un paquete LCP incompleto o con código no reconocido. Si se persiste en la transmisión del citado paquete, el enlace terminará cerrándose.

- **PROTOCOL-REJECT**

Indica que se ha recibido una trama PPP con un campo de protocolo no implementado. El extremo receptor de la trama deberá de cesar en el envío del citado protocolo.

- **ECHO-REQUEST Y ECHO-REPLY**

Proporcionan un mecanismo de mantenimiento del enlace. Cada cierto tiempo se genera una consulta con código ECHO-REQUEST que debe de ser devuelta con un ECHO-REPLY.

- **DISCARD-REQUEST**

Proporcionan un mecanismo para el descarte, eliminación, de tramas. Es empleado para pruebas.



5. Protocolos de Autenticación

El PPP dispone de una serie de protocolos que permiten autenticar y verificar un enlace, el cual únicamente se establecerá en el caso de que se compruebe que los valores de login (usuario) y password (clave) esperados en un extremo son los adecuados. Este método es habitualmente empleado en enlaces en los que los routers se conectan a una red vía circuitos conmutados (RDSI o RTB), aunque también puede ser empleada en circuitos punto a punto.

Esta comprobación se realiza previamente al establecimiento de los protocolos de control de red (NCP). En caso de que la autenticación sea exigida y no se complete de forma correcta se finalizará el establecimiento del enlace.

Existen dos métodos de autenticación definidos en la RFC -1334. Estos son:

5.1. Password Authentication Protocol (PAP)

Proporciona un método simple para autenticar un enlace, usando un establecimiento de 2 vías:

1. Una vez que se alcanza el estado OPEN en la negociación de los LCP, el extremo que desea conectarse envía al autenticador un usuario (login) y una clave (password).
2. El extremo que la recibe comprueba si es válida y envía la respuesta adecuada: aceptada o no la llamada.

Este método de autenticación no es muy seguro, debido a que tanto el usuario como la clave que se envían por la red viajan en “claro”, por lo que no disponen de ningún tipo de protección contra errores u otro tipo de ataques. Este problema es resuelto por el otro método de autenticación, CHAP.

a) Formato de paquetes PAP

Los paquetes PAP viajan con el mismo formato que hemos descrito para las tramas PPP. El campo de protocolo los diferencia (C023) y en el campo de Información va codificado el tipo de paquete y los datos que lleva asociados:

CÓDIGO	IDENTIF	LONG	DATOS
--------	---------	------	-------

CÓDIGO

Campo de un byte que identifica el tipo de paquete LCP de acuerdo a la siguiente tabla:

CÓDIGO	TIPO PAQUETE PAP
1	AUTHENTICATE-REQUEST
2	AUTHENTICATE-ACK
3	AUTHENTICATE-NAK

IDENTIFICADOR

Campo de un byte que permite identificar sobre el enlace peticiones y respuestas.

LONGITUD

Dos bytes que indican la longitud total de la trama PAP.



DATOS (Opcional)

Cero o más bytes cuyo formato está relacionado con el tipo de paquete PAP sobre el que viajan. Como hemos visto en la tabla, los paquetes PAP los podemos agrupar en tres tipos:

- **AUTHENTICATE-REQUEST**

Paquete que se transmite cuando se desea autenticar un enlace. En el viajan la clave y password empleados. Después de su recepción se debe de enviar una respuesta apropiada, con alguno de los siguientes paquetes.

- **AUTHENTICATE-ACK**

Los valores recibidos son aceptados. El campo de identificador de trama debe de coincidir con el del authenticate-request aceptado. Una vez que se ha recibido el ACK del extremo autenticador se puede proceder con el establecimiento de los protocolos de red (NCP).

- **AUTHENTICATE-NAK**

Los valores recibidos no son aceptados. El extremo que desea autenticar el enlace deberá de enviar un nuevo request con valores adecuados o finalizar el enlace.

5.2. Challenge Authentication Protocol (CHAP)

Proporciona un método “seguro” para autenticar un enlace, usando un establecimiento de 3 etapas:

1. Una vez que se alcanza el estado OPEN en la negociación de los LCP, el extremo autenticador envía una clave al extremo que desea conectarse, denominada Challenge. Esta clave es variable en todas las conexiones, generalmente es un valor aleatorio cuyo número de bytes depende del algoritmo empleado para el cifrado posterior. En este caso el método implementado es el algoritmo MD5, definido en la recomendación RFC 1321, que define una longitud de 16 bytes para el challenge.
2. El extremo que la recibe cifra con la clave recibida la clave (password) que tenga programada y envía la respuesta al extremo autenticador. La función de cifrado es la definida por el algoritmo MD5 y es la misma en ambos extremos.
3. Al recibir la respuesta, el autenticador verificará que lo recibido es lo esperado y permitirá (success) o no (failed) la continuación en el establecimiento de los protocolos de red.

La seguridad de este método depende del secreto de la clave en ambos extremos. En este método, la clave nunca viaja en “claro” por la red.

Además, este método permite la autenticación del enlace incluso una vez que se hayan establecido los protocolos de red (por ejemplo IP), para verificar la seguridad del mismo.

a) Formato de paquetes CHAP

Los paquetes CHAP viajan con el mismo formato que hemos descrito para las tramas PPP. El campo de protocolo los diferencia (C223) y en el campo de Información va codificado el tipo de paquete y los datos que lleva asociados:

CÓDIGO	IDENTIF	LONG	DATOS
--------	---------	------	-------

CÓDIGO

Campo de un byte que identifica el tipo de paquete LCP de acuerdo a la siguiente tabla:

CÓDIGO	TIPO PAQUETE CHAP
1	CHALLENGE



2	RESPONSE
3	SUCCESS
4	FAILED

IDENTIFICADOR

Campo de un byte que permite identificar sobre el enlace peticiones y respuestas.

LONGITUD

Dos bytes que indican la longitud total de la trama CHAP.

DATOS (Opcional)

Cero o más bytes cuyo formato está relacionado con el tipo de paquete CHAP sobre el que viajan.

Como hemos visto en la tabla, los paquetes CHAP los podemos agrupar en cuatro tipos:

- **CHALLENGE**

Paquete que se transmite por el extremo autenticador cuando se desea autenticar un enlace. En el viajan la clave que se debe de emplear para cifrar. Además puede viajar en claro el nombre de la red a la que se desea acceder. Este valor puede ser empleado en el caso de que el extremo que debe de enviar la respuesta envíe el valor adecuado en el caso de que este preparado para conectarse a distintas redes, es decir, puede programar distintas claves en función de la red a la que se desea conectar.

- **RESPONSE**

Paquete que envía el extremo en el que viaja el password cifrado con la clave recibida.

- **SUCCESS**

El valor recibido es aceptado. Una vez que se ha recibido el SUCCESS del extremo autenticador se puede proceder con el establecimiento de los protocolos de red (NCP).

- **FAILED**

El valor recibido no es aceptado. El extremo que desea autenticar el enlace deberá de enviar una nueva respuesta con valores adecuados o finalizar el enlace.



6. Protocolos de Control de Red (NCP)

El PPP dispone de una serie de protocolos de control de red NCP (Network Control Protocol), para establecer y configurar distintos protocolos de red que viajan sobre el PPP. El NCP correspondiente a cada protocolo será el encargado de configurar , habilitar y deshabilitar los protocolos de red entre ambos extremos del enlace.

Para la actual implementación del **Router Teldat** el único protocolo implementado es IPCP (Internet Protocol Control Protocol), descrito en la recomendación RFC-1332.

El IPCP permite indicar si se emplea o no compresión de Van Jacobson, y así mismo permite un mecanismo para intercambiar las direcciones IP entre ambos extremos o la asignación dinámica de número IP, requerida para conexiones a Infovía e Internet.



7. Referencias

- RFC-1661: The Point to Point protocol, W. Simpson, Julio-1994
- RFC-1662: PPP in HDLC-Like Framing, W. Simpson, Julio-1994
- RFC-1618: PPP in ISDN, W.Simpson, Mayo-1994
- RFC-1570: PPP LCP extensions, W. Simpson, Enero-1994
- RFC-1332: PPP Internet control protocol, G. McGregor, Mayo-1992
- RFC-1334: PPP Authentication protocols, B. Lloyd, Octubre-1992
- RFC-1172: Point-to-Point Protocol (PPP) initial configuration options. D. Perkins, R. Hobby. Julio-1990
- RFC-1994: PPP Challenge Handshake Authentication Protocol (CHAP). W. Simpson. Agosto-1996
- RFC-1321: The MD5 message-digest Algorithm. R. Rivest, Abril-1992
- RFC-1700: Assigned numbers, IETF, Octubre-1994
- RFC-1471: The Definitions of Managed Objects for the Link Control Protocol of the Point-to-Point Protocol, F. Kastenholz , Agosto-1993
- RFC-1631: The IP Network Address Translator (NAT) , Egevang & Francis, Mayo-1994
- RFC-1990: The PPP Multilink Protocol (MP), Network Working Group, Agosto-1996.



Capítulo 2

Configuración del Interfaz PPP



1. Asignación de interfaz PPP

- Para el caso de que se desee configurar un interfaz serie como interfaz PPP SINCRONO, desde el menú de configuración teclear:

```
Config>SET DATA-LINK PPP
which port will be changed[1]? 1
Config>
```

- Para el caso de que se desee configurar un interfaz serie como interfaz PPP ASINCRONO, desde el menú de configuración teclear:

```
Config>SET DATA-LINK ASPPP
which port will be changed[1]? 2
Config>
```

- En caso de que se desee configurar un interfaz PPP sobre un acceso básico RDSI se deberá de introducir:

```
Config>ADD DEVICE PPP-DIAL
Type basic access ISDN [2]? 1
If you are going to config more than two DIAL interfaces, you must config what t
hey have CSR:F011640 and CSR:F011660 over the ISDN 2 connector
Ifc number to delete: [0]? 7
Added PPP-DIAL interface with num: 4
Config>
```

Las versiones antiguas del **Router Teldat** soportaban un máximo de dos canales B, uno en cada conector RDSI. Desde la versión 6.0 se soportan hasta cuatro canales B si el equipo dispone de 6 líneas serie. Durante el proceso de agregar el interfaz PPP-DIAL se debe indicar la línea serie que se desea intercambiar por un tercer o cuarto canal B. Las líneas series disponibles para el intercambio son la 5 y la 6. Por tanto los canales B PPP-DIAL se pueden agregar siempre a costa de perder canales B X.25 o las líneas series 5 y 6. Es por esto que a la hora de agregar un interfaz PPP-DIAL se pregunta el interfaz a eliminar. Dicho interfaz será siempre un canal B X.25 o las líneas serie 5 ó 6.

NOTA: Para poder utilizar un tercer o cuarto canal B es necesario que los jumpers JP10 del equipo se encuentren en la posición RDSI. Si, por el contrario, se desean utilizar las líneas serie 5 y 6, dichos jumpers deberán situarse en la posición DTE5.

- En el caso de que se desee configurar un interfaz PPP sobre un canal B de un interfaz E1/PRI ISDN (E1 ó Primario RDSI) se deberá teclear:

```
Config>ADD DEVICE PPP-DIAL
Added PPP-DIAL interface with num: 2
Config>
```

Podemos comprobar que se ha añadido correctamente el interfaz creado listando los interfaces (y verificando que se ha generado un interfaz del tipo *PPP Generic Dial*):



```

Config>LIST DEVICES

Con   Ifc  Type of interface          CSR   CSR2  int
---   ---  ---
---   2   PPP Generic Dial          0     0     0
---   3   PPP Generic Dial          0     0     0
---   4   PPP Generic Dial          0     0     0
---   5   Router->Node              0     0     0
---   6   Node->Router              0     0     0
ISDN 1   1   G.703 port (E1)          F001600  F000C00  9E
LAN   0   Ethernet                  A000000  1D
WAN1  7   X25                       F001620  F000D00  9D
Config>

```

El **Router Teldat** con interfaz E1/PRI ISDN soporta un enlace de 2048 Kbps según las recomendaciones G.703 y G.704 con 30 ó 31 canales B disponibles en un principio. Durante el proceso de agregar el interfaz PPP-DIAL no hay que indicar nada sobre el tipo y número de canal sobre el que se desea establecer la conexión PPP ya que estos parámetros se configurarán posteriormente.

NOTA: El método de agregar interfaces PPP-DIAL es idéntico tanto cuando se trata de un acceso básico RDSI como cuando se añaden sobre un interfaz E1/Primario RDSI. Esto no da lugar a ambigüedades debido a que los routers disponen del hardware correspondiente a uno de los tipos de interfaz. Si está instalada la tarjeta que soporta el interfaz G.703 a 2048 Kbps el router la detecta y a partir de ese instante la configuración de los interfaces PPP-DIAL se hará sobre dicho interfaz.

- En caso de que se desee configurar un interfaz PPP sobre un interfaz de comandos AT se deberá de introducir:

```

Config>ADD DEVICE ATPPP-DIAL
which port will be changed[0]? 1
Added ATPPP-DIAL interface with num: 3
Config>

```

NOTA: El driver del interfaz siempre deberá de estar configurado como DTE.

Para todos los tipos de interfaces PPP disponibles, el protocolo de red soportado es el IP. Para activar este protocolo sobre cada uno de las interfaces PPP es necesario asignar una dirección IP a la interfaz, lo cual se realiza desde el menú de configuración del protocolo IP. Esta operación siempre se debe de realizar independientemente de que el interfaz vaya o no a obtener una dirección IP dinámica. Además debe notarse que no están soportadas más de una dirección IP por interfaz PPP, ya que el protocolo IPCP permite configurar una única dirección IP por interfaz. Por lo tanto no deben agregarse direcciones adicionales a los interfaces PPP.

A continuación se muestra cómo se debe realizar este proceso.



```

*PROCESS 4
User Configuration
Config>PROTOCOL IP
Internet protocol user configuration
IP config>ADD ADDRESS
Which net is this address for[0]? 5
New address [0.0.0.0]? 192.168.5.1
Address mask [255.255.255.0]? 255.255.255.0
IP config>LIST ADDRESSES
IP addresses for each interface:
  intf 0 192.7.1.252      255.255.255.0   NETWORK broadcast,   fill 0
  intf 1 192.168.1.1     255.255.255.0   NETWORK broadcast,   fill 0
  intf 2                                     IP disabled on this interface
  intf 3                                     IP disabled on this interface
  intf 4 192.168.4.1     255.255.255.0   NETWORK broadcast,   fill 0
  intf 5 192.168.5.1     255.255.255.0   NETWORK broadcast,   fill 0
  intf 6                                     IP disabled on this interface
IP config>EXIT
Config>SAVE
Save configuration [n]? Y

Saving configuration...OK
Config>

```



2. Configuración del interfaz PPP-RDSI

Para configurar un interfaz PPP-DIAL sobre RDSI debe teclearse **NETWORK n** desde el menú general de configuración, donde **n** es el número de interfaz. Por ejemplo si el interfaz 5 es un interfaz PPP-DIAL, se deberá teclear:

```
Config>NETWORK 5
Circuit Config
Circuit Config>
```

Las opciones desde el menú de configuración del interfaz PPP sobre RDSI son las siguientes:

```
Circuit Config>?
DISABLE
ENCAPSULATOR
ENABLE
LIST
SET
EXIT
```

LIST

Permite ver las opciones programada en lo referente al interfaz PPP sobre RDSI.

```
Circuit Config>LIST
Base interface: -1
Destination address:
Inactive time: 60
Permitted caller:
Circuit name:
Outgoing calls allowed: Yes
Incoming calls allowed: No
Control access enabled: No
Circuit Config>
```

“*Base interface*” se refiere al número del interfaz RDSI sobre el que se establece el enlace PPP.

“*Destination address*” es la dirección RDSI a la que se conectará el equipo.

“*Inactive time*” permite determinar el tiempo tras el cual se liberará una llamada establecida en ausencia de tráfico IP.

“*Outgoing calls allowed*” e “*Incoming calls allowed*” indican la posibilidad de hacer y recibir llamadas.

“*Control access enabled*” indica si se validará la pareja dirección destino/dirección origen con la lista global de parejas autorizadas. Dicha lista se configura en la facilidad global de control de acceso.

Si el interfaz base asociado está configurado en modo permanente se indica con un texto, y se omite la mayor parte de la información pues no es significativa.

```
Circuit Config>LIST
Base interface: 2 (permanent)
Circuit name:
Circuit Config>
```



SET INACTIVE TIME

```
Circuit Config>SET INACTIVE-TIME
Inactive time(0:always active)(0-65535)[60]? 120
Circuit Config>
```

Esta opción permite determinar el tiempo tras el cual se liberará una llamada establecida en ausencia de tráfico IP. En este caso la llamada a la dirección destino se efectuará cuando se detecte tráfico IP. Si el tiempo seleccionado es 0 la conexión se establecerá en ausencia de tráfico IP y no desconectará nunca.

SET DESTINATION-ADDRESS

```
Circuit Config>SET DESTINATION-ADDRESS
Destination address[]? 912579000
Circuit Config>
```

La dirección de destino es la dirección RDSI a la que se conectará el equipo.

SET PERMITTED-CALLER

```
Circuit Config>SET PERMITTED-CALLER
Permitted caller[]? 913004000
Circuit Config>
```

Con este parámetro se determina la dirección RDSI origen permitida. Por defecto (dirección vacía) se aceptan todas las llamadas RDSI.

SET BASE-INTERFACE

Permite configurar el interfaz base RDSI a utilizar con el interfaz PPP. Cada interfaz base RDSI está asociado a un canal B del acceso básico. De esta manera se puede controlar el acceso de múltiples PPP a los canales B del acceso básico RDSI.

Por defecto toma el valor -1 indicando que el interfaz PPP utilizará el primer canal B del acceso básico que encuentre.

```
Circuit Config>SET BASE-INTERFACE
Base interface:[-1]? 1
Circuit Config>
```

Si se configura como interfaz base el -1 y hay varios interfaces bases RDSI (alguno de ellos operando en modo permanente), en la asociación tienen preferencia los interfaces base que operan en modo permanente frente a los que operan en modo conmutado. No tiene sentido asociar más de una interfaz PPP a un interfaz base RDSI que opere en modo permanente pues sólo se utilizará el primero.

Para más información sobre los interfaces base RDSI consulte el capítulo 4.

SET NAME-CIRCUIT

Este parámetro es meramente informativo. Permite asociar una cadena de caracteres al interfaz.



```
Circuit Config>SET NAME-CIRCUIT  
Assign circuit name[]? Internet  
Circuit Config>
```

ENABLE/DISABLE OUTGOING

Con esta pareja de comandos es posible determinar si el equipo realizará llamadas salientes por la interfaz PPP sobre RDSI que se está configurando o, por el contrario, si el equipo no realizará llamadas.

```
Circuit Config>ENABLE OUTGOING  
Circuit Config>DISABLE OUTGOING  
Circuit Config>
```

ENABLE/DISABLE INCOMING

Al igual que en el caso anterior, el equipo puede contestar a las llamadas entrantes o ignorarlas.

```
Circuit Config>ENABLE INCOMING  
Circuit Config>DISABLE INCOMING  
Circuit Config>
```

ENABLE/DISABLE ACCESS

Permite al usuario determinar si se utilizará o no (habilitada/deshabilitada) la tabla de acceso global, con parejas dirección destino/dirección origen autorizadas, para establecer una llamada RDSI.

```
Circuit Config>ENABLE ACCESS  
Circuit Config>DISABLE ACCESS  
Circuit Config>
```

La tabla de acceso global es común a todos los interfaces y se configura desde el menú de configuración del control de acceso, al cual se accede desde el menú principal de configuración utilizando el comando **FEATURE CONTROL-ACCESS**. Desde el prompt *CtrlAcc Config>* se puede agregar, listar o borrar parejas dirección destino/dirección origen autorizadas.

```
Config>FEATURE CONTROL-ACCESS  
CtrlAcc Config>  
ADD  
CLEAR  
LIST  
EXIT  
CtrlAcc Config>ADD  
Destination address? 384760  
Permitted caller? 389010  
Enter another pair of addresses(Yes/No)? N  
CtrlAcc Config>LIST  
  
Destination address      Permitted caller  
-----  
384760                   389010  
CtrlAcc Config>
```

Con el comando **CLEAR** se permite borrar una pareja destino/origen, todas las entradas para una dirección destino dada o toda la tabla:

```
CtrlAcc Config>CLEAR ?  
ALL  
DESTINATION  
LOCAL-DESTINATION  
CtrlAcc Config>
```

Por ejemplo, para borrar una pareja destino/origen:



```
CtrlAcc Config>CLEAR LOCAL-DESTINATION  
Destination address? 384760  
Permitted caller? 389010  
Clear another pair of addresses(Yes/No)? N  
CtrlAcc Config>
```

ENCAPSULADOR

Permite acceder a la programación de los parámetros propios del interfaz PPP. Para configurar los parámetros propios de un interfaz PPP consultar el apartado 4, “*Configuración del interfaz PPP*”.

```
Circuit Config>ENCAPSULATOR  
  
-- Interface PPP. Configuration --  
PPP Config>
```

EXIT

Con este comando abandonamos la configuración de la interfaz PPP-DIAL y retornamos al menú principal de configuración.

```
Circuit Config>EXIT  
Config>
```



3. Configuración del interfaz PPP sobre E1/PRI ISDN

Para configurar un interfaz PPP-DIAL sobre un interfaz de tipo E1/PRI ISDN debe teclearse **NETWORK n** desde el menú general de configuración, donde **n** es el número de interfaz. Por ejemplo si el interfaz 2 es un interfaz de tipo *PPP Generic Dial*, se debe teclear:

```
Config>NETWORK 2
PPP-DIAL User Config
PPPD Cfg>
```

Las opciones desde el menú de configuración del interfaz PPP-DIAL son las siguientes:

```
PPPD Cfg>?
DIAL
PPP
EXIT
PPPD Cfg>
```

3.1. Dial

Permite acceder al menú de configuración de la parte asociada a la llamada del interfaz PPP-DIAL, con el prompt asociado *Dial Config*>. En el menú de configuración *Dial Config*> se especifican los parámetros relacionados con la asociación del enlace PPP sobre el interfaz E1/PRI ISDN.

```
PPPD Cfg>DIAL
Dial Config
Dial Config>
```

Dentro del menú *Dial Config*, disponemos de los siguientes comandos:

```
Dial Config>?
LIST
SET
EXIT
Dial Config>
```

a) LIST

Permite visualizar las opciones configuradas para la parte de “DIAL” del interfaz.

```
Dial Config>LIST
Circuit name      : PRUEBA
Base interface    : 1
Base circuit id   : 2
Dial Config>
```

“*Circuit name*” es el nombre del perfil de llamada asociado al interfaz PPP-DIAL. Es el identificador relaciona al circuito con las características de llamada que va a tener (dirección origen, dirección destino, tipo de llamadas permitidas, etc.).

“*Base interface*” se refiere al número de interfaz base sobre el que se establece el interfaz PPP (en este caso deberá ser el número del interfaz asociado a un *E1* o *PRIMARIO RDSI*).

“*Base circuit id*” es el número de canal B sobre el que se quiere establecer la conexión PPP dentro de la trama del *E1* o *PRIMARIO RDSI*. El contenido de este parámetro será tenido en cuenta por parte del sistema dependiendo del tipo de canal sobre el que desea establecer el



enlace PPP (semipermanente o conmutado). Además, en el caso de tener establecido el interfaz como Primario RDSI, no se puede utilizar el canal 16, reservado para la señalización RDSI.

b) SET

El comando SET permite configurar los valores de los parámetros asociados a la parte “DIAL” del interfaz *PPP Generic Dial*.

• SET BASE INTERFACE

Mediante este comando especificamos el número de interfaz asociado al interfaz base (E1 o Primario RDSI, según los casos) así como el número de canal B (válido sólo en el caso de semipermanentes).

```
Dial Config>SET BASE-INTERFACE
Base interface:[1]?
Base circuit id:[255]?1
Dial Config>
```

NOTA: El número de canal (Base circuit id) sólo tiene validez en el caso de conexiones PPP sobre canales SEMIPERMANENTES, ya que en el caso de enlaces sobre canales conmutados, el canal se asigna en el momento de realizar la llamada. El número 255 indica que no se configura ningún canal en particular, por lo que si se trata de conexiones semipermanentes no funcionará el enlace.

Además, en el caso de enlace PPP sobre canal semipermanente de Primario RDSI no se puede configurar el canal 16 (circuit id).

• SET NAME-CIRCUIT

Permite asignar el *Perfil de Llamada* del enlace. Este parámetro asocia el enlace con el perfil de llamada indicado (que contiene datos como qué tipo de llamadas se permiten, hacia dónde dirigir las llamadas salientes, qué llamadas entrantes se permiten, cuál es el tiempo de inactividad, así como si están habilitados los controles de acceso). Este parámetro es imprescindible cuando se trabaja sobre Primario RDSI; si no hay un perfil de llamada asociado, el enlace no se establecerá (igual que si se asocia un perfil que no existe o no está configurado). En el caso de E1 este parámetro deja de tener sentido, por lo que se ignora su contenido.

```
Dial Config>SET NAME-CIRCUIT
Assign circuit name[CIRCUIT1]?
Dial Config>
```

c) EXIT

Sale del prompt de configuración *Dial Config>*.

```
Dial Config>EXIT
PPPD Cfg>
```

3.2. PPP

Permite acceder a la programación de los parámetros propios del interfaz PPP. Para configurar los parámetros característicos de un interfaz PPP consultar el apartado 5, “*Configuración del interfaz PPP*”.



```
PPPD Cfg>PPP
-- Interface PPP. Configuration --
PPP Config>
```

3.3. EXIT

Salte del prompt de configuración PPP-DIAL, *PPPD Cfg>*.

```
PPPD Cfg>EXIT
Config>
```

3.4. Configuración del interfaz E1/PRI ISDN

Para establecer correctamente un enlace PPP-DIAL sobre un interfaz de tipo E1/PRI ISDN hay que configurar adecuadamente ciertos parámetros del interfaz E1/PRI ISDN según el comportamiento que se desea especificar. Las posibilidades que se presentan son:

a) Enlace PPP sobre canal del interfaz E1

En este caso las conexiones son siempre sobre canal semipermanente. Hay que configurar el interfaz E1/PRI ISDN para que funcione en modo E1. Para ver cómo se configura el interfaz E1/PRI ISDN consúltese el manual Dm 529 “Interfaz E1/PRI ISDN”.

b) Enlace PPP sobre canal Semipermanente del interfaz primario ISDN

En primer lugar se configura el interfaz E1/PRI ISDN para que se comporte como Primario RDSI. En este caso se tendrá que configurar el canal sobre el que se quiere establecer la conexión PPP como *PVC*. Para ver cómo se configura el interfaz E1/PRI ISDN consúltese el manual Dm 529 “Interfaz E1/PRI ISDN”.

c) Enlace PPP sobre canal Conmutado del interfaz primario ISDN

Como en el caso anterior, se configura el interfaz E1/PRI ISDN como Primario RDSI. Tendrá que haber algún canal del interfaz configurado como conmutado (*SVC*). Para ver cómo se configura el interfaz E1/PRI ISDN consúltese el manual Dm 529 “Interfaz E1/PRI ISDN”.



4. Configuración del interfaz AT-PPP

Para configurar un interfaz ATPPP-DIAL sobre un interfaz de comandos AT, debe teclearse **NETWORK n** desde el menú general de configuración, donde **n** es el número de interfaz. Por ejemplo si el interfaz 2 es un interfaz ATPPP-DIAL, se deberá teclear:

```
Config>NETWORK 2
Circuit Config
Circuit Config>
```

Las opciones desde el menú de configuración del interfaz PPP sobre comandos AT son las siguientes:

```
Circuit Config>?
SET
ENCAPSULATOR
LIST
EXIT
Circuit Config>
```

LIST

Permite ver las opciones programadas en lo referente al interfaz PPP sobre comandos AT.

```
Circuit Config>LIST
Base interface: 1
Destination address:
Inactive time: 60
Circuit Config>
```

“*Base interface*” se refiere al número del interfaz sobre el que se establece el interfaz de comandos AT.

“*Destination address*” es la dirección telefónica a la que se conectará el equipo.

“*Inactive time*” permite determinar el tiempo tras el cual se liberará una llamada establecida en ausencia de tráfico IP.

SET INACTIVE-TIME

Esta opción permite determinar el tiempo tras el cual se liberará una llamada establecida en ausencia de tráfico IP. En este caso la llamada a la dirección destino se efectuará cuando se detecte tráfico IP. Si el tiempo seleccionado es 0 la conexión se establecerá en ausencia de tráfico IP y no se desconectará nunca.

```
Circuit Config>SET INACTIVE-TIME
Inactive time(0:always active)(0-65535)[60]? 120
Circuit Config>
```

SET DESTINATION-ADDRESS

La dirección destino es la dirección a la que se conectará el equipo.

```
Circuit Config>SET DESTINATION-ADDRESS
Destination address[?] 912579000
Circuit Config>
```

ENCAPSULATOR

Permite acceder a la programación de los parámetros propios del interfaz PPP como se describe en el próximo apartado.



```
Circuit Config>ENCAPSULATOR  
ASYNCHRONOUS PPP  
  
-- Interface PPP. Configuration --  
PPP Config>
```

EXIT

Con este comando abandonamos la configuración de la interfaz ATPPP-DIAL y retornamos al menú principal de configuración.

```
Circuit Config>EXIT  
Config>
```



5. Configuración del interfaz PPP

Para los interfaces PPP-DIAL (PPP sobre canal B de RDSI Básico) y ATPPP-DIAL (PPP sobre interfaz de comandos AT) la configuración de los parámetros propios del interfaz PPP se realiza ejecutando el comando **ENCAPSULATOR** desde el menú de configuración del interfaz DIAL. Por ejemplo, para un interfaz ATPPP-DIAL sería:

```
Config>NETWORK 2
Circuit Config
Circuit Config>ENCAPSULATOR
ASYNCHRONOUS PPP

-- Interface PPP. Configuration --
PPP Config>
```

Para los interfaces PPP-DIAL sobre E1/PRI ISDN (canal B de enlace E1 o Primario RDSI) se accede al prompt de configuración de la parte PPP propiamente dicha mediante el comando **PPP** desde el prompt de configuración del interfaz PPP-E1/PRI ISDN (*PPPD Cfg>*):

```
PPPD Cfg>PPP

-- Interface PPP. Configuration --
PPP Config>
```

Para los interfaces PPP síncrono y asíncrono por línea serie, la configuración de los parámetros propios de PPP se realiza en el propio interfaz. Por ejemplo, para un interfaz PPP síncrono sobre línea serie se deberá teclear, suponiendo que el interfaz PPP es el número 3, lo siguiente:

```
Config>NETWORK 3

-- Interface PPP. Configuration --
PPP Config>
```

Los comandos disponibles son:

? (AYUDA)

Permite, en cualquier momento ver las opciones disponibles desde el menú de configuración en el que nos encontremos. A continuación de un comando permite ver cuales son las opciones disponibles para ese comando. Las opciones desde el menú de configuración del interfaz PPP son las siguientes:

```
PPP Config>?
LIST
SET
ENABLE
DISABLE
ADD
DELETE
EXIT
PPP Config>
```

LIST

Permite ver las opciones programadas en lo referente al interfaz PPP.



```

PPP Config>LIST ?
ALL
LINE
LCP
NCP
IPCP
AUTHENTICATION
FACILITY
USERS
INTERVAL-OF-CONNECTION
PPP Config>

```

LIST ALL

Lista todas las opciones programadas para el interfaz PPP.

LIST LINE

```

PPP Config>LIST LINE

Line Options
-----
Maximum Frame (MTU in bytes)      : 1500
Encoding                          : NRZ
Idle                              : FLAG
Clocking                          : EXTERNAL
Cable                             : DTE
Line speed (bps)                  : 64000
Transmit delay (sec)              : 0
PPP Config>

```

La descripción de los parámetros es la siguiente:

“*Maximum Frame*”: máximo tamaño de trama que se envía sobre el enlace PPP.

“*Encoding*”: tipo de codificación empleado para la transmisión, **NRZ** o **NRZI**.

“*Idle*”: indica el estado de la línea durante los periodos de reposo, **FLAG** o **MARK**. En caso de que el interfaz sea asíncrono, la inactividad consiste en la transmisión de 1’s binarios.

“*Clocking*”: indica si se el equipo proporciona el reloj del enlace (**INTERNAL**) o si obtiene el reloj del enlace (**EXTERNAL**). Sólo aparecerá si el interfaz PPP esta instalado sobre la línea serie sincrona.

“*Cable*”: indica el tipo de interfaz empleado, **DTE** o **DCE**. Sólo aparecerá si el interfaz PPP está instalado sobre la línea serie. En caso de que la interfaz PPP sea sobre comandos AT, el tipo de interfaz empleado siempre será **DTE**.

“*Line speed*”: velocidad de la línea que se está empleando.

“*Transmit delay*”: mínimo periodo de tiempo entre la transmisión de tramas sucesivas. El valor por defecto es 0, y significa que no hay restricciones.



LIST LCP

```
PPP Config>LIST LCP

LCP Parameters
-----
Tries Configure-Request      : 10
Tries Configure-Nak         : 10
Tries Terminate-Request     : 10
Timer between tries (sec)   : 3

LCP Options
-----
Interface MRU (bytes)       : 1500
Magic Number                : YES
Asynchronous Control Character Map : NO
Protocol Field Compression  : NO
Address Control Field Compression : NO
PPP Config>
```

Parámetros LCP:

“*Tries Configure-Request*”: indica la veces que se transmitirá un LCP CONFIGURE-REQUEST para establecer el enlace PPP.

“*Tries Configure-Nak*”: indica el número máximo de rechazos de trama CONFIGURE-REQUEST durante el establecimiento del enlace que se transmitirán antes de finalizarlo por no encontrar configuración compatible entre ambos extremos.

“*Tries Terminate-Request*”: indica el número de veces que se transmitirá la trama TERMINATE-REQUEST sin detectar respuesta de TERMINATE-ACK para finalizar un enlace de forma ordenada.

“*Timer between tries*”: tiempo entre transmisiones consecutivas de LCPs CONFIGURE-REQUEST, TERMINATE-REQUEST y ECHO-REPLY cuando no se recibe la contestación de forma adecuada.

Opciones LCP:

“*Interface MRU*”: máximo tamaño de trama PPP que será aceptada en recepción.

“*Magic Number*”: indica si se emplea o no la opción de número mágico a la hora de establecer el enlace.

“*Asynchronous Control Character Map*”: indica si se emplea o no la transparencia en transmisión sobre los caracteres de control (por ejemplo XON, XOFF) en caso de PPP asíncrono. Esto permite que cuando estos caracteres estén incluidos dentro de la trama no provoquen activación de los procesos de control de flujo en los módem o adaptadores empleados para la conexión.

“*Protocol Field Compression*”: indica si se emplea o no esta opción en el establecimiento del enlace. Consiste en que una vez negociados los LCP y establecido el NCP, el campo de protocolo de la trama PPP es comprimido y sólo se transmite un byte.

“*Address Control Field Compression*”: indica si se emplea o no esta opción en el establecimiento del enlace. Consiste en que una vez negociados los LCP y establecido el NCP, los campos de control y de dirección de la trama PPP no son transmitidos

LIST NCP

```
PPP Config>LIST NCP

NCP Parameters
-----
Tries Configure-Request      : 10
Tries Configure-Nak         : 10
Tries Terminate-Request     : 10
Timer between tries (sec)   : 3
PPP Config>
```



Parámetros NCP:

“*Tries Configure-Request*”: indica la veces que se transmitirá un NCP CONFIGURE-REQUEST para establecer el protocolo de red.

“*Tries Configure-Nak*”: indica el número máximo de rechazos de trama CONFIGURE-REQUEST durante el establecimiento del protocolo de red que se transmitirán antes de finalizarlo por no encontrar configuración compatible entre ambos extremos.

“*Tries Terminate-Request*”: indica el número de veces que se transmitirá la trama TERMINATE-REQUEST sin detectar respuesta de TERMINATE-ACK para finalizar un protocolo de red de forma ordenada.

“*Timer between tries*”: tiempo entre transmisiones consecutivas de NCP’s CONFIGURE-REQUEST y TERMINATE-REQUEST cuando no se recibe la contestación de forma adecuada.

LIST IPCP

```
PPP Config>LIST IPCP

IPCP Options
-----
IP Van Jacobson Compression      : NO
CRTP Compression                 : NO
IP get local address             : NO
IP mask local address            : 255.255.255.255
IP send address                  : YES
IP request remote address        : YES
IP remote address                : 0.0.0.0
PPP Config>
```

Opciones IPCP:

“*IP Van Jacobson Compression*”: indica si se emplea o no compresión de Van Jacobson.

“*CRTP Compression*”: indica si se emplea o no la compresión CRTP (RFC-2508). Sólo es posible configurar una de las dos compresiones.

“*IP get local address*”: indica si se solicita asignación de número IP al establecer el enlace, como es necesario en el caso de conexiones a Internet o Infovía Plus. El valor por defecto es no.

“*IP mask local address*”: en caso de solicitar asignación de número IP, indica la máscara a asociar al número IP. El valor por defecto es 255.255.255.255. Si se configura al valor 0.0.0.0, la máscara que se toma es la de la clase de la dirección.

“*IP send address*”: en caso de que no exista petición de número IP, indica si se transmite o no el número IP configurado para el interfaz. El valor por defecto es si.

“*IP request remote address*”: indica si se requiere o no la transmisión del número IP del extremo remoto. El valor por defecto es si.

“*IP remote address*”: en caso de que el extremo remoto solicite asignación de número IP, determina el número IP a transmitir. El valor por defecto es 0.0.0.0. Este valor indica que el número IP a enviar, es igual al primer número IP asignado al interfaz del extremo local por el que se establece la conexión PPP, menos 1. En esta situación, si el número IP del interfaz es la primera dirección (no broadcast) de la subred, se transmite este número IP mas 1, y si el número IP del interfaz es una dirección no numerada, es decir, del tipo 0.X.X.X, se cierra la conexión si el extremo remoto, solicita asignación de número IP.



LIST AUTHENTICATION

```
PPP Config>LIST AUTHENTICATION

Authentication Options
-----
Login:      teldat
Password:   *****
PPP Config>
```

Permite visualizar las opciones programadas para realizar la autenticación del enlace.

La autenticación implementada se realiza mediante el protocolo Password Authentication Protocol (PAP) o el protocolo Challenge Authentication Protocol, descritos en la RFC-1334. Estos protocolos permiten establecer un enlace únicamente cuando se proporciona un usuario y una clave correctos. Una vez finalizada la autenticación, si es correcta se pasará a negociar los protocolos de red del enlace.

Casos de acceso a Internet. Cuando se accede a una conexión a Internet el extremo remoto solicita un nombre de usuario y una clave para determinar quien debe de proporcionar el número IP en la conexión. Cuando el acceso se realiza a Internet, debe de ser el Centro Proveedor de Acceso que el usuario haya contratado el que proporcionará un número IP de los que tenga asignados.

LIST FACILITY

```
PPP Config>LIST FACILITY

Facilities
-----
NAT Disable
Authentication Disable
CRTP Compression Disable
Avoid RIP dial-up Disable
Multilink PPP Disable
Callback Disable
Backup Disable
PPP Config>
```

Permite comprobar en que estado se encuentran las facilidades disponibles para el protocolo PPP:

“*NAT*”: la facilidad “*Network Address Translator*” permite a elementos de una misma red compartir una única dirección IP.

“*Authentication*”: indica si el router va a exigir o no autenticación al extremo remoto durante la negociación para establecer el enlace. En caso de que este habilitada se indica que tipo de protocolo de autenticación se va a exigir al otro extremo, PAP o CHAP.

“*CRTP Compression*”: indica si el router tiene habilitada la compresión CRTP. Esta configuración es independiente de la opción que habilita la negociación de la compresión CRTP dentro del IPCP.

“*Multilink PPP*”: indica si el interfaz pertenece a un multienlace PPP. Esta facilidad sólo está disponible para interfaces PPP-DIAL (PPP sobre canal B de RDSI) y PPP sobre línea serie. El interfaz multilink PPP debe existir con antelación en el equipo. Para agregar un interfaz multilink PPP debe usarse el comando **ADD DEVICE MPPP** desde el menú general de configuración. Consultar la sección “Habilitar MPPP”.

“*Callback*”: indica si el interfaz puede ser activado en remoto mediante una llamada RDSI. Esta facilidad sólo está disponible para interfaces PPP-DIAL (PPP sobre canal B de RDSI). Si se quiere impedir que cualquier número remoto pueda activar el enlace, se debe configurar el llamante autorizado con el número deseado.

“*Backup*”: indica si el interfaz tiene configurado un interfaz de respaldo. Esta facilidad sólo está disponible para interfaces PPP-DIAL (PPP sobre canal B de RDSI).



LIST USERS

Muestra una lista de los usuarios autorizados para conectarse al equipo. Las claves son los valores permitidos en la autenticación exigida al extremo remoto. Para más información consultar la sección “ADD USERS”.

```
PPP Config>LIST USERS
N. Login                Password
-----
0  remoteuser_2         password_2
1  remoteuser_1         password_1
PPP Config>
```

LIST INTERVAL-OF-CONNECTION

Muestra el intervalo de tiempo para el que la conexión está permitida. Para más información consultar la sección “SET INTERVAL-OF-CONNECTION”.

```
PPP Config>LIST INTERVAL-OF-CONNECTION
Interval of connection:
Start: 00:00, End: 23:59, Days: S-M-T-W-T-F-S, Disconnection: YES
PPP Config>
```

SET

Permite modificar las opciones programadas en lo referente al interfaz PPP.

```
PPP Config>SET ?
LINE
LCP
NCP
IPCP
AUTHENTICATION
INTERVAL-OF-CONNECTION
PPP Config>
```

SET LINE

```
PPP Config>SET LINE ?
ENCODING
IDLE
FRAME-SIZE
LINE-SPEED
TRANSMIT-DELAY
PPP Config>
```

La descripción de los parámetros es la siguiente:

“*ENCODING*”: tipo de codificación empleado para la transmisión, NRZ, NRZI. El valor por defecto es NRZ.

“*IDLE*”: indica el estado de la línea durante los periodos de reposo, FLAG o MARK. El valor por defecto es FLAG.

“*FRAME-SIZE*”: máximo tamaño de trama que se envía sobre el enlace PPP. El rango está comprendido entre los valores 576 y 4.098 . El valor por defecto es 1.500.

“*LINE-SPEED*”: velocidad de la línea que se está empleando para el caso de que se configure como DCE o que el interfaz sea asíncrono. Esta opción no es modificable para el caso de PPP-DIAL (PPP sobre canal B RDSI).

“*TRANSMIT-DELAY*”: mínimo periodo de tiempo entre la transmisión de tramas sucesivas.



SET LINE ENCODING

```
PPP Config>SET LINE ENCODING ?
NRZI
NRZ
PPP Config>
```

SET LINE IDLE

```
PPP Config>SET LINE IDLE ?
FLAG
MARK
PPP Config>
```

SET LINE FRAME-SIZE

```
PPP Config>SET LINE FRAME-SIZE
Maximum Frame (MTU in bytes)      : [1500]? 100
Frame (MTU) is not in range (576-4089)
PPP Config>
```

SET LINE-SPEED

```
PPP Config>SET LINE LINE-SPEED
Line speed (bps)                   : [64000]? 100
Access speed is not in range (300-2048000)
PPP Config>
```

El valor por defecto de esta opción es 64000. En el caso de PPP sobre RDSI, esta opción no es modificable.

SET LINE TRANSMIT-DELAY

```
PPP Config>SET LINE TRANSMIT-DELAY
Transmit delay (sec)               : [0]? 0
PPP Config>
```

SET LCP

```
PPP Config>SET LCP ?
OPTIONS
PARAMETERS
PPP Config>
```

SET LCP OPTIONS

```
PPP Config>SET LCP OPTIONS
Interface MRU (bytes)              : [1500]? 1500
Magic Number                       : (Yes/No)(Y)? Y
Asynchronous Control Character Map : (Yes/No)(N)? N
Protocol Field Compression         : (Yes/No)(N)? N
Address Control Field Compression  : (Yes/No)(N)? N
PPP Config>
```

“*Interface MRU*”: máximo tamaño de trama PPP que será aceptada en recepción. El valor por defecto es 1.500. El rango está comprendido entre los valores 576 y 4.089.

“*Magic Number*”: indica si se emplea o no la opción de número mágico a la hora de establecer el enlace. Sirve para poder detectar si el enlace está en bucle o no mediante la transmisión de un número aleatorio entre los dos extremos basado en el reloj del sistema y el número de veces que se ha reiniciado éste. El número mágico tiene 4 bytes. La opción por defecto es SI.



“*Asynchronous Control Character Map*”: indica si se emplea o no la transparencia en transmisión sobre los caracteres de control (por ejemplo XON, XOFF) en caso de PPP asíncrono. Esto permite que cuando estos caracteres estén incluidos dentro de la trama no provoquen activación de los procesos de control de flujo en los módem o adaptadores empleados para la conexión. Es recomendable que en conexiones asíncronas la opción sea SI. Cuando esta opción es elegida la mascarará de caracteres de control (inferiores al carácter hexadecimal 0x20) a los que se aplicará la transparencia es 0x00A0 (únicamente a XON y XOFF)

“*Protocol Field Compression*”. indica si se emplea o no esta opción en el establecimiento del enlace. Permite prescindir del campo de protocolo una vez establecido el enlace. La opción por defecto es No. Es recomendable que en conexiones asíncronas la opción sea SI.

“*Address Control Field Compression*”: indica si se emplea o no esta opción en el establecimiento del enlace. Permite prescindir de los campos de control y direcciones una vez establecido el enlace. La opción por defecto es No. Es recomendable que en conexiones asíncronas la opción sea SI.

SET LCP PARAMETERS

```
PPP Config>SET LCP PARAMETERS
Tries Configure-Request      : [10]? 10
Tries Configure-Nak         : [10]? 10
Tries Terminate-Request     : [10]? 10
Timer between tries (sec)   : [3]? 3
PPP Config>
```

Parámetros LCP:

“*Tries Configure-Request*”: indica las veces que se transmitirá un LCP CONFIGURE-REQUEST para establecer el enlace PPP. Los valores permitidos están comprendidos entre 1 y 100. Por defecto es 10.

“*Tries Configure-Nak*”: indica el número máximo de rechazos de trama CONFIGURE-REQUEST durante el establecimiento del enlace que se transmitirán antes de finalizarlo por no encontrar configuración compatible entre ambos extremos. Los valores permitidos están comprendidos entre 1 y 100. El valor por defecto es 10.

“*Tries Terminate-Request*”: indica el número de veces que se transmitirá la trama TERMINATE-REQUEST sin detectar respuesta de TERMINATE-ACK para finalizar un enlace de forma ordenada. Los valores permitidos están comprendidos entre 1 y 20. El valor por defecto es 10.

“*Timer between tries*”: tiempo entre transmisiones consecutivas de LCP’s CONFIGURE-REQUEST, TERMINATE-REQUEST y ECHO-REPLY cuando no se recibe la contestación de forma adecuada. Los valores permitidos están comprendidos entre 1 y 30 segundos. El valor por defecto es 3.

SET NCP

```
PPP Config>SET NCP
Tries Configure-Request      : [10]? 10
Tries Configure-Nak         : [10]? 10
Tries Terminate-Request     : [10]? 10
Timer between tries (sec)   : [3]? 3
PPP Config>
```

Parámetros NCP:

“*Tries Configure-Request*”: indica las veces que se transmitirá un NCP CONFIGURE-REQUEST para establecer el protocolo de red. Los valores permitidos están comprendidos entre 1 y 100. El valor por defecto es 10.

“*Tries Configure-Nak*”: indica el número máximo de rechazos de trama CONFIGURE-REQUEST durante el establecimiento del protocolo de red que se transmitirán antes de finalizarlo por no encontrar



configuración compatible entre ambos extremos. Los valores permitidos están comprendidos entre 1 y 100. El valor por defecto es 10.

“*Tries Terminate-Request*”: indica el número de veces que se transmitirá la trama TERMINATE-REQUEST sin detectar respuesta de TERMINATE-ACK para finalizar un protocolo de red de forma ordenada. Los valores permitidos están comprendidos entre 1 y 20. El valor por defecto es 10.

“*Timer between tries*”: tiempo entre transmisiones consecutivas de NCPs CONFIGURE-REQUEST y TERMINATE-REQUEST cuando no se recibe la contestación de forma adecuada. Los valores permitidos están comprendidos entre 1 y 30 segundos. El valor por defecto es 3.

SET IPCP

```
PPP Config>SET IPCP
IP Van Jacobson Compression      : (Yes/No)(N)? N
CRTP Compression                 : (Yes/No)(N)? N
IP get local address             : (Yes/No)(N)? Y
IP mask local address            : [255.255.255.255]? 255.255.255.255
IP send address                  : (Yes/No)(Y)? Y
IP request remote address        : (Yes/No)(Y)? Y
IP remote address                : [0.0.0.0]? 0.0.0.0
PPP Config>
```

Opciones IPCP:

“*IP Van Jacobson Compression*”: indica si se emplea o no compresión de Van Jacobson. El valor por defecto es NO.

“*CRTP Compression*”: indica si se usa o no la compresión CRTP. El valor por defecto es NO.

“*IP get local address*”: indica si se solicita asignación de número IP al establecer el enlace, como es necesario en el caso de conexiones a Internet. El número IP asignado puede ser visualizado desde la consola. El valor por defecto es NO.

“*IP mask local address*”: en caso de solicitar asignación de número IP, indica la máscara a asociar al número IP. El valor por defecto es 255.255.255.255. Si se configura al valor 0.0.0.0, la máscara que se toma es la de la clase de la dirección.

“*IP send address*”: en caso de que no exista petición de número IP indica si se transmite o no el número IP configurado para el interfaz. El valor por defecto es YES.

“*IP request remote address*”: indica si se requiere o no la transmisión del número IP del extremo remoto. El número IP del extremo remoto puede ser visualizado desde la consola. El valor por defecto es YES.

“*IP remote address*”: en caso de que el extremo remoto solicite asignación de número IP, determina el número IP a transmitir. El valor por defecto es 0.0.0.0. Este valor indica que el número IP a enviar, es igual al primer número IP asignado al interfaz del extremo local por el que se establece la conexión PPP, menos 1. En esta situación, si el número IP del interfaz es la primera dirección (no broadcast) de la subred, se transmite este número IP mas 1, y si el número IP del interfaz es una dirección no numerada, es decir, del tipo 0.X.X.X, se cierra la conexión si el extremo remoto, solicita asignación de número IP.



SET AUTHENTICATION

```
PPP Config>SET AUTHENTICATION
Login:      []? teldat
Password:   *****
Password:   *****
PPP Config>
```

Permite programar el usuario y clave que serán enviados durante el proceso de autenticación en conexiones a Internet. Por defecto, tanto el usuario como la clave no están configurados.

Si el extremo remoto solicita autenticación, serán estos valores los que se envíen para autenticar el enlace según el protocolo seleccionado: si es PAP serán enviados en claro, y si es CHAP serán enviados cifrados mediante el algoritmo MD5 con una clave enviada previamente por el extremo autenticador.

Es importante destacar que la autenticación aquí configurada es la autenticación con la que el equipo se indentifica ante el extremo remoto en el caso en que el extremo remoto pida dicha autenticación. Esto es diferente de la autenticación que el router puede solicitar al extremo remoto, que se configura con los comandos **ENABLE AUTHENTICATION** (PAP o CHAP) y **ADD USERS**.

SET INTERVAL-OF-CONNECTION

Permite especificar un intervalo, fuera del cual el equipo no se podrá conectar con la red externa, incluso aunque haya tráfico que cursar.

En el intervalo permitido de conexión se definen los días de la semana permitidos y la hora de comienzo y final del intervalo permitido. Si la hora de comienzo es posterior a la de final, querrá decir que hay un cambio de día en el intervalo permitido, si no, todas las horas del intervalo son del mismo día.

Si el tiempo de liberación por ausencia de datos es cero, se garantiza que la conexión permanecerá establecida mientras estemos dentro del intervalo permitido de conexión, aunque no haya tráfico que cursar. Esto es, la conexión se establecerá automáticamente cuando se entre en el intervalo permitido y se desconectará, también automáticamente, cuando se salga del intervalo permitido.

El intervalo tiene una precisión de un minuto, esto es, desde que el reloj del router marca el comienzo o final del intervalo hasta que el equipo se conecta o desconecta, respectivamente, puede pasar como mucho un minuto.

Además el intervalo de conexión permite que una vez fuera del intervalo de conexión, la llamada se desconecte inmediatamente aunque se esté cursando tráfico o tras el tiempo de liberación por ausencia de datos.

En el siguiente ejemplo se configura un intervalo en el que se permite la conexión en todo momento, que es la configuración por defecto.



```

PPP Config>SET INTERVAL-OF-CONNECTION
Insert hour of the beginning of the allowed interval of connection [0]? 0
Insert minute of the beginning of the allowed interval of connection [0]? 0
Insert hour of the end of the allowed interval of connection [23]? 23
Insert minute of the end of the allowed interval of connection [59]? 59
Sunday (Yes/No)(Y)? Y
Monday (Yes/No)(Y)? Y
Tuesday (Yes/No)(Y)? Y
Wednesday (Yes/No)(Y)? Y
Thursday (Yes/No)(Y)? Y
Friday (Yes/No)(Y)? Y
Saturday (Yes/No)(Y)? Y
Do you wish disconnection when leaving the interval (Yes/No)(Y)? Y
PPP Config>

```

ENABLE

Permite activar determinadas facilidades del PPP sobre este interfaz.

```

PPP Config>ENABLE ?
NAT
AUTHENTICATION
MPPP
CALLBACK
BACKUP
CRTP
RIP-NO-DIAL
PPP Config>

```

ENABLE NAT

Permite activar la facilidad NAT, Network Address Translator, sobre el interfaz PPP. Esta opción es empleada en el caso de accesos a Internet, que permite habilitar los procedimientos de cambio de direcciones IP descritos en la RFC "The IP Network Address Translator (NAT)", RFC 1631 y el Internet Draft "Extending NAT".

La activación se realiza mediante el comando:

```

PPP Config>ENABLE NAT
PPP Config>

```

ENABLE AUTHENTICATION

Permite activar la facilidad de autenticación según el protocolo seleccionado, Password Authentication Protocol (PAP) o Challenge Authentication Protocol (CHAP).

En caso de que la facilidad de autenticación se encuentre habilitada se exigirá al extremo remoto que envíe el login y el password de acuerdo al método que se haya seleccionado. Solamente se podrá establecer el enlace en el caso de que el proceso se haya completado con éxito.

En ambos casos, el usuario, con su correspondiente clave, debe haber sido añadido en la tabla de usuarios permitidos con el comando **ADD USERS**.

```

PPP Config>ENABLE AUTHENTICATION ?
PAP
CHAP
PPP Config>

```

Para habilitar el PAP:

```

PPP Config>ENABLE AUTHENTICATION PAP
PPP Config>

```

Para habilitar el CHAP:



```
PPP Config>ENABLE AUTHENTICATION CHAP
PPP Config>
```

A la hora de procesar la facilidad de autenticación se tendrán en cuenta:

Si el extremo local ha sido programado con autenticación habilitada pero se recibe en los paquetes LCP del extremo remoto solicitud de autenticación, independientemente del método seleccionado, se sigue la solicitada por el extremo remoto, enviando el login y password que se hayan programado.

Si el extremo local con autenticación habilitada no recibe solicitud de autenticación del extremo remoto la exigirá de acuerdo al método seleccionado.

En el caso de que se exija autenticación, todos los paquetes de negociación de protocolos de red (NCP's) serán descartados hasta que no se haya completado con éxito este proceso.

ENABLE MPPP

Esta facilidad agrega el enlace PPP-DIAL (PPP sobre canal B de RDSI) a un mazo Multilink PPP. También es posible agregar un enlace PPP sobre línea serie a un mazo MPPP, pero en este caso únicamente deberá pertenecer dicho enlace al mazo MPPP.

El interfaz MPPP debe existir previamente en el equipo. Para agregar un interfaz MPPP debe usarse el comando **ADD DEVICE MPPP** desde el menú general de configuración.

```
PPP Config>ENABLE MPPP
Enter Multilink PPP interface this one belongs to[0]? 4
PPP Config>
```

En el ejemplo, el interfaz MPPP es el número 4 del equipo.

ENABLE CALLBACK

Indica que el interfaz puede ser activado en remoto mediante una llamada RDSI. Esta facilidad sólo está disponible para interfaces PPP-DIAL (PPP sobre canal B de RDSI). Si se quiere impedir que cualquier número remoto pueda activar el enlace, se debe configurar el llamante autorizado con el número deseado.

```
PPP Config>ENABLE CALLBACK
Authorized calling number: []? 347821
PPP Config>
```

ENABLE BACKUP

Indica que el interfaz tiene configurado un interfaz de respaldo. Esta facilidad sólo está disponible para interfaces PPP-DIAL (PPP sobre canal B de RDSI). El interfaz de respaldo puede ser PPP sobre canal B de RDSI o PPP sobre interfaz de comandos AT.

Las condiciones que provocan el paso a backup de un interfaz PPP-DIAL son dos:

1. **Timeout de IPCP.** Que pasado un tiempo configurable desde que se solicitó la conexión, el protocolo IPCP del enlace PPP de la conexión RDSI no esté establecido, esto es, no se haya llegado a establecer el nivel IP en la conexión.
2. **Número máximo de intentos de llamada.** Que desde que se solicita la conexión, se realicen un máximo de intentos de llamada sin éxito, esto es, sin llegar a establecerse la llamada RDSI. Nótese que en cuanto la llamada RDSI se establezca, será considerada como válida, independientemente del éxito o fracaso de la negociación PPP posterior.



Estas dos condiciones actúan simultáneamente, de tal forma que la primera que se cumpla provoca el paso a backup. Si la llamada se establece normalmente y el IPCP se negocia en el plazo fijado, el paso a backup no se produce. Si se pasa a backup, los parámetros de backup se activan, las rutas del canal con fallo se cambian a la conexión de backup, para garantizar el tráfico del usuario, y se realiza la llamada de backup. Los parámetros configurables en el backup son los siguientes:

1. **Outgoing Interface.** Es el interfaz por el que se intentará la llamada de backup. Puede ser un interfaz PPP sobre canal B de RDSI, incluido el propio interfaz, o un interfaz PPP sobre comandos AT.
2. **Priority.** Indica qué canal B RDSI tiene más prioridad en el caso en que dos canales B RDSI tengan habilitado el backup por el mismo interfaz de salida. La prioridad puede ser alta o baja. El canal B con mayor prioridad “ganará” el interfaz de salida si ambos canales B lo solicitan a la vez. Además echará al otro canal B de su interfaz de salida si el de prioridad baja está cursando un backup y el de prioridad alta solicita backup por el mismo interfaz de salida. Si las prioridades son iguales, ningún canal tiene prioridad sobre el otro en caso de coincidir en la solicitud de backup.
3. **IPCP Timeout.** Es el tiempo máximo que puede transcurrir desde que se solicita una conexión hasta que se dispara el backup de esa conexión si en ese tiempo no se ha establecido el IPCP.
4. **Maximum number of calls.** Es el número máximo de intentos de llamada RDSI consecutivos y sin éxito permitidos antes de que se dispare el backup.
5. **Telephone.** Es el número de teléfono destino de la conexión de backup. Este teléfono puede ser el mismo que el de la conexión que está fallando o puede ser otro número distinto.
6. **Login y password.** Son el usuario y password empleados para identificar la conexión de backup. Pueden ser el mismo usuario y password que los de la conexión que está fallando o pueden ser otro usuario y password diferentes. Tiene sentido que el usuario y password de backup sean los mismos que el de la conexión que está fallando, si el interfaz de salida es PPP sobre comandos AT o si el teléfono de backup es diferente, para por ejemplo, hacer backup contra otro extremo remoto.



```

PPP Config>ENABLE BACKUP
Outgoing interface: [0]? 2
Priority (1.- Low, 2.- High): [2]? 1
IPCP timeout: [60]? 60
Call attempts before entering backup: [2]? 2
Backup telephone: []? 987654321
Login: usuario
Password: *****
Password: *****
PPP Config>LIST FACILITY

Facilities
-----
NAT Disable
Authenticacion Disable
CRTP Compression Disable
Avoid RIP dial-up Disable
Multilink PPP Disable
Callback Disable
Backup Enable:
  Out.Inter. Priority IPCP T-Out Call Telephone User
  -----
  2           Low    60          2    987654321 usuario
PPP Config>

```

ENABLE CRTP

Permite Habilitar la compresión CRTP. Se puede configurar el envío del checksum de UDP en la cabecera comprimida.

```

PPP Config>ENABLE CRTP
UDP Checksum (0.- Enabled, 1.- Disabled): [0]? 1
PPP Config>

```

ENABLE RIP-NO-DIAL

Cuando se habilita una interfaz PPP-DIAL para que realice llamadas salientes se presenta un problema si además está habilitado el protocolo RIP sobre dicha interfaz. Éste consiste en que el protocolo RIP empezará a mandar paquetes IP sobre la interfaz PPP, forzando la llamada por tráfico. Además, y debido a que el protocolo RIP manda mensajes cada cierto tiempo, la llamada nunca se liberará por ausencia de tráfico.

Para corregir este problema en aquellos casos que se desee usar enrutamiento dinámico se ha establecido esta opción. Si se habilita, los paquetes RIP no provocarán la generación de una llamada saliente y tampoco se considerarán a la hora de liberar una llamada previamente establecida (es decir, si el único tráfico IP que existe en el enlace es debido al protocolo RIP, la llamada se liberará).

```

PPP Config>ENABLE RIP-NO-DIAL
PPP Config>

```

DISABLE

Permite deshabilitar determinadas facilidades del PPP sobre este interfaz.

```

PPP Config>DISABLE ?
NAT
AUTHENTICATION
MPPP
CALLBACK
BACKUP
CRTP
RIP-NO-DIAL
PPP Config>

```



DISABLE NAT

Permite deshabilitar la facilidad NAT, Network Address Translator, sobre el interfaz PPP. Esta opción es la que se deberá de emplear en el caso de que el router sea utilizado para efectuar el acceso a redes privadas (intranets).

```
PPP Config>DISABLE NAT
PPP Config>
```

DISABLE AUTHENTICATION

Permite deshabilitar la facilidad de autenticación. No se exigirá autenticación al extremo remoto para establecer un enlace.

```
PPP Config>DISABLE AUTHENTICATION
PPP Config>
```

DISABLE MPPP

Excluye el interfaz del mazo Multilink PPP.

```
PPP Config>DISABLE MPPP
PPP Config>
```

DISABLE CALLBACK

Deshabilita la facilidad de callback de este interfaz.

```
PPP Config>DISABLE CALLBACK
PPP Config>
```

DISABLE BACKUP

Deshabilita la facilidad de backup de este interfaz.

```
PPP Config>DISABLE BACKUP
PPP Config>
```

DISABLE CRTP

Deshabilita la compresión CRTP.

```
PPP Config>DISABLE CRTP
PPP Config>
```

DISABLE RIP-NO-DIAL

Deshabilitando esta opción, el tráfico RIP provocará llamadas en las interfaces PPP sobre canal B o sobre AT.

```
PPP Config>DISABLE RIP-NO-DIAL
PPP Config>
```

ADD USERS

Permite agregar pares usuario-password autorizados. Si el interfaz tiene habilitada la facilidad de autenticación (tipo PAP o CHAP), se solicitará autenticación al extremo remoto. La autenticación aportada por el extremo remoto debe coincidir con una de las claves configuradas.

No se debe confundir la autenticación con la que el interfaz se autentica ante el extremo remoto y la autenticación con la que el extremo remoto se autentica ante el interfaz. La primera se configura con el comando **SET AUTHENTICATION** y la segunda se configura con los comandos **ENABLE AUTHENTICATION** y **ADD USERS**.

El protocolo PPP es lo suficientemente flexible como para que cada extremo pueda solicitar el tipo de autenticación que desee al extremo remoto o no solicitar autenticación alguna. Lo normal en cualquier



caso es que un router de acceso a una red dada, como Internet, no solicite autenticación al proveedor del servicio pero sí tenga que autenticarse ante dicho proveedor. Desde el punto de vista del proveedor es él el que no se autentica pero sí solicita al usuario remoto que se autentique.

```
PPP Config>ADD USERS
Login:    []? usuarioremoto1
Password: password1
PPP Config>
```

DELETE USERS

Permite borrar pares usuario-password autorizados.

```
PPP Config>DELETE USERS
Login:    []? usuarioremoto1
PPP Config>
```

EXIT

Con este comando se abandona la configuración de los parámetros propios del interfaz PPP.

```
PPP Config>EXIT
Circuit Config>
```



Capítulo 3

Configuración del interfaz MPPP



1. Configuración de los interfaces

Para configurar el equipo con Multilink PPP primero es necesario disponer del interfaz MPPP y de uno o más interfaces PPP sobre canal B de RDSI. Para ello primero agregaremos los canales B que deseemos y el interfaz MPPP. Tras salvar la configuración de interfaces deseada y reiniciar el equipo podremos configurar los parámetros deseados.

Vamos a agregar dos canales B de RDSI del mismo acceso básico que asociaremos a un interfaz MPPP:

```
Teladat                (c)1996,97,98,99

Router model NUCLEOX-PLUS 41 CPU M68360      S/N: XXXX/XXXXX
1 LAN, 2 WAN Lines, 2 ISDN Lines

*PROCESS 4
User Configuration
Config>LIST DEVICES

Con   Ifc Type of interface                CSR   CSR2  int
---   --  -
---   --  -
---   --  -
ISDN 1  5 ISDN D channel: X25              A000000      1B
ISDN 1  7 ISDN B channel: X25             F001640  F000E00  9C
ISDN 2  6 ISDN D channel: X25             A200000      1B
ISDN 2  8 ISDN B channel: X25             F001660  F000F00  9B
LAN     0 Ethernet                        9000000      1C
WAN1    3 X25                              F001600  F000C00  9E
WAN2    4 X25                              F001620  F000D00  9D
Config>ADD DEVICE PPP-DIAL
Type basic access ISDN [2]? 1
If you are going to config more than two DIAL interfaces, you must config what t
hey have CSR:F011640 and CSR:F011660 over the ISDN 2 connector
Ifc number to delete: [0]? 7
Added PPP-DIAL interface with num: 2
Config>LIST DEVICES

Con   Ifc Type of interface                CSR   CSR2  int
---   --  -
---   --  -
---   --  -
ISDN 1  1 ISDN                            F001640  F000E00  9C
ISDN 1  2 B channel: PPP                   0        0
ISDN 1  7 ISDN D channel: X25             A000000      1B
ISDN 2  8 ISDN D channel: X25             A200000      1B
ISDN 2  9 ISDN B channel: X25             F001660  F000F00  9B
LAN     0 Ethernet                        9000000      1C
WAN1    5 X25                              F001600  F000C00  9E
WAN2    6 X25                              F001620  F000D00  9D
Config>ADD DEVICE PPP-DIAL
Type basic access ISDN [2]? 1
If you are going to config more than two DIAL interfaces, you must config what t
hey have CSR:F011640 and CSR:F011660 over the ISDN 2 connector
Do you wish to add another ISDN interface to this basic access?[n]? Y
Ifc number to delete: [0]? 9
Added PPP-DIAL interface with num: 4
```



```

Config>LIST DEVICES

Con   Ifc  Type of interface          CSR   CSR2  int
---   ---  ---
---   5   Router->Node              0     0     0
---   6   Node->Router              0     0     0
ISDN  1   1 ISDN                    F001640 F000E00 9C
ISDN  1   2 ISDN                    F001660 F000F00 9B
ISDN  1   3 B channel: PPP          0     0     0
ISDN  1   4 B channel: PPP          0     0     0
ISDN  1   9 ISDN D channel: X25     A000000 1B
ISDN  2  10 ISDN D channel: X25     A200000 1B
LAN   0   Ethernet                  9000000 1C
WAN1  7   X25                      F001600 F000C00 9E
WAN2  8   X25                      F001620 F000D00 9D

Config>ADD DEVICE MPPP
Added MPPP interface with num: 5
Config>SAVE
Save configuration [n]? Y

Saving configuration...OK
Config>
*RESTART
Are you sure to restart the system?(Yes/No)? Y
Disk configuration read
Initializing

Teladat          (c)1996,97,98,99

Router model NUCLEOX-PLUS 41 CPU M68360      S/N: XXXX/XXXXX
1 LAN, 2 WAN Lines, 2 ISDN Lines

*PROCESS 4
User Configuration
Config>LIST DEVICES

Con   Ifc  Type of interface          CSR   CSR2  int
---   ---  ---
---   5   Multilink PPP            0     0     0
---   6   Router->Node            0     0     0
---   7   Node->Router            0     0     0
ISDN  1   1 ISDN                    F001640 F000E00 9C
ISDN  1   2 ISDN                    F001660 F000F00 9B
ISDN  1   3 B channel: PPP          0     0     0
ISDN  1   4 B channel: PPP          0     0     0
ISDN  1  10 ISDN D channel: X25     A000000 1B
ISDN  2  11 ISDN D channel: X25     A200000 1B
LAN   0   Ethernet                  9000000 1C
WAN1  8   X25                      F001600 F000C00 9E
WAN2  9   X25                      F001620 F000D00 9D
Config>

```

En este punto observamos que tenemos dos interfaces PPP sobre canal B de RDSI (los números 3 y 4) y un interfaz MPPP (el número 5). Los parámetros de cada interfaz PPP se configuran en cada uno de ellos. En concreto es fundamental activar en cada PPP el Multilink PPP sobre el interfaz MPPP (interfaz número 5 en el ejemplo):



```

Config>NETWORK 3
Circuit Config
Circuit Config>ENCAPSULATOR

-- Interface PPP. Configuration --
PPP Config>ENABLE MPPP
Enter Multilink PPP interface this one belongs to[0]? 5
PPP Config>EXIT
Circuit Config>EXIT
Config>NETWORK 4
Circuit Config
Circuit Config>ENCAPSULATOR

-- Interface PPP. Configuration --
PPP Config>ENABLE MPPP
Enter Multilink PPP interface this one belongs to[0]? 5
PPP Config>LIST FACILITY

Facilities
-----
NAT Disable
Authenticacion Disable
CRTP Compression Disable
Avoid RIP dial-up Disable
Multilink PPP Enable Bundle: 5
Callback Disable
Backup Disable
PPP Config>

```

El interfaz MPPP disponible en el equipo funciona bajo demanda de tráfico, esto es, activa o desactiva los canales B del multilink en función de unos umbrales de tráfico definidos. La definición de esos umbrales se realiza en el interfaz MPPP deseado y se explica a continuación.



2. Configuración de los parámetros MPPP

La implementación del protocolo Multilink PPP en el router tiene las siguientes características:

1. Sólo es posible agregar los canales B del acceso básico de RDSI. (También es posible configurar MPPP en las líneas serie PPP, pero sólo para permitir la fragmentación, es decir cada mazo tiene una única línea serie).
2. La adición y posterior substracción de canales B se puede realizar en cualquier momento en función de los parámetros de ancho de banda por demanda de la sesión Multilink PPP.
3. Cuando están establecidos dos o más canales B, el tráfico PPP se alterna en los canales.
4. Si la sesión Multilink se configura como expropiable, se pueden excluir dinámicamente canales B de la sesión MPPP cuando un interfaz PPP Dial sobre RDSI necesita cursar una llamada y todos los canales B del equipo están ocupados.

Los parámetros característicos de la sesión Multilink PPP que determinan su comportamiento se describen a continuación. Los cinco primeros rigen su respuesta al patrón de ancho de banda bajo demanda, esto es, posteriores canales B se establecen o liberan en función del tráfico existente en la sesión Multilink. El último, recoge la posibilidad de configurar la sesión MPPP como expropiable en el sentido descrito anteriormente.

1. **Umbral de activación.** Porcentaje de ocupación del MPPP para la activación de otro canal B en el Multilink. Esto es, si durante el intervalo de activación la ocupación media de los canales B activos supera este valor, se activará un nuevo canal B, en el caso de que haya canales B disponibles. El valor por defecto de este parámetro es 90 %.
2. **Umbral de desactivación.** Porcentaje de ocupación de los canales B para la desactivación de un canal B del Multilink. Esto es, si durante el intervalo de desactivación la ocupación media de los canales B no llega a este valor, se desactivará un canal B. El valor por defecto de este parámetro es 50 %.
3. **Intervalo de activación.** Si durante los segundos indicados en este parámetro la ocupación media del MPPP supera el umbral de activación, se activará un nuevo canal B, en el caso de que haya canales B disponibles. Este parámetro se mide en segundos y su valor por defecto es 120 segundos.
4. **Intervalo de desactivación.** Si durante los segundos indicados en este parámetro la ocupación media de los canales B no llega al umbral de desactivación, se desactivará un canal B. Este parámetro se mide en segundos y su valor por defecto es 300 segundos.
5. **Sentido.** Indica el sentido del tráfico considerado para calcular la carga media de los canales. Puede ser entrante (desde la red externa hacia el equipo), saliente (desde el equipo hacia la red externa) o ambos. Para circunstancias normales de acceso a una red externa, como por ejemplo Internet, en donde la mayoría del tráfico es entrante, se recomienda configurar el valor entrante. El valor por defecto de este parámetro es entrante.
6. **Expropiación.** Propiedad que determina si los canales B utilizados en la sesión Multilink pueden ser excluidos dinámicamente por interfaces PPP Dial, en el caso de que estos necesiten cursar tráfico y no se disponga de canales B libres en el equipo. El valor por defecto de este parámetro es no expropiable.



7. **Fragmentación.** La fragmentación VOICE-IP fija la longitud máxima de trama del MPPP, toda trama mayor se fragmenta y toda trama menor se envía con el encapsulado PPP para intercalar así las tramas de voz con los fragmentos de las tramas de datos. Esta opción está deshabilitada por defecto.

Para configurar los parámetros de un interfaz MPPP se debe entrar en el interfaz MPPP:

```
Config>NETWORK 5
-- Multilink PPP Net Config --
MPPP config>
```

Los comandos disponibles son:

? (AYUDA)

Permite, en cualquier momento ver las opciones disponibles desde el menú de configuración en el que nos encontremos. A continuación de un comando permite ver cuales son las opciones disponibles para ese comando. Las opciones desde el menú de configuración del interfaz MPPP son las siguientes:

```
MPPP config>?
SET
LIST
EXIT
MPPP config>
```

LIST

Permite ver los parámetros de MPPP programados en el interfaz.

```
MPPP config>LIST
Multilink PPP parameters
-----
Activation threshold      : 90 %
Deactivation threshold    : 50 %
Interval of activation    : 120 s
Interval of deactivation  : 300 s
Direction of load        : Inbound
Pre-emptive               : No
Fragmentation Disabled
MPPP config>
```

SET

Permite configurar los parámetros de ancho de banda por demanda de tráfico así como las opciones de expropiación y fragmentación.

```
MPPP config>SET ?
THRESHOLD
INTERVAL
DIRECTION
PRE-EMPTION
FRAGMENTATION
MPPP config>
```

SET THRESHOLD

Permite configurar el umbral de activación y de desactivación del ancho de banda por demanda de tráfico.



```
MPPP config>SET THRESHOLD ACTIVATION
Enter activation threshold (0 - 100)[90]? 90
MPPP config>SET THRESHOLD DEACTIVATION
Enter deactivation threshold (0 - 100)[50]? 50
MPPP config>
```

SET INTERVAL

Permite configurar el intervalo de activación y de desactivación del ancho de banda por demanda de tráfico.

```
MPPP config>SET INTERVAL ACTIVATION
Enter activation interval (28 - 1800)[120]? 120
MPPP config>SET INTERVAL DEACTIVATION
Enter deactivation interval (28 - 1800)[300]? 300
MPPP config>
```

SET DIRECTION

Permite configurar el sentido de la carga que afecta al ancho de banda por demanda de tráfico.

```
MPPP config>SET DIRECTION
Enter load direction (1.- Inbound, 2.- Outbound, 3.- Either)[1]? 1
MPPP config>
```

SET PRE-EMPTION

Permite configurar la cualidad de expropiable del interfaz MPPP.

```
MPPP config>SET PRE-EMPTION
Do you wish to configure the multilink bundle as pre-emptive(Yes/No)(N)? Y
MPPP config>
```

NOTA: La propiedad de expropiación no es compatible con la configuración de los canales B del interfaz Multilink como permanentes.

SET FRAGMENTATION

Permite habilitar la fragmentación en el interfaz MPPP.

```
MPPP config>SET FRAGMENTATION VOICE-IP
Fragmentation (0.- Disabled, 1.- Enabled)[0]? 1
Fragment Size[0]? 256
MPPP config>
```

EXIT

Vuelve al menú general de configuración.

```
MPPP config>EXIT
Config>
```



Capítulo 4
Ejemplos de configuración para acceso
por RDSI



1. Conexión a Internet por RDSI

A continuación se describe la cadena de comandos necesaria para la configuración del router que permiten el acceso a Internet a través de RDSI.

El proceso de configuración lo realizaremos en dos partes.

1. Primero, añadimos el interfaz PPP sobre una línea RDSI y le asignamos una dirección IP cualquiera. Además agregaremos una ruta de forma que podamos acceder al servidor de Teldat a través de esta interfaz. Esto permitirá que en caso de que no este establecida la llamada RDSI, esta se establezca por tráfico IP, es decir, porque aparezcan datagramas con dirección de destino 195.53.0.x. Así mismo debemos de asignar una dirección al interfaz de Ethernet para poder conectar el router a la red. Una vez realizada esta operación arrancamos de nuevo el equipo.

```
Teldat                (c)1996,97,98,99

Router model NUCLEOX-PLUS 41 CPU M68360      S/N: XXXX/XXXXX
1 LAN, 2 WAN Lines, 2 ISDN Lines

*PROCESS 4
User Configuration
Config>LIST DEVICES

Con   Ifc  Type of interface          CSR   CSR2  int
---   ---  ---
---   1   Router->Node              0     0     0
---   2   Node->Router              0     0     0
ISDN 1  5   ISDN D channel: X25      A000000  1B
ISDN 1  7   ISDN B channel: X25      F001640  F000E00  9C
ISDN 2  6   ISDN D channel: X25      A200000  1B
ISDN 2  8   ISDN B channel: X25      F001660  F000F00  9B
LAN     0   Ethernet                  9000000  1C
WAN1    3   X25                       F001600  F000C00  9E
WAN2    4   X25                       F001620  F000D00  9D

Config>ADD DEVICE PPP-DIAL
Type basic access ISDN [2]? 1
If you are going to config more than two DIAL interfaces, you must config what t
hey have CSR:F011640 and CSR:F011660 over the ISDN 2 connector
Ifc number to delete: [0]? 7
Added PPP-DIAL interface with num: 2
Config>LIST DEVICES

Con   Ifc  Type of interface          CSR   CSR2  int
---   ---  ---
---   3   Router->Node              0     0     0
---   4   Node->Router              0     0     0
ISDN 1  1   ISDN                      F001640  F000E00  9C
ISDN 1  2   B channel: PPP            0     0     0
ISDN 1  7   ISDN D channel: X25      A000000  1B
ISDN 2  8   ISDN D channel: X25      A200000  1B
ISDN 2  9   ISDN B channel: X25      F001660  F000F00  9B
LAN     0   Ethernet                  9000000  1C
WAN1    5   X25                       F001600  F000C00  9E
WAN2    6   X25                       F001620  F000D00  9D

Config>PROTOCOL IP
Internet protocol user configuration
IP config>ADD ADDRESS
Which net is this address for[0]? 2
New address [0.0.0.0]? 192.6.3.1
Address mask [255.255.255.0]? 255.255.255.0
```



```
IP config>ADD ADDRESS
Which net is this address for[0]? 0
New address [0.0.0.0]? 192.6.1.224
Address mask [255.255.255.0]? 255.255.255.0
IP config>ADD ROUTE
IP destination [0.0.0.0]? 195.53.0.0
Address mask [0.0.0.0]? 255.255.255.0
Via gateway at [0.0.0.0]? 192.6.3.1
Cost[1]? 1
IP config>EXIT
Config>SAVE
Save configuration [n]? Y

Saving configuration...OK
Config>
*RESTART
Are you sure to restart the system?(Yes/No)? Y
Disk configuration read
Initializing

Teldat (c)1996,97,98,99

Router model NUCLEOX-PLUS 41 CPU M68360 S/N: XXXX/XXXXXX
1 LAN, 2 WAN Lines, 2 ISDN Lines

*
```

<CTRL-P>

Si comprobamos la configuración del interfaz base RDSI se verá que la conexión por defecto es del tipo conmutado, por lo que no es preciso configurar nada más.

```
*PROCESS 4
User Configuration
Config>NETWORK 1
ISDN Config
Config ISDN>LIST
Local destination:
Maximum frame size: 2048
ISDN Connection Type : Switched
Config ISDN>
```

2. A continuación pasamos a configurar el interfaz PPP propiamente dicho. Los parámetros principales que debemos de configurar son:

- Dirección destino: Número del nodo de acceso del ISP que se desea usar.
- Permitimos llamadas salientes.
- Usuario y clave para el acceso al ISP.
- Petición de asignación de número IP.

La secuencia de comandos sería la siguiente:



```

*PROCESS 4

Config>NETWORK 2
Circuit Config
Circuit Config>LIST
Base interface: -1
Destination address:
Inactive time: 60
Permitted caller:
Circuit name:
Outgoing calls allowed: Yes
Incoming calls allowed: No
Control access enabled: No
Circuit Config>SET DESTINATION-ADDRESS
Destination address[]? 917529000
Circuit Config>ENCAPSULATOR

-- Interface PPP. Configuration --
PPP Config>SET AUTHENTICATION
Login: []? infoviaplus
Password: *****
Password: *****
PPP Config>SET IPCP
IP Van Jacobson Compression      : (Yes/No)(N)? N
CRTP Compression                 : (Yes/No)(N)? N
IP get local address              : (Yes/No)(N)? Y
IP mask local address             : [255.255.255.255]? 255.255.255.255
IP send address                   : (Yes/No)(Y)? N
IP request remote address         : (Yes/No)(Y)? N
IP remote address                 : [0.0.0.0]? 0.0.0.0
PPP Config>ENABLE NAT
PPP Config>EXIT
Circuit Config>EXIT
Config>SAVE
Save configuration [n]? Y

Saving configuration...OK
Config>
*RESTART
Are you sure to restart the system?(Yes/No)? Y
Disk configuration read
Initializing

Teldat                (c)1996,97,98,99

Router model NUCLEOX-PLUS 41 CPU M68360      S/N: XXXX/XXXXX
1 LAN, 2 WAN Lines, 2 ISDN Lines

*

```

3. Con esta configuración la llamada RDSI se establecerá por tráfico. Por último podemos comprobar mediante un ping si tenemos correctamente configurado el interfaz. Se deberá de establecer la llamada RDSI y obtener respuesta a los pings enviados. La secuencia de comandos será la siguiente:



```

*PROCESS 3
Console Operator
+PROTOCOL IP
IP>INTERFACE
Interface  IP Address(es)  Mask(s)
  Eth/0    192.6.1.224      255.255.255.0
  PPP/0    192.6.3.1        255.255.255.0
  R->N/0   192.168.252.1    255.255.255.0
IP>DUMP
Type      Dest net          Mask      Cost Age  Next hop(s)

  Dir(1)   192.6.1.0        ffffffff0 1    0    Eth/0
  Dir(1)   192.6.3.0        ffffffff0 1    0    PPP/0
  Dir(1)   192.168.252.0    ffffffff0 1    0    R->N/0
  Stat(1)  195.53.0.0       ffffffff0 1    0    192.6.3.1

Routing table size: 768 nets (52224 bytes), 4 nets known
IP>PING 195.53.0.2
PING 195.53.0.2: 56 data bytes

----195.53.0.2 PING Statistics----
32 packets transmitted, 0 packets received, 100% packet loss
IP>INTERFACE
Interface  IP Address(es)  Mask(s)
  Eth/0    192.6.1.224      255.255.255.0
  PPP/0    193.153.67.59    255.255.255.255
  R->N/0   192.168.252.1    255.255.255.0
IP>DUMP
Type      Dest net          Mask      Cost Age  Next hop(s)

  Dir(1)   192.6.1.0        ffffffff0 1    0    Eth/0
  Dir(1)   192.168.252.0    ffffffff0 1    0    R->N/0
  Sbnt(0)  193.153.67.0     ffffffff0 1    0    None
  Dir(1)   193.153.67.59    ffffffff  1    0    PPP/0
  Stat(1)  195.53.0.0       ffffffff0 1    0    193.153.67.59

Routing table size: 768 nets (52224 bytes), 5 nets known
IP>

```

Se puede observar cómo se ha asignado dinámicamente una nueva dirección al interfaz PPP (193.153.67.59). También se puede observar que se pierden todos los paquetes del ping que se realiza. Esto es debido a que los paquetes IP que se mandan tienen como dirección origen la dirección de la interfaz PPP antes de realizar la negociación IPCP (192.6.3.1), dirección que es desconocida dentro de Internet. Si posteriormente volvemos a ejecutar el ping, los paquetes se recibirán correctamente porque ahora la dirección IP origen será la obtenida del ISP (193.153.67.59), una dirección válida.

NOTA: Cuando no se emplea la generación de configuración desde el menú de configuración rápida del Router Teldat no olvidar configurar en el terminal la dirección IP del servidor DNS que se va a emplear, que en el caso de Internet es proporcionada por el ISP.



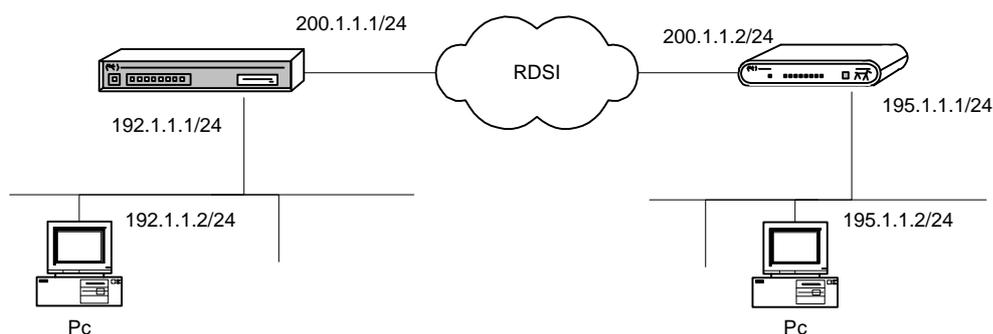
2. Conexión por RDSI en modo permanente

En algunos casos la operadora telefónica ofrece la posibilidad de contratar conexiones RDSI permanentes entre dos abonados de líneas RDSI, utilizando para ello uno o varios canales B del acceso básico que le llega al abonado. En este caso no es preciso realizar llamada alguna y la conexión se comporta como si se tratara de una línea punto a punto.

Es importante recalcar que para utilizar esta posibilidad son necesarios dos elementos:

- Contratar el servicio RDSI permanente entre ambos extremos con su operadora.
- Disponer de dos router que soporten el modo de funcionamiento RDSI permanente y situarlos en ambos extremos de la conexión RDSI permanente.

En este apartado se mostrará un ejemplo de configuración para unir por PPP sobre un enlace RDSI permanente dos redes IP remotas utilizando en ambos extremos el canal B1 (esto no tiene por qué cumplirse en su caso particular). El proceso de configuración se realizará en dos partes: en la primera se creará el interfaz PPP sobre RDSI y en el segundo se configurará el IP. El diagrama de conexión es el siguiente:



- a) Creación del interfaz PPP: Se crea un interfaz PPP y se configura el interfaz RDSI base como permanente sobre el canal B1 (dato aportado por la operadora de telefonía). Se utiliza la configuración de encapsulado de PPP por defecto pues para este ejemplo no es preciso configurar nada más. Este paso se ha de repetir de igual manera para ambos routers.

```
Teladat                (c)1996,97,98,99
Router model NUCLEOX-PLUS 41 CPU M68360      S/N: XXXX/XXXXXX
1 LAN, 2 WAN Lines, 2 ISDN Lines
```



```

*PROCESS 4
User Configuration
Config>LIST DEVICES

Con      Ifc  Type of interface          CSR      CSR2  int
---      --  -
---      1  Router->Node              0        0     0
---      2  Node->Router              0        0     0
ISDN 1   5  ISDN D channel: X25      A000000  1B
ISDN 1   7  ISDN B channel: X25      F001640  F000E00  9C
ISDN 2   6  ISDN D channel: X25      A200000  1B
ISDN 2   8  ISDN B channel: X25      F001660  F000F00  9B
LAN      0  Ethernet                  9000000  1C
WAN1     3  X25                      F001600  F000C00  9E
WAN2     4  X25                      F001620  F000D00  9D

Config>ADD DEVICE PPP-DIAL
Type basic access ISDN [2]? 1
If you are going to config more than two DIAL interfaces, you must config what they have CSR:F001640 and CSR:F001660 over the ISDN 2 connector
Ifc number to delete: [0]? 7
Added PPP-DIAL interface with num: 2
Config>LIST DEVICES

Con      Ifc  Type of interface          CSR      CSR2  int
---      --  -
---      3  Router->Node              0        0     0
---      4  Node->Router              0        0     0
ISDN 1   1  ISDN                      F001640  F000E00  9C
ISDN 1   2  B channel: PPP            0        0     0
ISDN 1   7  ISDN D channel: X25      A000000  1B
ISDN 2   8  ISDN D channel: X25      A200000  1B
ISDN 2   9  ISDN B channel: X25      F001660  F000F00  9B
LAN      0  Ethernet                  9000000  1C
WAN1     5  X25                      F001600  F000C00  9E
WAN2     6  X25                      F001620  F000D00  9D

Config>SAVE
Save configuration [n]? Y

Saving configuration...OK
Config>
*RESTART
Are you sure to restart the system?(Yes/No)? Y
Disk configuration read
Initializing

Teladat          (c)1996,97,98,99

Router model NUCLEOX-PLUS 41 CPU M68360      S/N: XXXX/XXXXX
1 LAN, 2 WAN Lines, 2 ISDN Lines

*PROCESS 4
User Configuration
Config>NETWORK 1
ISDN Config
Config ISDN>LIST
Local destination:
Maximum frame size: 2048
ISDN Connection Type : Switched
Config ISDN>SET CONNECTION-TYPE
ISDN Connection Type (0 Switched, 1 Permanent B1, 2 Permanent B2)[0]? 1
Config ISDN>LIST
Local destination:
Maximum frame size: 2048
ISDN Connection Type : Permanent B1

```

<CTRL-P>



```

Config ISDN>EXIT
Config>NETWORK 2
Circuit Config
Circuit Config>LIST
Base interface: -1
Destination address:
Inactive time: 60
Permitted caller:
Circuit name:
Outgoing calls allowed: Yes
Incoming calls allowed: No
Control access enabled: No
Circuit Config>SET BASE-INTERFACE
Base interface:[-1]? 1
Circuit Config>LIST
Base interface: 1 (permanent)
Circuit name:
Control access enabled: No
Circuit Config>EXIT
Config>

```

- b) Asignación de las direcciones IP de los interfaces y de las rutas. En este caso se configura el router situado a la izquierda de la figura (200.1.1.1/24 para el interfaz PPP y 192.1.1.1/24 para el interfaz LAN). Para el otro router el modo de configuración es igual pero con las direcciones 200.1.1.2/24 para el interfaz PPP y 195.1.1.1/24 para el interfaz LAN, y con una ruta a la 192.1.1.0/24 a través de la dirección 200.1.1.1.

```

Config>PROTOCOL IP
Internet protocol user configuration
IP config>ADD ADDRESS
Which net is this address for[0]? 2
New address [0.0.0.0]? 200.1.1.1
Address mask [255.255.255.0]? 255.255.255.0
IP config>ADD ADDRESS
Which net is this address for[0]? 0
New address [0.0.0.0]? 192.1.1.1
Address mask [255.255.255.0]? 255.255.255.0
IP config>ADD ROUTE
IP destination [0.0.0.0]? 195.1.1.0
Address mask [0.0.0.0]? 255.255.255.0
Via gateway at [0.0.0.0]? 200.1.1.1
Cost[1]? 1
IP config>EXIT
Config>SAVE
Save configuration [n]? Y

Saving configuration...OK
Config>
*RESTART
Are you sure to restart the system?(Yes/No)? Y
Disk configuration read
Initializing

Teladat (c)1996,97,98,99

Router model NUCLEOX-PLUS 41 CPU M68360 S/N: XXXX/XXXXX
1 LAN, 2 WAN Lines, 2 ISDN Lines

*

```

Una vez configurados ambos equipos se puede probar la conexión haciendo pines desde dos sitios: desde los propios routers (desde el proceso de monitorización de IP, tal y como se hizo en el apartado 1) o desde los PC u otros equipos situados en las LANes de ambos extremos: para ello será necesario agregar las correspondiente rutas de acceso a las redes IP remotas.



Capítulo 5
Ejemplo de configuración (Internet-
Acceso por RTB)



1. Ejemplo de configuración (Internet-Acceso RTB)

A continuación se describe la cadena de comandos necesaria para la configuración del router que permiten el acceso a la red Internet a través de RTB (Red Telefónica Básica) sobre un interfaz de comandos AT, que permitirá manejar un módem externo para realizar la conexión.

El proceso de configuración lo realizaremos en cuatro partes, tres para configurar y una para establecer y comprobar la conexión.

1. Primero, añadimos el interfaz PPP asíncrono sobre un interfaz de comandos AT y le asignamos una dirección IP cualquiera. Además establecemos la ruta para que todos los datagramas dirigidos a la red 195.53.0.x salgan por ese interfaz. Esto permitirá que en caso de que no esté establecida la llamada, esta se establezca por tráfico IP, es decir, porque aparezcan datagramas con dirección de destino 193.152.x.x. Así mismo debemos de asignar una dirección al interfaz de Ethernet para poder conectar el router a la red. Una vez realizada esta operación arrancamos de nuevo el equipo.

```
Tel dat          (c)1996,97,98,99

Router model NUCLEOX-PLUS 41 CPU M68360      S/N: XXXX/XXXXX
1 LAN, 2 WAN Lines, 2 ISDN Lines

*PROCESS 4
User Configuration
Config>ADD DEVICE ATPPP-DIAL
which port will be changed[0]? 1
Added ATPPP-DIAL interface with num: 2
Config>PROTOCOL IP
Internet protocol user configuration
IP config>ADD ADDRESS
Which net is this address for[0]? 2
New address [0.0.0.0]? 192.168.1.1
Address mask [255.255.255.0]? 255.255.255.0
IP config>ADD ADDRESS
Which net is this address for[0]? 0
New address [0.0.0.0]? 192.7.1.253
Address mask [255.255.255.0]? 255.255.255.0
IP config>ADD ROUTE
IP destination [0.0.0.0]? 195.53.0.0
Address mask [0.0.0.0]? 255.255.255.0
Via gateway at [0.0.0.0]? 192.168.1.1
Cost[1]? 1
IP config>EXIT
Config>SAVE
Save configuration [n]? Y

Saving configuration...OK
Config><CTRL-P>
*RESTART
Are you sure to restart the system?(Yes/No)? Y
Disk configuration read
Initializing

Tel dat          (c)1996,97,98,99

Router model NUCLEOX-PLUS 41 CPU M68360      S/N: XXXX/XXXXX
1 LAN, 2 WAN Lines, 2 ISDN Lines

*
```

2. A continuación pasamos a configurar el interfaz PPP propiamente dicho. Los parámetros principales que debemos de configurar son:



- Dirección destino: Número del Nodo de Acceso al ISP que se desee utilizar.
- Velocidad de línea. Será a la que se enviarán los comandos de marcación y configuración al módem.
- Parámetros LCP para la conexión en modo asíncrono. ACCM, Compresión de protocolo y Compresión de campos de control y de dirección de la trama y Número Mágico.
- Login y Password para el acceso a Internet (remoteuser1-password1).
- Petición de asignación de número IP.

La secuencia de comandos sería la siguiente:

```
*PROCESS 4
User Configuration
Config>NETWORK 2
Circuit Config
Circuit Config>LIST
Base interface: 1
Destination address:
Inactive time: 60
Circuit Config>SET DESTINATION-ADDRESS
Destination address[]? 917529000
Circuit Config>ENCAPSULATOR
ASYNCHRONOUS PPP

-- Interface PPP. Configuration --
PPP Config>SET LINE LINE-SPEED
Line speed (bps) : [64000]? 115200
PPP Config>SET AUTHENTICATION
Login: []? remoteuser1
Password: *****
Password: *****
PPP Config>SET LCP OPTIONS
Interface MRU (bytes) : [1500]? 1500
Magic Number : (Yes/No)(Y)? Y
Asynchronous Control Character Map : (Yes/No)(N)? Y
Protocol Field Compression : (Yes/No)(N)? Y
Address Control Field Compression : (Yes/No)(N)? Y
PPP Config>SET IPCP
IP Van Jacobson Compression : (Yes/No)(N)? N
CRTP Compression : (Yes/No)(N)? N
IP get local address : (Yes/No)(N)? Y
IP mask local address : [255.255.255.255]? 255.255.255.255
IP send address : (Yes/No)(Y)? Y
IP request remote address : (Yes/No)(Y)? Y
IP remote address : [0.0.0.0]? 0.0.0.0
PPP Config>ENABLE NAT
PPP Config>EXIT
Circuit Config>EXIT
Config>SAVE
Save configuration [n]? Y

Saving configuration...OK
Config><CTRL-P>
*
```

3. En tercer lugar, debemos de configurar el interfaz de comandos AT que van a ser empleado en el manejo del módem. El manejo del módem desde el **Router Teldat** se realiza mediante comandos y manejo de señales. Para controlar el establecimiento y finalización de la llamada el **Router Teldat** únicamente comprueba el estado de las señales del interfaz, por esto, éstas deben de ser programadas en el módem para que se activen según la norma y no de modo fijo. En la siguiente tabla se indican los parámetros configurables para el módem externo y el valor por defecto que toman:

Comando	Valor	Significado
Modo de Conexión	C	Modo de Comandos



Modo de Marcación	T	Marcación por tonos multifrecuencia (DTMF)
Control DCD	&C1	La señal de portadora, 109, sigue al estado de la portadora en línea
Control DSR	&S1	La señal Data Set Ready - 107 por V.24. Se activará a ON después de haber detectado tono de respuesta tras la marcación
Control DTR	&D2	La caída del circuito Data Terminal Ready - 108 provoca que el módem cuelgue y que se inhiba la respuesta automática.
Control CTS	&R1	La señal CTS tendrá estado OFF únicamente si lo requiere el control de Flujo.
V.42/V.42 bis	&Q5	El módem intentará negociar una conexión con corrección de errores y compresión de datos
Control flujo	&K3	El control de flujo seleccionado es por Hardware, (RTS/CTS)
Respuesta automática	dis	Respuesta automática deshabilitada.

A pesar de que los comandos por defecto son empleados por la mayoría de los fabricantes de modems, puede ser que alguno de los comandos anteriormente indicado no esté implementado en el módem que se vaya a emplear

En caso de que sea necesario modificar alguno de ellos, la opción elegida de acuerdo al conjunto de comandos implementados en el módem deberá de cumplir:

Modo de conexión que va a emplear el módem, marcación por comandos o por DTR. En caso de que el modo de conexión sea por DTR, el **Router Teldat** cuando quiera establecer una llamada activará el circuito DTR 108 del interfaz. Si el modo deseado es por comandos, además enviará el comando de marcación (ATD) seguido del número programado.

Modo de marcación que va a emplear el módem, tonos o pulsos. Dependerá del tipo de acceso a la red RTB que disponga el usuario.

Comando de control de portadora (DCD). Deberá de seleccionarse de modo que el circuito DCD (109) funcione por V.24, es decir, que el circuito 109 señalice el estado de la portadora en línea.

Comando de control de DSR. Deberá de seleccionarse de modo que el circuito DSR (107) funcione por V.24, se activará cuando detecte respuesta del extremo remoto.

Comando de control de DTR. Deberá de seleccionarse de modo que el módem desconecte por ausencia de DTR. Cuando el **Router Teldat** desea realizar la desconexión por ausencia de tráfico desactivará el circuito 108 del terminal hacia el módem. Así mismo permite que en estado de desconexión el módem no responda a las llamadas entrantes.

Comando de control de CTS. Deberá de seleccionarse de modo que el módem proporcione CTS (106) mientras se encuentre en modo de comandos. La señal 106 estará inactiva únicamente cuando lo requiera el control de flujo.



Comando de activación de norma V.42/V.42bis. Deberá de seleccionarse de modo que la conexión se realice con corrección y compresión de datos. Si bien puede no requerirse corrección y compresión, si es recomendable elegirla, ya que permite obtener una mayor velocidad efectiva (Throughput) en el enlace

Comando de selección de control de flujo en el módem. Siempre deberá de seleccionarse control de flujo Hardware (RTS/CTS).

Respuesta automática. Permite que el interfaz ATDIAL acepte llamadas entrantes. Si esta opción está habilitada, se deben emplear modems que soporten comandos AT ya que el equipo no monitoriza la señal RI125 del V.24. Además, uno de los extremos debe de no tener configurado número de destino en el interfaz PPPAT para que no se de el caso de que se produzca colisión de llamadas, entrantes y salientes. Con esta opción habilitada, el interfaz ATDIAL puede emplearse como interfaz de backup entre dos extremos siendo uno el que llame y otro el que responda.

La secuencia de comandos para la programación sería la siguiente:

```
*PROCESS 4

Config>NETWORK 1

-- Interface AT. Configuration --
AT Config>?
LIST
SET
ENABLE
DISABLE
EXIT
AT Config>LIST
      Connection mode      = C (Commands)
      Dial mode            = T (Tone)
      DCD control command  = &C1
      DSR control command  = &S1
      DTR control command  = &D2
      CTS control command  = &R1
      V.42/v.42 bis command= &Q5
      Flow control command = &K3
      Automatic Answer     = Disabled
AT Config>SET ?
CONNECTION
DIAL
DCD-CONTROL
DSR-CONTROL
DTR-CONTROL
CTS-CONTROL
V42-CONTROL
FLOW-CONTROL
```



```
AT Config>SET CONNECTION
Connection Mode (C = Commands, D = DTR) = C
AT Config>SET DIAL
Dial Mode (T = Tone, P = Pulse) = T
AT Config>SET DCD-CONTROL
DCD control command = [&C1]? &C1
AT Config>SET DSR-CONTROL
DSR control command = [&S1]? &S1
AT Config>SET DTR-CONTROL
DTR control command = [&D2]? &D2
AT Config>SET CTS-CONTROL
CTS control command = [&R1]? &R1
AT Config>SET V42-CONTROL
V.42/V.42 bis command = [&Q5]? &Q5
AT Config>SET FLOW-CONTROL
Flow control command = [&K3]? &K3
AT Config>ENABLE ?
AUTO-ANSWER
AT Config>DISABLE ?
AUTO-ANSWER
AT Config>EXIT
Config>SAVE
Save configuration [n]? Y

Saving configuration...OK
Config>
*RESTART
Are you sure to restart the system?(Yes/No)? Y
Disk configuration read
Initializing

Teldat (c)1996,97,98,99

Router model NUCLEOX-PLUS 41 CPU M68360 S/N: XXXX/XXXXX
1 LAN, 2 WAN Lines, 2 ISDN Lines

*
```

<CTRL-P>

Con esta configuración la llamada por comandos AT hacia el módem se establecerá por tráfico. Por último podemos comprobar mediante un ping si tenemos correctamente configurado el interfaz. Se deberá de establecer la llamada RTB y obtener respuesta a los pings enviados. La secuencia de comandos será la siguiente:



```

*PROCESS 3
Console Operator
+PROTOCOL IP
IP>INTERFACE
Interface IP Address(es) Mask(s)
  Eth/0 192.7.1.253 255.255.255.0
  PPP/0 192.168.1.1 255.255.255.0
  R->N/0 192.168.252.1 255.255.255.0
IP>DUMP
Type Dest net Mask Cost Age Next hop(s)

  Dir(1) 192.7.1.0 ffffffff00 1 0 Eth/0
  Dir(1) 192.168.1.0 ffffffff00 1 0 PPP/0
  Dir(1) 192.168.252.0 ffffffff00 1 0 R->N/0
  Stat(1) 195.53.0.0 ffffffff00 1 0 192.168.1.1

Routing table size: 768 nets (52224 bytes), 4 nets known
IP>PING 195.53.0.2
PING 195.53.0.2: 56 data bytes

----195.53.0.2 PING Statistics----
34 packets transmitted, 0 packets received, 100% packet loss
IP>INTERFACE
Interface IP Address(es) Mask(s)
  Eth/0 192.7.1.253 255.255.255.0
  PPP/0 193.153.66.40 255.255.255.255
  R->N/0 192.168.252.1 255.255.255.0
IP>DUMP
Type Dest net Mask Cost Age Next hop(s)

  Dir(1) 192.7.1.0 ffffffff00 1 0 Eth/0
  Dir(1) 192.168.252.0 ffffffff00 1 0 R->N/0
  Sbnt(0) 193.153.66.0 ffffffff00 1 0 None
  Dir(1) 193.153.66.40 ffffffff 1 0 PPP/0
  Stat(1) 195.53.0.0 ffffffff00 1 0 193.153.66.40

Routing table size: 768 nets (52224 bytes), 5 nets known
IP>PING 195.53.0.2
PING 195.53.0.2: 56 data bytes
64 bytes from 195.53.0.2: icmp_seq=0. time=686. ms
64 bytes from 195.53.0.2: icmp_seq=1. time=744. ms
64 bytes from 195.53.0.2: icmp_seq=2. time=813. ms

----195.53.0.2 PING Statistics----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip (ms) min/avg/max = 686/747/813
IP>

```

Se puede observar como se ha asignado dinámicamente una nueva dirección al interfaz PPP (193.153.66.40) correspondiente al conjunto de direcciones del ISP.

NOTAS: *El establecimiento de la conexión a Internet utilizando un módem requiere un tiempo de conexión más elevado que en el caso de RDSI. Si se están empleando navegadores desde terminales conectados a la red LAN, puede ocurrir que si la llamada no este establecida, aún estableciéndose de forma correcta por tráfico, no se actualicen las páginas de forma correcta ya que los datagramas enviados son descartados hasta que no se ha establecido la conexión. Es aconsejable transcurrido un tiempo actualizarlas de forma manual.*

Cuando no se emplea la generación de configuración desde el menú de configuración rápida del Router TELDAT no olvidar configurar en el terminal la dirección IP del servidor DNS que se va a emplear, que en el caso de Internet es proporcionada por el ISP.



Capítulo 6

Monitorización del Interfaz PPP



1. Estadísticos del interfaz PPP

Para visualizar los estadísticos del interfaz teclear desde el prompt de monitorización (+) el comando **DEVICE**, indicando a continuación el número de la interfaz cuyos estadísticos se desean obtener. La información obtenida dependerá del medio físico utilizado como soporte.

Para el caso de un interfaz PPP sobre línea serie síncrona, la información que se muestra es:

```
+DEVICE 1

Ifc Interface      CSR      Vect      Auto-test  Auto-test  Maintenance
1   PPP/0         F001600   9e        valids     failures   failures
                                0          4          0

Driver type:                DTE

V.24 circuit:              105 106 107 108 109
Nicknames:                 RTS CTS DSR DTR DCD
State:                     ON  OFF OFF ON  OFF

Line speed:                unknown
Last port reset:          26 seconds ago

Input frame errors:
CRC error                  =          0 alignment (byte length) =          0
missed frame              =          0 too long (> 02062 bytes) =          0
aborted frame             =          0 DMA/FIFO overrun         =          0

Output frame counters:
DMA/FIFO underrun errs =          0 Output aborts sent      =          0
+
```

Para el caso de un interfaz PPP sobre línea serie asíncrona, la información que se muestra es:

```
+DEVICE 2

Ifc Interface      CSR      Vect      Auto-test  Auto-test  Maintenance
2   PPP/1         F001620   9d        valids     failures   failures
                                0          0          0
Interface DTE
V.24 circuits:105 106 107 108 109 125 141
Nicknames:      RTS CTS DSR DTR DCD RI  LL
State:          ON  OFF OFF ON  OFF --- ---

Speed (bps)      =      115200
Throughput (bps) =          0
Last throughput (bps) =          0
Bits per character =          8
Stop bits        =          1
Parity selected  =      NONE
Parity errors    =          0
Data errors      =          0
Overrun errors   =          0
Last reset       = 4 minutes 36 seconds
+
```

Para el caso de un interfaz PPP sobre un acceso básico RDSI, la información que se muestra es:



```
+DEVICE 5

Ifc  Interface      CSR   Vect   Auto-test  Auto-test  Maintenance
5    PPP/2          0     0     valids    failures   failures
                                1         0
                                0

      PPP over ISDN line
      Speed rate 64000 bps
+
```

Para el caso de un interfaz PPP sobre un interfaz de comandos AT, la información que se muestra es:

```
+DEVICE 2

Ifc  Interface      CSR   Vect   Auto-test  Auto-test  Maintenance
2    PPP/0          0     0     valids    failures   failures
                                3         0
                                0

      PPP over AT-COM interface
      Line speed  115200 bps
+
```



2. Consola PPP

Teclar desde el prompt de monitorización (+)

```
+NETWORK 1
-- PPP Console --
PPP>
```

? (AYUDA)

Permite, en cualquier momento ver las opciones disponibles desde el menú de consola en el que nos encontremos. A continuación de un comando permite ver cuales son las opciones disponibles para ese comando. Las opciones desde el menú de consola del interfaz PPP son las siguientes:

```
PPP>?
LIST
CLEAR
RESET-link
EXIT
PPP>
```

LIST

```
PPP>LIST ?
ALL
CONTROL
LCP
IPCP
COMPRESSION-VAN_JACOBSON
CRTP
PPP>
```

LIST CONTROL LCP

```
PPP>LIST CONTROL LCP
Version          : 2.0.0
State LCP        : INITIAL
Previous state LCP : INITIAL

LCP Options      Local          Remote
-----
Max Receive Unit: 1500           1500
Async Char Mask : 0x00000000    0x00000000
Authentication   : 0xffffc023   0x00000000
Magic Number     : 0xa71f3b07    0x00000000
Protocol Compr   : NO            NO
Addr/Ctrl Compr  : NO            NO
32-Bit Checksum  : NO            NO
PPP>
```

Permite monitorizar las opciones transmitidas y recibidas en el establecimiento del enlace así como el estado actual del protocolo PPP.

LIST CONTROL IPCP

```
PPP>LIST CONTROL IPCP
State IPCP       : INITIAL
Previous state IPCP : INITIAL

IPCP Options     Local          Remote
-----
IP Address       : 192.168.1.1    0.0.0.0
Van Jacobson Cmp: NO            NO
PPP>
```



Permite monitorizar las opciones transmitidas y recibidas en el establecimiento del protocolo de nivel de RED. En caso de que se esté utilizando asignación dinámica se podrá comprobar el número IP asignado. Así mismo, si ha sido recibido, se podrá monitorizar el número IP del extremo remoto.

LIST LCP

```
PPP>LIST LCP
LCP Statistics      Received      Send
-----
Frames      :      0      0
Bytes       :      0      0
Config. Request:      0      0
Config. Ack  :      0      0
Config. Nak  :      0      0
Config. Reject:      0      0
Termin. Request:      0      0
Termin. Ack  :      0      0
Echo Request:      0      0
Echo Reply  :      0      0
PPP>
```

Permite monitorizar el número de tramas LCP recibidas y enviadas por el citado interfaz, así como el número de bytes y tramas recibidas y transmitidas.

LIST IPCP

```
PPP>LIST IPCP
IPCP Statistics      Received      Send
-----
Config. Request:      0      0
Config. Ack  :      0      0
Config. Nak  :      0      0
Config. Reject:      0      0
Termin. Request:      0      0
Termin. Ack  :      0      0
PPP>
```

Permite monitorizar el número de tramas NCP recibidas y enviadas por el citado interfaz.

CLEAR

```
PPP>CLEAR
PPP>
```

Reinicia todos los estadísticos del interfaz.

RESET-LINK

```
PPP>RESET-LINK
Are you sure(Yes/No)? Y
PPP>
```

Tira el enlace PPP sobre canal B de RDSI o sobre interfaz de comandos AT.

EXIT

```
PPP>EXIT
+
```

Abandona el modo de monitorización del interfaz PPP.



Capítulo 7

Eventos del Protocolo PPP



1. Monitorización de eventos del protocolo PPP

Permiten monitorizar en tiempo real los eventos que suceden sobre uno o varios interfaces PPP cuando está habilitado el sistema de eventos para ese protocolo.

La forma en que se habilitan desde el menú de configuración es la siguiente:

```
*PROCESS 4
User Configuration
Config>EVENT

-- ELS Config --
ELS Config>ENABLE TRACE SUBSYSTEM PPP ALL
ELS Config>EXIT
Config>SAVE
Save configuration [n]? Y

Saving configuration...OK
Config>
```

Así mismo pueden ser habilitados desde el menú de monitorización en cualquier momento sin necesidad de que esté almacenada en la configuración de la siguiente forma:

```
*PROCESS 3
Console Operator
+EVENT

-- ELS Monitor --
ELS>ENABLE TRACE SUBSYSTEM PPP ALL
ELS>EXIT
+
```

El listado de eventos disponibles para el protocolo PPP es el siguiente:

PPP.001

Nivel: Comentario de un hecho normal, INFO-N/C-INFO

Sintaxis Corta:

PPP.001 Req brng up IP, addr = *IP_address* nt *network ID*

Sintaxis Larga:

PPP.001 Request to bring up IP, local address = *IP_address*, on network *network ID*

Descripción:

Rutina ppp_pprint llamada por el protocolo IP.

PPP.002

Nivel: Comentario de un hecho normal, INFO-N/C-INFO

Sintaxis Corta:

PPP.002 Srl prt up nt *network ID*

Sintaxis Larga:

PPP.002 Serial Port came up sucessfully on network *network ID*

Descripción:

pppslfts2 finalizado selftest del driver. Driver inicializado.



PPP.003

Nivel: Comentario de un hecho normal, INFO-N/C-INFO

Sintaxis Corta:

PPP.003 Mnt nt *network ID*

Sintaxis Larga:

PPP.003 Doing maint on network *network ID*

Descripción:

Efectuado mantenimiento pppmnt.

PPP.004

Nivel: Comentario de un hecho normal, INFO-N/C-INFO

Sintaxis Corta:

PPP.004 Nt opn fr outb *Protocol_Name* nt *network ID*

Sintaxis Larga:

PPP.004 Outbound data discarded, not open for protocol *Protocol_Name* on network *network ID*

Descripción:

Funcion pppout llamada por protocolo IP sin que este en estado OPEN. No se ha completado el establecimiento del protocolo IPCP.

PPP.005

Nivel: Error externo anormal, ERROR-AE/UE-ERROR

Sintaxis Corta:

PPP.005 Rcv Bd CRC, fr sz *frame_size* nt *network ID*

Sintaxis Larga:

PPP.005 Received packed with bad crc, frame size *frame_size*, on network *network ID*

Descripción:

Recibido paquete IP con error de CRC.

PPP.006

Nivel: Error externo normal, ERROR-NE/CE-ERROR

Sintaxis Corta:

PPP.006 I_ERR on rcv nt *network ID*

Sintaxis Larga:

PPP.006 Packet received with I_ERR set on network *network ID*

Descripción:

Funcion pppin detecta paquete con bit I_ERR.

PPP.007

Nivel: Error externo anormal, ERROR-AE/UE-ERROR



Sintaxis Corta:

PPP.007 Rcv Bd fr addr 0xAddress nt network ID

Sintaxis Larga:

PPP.007 Received packed with bad frame address = 0xAddress, on network network ID

Descripción:

Funcion pppin detecta paquete con campo de direccion invalido, no 0xFF.

PPP.008

Nivel: Error externo anormal, ERROR-AE/UE-ERROR

Sintaxis Corta:

PPP.008 Rcv Bd fr cntrl 0xControl_Field nt network ID

Sintaxis Larga:

PPP.008 Received packed with bad frame control field = 0xControl_Field, on network network ID

Descripción:

Funcion pppin detecta paquete con campo de control invalido, no 0x03 (UI).

PPP.009

Nivel: Error externo anormal, ERROR-AE/UE-ERROR

Sintaxis Corta:

PPP.009 Rcv inv prtcl 0xProtocol nt network ID

Sintaxis Larga:

PPP.009 Received packed with invalid protocol = 0xProtocol, on network network ID

Descripción:

Funcion pppin detecta paquete con campo de protocolo no reconocido.

PPP.010

Nivel: Error externo normal, ERROR-NE/CE-ERROR

Sintaxis Corta:

PPP.010 Nt opn fr inb Protocol_Name, nt network ID

Sintaxis Larga:

PPP.010 Inbound data discarded, not open for protocol Protocol_Name, on network network ID

Descripción:

Funcion pppin detecta paquetes de un protocolo que no esta en estado OPEN.

PPP.011

Nivel: Error externo normal, ERROR-NE/CE-ERROR

Sintaxis Corta:

PPP.011 Nt opn fr inb Control_Protocol_Name, nt network ID

Sintaxis Larga:



PPP.011 Inbound *Control_Protocol_Name*, discarded, not open for IPCP, on network *network ID*

Descripción:

Funcion pppin detecta tramas NCP sin que el LCP haya llegado a estado OPEN.

PPP.012

Nivel: Error externo normal, ERROR-NE/CE-ERROR

Sintaxis Corta:

PPP.012 PAP nt supp nt *network ID*

Sintaxis Larga:

PPP.012 Received PAP packet, PAP unsupported, on network *network ID*

Descripción:

Funcion pppin detecta paquete PAP no esperado.

Causa:

Se ha recibido un paquete de autentificacion aunque durante la negociacion LCP no se ha indicado esta opcion.

PPP.013

Nivel: Error externo normal, ERROR-NE/CE-ERROR

Sintaxis Corta:

PPP.013 prot 0x*Protocol* nt supp nt *network ID*

Sintaxis Larga:

PPP.013 Received packet with unsupported protocol 0x*Protocol* on network *network ID*

Descripción:

Funcion pppin detecta un paquete de un protocolo no implementado.

PPP.014

Nivel: Error externo anormal, ERROR-AE/UE-ERROR

Sintaxis Corta:

PPP.014 Nt Rcv flg, fr sz *frame_size* nt *network ID*

Sintaxis Larga:

PPP.014 Not Received end flag on frame with size *frame_size*, on network *network ID*

Descripción:

Funcion pppas_in no encuentra el flag de fin de trama.

Causa:

En modo de funcionamiento asincrono se ha recibido un trama que no tiene el flag de final esperado, debido a que es mas larga de lo indicado en la negociacion del MRU.

PPP.015

Nivel: Error interno anormal, ERROR-AI/UI-ERROR

Sintaxis Corta:



PPP.015 *fsm_name/state_name* snd bd *code*, xmt, nt *network ID*

Sintaxis Larga:

PPP.015 FSM = *fsm_name*, state = *state_name*, tried to send bad *code*, on network *network ID*

Descripción:

Llamada a la maquina de estados con un paquete con error de codigo

PPP.016

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

PPP.016 *fsm_name/state_name* snd *code*, id *id* len *len*, nt *network ID*

Sintaxis Larga:

PPP.016 FSM = *fsm_name*, state = *state_name*, sending *code*, id *id*, len *len*, on network *network ID*

Descripción:

Llamada a la maquina de estados. Indica el tipo de trama que se ha enviado.

PPP.017

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

PPP.017 *fsm_name/state_name* rcv *code*, id *id* len *len*, nt *network ID*

Sintaxis Larga:

PPP.017 FSM = *fsm_name*, state = *state_name*, received *code*, id *id*, len *len*, on network *network ID*

Descripción:

Llamada a la maquina de estados. Indica el tipo de trama que se ha recibido.

PPP.018

Nivel: Error externo normal, ERROR-NE/CE-ERROR

Sintaxis Corta:

PPP.018 *fsm_name msg_type* retr exc nt *network ID*

Sintaxis Larga:

PPP.018 *fsm_name msg_type* retries exceeded on network *network ID*

Descripción:

Se ha excedido el numero de intentos de transmision de un tipo de trama sin haberse recibido la respuesta adecuada desde el extremo remoto

PPP.019

Nivel: Comentario de un hecho normal, INFO-N/C-INFO

Sintaxis Corta:

PPP.019 SCRIPT: Inic script nt *network ID*

Sintaxis Larga:



PPP.019 SCRIPT: Iniciado script en red *network ID*

Descripción:

Se ha empezado a ejecutar el script tras haber recibido el connect de la red.

PPP.020

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

PPP.020 SCRIPT: *rcb matched_item nt network ID*

Sintaxis Larga:

PPP.020 SCRIPT: recibida concordancia *matched_item* en red *network ID*

Descripción:

Se ha recibido una secuencia de caracteres que concuerda con la del elemento actual del script.

PPP.021

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

PPP.021 SCRIPT: *esp wait_tmp seg nt network ID*

Sintaxis Larga:

PPP.021 SCRIPT: esperando *wait_tmp* segundo(s) en red *network ID*

Descripción:

Se esta esperando un tiempo correspondiente con el elemento actual del script. Esta traza corresponde a un elemento 'wait and send' del script.

PPP.022

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

PPP.022 SCRIPT: no concuerda, tira paq *nt network ID*

Sintaxis Larga:

PPP.022 SCRIPT: no concuerda, tira paquete en red *network ID*

Descripción:

Se tira paquete por no concordar con elemento actual del script. Esta traza suele corresponder con respuestas del proveedor que no son relevantes desde el punto de vista del script.

PPP.023

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

PPP.023 SCRIPT: *env resp_item nt network ID*

Sintaxis Larga:

PPP.023 SCRIPT: enviado *resp_item* en red *network ID*

Descripción:

Se ha enviado la respuesta correspondiente al elemento actual del script. Si el elemento es de



tipo PASSWORD se muestra la palabra "PASSWORD" en vez de la respuesta realmente mandada.

PPP.024

Nivel: Comentario de un hecho normal, INFO-N/C-INFO

Sintaxis Corta:

PPP.024 SCRIPT: Fin script nt *network ID*

Sintaxis Larga:

PPP.024 SCRIPT: Finalizado script en red *network ID*

Descripción:

Se ha terminado de ejecutar el script. Se empezara el PPP en el interfaz.

PPP.025

Nivel: Comentario de un hecho normal, INFO-N/C-INFO

Sintaxis Corta:

PPP.025 Agr PPP a mazo nt *network ID*

Sintaxis Larga:

PPP.025 Agregada PPP a mazo Multilink PPP red *network ID*

Descripción:

Se ha agregado una net PPP a un mazo multilink por demanda de trafico

PPP.026

Nivel: Comentario de un hecho normal, INFO-N/C-INFO

Sintaxis Corta:

PPP.026 Excl PPP del mazo nt *network ID*

Sintaxis Larga:

PPP.026 Excluida PPP del mazo Multilink PPP red *network ID*

Descripción:

Se ha excluido una net PPP de un mazo multilink por demanda de trafico

PPP.027

Nivel: Error externo anormal, ERROR-AE/UE-ERROR

Sintaxis Corta:

PPP.027 Excl PPP del mazo nt *network ID*

Sintaxis Larga:

PPP.027 Excluida PPP del mazo Multilink PPP red *network ID*

Descripción:

Se ha excluido una net PPP de un mazo multilink por errores de autenticacion o de IPCP.

Causa:

Llamadas adicionales de nets PPP que se agregan a un mazo multilink estan teniendo problemas en la autenticacion o la negociacion del protocolo IPCP



Acción:

Revisar las opciones de IPCP y la autenticación de la net PPP

PPP.028

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

PPP.028 rx sec *sec_rx* esp *sec_esp* nt *network ID*

Sintaxis Larga:

PPP.028 recibida sec *sec_rx*, esperada *sec_esp*, red *network ID*

Descripción:

Secuencia Multilink PPP recibida y esperada en net PPP

PPP.029

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

PPP.029 tx sec *sec_tx* nt *network ID*

Sintaxis Larga:

PPP.029 transmitida sec *sec_tx* red *network ID*

Descripción:

Secuencia Multilink PPP transmitida por net PPP

PPP.030

Nivel: Traza de operación normal, TRAZA-N/C-TRACE

Sintaxis Corta:

PPP.030 post sec *sec_rx* esp *sec_esp* nt *network ID*

Sintaxis Larga:

PPP.030 postpuesta sec *sec_rx*, esperada *sec_esp*, red *network ID*

Descripción:

Secuencia Multilink PPP recibida y esperada en net PPP, como la secuencia recibida es mayor que la esperada, la recepción se postpone y el paquete se encola hasta poder ser procesado

PPP.031

Nivel: Error externo anormal, ERROR-AE/UE-ERROR

Sintaxis Corta:

PPP.031 rx sec *sec_rx* esp *sec_esp* nt *network ID*

Sintaxis Larga:

PPP.031 recibida sec *sec_rx* menor que esperada *sec_esp*, red *network ID*

Descripción:

Secuencia Multilink PPP recibida es menor que la esperada en net PPP. Se viola la norma de número de secuencia siempre incrementándose. Se descarta el paquete por este motivo. Puede indicar problemas en el extremo remoto



PPP.035

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

PPP.035 mk mru *Max_Receive_Unit* nt *network ID*

Sintaxis Larga:

PPP.035 making max receive unit whit value *Max_Receive_Unit* on network *network ID*

Descripción:

Construida opcion MRU para la negociacion LCP

PPP.036

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

PPP.036 mk accm 0x*Asynchronous_Control_Character_Map* nt *network ID*

Sintaxis Larga:

PPP.036 making asynchronous control character map =
0x*Asynchronous_Control_Character_Map* on network *network ID*x

Descripción:

Construida opcion ACCM para la negociacion LCP

PPP.037

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

PPP.037 mk auth 0x*Authenticate_Protocol* nt *network ID*

Sintaxis Larga:

PPP.037 making authenticate protocol = 0x*Authenticate_Protocol* on network *network ID*

Descripción:

Construida opcion PAP para la negociacion LCP

PPP.038

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

PPP.038 mk mag 0x*Magic_Number* nt *network ID*

Sintaxis Larga:

PPP.038 making magic number = 0x*Magic_Number* on network *network ID*

Descripción:

Construida opcion de Numero Magico para la negociacion LCP

PPP.039



Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

PPP.039 mk pfc nt *network ID*

Sintaxis Larga:

PPP.039 making protocol field compression on network *network ID*

Descripción:

Construida opcion PFC para la negociacion LCP

PPP.040

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

PPP.040 mk acfc nt *network ID*

Sintaxis Larga:

PPP.040 making address/control field compression on network *network ID*

Descripción:

Construida opcion ACFC para la negociacion LCP

PPP.041

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

PPP.041 mk qp 0x*Quality_Protocol*, p = *Period* nt *network ID*

Sintaxis Larga:

PPP.041 making quality protocol = 0x*Quality_Protocol*, period *Period* on network *network ID*

Descripción:

Construida opcion Quality Protocol para la negociacion LCP

PPP.042

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

PPP.042 mk fcs nt *network ID*

Sintaxis Larga:

PPP.042 making 32-bits fcs on network *network ID*

Descripción:

Construida opcion longitud de FCS (CRC) para la negociacion LCP

PPP.044

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

PPP.044 ck mru *Max_Receive_Unit* nt *network ID*

Sintaxis Larga:



PPP.044 checking max receive unit whit value *Max_Receive_Unit* on network *network ID*

Descripción:

Procesada opcion MRU recibida en la negociacion LCP.

PPP.045

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

PPP.045 ck accm 0xAsynchronous_Control_Character_Map nt *network ID*

Sintaxis Larga:

PPP.045 checking asynchronous control character map =
0xAsynchronous_Control_Character_Map on network *network ID*

Descripción:

Procesada opcion ACCM recibida en la negociacion LCP.

PPP.046

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

PPP.046 ck auth 0xAuthenticate_Protocol nt *network ID*

Sintaxis Larga:

PPP.046 checking authenticate protocol = 0xAuthenticate_Protocol on network *network ID*

Descripción:

Procesada opcion PAP recibida en la negociacion LCP.

PPP.047

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

PPP.047 ck mag 0xMagic_Number nt *network ID*

Sintaxis Larga:

PPP.047 checking magic number = 0xMagic_Number on network *network ID*

Descripción:

Procesada opcion de Numero Magico recibida en la negociacion LCP.

PPP.048

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

PPP.048 ck pfc nt *network ID*

Sintaxis Larga:

PPP.048 checking protocol field compression on network *network ID*

Descripción:

Procesada opcion PFC recibida en la negociacion LCP.



PPP.049

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

PPP.049 ck acfc nt *network ID*

Sintaxis Larga:

PPP.049 checking address/control field compression on network *network ID*

Descripción:

Procesada opcion ACFC recibida en la negociacion LCP.

PPP.050

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

PPP.050 ck qp 0x*Quality_Protocol*, p = *Period* nt *network ID*

Sintaxis Larga:

PPP.050 checking quality protocol = 0x*Quality_Protocol*, period *Period* on network *network ID*

Descripción:

Procesada opcion Quality Protocol recibida en la negociacion LCP.

PPP.051

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

PPP.051 ck fcs nt *network ID*

Sintaxis Larga:

PPP.051 checking 32-bits fcs on network *network ID*

Descripción:

Procesada opcion de longitud de FCS (CRC) recibida en la negociacion LCP.

PPP.052

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

PPP.052 ck lcp unk 0x*Unknown_Option* nt *network ID*

Sintaxis Larga:

PPP.052 making unknown lcp option 0x*Unknown_Option* on network *network ID*

Descripción:

Procesada opcion no reconocida recibida en la negociacion LCP.

Causa:

Se ha recibido una opcion en la negociacion LCP que no esta implementada.



PPP.053

Nivel: Comentario de un hecho normal, INFO-N/C-INFO

Sintaxis Corta:

PPP.053 rc LCP-Idnt *Identification* nt *network ID*

Sintaxis Larga:

PPP.053 recibido LCP-*Identification Identification* nt *network ID*

Descripción:

Se ha recibido un paquete LCP *Identification*. Este paquete informa de extremo remoto.

PPP.054

Nivel: Error externo anormal, ERROR-AE/UE-ERROR

Sintaxis Corta:

PPP.054 Bd *network ID*

Sintaxis Larga:

PPP.054 Bad *network ID*

Descripción:

Funcion *lcprsmg* detecta trama con id no valido.

Causa:

No coincide el id de respuesta a una trama *configure request* o *terminate request* con el id esperado

PPP.055

Nivel: Error externo anormal, ERROR-AE/UE-ERROR

Sintaxis Corta:

PPP.055 Bd *network ID*

Sintaxis Larga:

PPP.055 Bad *network ID*

Descripción:

Funcion *lcprsmg* detecta trama con longitud no valida.

Causa:

Se ha recibido una trama en la que no coincide el numero de datos recibidos con la longitud que se indica para ellos.

PPP.056

Nivel: Error externo anormal, ERROR-AE/UE-ERROR

Sintaxis Corta:

PPP.056 *Msmtdhd network ID*

Sintaxis Larga:

PPP.056 Mis-matched data in *network ID*

Descripción:

Funcion *lcprsmg* detecta trama con datos no esperados.



Causa:

Se ha recibido asentimiento a opciones de negociacion que no han sido enviadas.

PPP.057

Nivel: Error externo anormal, ERROR-AE/UE-ERROR

Sintaxis Corta:

PPP.057 Bd *network ID*

Sintaxis Larga:

PPP.057 Bad *network ID*

Descripción:

Funcion lcpmsg detecta trama nak con id invalido

Causa:

La trama de rechazo a opciones de negociacion LCP se recibe con un id que no coincide con el esperado.

PPP.058

Nivel: Error externo anormal, ERROR-AE/UE-ERROR

Sintaxis Corta:

PPP.058 Bd *network ID*

Sintaxis Larga:

PPP.058 Bad *network ID*

Descripción:

Funcion lcpmsg detecta trama nak con longitud invalida

Causa:

La trama de rechazo a opciones de negociacion LCP se recibe con una longitud que no coincide con la esperada.

PPP.059

Nivel: Comentario de un hecho normal, INFO-N/C-INFO

Sintaxis Corta:

PPP.059 Usr *user_login* auth suc, nt *network ID*

Sintaxis Larga:

PPP.059 User *user_login* authenticate successful, on network *network ID*

Descripción:

Se ha completado con exito el proceso de autentificacion para el usuario indicado

PPP.060

Nivel: Comentario de un hecho normal, INFO-N/C-INFO

Sintaxis Corta:

PPP.060 Usr *user_login* auth fail, nt *network ID*

Sintaxis Larga:



PPP.060 User *user_login* authenticate failed, on network *network ID*

Descripción:

No se ha completado con éxito el proceso de autenticación para el usuario indicado

Causa:

La programación del usuario-clave no es reconocida.

Acción:

Reprogramar las opciones de usuario y clave para el PAP. Si el problema persiste consultar con su proveedor de acceso al servicio

PPP.061

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

PPP.061 mk mrru *Max_Receive_Reconstructed_Unit* nt *network ID*

Sintaxis Larga:

PPP.061 making max receive reconstructed unit whit value *Max_Receive_Reconstructed_Unit* on network *network ID*

Descripción:

Construida opción MRRU para la negociación LCP

PPP.062

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

PPP.062 mk ssnfh nt *network ID*

Sintaxis Larga:

PPP.062 making short sequence number header format on network *network ID*

Descripción:

Construida opción SSNHF para la negociación LCP

PPP.063

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

PPP.063 mk endpd *Endpoint_Discriminator_Class* nt *network ID*

Sintaxis Larga:

PPP.063 making endpoint discriminator whit value *Endpoint_Discriminator_Class* on network *network ID*

Descripción:

Construida opción ENDPD para la negociación LCP

PPP.066

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:



PPP.066 mk adds *src_addr*, *dest_addr* nt *network ID*

Sintaxis Larga:

PPP.066 making IPCP addresses option, addresses *src_addr*, *dest_addr*, on network *network ID*

Descripción:

Construida opcion de addresses para la negociacion IPCP

PPP.067

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

PPP.067 mk cmp *0xcomp_protocol*, *slt=0xslot*, *slt_cmp=0xslot_comp* nt *network ID*

Sintaxis Larga:

PPP.067 making compression option *0xcomp_protocol* *slot=0xslot*, *slot_comp=0xslot_comp* on network *network ID*

Descripción:

Construida opcion de compresion IP para la negociacion IPCP

PPP.068

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

PPP.068 mk ad *ip_address* nt *network ID*

Sintaxis Larga:

PPP.068 making IPCP address option, address = *ip_address* on network *network ID*

Descripción:

Construida opcion de address para la negociacion IPCP

PPP.069

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

PPP.069 mk ipcp unk nt *network ID*

Sintaxis Larga:

PPP.069 making unknown lcp option on network *network ID*

Descripción:

Inicializado buffer para almacenar opciones de negociacion IPCP recibidas y no reconocidas o no implementadas.

PPP.070

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

PPP.070 ck adds *src_addr*, *dest_addr* nt *network ID*

Sintaxis Larga:



PPP.070 checking IPCP addresses option, addresses *src_addr*, *dest_addr*, on network *network ID*

Descripción:

Procesada opcion de addresses recibida en la negociacion IPCP.

PPP.071

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

PPP.071 ck cmp 0xcomp_protocol slt=0xslot, slt_cmp=0xslot_comp nt network ID

Sintaxis Larga:

PPP.071 checking compression option 0xcomp_protocol slot=0xslot, slot_cmp=0xslot_comp on network *network ID*

Descripción:

Procesada opcion de compresion IP recibida en la negociacion IPCP.

PPP.072

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

PPP.072 ck ad ip_address nt network ID

Sintaxis Larga:

PPP.072 checkinig IPCP address option, address = *ip_address* on network *network ID*

Descripción:

Procesada opcion de address recibida en la negociacion IPCP.

PPP.073

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

PPP.073 ck ipcp unk 0xunk_option nt network ID

Sintaxis Larga:

PPP.073 ckecking unknown lcp option 0xunk_option on network *network ID*

Descripción:

Procesada opcion no reconocida recibida en la negociacion IPCP.

PPP.074

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

PPP.074 ck mrru Max_Receive_Reconstructed_Unit nt network ID

Sintaxis Larga:

PPP.074 checking max receive reconstructed unit whit value
Max_Receive_Reconstructed_Unit on network *network ID*

Descripción:



Procesada opcion MRRU recibida en la negociacion LCP

PPP.075

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

PPP.075 ck ssnfh nt *network ID*

Sintaxis Larga:

PPP.075 checking short sequence number header format on network *network ID*

Descripción:

Procesada opcion SSNHF recibida en la negociacion LCP

PPP.076

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

PPP.076 ck endpd *Endpoint_Discrimator_Class* nt *network ID*

Sintaxis Larga:

PPP.076 checking endpoint discriminator whit value *Endpoint_Discrimator_Class* on network *network ID*

Descripción:

Procesada opcion ENDPD para la negociacion LCP

PPP.078

Nivel: Comentario de un hecho normal, INFO-N/C-INFO

Sintaxis Corta:

PPP.078 Mdm Chg 0x*network ID*

Sintaxis Larga:

PPP.078 Modem status changed 0x*network ID*

Descripción:

Cambio de estado en las señales del interfaz

PPP.079

Nivel: Error externo anormal, ERROR-AE/UE-ERROR

Sintaxis Corta:

PPP.079 Prt rej rcv, prt= 0x*Protocol_rejected* nt *network ID*

Sintaxis Larga:

PPP.079 Protocol reject received for protocol 0x*Protocol_rejected*, on network *network ID*

Descripción:

Se ha recibido un protocolo reject.

Causa:

Se han enviado paquetes de un protocolo que no esta implementado o que no es reconocido por el extremo remoto.



PPP.080

Nivel: Error externo anormal, ERROR-AE/UE-ERROR

Sintaxis Corta:

PPP.080 MPPP sq rx lst = *value* nt *network ID*

Sintaxis Larga:

PPP.080 MPPP sequence reception lost *value* = *value* , on network *network ID*

Descripción:

Se ha perdido una secuencia en recepcion cuando se ha detectado que se ha llenado el buffer disponible para reordenado de tramas recibidas

Causa:

Se ha perdido algun paquete o se han recibido errores que han provocado la perdida de alguna trama en recepcion

PPP.081

Nivel: Error externo anormal, ERROR-AE/UE-ERROR

Sintaxis Corta:

PPP.081 rc bd mgc 0xrcv_mag_num, ours 0xour_mag_num, nt *network ID*

Sintaxis Larga:

PPP.081 Received bad magic number 0xrcv_mag_num, ours 0xour_mag_num, on network *network ID*

Descripción:

Se ha recibido una trama con un numero magico que no coincide con el que se ha indicado durante la negociacion LCP

PPP.083

Nivel: Comentario de un hecho normal, INFO-N/C-INFO

Sintaxis Corta:

PPP.083 Dial Req Call, addr = *call_address* nt *network ID*

Sintaxis Larga:

PPP.083 Dial Request Call, Destination address = *call_address*, on network *network ID*

Descripción:

Se realiza un llamada a la direccion indicada

PPP.084

Nivel: Comentario de un hecho normal, INFO-N/C-INFO

Sintaxis Corta:

PPP.084 Out Call *destination_address* cmp nt *network ID*

Sintaxis Larga:

PPP.084 Out Call established to *destination_address* ,on network *network ID*

Descripción:



Completada con éxito la llamada a la dirección indicada

PPP.085

Nivel: Comentario de un hecho normal, INFO-N/C-INFO

Sintaxis Corta:

PPP.085 Clr Call, idle timeout, *idle_time* sec, nt *network ID*

Sintaxis Larga:

PPP.085 Clear Call, absence data in time = *idle_time* sec on network *network ID*

Descripción:

Desconexión de una llamada por ausencia de tráfico durante el periodo indicado. Los paquetes de mantenimiento (eco) no son computados a la hora de considerar el tiempo sin tráfico.

PPP.086

Nivel: Comentario de un hecho normal, INFO-N/C-INFO

Sintaxis Corta:

PPP.086 Call nt stb to *destination_address* nt *network ID*

Sintaxis Larga:

PPP.086 Call not established to *destination_address*, no answer ,on network *network ID*

Descripción:

No se ha completado la llamada a la dirección indicada por que no se ha detectado respuesta del extremo remoto

PPP.087

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

PPP.087 Pkt *source_ip_address* -> *destination_ip_address* nt *Network ID*

Sintaxis Larga:

PPP.087 Discarded packet from *source_ip_address* for *destination_ip_address* ,on network *Network ID*

Descripción:

Solo para pruebas, para ver quien activa la llamada

PPP.088

Nivel: Comentario de un hecho normal, INFO-N/C-INFO

Sintaxis Corta:

PPP.088 Clr Call *destination_address* rel nt *network ID*

Sintaxis Larga:

PPP.088 Out Call released to *destination_address* ,on network *network ID*

Descripción:

Liberación de la llamada a la dirección indicada



PPP.089

Nivel: Comentario de un hecho normal, INFO-N/C-INFO

Sintaxis Corta:

PPP.089 In Call cmp nt *network ID*

Sintaxis Larga:

PPP.089 Input Call established on network *network ID*

Descripción:

Completada con éxito la respuesta a una llamada entrante



2. Ejemplo de eventos del protocolo PPP

A continuación se muestra una traza de eventos típica de una conexión a través de RDSI:

```
*PROCESS 2
25/03/99 14:29:31 PPP.083 Dial Req Call, addr = 917529000 nt 5 int PPP/1
25/03/99 14:29:32 PPP.084 Out Call 917529000 cmp nt 5 int PPP/1
25/03/99 14:29:32 PPP.035 mk mru 1500 nt 5 int PPP/1
25/03/99 14:29:32 PPP.038 mk mag 0x2B7C9649 nt 5 int PPP/1
25/03/99 14:29:32 PPP.068 mk ad 0.0.0.0 nt 5 int PPP/1
25/03/99 14:29:32 PPP.016 LCP FSM/CLOSED snd scr , id 0 len 14, nt 5 int PPP/1
25/03/99 14:29:35 PPP.016 LCP FSM/REQ_SENT snd scr , id 0 len 14, nt 5 int PPP/1
25/03/99 14:29:35 PPP.074 ck mrru 1500 nt 5 int PPP/1
25/03/99 14:29:35 PPP.076 ck endpd 0 nt 5 int PPP/1
25/03/99 14:29:35 PPP.047 ck mag 0xF408EBB8 nt 5 int PPP/1
25/03/99 14:29:35 PPP.046 ck auth 0xFFFFFC023 nt 5 int PPP/1
25/03/99 14:29:35 PPP.017 LCP FSM/REQ_SENT rcv RCR- , id 1 len 21, nt 5 int PPP/1
25/03/99 14:29:35 PPP.016 LCP FSM/REQ_SENT snd scn , id 1 len 11, nt 5 int PPP/1
25/03/99 14:29:35 PPP.047 ck mag 0xF408EBB8 nt 5 int PPP/1
25/03/99 14:29:35 PPP.046 ck auth 0xFFFFFC023 nt 5 int PPP/1
25/03/99 14:29:35 PPP.017 LCP FSM/REQ_SENT rcv RCR+ , id 2 len 14, nt 5 int PPP/1
25/03/99 14:29:35 PPP.016 LCP FSM/REQ_SENT snd sca , id 2 len 14, nt 5 int PPP/1
25/03/99 14:29:38 PPP.016 LCP FSM/ACK_SENT snd scr , id 0 len 14, nt 5 int PPP/1
25/03/99 14:29:38 PPP.017 LCP FSM/ACK_SENT rcv RCA , id 0 len 14, nt 5 int PPP/1
25/03/99 14:29:38 PPP.016 PAP FSM/INITIAL snd scr , id 1 len 28, nt 5 int PPP/1
25/03/99 14:29:38 PPP.003 Mnt nt 5 int PPP/1
25/03/99 14:29:38 PPP.016 LCP FSM/OPENED snd serq , id 1 len 8, nt 5 int PPP/1
25/03/99 14:29:38 PPP.017 LCP FSM/OPENED rcv RXR , id 1 len 8, nt 5 int PPP/1
25/03/99 14:29:38 PPP.017 PAP FSM/REQ_SENT rcv RCA , id 1 len 20, nt 5 int PPP/1
25/03/99 14:29:38 PPP.059 Usr infoviaplus auth suc, nt 5 int PPP/1
25/03/99 14:29:38 PPP.016 IPCP FSM/CLOSED snd scr , id 1 len 10, nt 5 int PPP/1
25/03/99 14:29:38 PPP.072 ck ad 193.152.22.2 nt 5 int PPP/1
25/03/99 14:29:38 PPP.017 IPCP FSM/REQ_SENT rcv RCR+ , id 1 len 10, nt 5 int PPP/1
25/03/99 14:29:38 PPP.016 IPCP FSM/REQ_SENT snd sca , id 1 len 10, nt 5 int PPP/1
25/03/99 14:29:38 PPP.072 ck ad 193.153.67.106 nt 5 int PPP/1
25/03/99 14:29:38 PPP.017 IPCP FSM/ACK_SENT rcv RCN , id 1 len 10, nt 5 int PPP/1
25/03/99 14:29:38 PPP.016 IPCP FSM/ACK_SENT snd scr , id 2 len 10, nt 5 int PPP/1
25/03/99 14:29:38 PPP.017 IPCP FSM/ACK_SENT rcv RCA , id 2 len 10, nt 5 int PPP/1
25/03/99 14:29:38 PPP.001 Req brng up IP, addr = 193.153.67.106 nt 5 int PPP/1
25/03/99 14:29:38 PPP.013 prot 0x80FD nt supp nt 5 int PPP/1
25/03/99 14:29:48 PPP.003 Mnt nt 5 int PPP/1
25/03/99 14:29:48 PPP.016 LCP FSM/OPENED snd serq , id 2 len 8, nt 5 int PPP/1
25/03/99 14:29:48 PPP.017 LCP FSM/OPENED rcv RXR , id 2 len 8, nt 5 int PPP/1
25/03/99 14:29:58 PPP.003 Mnt nt 5 int PPP/1
25/03/99 14:29:58 PPP.016 LCP FSM/OPENED snd serq , id 3 len 8, nt 5 int PPP/1
25/03/99 14:29:58 PPP.017 LCP FSM/OPENED rcv RXR , id 3 len 8, nt 5 int PPP/1
<CTRL-P>
*
```

