Teldat Router

PPP Interface

Doc. *DM510-I* Rev. *8.31*
May, 2000

INDEX

Chapter 1
PPP Interface

1. Description

The PPP protocol provides a mechanism to transmit datagrams of various protocols over a point to point link. This protocol is specified in the RFC-1661. PPP supports data transmission both in synchronous and asynchronous forms and provides the following services:

- LCP(Link Control Protocol) link control establishment, configure and test the link.
- Encapsulate in order to transmit the datagrams over the link.
- Authentication protocols in order to demand the PPP remote end link authenticates before being able to transmit the data over the link. In the current implementation, PAP (Password Authentication Protocol) protocol (described in the RFC-1172) and CHAP (Challenge Handshake Authentication Protocol) protocol (described in the RFC-1994) are supported.
- PPP Multilink Protocol complying with the RFC-1990. The PPP Multilink protocol supports dividing, recombining and sequencing of datagrams through multiple data links. The current implementation permits the addition of ISDN B channels to one or various MPPP logical channels. It is also possible to aggregate PPP interfaces (both synchronous and asynchronous) to an MPPP channel over WAN, although in this case you should only aggregate one PPP interface in each MPPP channel.
- NCP protocols (Network Control Protocols) in order to establish and configure the various network protocols which travel over PPP.

NB. In the current implementation, the network protocol supported over PPP is IP (Internet Protocol) with its corresponding IPCP control protocol (Internet Protocol Control Protocol) described in RFC-1332.

To carry out the connection establishment over a point to point link, the originator PPP sends LCP packets in order to configure and test the link. Once this has been established at link level (data-link layer), the PPP sends NCP packets corresponding to the supported protocols (in this case it is only IPCP) in order to configure and establish the network level in the link (Network layer). Once these protocols have been configured, the PPP transmits the datagrams of each protocol over the link.

In order to implement the PPP in an asynchronous form, the adaptation is carried out in compliance with the RFC-1662.

In the current implementation, there exists four possibilities:

1. Define a PPP interface over a serial line in a synchronous format which through a cable or an external device or a terminal adapter, permits you to establish the link with the other end.
2. Aggregate a PPP interface over a basic access in order to connect through ISDN with the other end. In this case, the data format is synchronous in transmission.
3. Define a PPP interface over a serial line in an asynchronous format which through a cable or an external device or a terminal adapter, permits you to establish the link with the other end.
4. Aggregate a PPP interface over an AT command interface in order to connect through a modem with the other end. In this case, the data format is asynchronous in transmission.

2. PPP Frame structure

The PPP transmits frames which have the same structure as the HDLC frames. The PPP uses a synchronous method of transmission, bit orientated with the following frame structure:

FLAG	ADDRESS	CONTROL	PROTOCOL	INFORMATION	FCS	FLAG

FLAG

Indicates the beginning and end of each frame with a unique pattern: 01111110. Supports frame synchronism. Among the rest of the frame data, transparency is implemented, bit-stuffing, so this character does not appear. The transparency consists of once five consecutive 1's have been transmitted, an 0 is transmitted. This 0 is excluded from the data on reception.

ADDRESS

HDLC frame address field. 11111111 is always used in the PPP protocol. Individual addresses are not assigned.

CONTROL

Control field. All the PPP frames are HDLC unnumbered information (UI) frames with a field value of 00000011.

PROTOCOL

This is a 2 byte field which distinguishes the various protocols transported over the point to point link. All those which contain a value of Cxxx in this field correspond to the link configuration protocols (LCP, PAP). Those which contain a value of 8xxx correspond to the network control protocols (NCP) and the value 0xxx corresponds to specific datagram transmissions over the link.

INFORMATION

Zero or more bytes contained in the datagram for the transported protocol. If the protocol is LCP or NCP this field will contain parameters to configure the link.

FCS

Field used to include the error detection mechanism which in this case is the cyclic redundancy check (CRC) for 2 byte error detection.

2.1. Asynchronous PPP adaptation

When the data transmission format is asynchronous, the same framing is carried out as in the synchronous, according to the RFC-1662. The transported bytes are encapsulated within the frame previously described, but a transparency character is used, 0x7D in order to implement the bit-stuffing.

In the transmission direction, after the FCS check, all the characters to be sent are examined. Each flag, control character (below 0x20), escape character (0x7D) or anything else defined in the ACCM, is substituted for a transparency character and an additional character which is the result of an OR-exclusive with 0x20.

At reception, before the FCS check, all the frame bytes are examined. When the transparency character appears, it is eliminated and the following character is substituted by its OR-exclusive with 0x20.

The check and the subsequent CRC check (FCS) of the frame is carried out through a polynomial defined in the RFC-1662 and its subsequent transmission is also affected by the transparency. E.G. the 0x11 character (XON) is encoded within the frame in transmission as 0x7D + 0x31. At reception, the 0x7D and the following byte are substituted by its OR exclusive with 0x20, resulting in 0x11.

3. Link Control Protocol

The PPP LCP supports the establishment, configuration, maintenance and finalizing of a link. This process consists of 4 stages:

1. Before exchanging IP datagrams over the link, the LCP opens communications between the ends through an exchange of CONFIGURE-REQUEST LCP packets. Once the configuration has been accepted between the two ends with the CONFIGURE-ACK packets, the link is in an “OPEN” state.
2. Once the LCP has determined that the link is OPEN, it determines if it is of a high enough quality to start the network protocols. It is here, during this process that link authentication is carried out if required.
3. Once the LCP has checked the link quality is high enough, the NCP control protocols at the network layer are started.
4. Finally, once these have been established, the LCP, through the ECHO-REQUEST and ECHO-REPLY transmission packets, takes over the link maintenance. If you wish to terminate the connection (e.g. due to inactivity), the LCP terminates the link though the TERMINATE-REQUEST and TERMINATE-ACK transmission packets.

4. LCP packet format

The LCP packets travel in the same format as previously described. These are distinguished in the protocol field (C021) and in the Information field, the packet type and the associated data are encoded:

CODE	IDENTIFIER	SIZE	DATA

CODE

One byte field which identifies the LCP packet type according to the following table:

CODE	LCP PACKET TYPE
1	CONFIGURE-REQUEST (Establishment)
2	CONFIGURE-ACK (Establishment)
3	CONFIGURE-NAK (Establishment)
4	CONFIGURE-REJECT (Establishment)
5	TERMINATE-REQUEST (Terminate)
6	TERMINATE-ACK (Terminate)
7	CODE-REJECT (Maintenance)
8	PROTOCOL-REJECT (Maintenance)
9	ECHO-REQUEST (Maintenance)
10	ECHO-REPLY (Maintenance)
11	DISCARD-REQUEST (Maintenance)

IDENTIFIER

One byte field which supports link requests and answers identification.

SIZE

Two bytes which indicate the total length of the LCP frame. Where an asynchronous mode is used, this does not include the possible transparent characters which exist within the frame.

DATA (Optional)

With zero or more bytes whose format is related to the type of LCP packet through which it travels.

As seen in the table, the LCP packets can in grouped into three types:

- Packets in order to establish the link
  - **CONFIGURE-REQUEST**

    Packet to be transmitted when you wish to open a link. Within this all the configuration options are found. At reception, it should send an appropriate answer with one of the following packets.
  - **CONFIGURE-ACK**

    The received configuration options are accepted. The frame identifier field should coincide with the accepted configure-request. Once the two ends have received the ACK from the remote end, the link enters an OPEN state.
  - **CONFIGURE-NAK**

    Some of the configuration options received in the frame with the identifier used are not accepted but the recommended value is sent or accepted by the extreme. When a NAK is received, the receptor should generate a new CONFIGURE-REQUEST which contains the accepted values indicated.

- **CONFIGURE-REJECT**

  Some of the configuration options received in the frame with the identifier used are not accepted or acknowledged. When a REJECT is received, the receptor should generate a new CONFIGURE-REQUEST which does not contain the rejected values.

- Packets to terminate the link
  - **TERMINATE-REQUEST**

    Packet which is transmitted when you wish to terminate, close, the link.
  - **TERMINATE-ACK**

    Packet which is transmitted after a TERMINATE-REQUEST is received. The reception of an unexpected TERMINATE-ACK indicates that the link has been closed.
- Packets for link maintenance
  - **CODE-REJECT**

    Indicates that an incomplete LCP packet has been received or one with an unknown code. If the packet persists in being transmitted, the link will close.
  - **PROTOCOL-REJECT**

    Indicates that a PPP frame with a non implemented protocol field has been received. The end frame receptor should cease sending this protocol.
  - **ECHO-REQUEST and ECHO-REPLY**

    Provides link maintenance mechanism. This regularly generates a code request ECHO - REQUEST which should be returned with an ECHO-REPLY.
  - **DISCARD-REQUEST**

    Provides a discard, elimination, frame mechanism. This is used for checking.

5. Authentication Protocols

PPP has a series of protocols available which allow you to authenticate and verify the link. This is only established when it is checked that the login (user) and the password values expected in the extreme end are correct. This method is usually used in links where routers connect to the network via switched circuits (ISDN or PSTN) although it can be used in point to point circuits.

This check is carried out before establishing the network control protocols (NCP). If authentication is demanded and it not completed correctly, the link establishment is terminated.

There are two authentication methods defined in the RFC-1334. These are:

5.1. Password Authentication Protocol (PAP)

Provides a simple method to authenticate a link using 2-ways:

1. Once you have achieved an OPEN state in the LCP negotiation, the extreme end you wish to contact sends a user (login) and password to the authenticator.
2. The extreme end checks that this is valid and sends a response, accepting or rejecting the call.

This authentication method is not very safe due to the fact that the user and password are sent over the network in clear. This means that there is no type of protection against errors or other attacks. This problem is resolved by another authentication method, CHAP.

a) PAP packet format

The PAP packets travel in the same format as previously described for the PPP frames. The protocol field differentiates them (C023) and the type of packet and associated data are encrypted in the Information field:

CODE	IDENTIFIER	SIZE	DATA

CODE

One byte field which identifies the type of LCP packet complying with the following table:

CODE	PAP PACKET TYPE
1	AUTHENTICATE-REQUEST
2	AUTHENTICATE-ACK
3	AUTHENTICATE-NAK

IDENTIFIER

One byte field which permits you to identify requests and responses over the link.

SIZE

Two bytes which indicate the total length of the PAP frame.

DATA (Optional)

With zero or more bytes whose format is related to the type of PAP packet through which it travels.

As seen in the table, the PAP packets can in grouped into three types:

- **AUTHENTICATE-REQUEST**

Packet to be transmitted when you wish to authenticate a link. The login and password used are sent within this. At reception, it should send an appropriate answer with one of the following packets.

- **AUTHENTICATE-ACK**

The received values are accepted. The frame identifier field should coincide with the accepted authenticate-request. Once the ACK from the extreme authenticator has been received, you can continue to establish the network control protocols (NCP).

- **AUTHENTICATE-NAK**

The values are not accepted. The extreme which wishes to authenticate the link needs to send a new request with adequate values or terminate the link.

5.2. Challenge Authentication Protocol (CHAP)

Provides a “safe” method to authenticate a link using a 3-way handshake.

1. Once an OPEN state has been achieved in the LCP negotiation, the end authenticator sends a password to the other end, known as Challenge. This password is variable in all the connections generally being a random value whose number of bytes depend on the algorithm used for the subsequent encoding. In this case the method implemented is the MD5 algorithm defined in the RFC - 1321 recommendation. This defines a length of 16 bytes for the challenge.
2. The end which receives the challenge, encrypts this with the password which it has programmed and sends the response to the authenticator end. The encryption function is defined by the MD5 algorithm and is the same at both ends.
3. On receiving the response, the authenticator verifies that what he has received is what was expected and permits (success) or not (failed) to continue establishing the network protocols.

The security of this method depends on the secrecy of the password at both ends. With this method, the password never passes through the network in “clear”.

This method also permits link authentication even once the network protocols have been established (e.g. IP) to check their security.

a) CHAP packets format

The CHAP packets travel in the same format as previously described for the PPP frames. The protocol field differentiates them (C223) and the type of packet and associated data are encrypted in the Information field:

CODE	IDENTIFIER	SIZE	DATA

CODE

One byte field which identifies the type of LCP packet complying with the following table:

CODE	CHAP PACKET TYPE
1	CHALLENGE
2	RESPONSE
3	SUCCESS
4	FAILED

IDENTIFIER

One byte field which permits you to identify requests and responses over the link.

SIZE

Two bytes which indicate the total length of the CHAP frame.

DATA (Optional)

With zero or more bytes whose format is related to the type of CHAP packet through which it travels.

As seen in the table, the CHAP packets can in grouped into four types:

- **CHALLENGE**

  Packets which are transmitted by the extreme authenticator when you wish to authenticate a link. The challenge that should be used for encryption travels within these and the name of the network you wish to access is indicated in clear. This value can be used where the responding end sends the correct value and is ready to connect to various networks. I.e. you can program distinct passwords depending on the network you wish to access.

- **RESPONSE**

  Packet sent to the other end in which the encrypted password with the received password travels.

- **SUCCESS**

  The received value is accepted. Once the SUCCESS is received from the extreme authenticator, you can proceed to establish the network protocols (NCP).

- **FAILED**

  The received value is not accepted. The extreme which wishes to authenticate the link must send a new request with the correct values or terminate the link

6. Network Control Protocol (NCP)

The PPP has a series of network control protocols (NCP) in order to establish and configure the various network protocols which travel over PPP. The corresponding NCP to each protocol configures, enables and disables the network protocols between the two link ends.

Currently, the only protocol implemented in the **Teldat Router** is IPCP (Internet Protocol Control Protocol) described in the RFC-1332 recommendation.

The IPCP allows you to indicate using the Van Jacobson compression (or not) and in that way permits a mechanism in order to exchange IP addresses between both ends or the dynamic assignation of the IP number necessary for the InfoVía and Internet connections.

7. Request for Comments

RFC-1661: The Point to Point protocol, W. Simpson, July-1994

RFC-1662: PPP in HDLC-Like Framing, W. Simpson, July-1994

RFC-1618: PPP in ISDN, W.Simpson, May-1994

RFC-1570: PPP LCP extensions, W. Simpson, January-1994

RFC-1332: PPP Internet control protocol, G. McGregor, May-1992

RFC-1334: PPP Authentication protocols, B. Lloyd, October-1992

RFC-1172: Point-to-Point Protocol (PPP) initial configuration options. D. Perkins, R. Hobby. July-1990

RFC-1994: PPP Challenge Handshake Authentication Protocol (CHAP). W. Simpson. August-1996

RFC-1321: The MD5 message-digest Algorithm. R. Rivest, April-1992

RFC-1700: Assigned numbers, IETF, October-1994

RFC-1471: The Definitions of Managed Objects for the Link Control Protocol of the Point-to-Point Protocol, F. Kastenholz , August-1993

RFC-1631: The IP Network Address Translator (NAT) , Egevang & Francis, May-1994

RFC-1990: The PPP Multilink Protocol (MP), Network Working Group, August-1996

Chapter 2
PPP Interface Configuration

1. PPP interface assignation

- Should you wish to configure a serial interface such as SYNCHRONOUS PPP interface from the configuration menu, enter:

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

- Should you wish to configure a serial interface such as ASYNCHRONOUS PPP interface from the configuration menu, enter:

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

- Should you wish to configure a PPP interface over an ISDN basic access, enter:

```
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>
```

Older versions of the **Teldat Router** support a maximum of two B channels, one in each ISDN connector. From the 6.0 version up to four B channels can be supported provided that the device has 6 serial lines available. During the procedure to add the PPP-DIAL interface, you must indicate which serial line you wish to exchange for a third or a fourth B channel The serial lines available for this exchange are the fifth and the sixth. This means that the PPP-DIAL B channels are always added at the cost of losing the X.25 B channels or the serial lines 5 and 6. When you add a PPP-DIAL interface, you will be asked which interface is to be eliminated, i.e. the X.25 B channel or serial lines 5 or 6.

NOTE: In order to use a third or fourth B channel, the PJ10 jumpers in the device must be set on ISDN position. If you wish to use the serial lines 5 and 6, the jumpers must be set on DTE5.

- Should you wish to configure a PPP interface over an E1/PRI ISDN interface B channel, enter the following:

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

You can check that the created interface has been correctly added by listing the interfaces (and checking that a *PPP Generic Dial* interface has been generated).

```
Config>LIST DEVICES

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

The **Teldat Router** with an E1/PRI ISDN interface supports a link of 2048 Kbps complying with the G.703 and G.704 recommendations with 30 or 31 B channels available in the principal. While aggregating the PPP-DIAL interface, you do not have to indicate the channel type or number over which you wish to establish the PPP connection as these parameters have been previously configured.

NOTE: The method used to aggregate PPP-DIAL interfaces is identical both when dealing with an ISDN basic access or when they are added to an E1/PRI ISDN interface. This does not give rise to ambiguities due to the fact that the router possess the hardware corresponding to one of the interface types. If you have a card installed supporting G.703 interface at 2048 Kbps, the router detects this and the configuration of the PPP-DIAL interfaces is carried out over this interface.

- Should you wish to configure a PPP interface over an AT command interface, enter:

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

NOTE: The Interface driver should always be configured as DTE.

The protocol supported over all types of available PPP interfaces is IP. In order to activate the IP over the PPP protocol it is necessary to assign an IP address to this interface. To do this you need to enter the IP protocol configuration and assign an IP address. This operation should always be carried out independently whether the interface obtains a dynamic IP address or not. Please note that only one IP address is supported for each PPP interface as the IPCP protocol only allows you to configure one for each PPP interface. Additional addresses should not be added to the PPP interface.

The example displayed below shows you how to carry out this procedure.

```
*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. ISDN-PPP interface configuration

In order to configure a PPP-DIAL interface over ISDN you need to enter **NETWORK x** from the general configuration menu where **x** is the interface number. E.g. if the number 5 interface is the PPP-DIAL interface, you should enter:

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

The options for the PPP interface over ISDN are the following:

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

LIST

This allows you to see the programmed options referring to the PPP interface over ISDN.

```
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" refers to the number of the ISDN interface over which the PPP link is established.

"Destination address" is the ISDN address to which the device is connected.

"*Inactive time*" allows you to determine the time delay after which the established call is released due to absence of IP traffic.

"Outgoing calls allowed" and *"Incoming calls allowed"* indicate the possibility of making and receiving calls.

"Control access enabled" indicates if the number pair destination address/source address is validated with the global list of permitted pairs. This list is configured in the global access control feature.

If the associated base interface is configured in a permanent mode, this is indicated with the following text and the majority of the information is omitted as it is redundant.

```
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>
```

This option permits you to determine the time after which the established call is released due to absence of IP traffic. In this case the call made to the destination address is carried out when IP traffic is detected. If the time configured is 0, then the connection is established in absence of IP traffic and is never released.

SET DESTINATION-ADDRESS

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

The destination address is the ISDN address which the device is connected to.

SET PERMITTED-CALLER

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

This parameter determines the origin ISDN address permitted. All ISDN calls are accepted by default (empty address).

SET BASE-INTERFACE

This allows you to configure the ISDN base interface to be used with the PPP interface. Each ISDN base interface is associated with a basic access B channel. In this way, the multiple PPP access to the ISDN basic access B channels can be controlled.

The value -1 is configured by default indicating that the PPP interface uses the first basic access B channel that it finds.

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

If the base interface is configured as -1 and there are various ISDN base interfaces (some of them operating in a permanent mode), those associated interfaces which operate in a permanent mode have preference over those that operate in a switched mode. It is unnecessary to associate more than one PPP interface to an ISDN base interface operating in permanent mode as this is the only one that will be used.

For further information on ISDN base interfaces, please consult chapter 4.

SET NAME-CIRCUIT

This parameter exists for information purposes only. It allows you to associate a character string to the interface.

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

ENABLE/DISABLE OUTGOING

Through this pair of commands it is possible to determine if the device is executing outgoing calls through the PPP interface over ISDN if this is configured or, on the contrary, the device is not carrying out calls.

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

ENABLE/DISABLE INCOMING

This is similar to the above case, the device can respond to incoming calls or ignore them.

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

ENABLE/DISABLE ACCESS

Permit the user to use or not (enable/disable) the global access table with the destination address/source address pairs in order to establish an ISDN call.

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

The global access table is common to all interfaces and is configured through the control access configuration menu. You can enter this menu using the **FEATURE CONTROL-ACCESS** command. From the *CtrlAcc Config>* prompt you can add, list or clear authorized destination address/ source address pairs.

```
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>
```

With the **CLEAR** command you can delete an source-destination pair, all entries for a given destination address or the whole table:

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

E.g. to delete an source - destination pair:

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

ENCAPSULADOR

This allows you to access the PPP interface’s own parameters programming. In order to configure these PPP interface parameters, please consult section 4 “PPP interface configuration”.

```
Circuit Config>ENCAPSULATOR

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

EXIT

Through this command you can exit the PPP-DIAL interface configuration and return to the main configuration menu.

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

3. PPP interface over E1/PRI ISDN Configuration

In order to configure a PPP-DIAL interface over an E1/PRI ISDN interface, you must enter NETWORK from the general configuration menu where n is the interface number. E.G. if interface 2 is a *PPP Generic Dial* interface, you must enter:

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

The options available in the PPP interface configuration menu are as follows:

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

3.1. DIAL

This command permits you to access the part of the configuration menu associated to the PPP-DIAL interface call with the associated prompt *Dial Config>*. In the *Dial Config>* configuration menu, the parameters related to the PPP link over the E1/PRI ISDN interface are specified.

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

The following commands are available within the Dial config menu:

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

a) LIST

This permits you to view the configured options for the "DIAL" part of the interface:

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

"Circuit name" this is the call profile name associated to the PPP-DIAL interface. It is the identifier related to the circuit possessing the call characteristics such as source address, destination address, permitted calls etc.

"Base interface" this refers to the base interface number over which the PPP interface is established (in this case it should be the number of the interface associated to an *E1* or *PRIMARY ISDN*).

"Base circuit id" This is the B channel number over which the PPP connection is established in the *E1* or *PRIMARY ISDN* frame. The parameter content depends on the type of channel where the PPP link is going to be established (permanent or switched). In cases where the interface is established as a Primary ISDN, channel 16 cannot be used as this is reserved for ISDN signaling.

b) SET

The SET command permits you to configure the parameter values associated to the "DIAL" part of the *PPP Generic Dial* interface.

- ### SET BASE-INTERFACE

Through this command you can specify the interface number associated to the base interface (depending on whether it is an E1 or Primary ISDN) as well as the B channel number (this is only valid in cases of permanent connections).

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

NOTE: The channel number (Base circuit id) is significant only in cases of PPP connections over PERMANENT channels as in cases of switched channels the channel is assigned when the call is being carried out. The number 255 indicates that there is no associated channel so if you are dealing with permanent connections, the link will not function.

In cases of PPP link over a Primary ISDN permanent channel, you cannot configure channel 16 (circuit id).

- ### SET NAME-CIRCUIT

This permits you to assign the *Dial Profile* link. This parameter associates the link with the indicated call profile (this contains data such as types of calls permitted, where to send the outgoing calls, which incoming calls are permitted, inactivity time and whether the access controls are enabled or not). This profile is absolutely essential when working over a Primary ISDN: if there is no call profile associated, the link will not establish (in the same way if you associated a profile that does not exist or is not configured). This parameter in cases dealing with E1 have no meaning consequently the contents are ignored.

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

c) EXIT

This command exits the *Dial Config>* configuration.

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

3.2. PPP

This permits you to access the PPP interface’s own parameter programming. In order to configure the characteristic parameters for a PPP interface, please consult chapter 5 ‘PPP interface Configuration’.

```
PPPD Cfg>PPP

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

3.3. EXIT

This command exits the PPP-DIAL *PPPD Cfg>* configuration.

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

3.4. E1/PRI ISDN interface Configuration

In order to correctly establish a PPP-DIAL link over an E1/PRI ISDN interface you must correctly configure certain E1/PRI ISDN interface parameters according to the behavior you wish to specify. The possibilities are:

a) *PPP link over an E1 interface channel*

In this case, the connections are always over a permanent channel. You need to configure the E1/PRI ISDN interface to operate in E1 mode. For further information on how to configure the E1/PRI ISDN interface, please consult the Dm529-I “E1/PRI ISDN Interface” manual.

b) *PPP link over Primary ISDN interface Permanent channel*

First you must configure the E1/PRI ISDN interface so it behaves as a Primary ISDN. In this case, you need to configure the channel where you wish to establish the PPP connection as *PVC*. For further information on how to configure the E1/PRI ISDN interface, please consult the Dm529-I “E1/PRI ISDN Interface” manual.

c) *PPP link over Primary ISDN interface switched channel*

As in the above case, you need to configure the E1/PRI ISDN interface as Primary ISDN and there must be a Primary ISDN interface channel configured as switched (*SVC*). For further information on how to configure the E1/PRI ISDN interface, please consult the Dm529-I “E1/PRI ISDN Interface” manual.

4. PPP-AT interface configuration

In order to configure an ATPPP-DIAL interface over an AT command interface. you need to enter **NETWORK x** from the general configuration menu where **x** is the interface number. E.g. if the number 2 interface is the ATPPP-DIAL interface, you should enter:

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

The options from the configuration menu for the PPP interface over AT commands are the following:

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

LIST

Allows you to see the programmed options referring to the PPP interface over AT commands.

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

"Base interface" refers to the number of the interface over which the AT command interface is established.

"Destination address" is the telephone address to which the device is connected.

"Inactive time" allows you to determine the time delay after which the established call is released due to absence of IP traffic.

SET INACTIVE-TIME

Inactive time permits you to determine the time after which the established call is released due to absence of IP traffic. In this case the call made to the destination address is carried out when IP traffic is detected. If the time configured is 0, then the connection is established in the absence of IP traffic and is never released.

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

SET DESTINATION-ADDRESS

The destination address is the address which the device is connected to.

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

ENCAPSULATOR

Allows you to access the PPP interface’s own parameter programming as described in the next section.

```
Circuit Config>ENCAPSULATOR
ASYNCHRONOUS PPP

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

EXIT

Through this command you can exit the ATPPP-DIAL interface configuration and return to the main configuration menu.

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

5. PPP interface configuration

This is for the PPP-DIAL interfaces (PPP over Basic ISDN B channel) and ATPPP-DIAL (PPP over AT commands interface). The configuration of the PPP interface's own parameters is carried out by executing the **ENCAPSULATOR** command from the interface configuration menu. E.g. an ATPPP-DIAL interface would be:

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

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

For PPP-DIAL interfaces over E1/PRI ISDN (E1 link B channel or ISDN primary) you access the configuration prompt of the PPP part through the **PPP** command from the PPP-E1/PRI ISDN interface configuration prompt (PPPD *Cfg>*):

```
PPPD Cfg>PPP

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

For the synchronous and asynchronous PPP interfaces over serial line, the configuration of the PPP's own parameters are carried out in the interface. E.g. for a synchronous PPP interface over serial line, assuming that the PPP interface is number 3, enter the following:

```
Config>NETWORK 3

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

The available commands are:

? (HELP)

This allows you to view the available options at any time from the configuration menu where you are located. Through a command you can see what options are available for that particular command. The options from the PPP interface configuration menu are the following:

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

LIST

Allows you to see the programmed options referring to the PPP interface.

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

LIST ALL

Lists all the programmed options for the PPP interface.

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>
```

The following is a description of the parameters:

“Maximum Frame”: Maximum frame length sent over the PPP link.

“Encoding”: Type used for the transmission, **NRZ** or **NRZI**.

“Idle”: Indicates the status of the line during idle periods, **FLAG** or **MARK**. If the interface is asynchronous, inactivity consists of transmitting 1’s binaries.

“Clocking”: Indicates if an **INTERNAL** clock is provided, or if an **EXTERNAL** clock is necessary. This will only appear if the PPP interface is installed over a synchronous serial line.

“Cable”: Indicates the type of interface used, e.g. **DTE** or **DCE**. This will only appear if the PPP interface is installed over a serial line. If you require an asynchronous PPP or PPP over AT commands, the type of interface used is always **DTE**.

“Line speed”: Speed of the Line used.

“Transmit delay”: Minimum period of time between successive frame transmissions. The default option is 0 and indicates that there are no restrictions.

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>
```

LCP Parameters:

"Tries Configure-Request": indicates the number of times an LCP CONFIGURE-REQUEST is transmitted to establish the PPP link.

"Tries Configure-Nak": indicates the maximum number of times the CONFIGURE-REQUEST frame is rejected during the link establishment. These are transmitted before finalizing because a compatible configuration has not been found between both ends.

"Tries Terminate-Request": indicates the number of times a TERMINATE-REQUEST frame is transmitted without detecting a response from the TERMINATE-ACK to finalize the link in an orderly manner.

"Timers between tries": this is the time between consecutive LCPs CONFIGURE-REQUEST, TERMINATE-REQUEST and ECHO-REPLY transmissions, when an adequate response has not be received.

LCP Options:

"Interface MRU": Maximum PPP frame size which is accepted at reception.

"Magic Number": Indicates if the magic number option is used or not when the link is being established.

"Asynchronous Control Character Map": Indicates if transparency is used or not in the transmission of control characters (e.g. XON, XOFF) in asynchronous PPP. This permits that when these characters are included in the frame, they do not activate the flow control processes in modems or adapters used in the connections.

"Protocol Field Compression": Indicates if this option is used or not when establishing the link. It is used in asynchronous PPP and indicates that once the LCP is negotiated and the NCP established, the PPP frame protocol field is compressed and only transmits one byte.

"Address Control Field Compression": Indicates if this option is used or not in establishing the link. It is used in asynchronous PPP and indicates that once the LCP is negotiated and the NCP established, the PPP frame control and address fields are not transmitted.

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>
```

NCP Parameters:

"Tries Configure-Request": indicates the number of times a NCP CONFIGURE-REQUEST is transmitted in order to establish the network protocol.

"Tries Configure-Nak": indicates the maximum number of times a CONFIGURE-REQUEST frame is rejected during the establishment of the network protocol. These are transmitted before finalizing because a compatible configuration has not been found between the two ends.

"Tries Terminate-Request": indicates the number of times a TERMINATE-REQUEST frame is transmitted without detecting a response from the TERMINATE-ACK to finalize the network protocol in an orderly manner.

"Time between tries": this is the time between consecutive LCPs CONFIGURE-REQUEST and TERMINATE-REQUEST transmissions, when an adequate response has not be received.

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>
```

IPCP Options:

"IP Van Jacobson Compression": Indicates if Van Jacobson compression is used or not.

"CRTP Compression": indicates if CRTP compression (RFC-2508) is used or not. You can only configure one of the two compression systems.

"IP get local address": Indicates whether to request an IP number when establishing the link. This is necessary in the case of connections to Internet. The default value is no.

"IP mask local address": in cases where you need to request an IP number assignation, indicate the mask to be associated to the IP number. The default value is 255.255.255.255. If the value is configured at 0.0.0.0. the mask will be taken from the class the address belongs to.

"IP send address": Where there is no request for an IP number, this indicates whether to transmit the IP number configured for the interface or not. The default value is no.

"IP request remote address": Indicates if you require the transmission of the remote end's IP number or not. The default value is no.

"IP remote address": in cases where the remote end requests IP number assignation, determine the IP number to be transmitted. The default value is 0.0.0.0. This value indicates that the IP number to be sent is the same as the first IP number assigned to the interface at the local end through which the PPP

connection minus 1, is established. In this situation, if the interface IP number is the first subnet address (not broadcast), this IP number is transmitted plus 1. If the interface IP number is an unnumbered address, i.e. 0.X.X.X. type, the connection will close should the remote end requests IP number assignation.

LIST AUTHENTICATION

```
PPP Config>LIST AUTHENTICATION

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

This allows you to view the programmed options in order to carry out link authentication.

The implemented authentication is carried out through Password Authentication Protocol (PAP) or Challenge Authentication Protocol, described in the RFC-1334. These protocols allows you to establish a link only when a correct login and password are given. Once the authentication is finalized and providing it is correct, the link network protocol negotiation takes place.

Access to Internet. When you access an Internet connection, the remote end requests a user name and a password to determine who should provide the IP number in the connection. When access is carried out for Internet, the Access Center Provider contracted by the user proportions the IP number from those assigned.

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>
```

This allows you to check the state of the available features for the PPP protocol:

"NAT": The *"Network Address Translator"* feature allows elements of the same network share a single IP address

"Authentication": Indicates if the router is going to demand authentication from the remote end or not during the negotiation to establish the link. If this is enabled, it indicates what type of authentication protocol it will demand, PAP or CHAP.

"CRTP Compression": indicates if the CRTP compression is enabled in the router. This configuration is independent of the option enabling CRTP compression negotiation within the IPCP.

"Multilink PPP": Indicates if the interface pertains to a PPP multilink. This feature is only available for PPP-DIAL (PPP over an ISDN B channel) interfaces. The PPP Multilink interface must already exist in the device. In order to add a PPP multilink interface, you should use the **ADD DEVICE PPP** command from the general configuration menu. Consult the "Enable MPPP" section.

"Callback": Indicates if the interface can be activated from the remote through an ISDN call. This feature is only available for PPP-DIAL (PPP over an ISDN B channel) interfaces. If you wish to

prevent any remote number from activating the link, you need to configure an authorizing call with the required number.

"Backup": Indicates if the interface can have a backup interface configured. This feature is only available for PPP-DIAL (PPP over an ISDN B channel) interfaces.

LIST USERS

Displays a list of users who are authorized to connect to the device. The users are values permitted in the authentication demanded from the remote end. For further information, please see the **ADD USERS** section.

```
PPP Config>LIST USERS

N. Login                              Password
-- --------------------------------   --------------------------------
0  remoteuser_2                       password_2
1  remoteuser_1                       password_1

PPP Config>
```

LIST INTERVAL-OF-CONNECTION

Displays the time interval for the connection is allowed. For further information, please refer to the **SET INTERVAL-OF-CONNECTION** section.

```
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

Permits you to modify the programmed options referring to the PPP interface.

```
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>
```

The following is a description of the parameters:

"ENCODING": Type used for the transmission, NRZ, NRZI. The default value is NRZ.

"IDLE": Indicates the status of the line during idle periods, FLAG or MARK. The default value is FLAG.

"FRAME-SIZE": Maximum frame size sent over the PPP link. The range value is between 576 and 4.098. The default value is 1.500.

"LINE SPEED": This is the line speed used where it is configured as a DCE or where the interface is asynchronous. This option can only be modified where the PPP interface is configured over a serial line or over AT commands.

"TRANSMIT-DELAY": Minimum time period between successive frame transmissions.

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>
```

The default value for this option is 64000. This option cannot be modified in cases of PPP over ISDN.

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": Maximum PPP frame size accepted at reception. The default value is 1.500. The range is between 576 and 4.089.

"Magic Number": Indicates if the magic option is used or not when establishing the link. This serves to detect if the link is sending a loop or not through the transmission of a random number between the two ends based on the system clock and the number of start ups. The magic number contains 4 bytes. The default option is No.

"Asynchronous Control Character Map": Indicates if transparency is used or not in the transmission of control characters (e.g. XON, XOFF) in asynchronous PPP. This permits that when these characters are included in the frame, they do not activate the flow control processes in modems or adapters used in the connections. We recommend that the option is YES in asynchronous connections. When this option is chosen where transparency is applied, the control character mask (lower than the hexadecimal character 0x20) is 0x00A0 (only to XON and XOFF).

"Protocol Field Compression": Indicates if this option is used or not when establishing the link. This allows you to disregard the protocol field once the link has been established. The default option is No. It is recommended in asynchronous connections the option is YES.

"Address Control Field Compression": Indicates if this option is used when establishing the link. This allows you to disregard the control and address fields once the link has been established. The default option is No. We recommend in asynchronous connections, the option is YES.

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>
```

LCP Parameters:

"Tries Configure-Request" : indicates the number of times the LCP CONFIGURE-REQUEST is transmitted in order to establish the PPP link. The permitted values range between 1 and 100. The default value is 20.

"Tries Configure-Nak" : indicates the maximum number of times a CONFIGURE-REQUEST frame is rejected during the establishment of the link. These are transmitted before finalizing because a compatible configuration has not been found between the two ends. The permitted values range between 1 and 100. The default value is 10.

"Tries Terminate-Request" : indicates the number of times a TERMINATE-REQUEST frame is transmitted without detecting a response from the TERMINATE-ACK to finalize the link. The permitted values range between 1 and 20. The default value is 10.

"Timer between tries" : this is the time between consecutive LCPs CONFIGURE-REQUEST, TERMINATE-REQUEST and ECHO-REPLY transmissions, when an adequate response has not be received. The permitted values range between 1 and 30 seconds. The default value is 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>
```

NCP Parameters:

"Tries Configure-Request" : indicates the number of times the NCP CONFIGURE-REQUEST is transmitted in order to establish the network protocol. The permitted values range between 1 and 100. The default value is 10.

"Tries Configure-Nak" : indicates the maximum number of times a CONFIGURE-REQUEST frame is rejected during the establishment of the network protocol. These are transmitted before finalizing

because a compatible configuration has not been found between the two ends. The permitted values range between 1 and 100. The default value is 10.

"Tries Terminate-Request" : indicates the number of times a TERMINATE-REQUEST frame is transmitted without detecting a response from the TERMINATE-ACK to finalize the network protocol in an orderly way. The permitted values range between 1 and 20. The default value is 10.

"Timer between tries" : this is the time between consecutive NCPs CONFIGURE-REQUEST and TERMINATE-REQUEST transmissions, when an adequate response has not be received. The permitted values range between 1 and 30 seconds. The default value is 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>
```

IPCP Options:

"IP Van Jacobson Compression": Indicates if Van Jacobson compression is used or not. Default value is NO.

"CRTP Compression": indicates if the CRTP compression is used or not. The default value is NO.

"IP get local address": Indicates whether to request an IP number when establishing the link. This is necessary in the case of connections to Internet. The assigned IP number can be viewed from the console. The default value is NO.

"IP mask local address": if requesting an IP number assignation, you must indicate the mask to be associated with the IP number. The default value is 255.255.255.255. If an 0.0.0.0. value is set, then the mask is taken from the class the address pertains to.

"IP send address": Where there is no request for an IP number, this indicates whether to transmit the IP number configured for the interface or not. The default value is YES.

"IP request remote address": Indicates if you require the transmission of the remote end's IP number or not. The remote end IP number can be viewed from the console. The default value is YES.

"IP remote address": in cases where the remote end requests IP number assignation, determine the IP number to be transmitted. The default value is 0.0.0.0. This value indicates that the IP number to be sent is the same as the first IP number assigned to the interface at the local end through which the PPP connection minus 1, is established. In this situation, if the interface IP number is the first subnet address (not broadcast), this IP number is transmitted plus 1. If the interface IP number is an unnumbered address, i.e. 0.X.X.X. type, the connection will close should the remote end requests IP number assignation.

SET AUTHENTICATION

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

This allows you to program the user and password which are sent during the authentication process in connections to Internet. Neither the user nor the password are configured by default.

If the remote end requests authentication, it is these values that are sent to authenticate the link according to the chosen protocol: if this is PAP, they are sent in clear, if it is CHAP, they are encrypted through the MD5 algorithm with a password previously sent by the authenticator end.

It is important to note that the configured authentication here is the one that identifies the device to the remote end should the remote end demand this. This is different to the authentication requested by a router to a remote end which is configured through the **ENABLE AUTHENTICATION** (PAP or CHAP) and **ADD USERS** commands.

SET INTERVAL-OF-CONNECTION

This permits you to specify an interval outside which the device cannot connect to the external network even if there is traffic being sent.

In the permitted connection interval, the days of the week are defined together with the times (start and end). If the starting time is subsequent to the finalizing time, this means that there has been a change of day in the permitted interval, if not all the interval hours are during the same day.

If the release time due to absence of data is zero, the connection is guaranteed to be permanently established while you are within the permitted connection time even if there is no traffic. This means that the connection is automatically established when it enters into the permitted interval and automatically disconnects when the permitted interval ends.

The interval is accurate to a minute. This means a maximum of one minute passes while the device connects or disconnects once the router clock marks the beginning or the end of the interval.

Once out of the connection interval time, the call is disconnected immediately even if there is traffic or after the call is released due to absence of traffic.

In the following example, a time interval is configured which permits a permanent connection. This is the default configuration.

```
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

Permits you to activate determine PPP features over this interface.

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

ENABLE NAT

Permits you to activate the Network Address Translator (NAT) feature over the PPP interface. This option is used when accessing Internet which allows you to enable the IP address change procedure described in the RFC-1631 "The IP Network Address Translator (NAT)" and the Internet Draft, “Extending NAT”.

This is activated through the following command:

```
PPP Config>ENABLE NAT
PPP Config>
```

ENABLE AUTHENTICATION

This allows you to activate the authentication feature according to the chosen protocol, Password Authentication Protocol (PAP) or Challenge Authentication Protocol (CHAP).

In cases where the authentication feature is enabled, it will demand the remote end sends the login and the password according the method selected. A link can only be established where this process has been successfully completed.

In both cases, the user together with his corresponding password, must have been added to the authorized user table through the **ADD USERS** command.

```
PPP Config>ENABLE AUTHENTICATION ?
PAP
CHAP
PPP Config>
```

In order to enable PAP:

```
PPP Config>ENABLE AUTHENTICATION PAP
PPP Config>
```

In order to enable CHAP:

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

When you process the authentication feature, please take note the following:

If the local end has been programmed with enabled authentication but receives an authentication request from the remote end in the LCP packets, the authentication request is followed up and the programmed login and password sent independently of the method chosen.

If the local end with enabled authentication does not receive an authentication request from the remote end, it will be demanded according the method selected.

In cases where authentication is demanded, all the network protocol negotiation packets (NCP’s) are discarded until this process is successfully completed.

ENABLE MPPP

This feature adds the PPP-DIAL link (PPP over an ISDN B channel) to the interfaces pertaining to the PPP Multilink pipeline. It is also possible to aggregate a PPP link over a serial line to an MPPP pipeline, however in this case the link should only pertain to the MPPP pipeline. The MPPP interface should already exist in the device. In order to add an MPPP interface, use the **ADD INTERFACE MPPP** command from the general configuration menu.

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

In the example shown the MPPP interface in the device is number 4.

ENABLE CALLBACK

This indicates that the interface can be remotely activated by an ISDN call. This feature is only available for PPP-DIAL interfaces (PPP over ISDN B channel). If you wish to prevent any remote number activate the link, you must configure an authorized number.

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

ENABLE BACKUP

This indicates that the interface has a backup interface configured. This feature is only available for PPP-DIAL interfaces (PPP over ISDN B channel). The backup interface can be PPP over ISDN B channel or PPP over AT commands interface.

The conditions for switch to backup from a PPP-DIAL interface are two:

1. **IPCP Timeout**. The configured time from requesting the connection has elapsed, the PPP link IPCP protocol in the ISDN connection has not been established. This means that the IP level in the connection has not been established.
2. **Maximum number of call attempts.** From the time the connection is requested, a maximum number of call retries are carried out unsuccessfully. This means the ISDN call was not established. Please note that when the ISDN call is established, it is considered valid independently of the success or failure or the subsequent PPP negotiation.

These two conditions act simultaneously in such a way that the first condition filled provokes the switch to backup. If the call is established normally and the IPCP negotiated within the time limit, switch to backup is not activated. If there is a switch to backup, the backup parameters are activated, the channel routes with errors change to the backup connection in order to guarantee the user traffic and the backup call is carried out. The configurable parameters in backup are the following:

1. **Outgoing Interface**. This is the interface where the backup call is carried out from. It can be a PPP interface over an ISDN B channel which can include it's own interface or a PPP interface over AT commands.
2. **Priority**. This indicates which ISDN B channel has greater priority in cases where there are two ISDN B channels enabled for backup via the same outgoing interface. Priority can be high or low. The B channel with the greater priority "wins" the outgoing interface if both B channels make the request at the same time. Furthermore this channel will take over the outgoing interface if the B channel with less priority is using it and the higher priority B

channel requests backup through the same. If the priorities are the same, then neither channel has priority over the other where backup requests are made at the same time.

3. **IPCP Timeout.** This is the maximum amount of time that can lapse when requesting a connection until a switch to backup occurs, if within this time the IPCP has not been established.
4. **Maximum number of calls**. This is the maximum number of unsuccessful consecutive ISDN calls permitted before switching to backup.
5. **Telephone**. This is the destination telephone number of the backup connection. This number can be the same as the failed connection or different.
6. **Login and password**. This is the user and password used in order to identify the backup connection. It can be the same user and password as in the failed connection or different. It makes sense that the backup user and password are the same as the failed connection if the outgoing interface is PPP over AT commands or if the backup telephone is different, e.g. it provides backup for another remote end.

```
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:    user
Password: *******
Password: *******
PPP Config>LIST FACILITY

Facilities
----------
 NAT Disable
 Authentitacion 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  user
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

When a PPP-DIAL interface is enabled to execute outgoing calls, a problem occurs if RIP protocol is also enabled over the same interface. In this situation the RIP protocol sends IP packets over the PPP interface every so often thus provoking a call and owing to this, the call is never released due to absence of traffic.

To resolve this problem in those cases where you wish to use dynamic routing, an ENABLE RIP-NO-DIAL option has been established. If this is enabled, the RIP packets will not provoke an outgoing call and are ignored when a previously established call is released (i.e. if the only traffic existing in the link is IP due to the RIP protocol, the call is released).

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

DISABLE

Allows you to disable determined PPP features over this interface.

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

DISABLE NAT

This allows you disable the NAT, Network Address Translator, over the PPP interface. This option should be used in cases where the router is used to effect private network access (intranets).

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

DISABLE AUTHENTICATION

Permits you to inhibit the authentication feature. Authentication will not be demanded form the remote end in order to establish the link.

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

DISABLE MPPP

This excludes the interface from the Multilink PPP pipeline.

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

DISABLE CALLBACK

Disables the callback feature from this interface.

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

DISABLE BACKUP

Disables the backup feature from this interface.

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

DISABLE CRTP

Disables CRTP compression.

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

DISABLE RIP-NO-DIAL

Disabling this option means that the RIP traffic provokes calls in the PPP interfaces over a B channel or AT.

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

ADD USERS

This allows you to add the pairs of authorized user-passwords. If the authentication feature is enabled in the interface (PAP or CHAP), authentication will be requested from the remote end. Authentication provided by the remote end must coincide with one of the configured passwords.

Authentication should not be confused between the cases of when the interface is requested to authenticate to the remote end and the remote end is requested to authenticate to the interface. The first is configured with the **SET AUTHENTICATION** command, and the second through the **ENABLE AUTHENTICATION** and **ADD USERS** commands.

The PPP protocol is sufficiently flexible in order that each end can request the type of authentication required from the remote end or not request it at all. In any case, the most normal situation is that a router accessing networks e.g. Internet, does not request authentication from the service provider but has to send authentication to the provider. From the provider's point of view, he does not authenticate but does request authentication from the remote user.

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

DELETE USERS

Allows you to delete the pairs of authorized user-password.

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

EXIT

Through this command you exit the PPP interface's own parameter configuration.

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

Chapter 3
MPPP Interface Configuration

1. Interface Configuration

In order to configure the device with PPP Multilink it is necessary to have an MPPP interface available and one or more PPP interfaces over an ISDN B channel. For this you need to aggregate the B channels required and the MPPP interface. Once the interface configurations have been saved and the device re started, you can configure the required parameters.

Here below we are going to aggregate two ISDN B channels from the same basic access associated to a MPPP interface:

```
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
---      2 Node->Router                          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
---      4 Node->Router                          0             0
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
---      6 Node->Router                          0             0
ISDN 1   1 ISDN                            F001640  F000E00   9C
ISDN 1   2 ISDN                            F001660  F000F00   9B
ISDN 1   3 B channel: PPP                        0             0
ISDN 1   4 B channel: PPP                        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>                                                            <CTRL-P>
*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

*PROCESS 4
User Configuration
Config>LIST DEVICES

Con    Ifc Type of interface                   CSR     CSR2  int
---      5 Multilink PPP                         0             0
---      6 Router->Node                          0             0
---      7 Node->Router                          0             0
ISDN 1   1 ISDN                            F001640  F000E00   9C
ISDN 1   2 ISDN                            F001660  F000F00   9B
ISDN 1   3 B channel: PPP                        0             0
ISDN 1   4 B channel: PPP                        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>
```

At this point you can see that there are two PPP interfaces over an ISDN B channel (numbers 3 and 4) and an MPPP interface (number 5). The parameters for each PPP interface are configured individually in each one. Specifically it is vital to activate the PPP Multilink over the MPPP interface in each PPP (interface number 5 in the example):

```
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
 Authentication Disable
 CRTP  Compression Disable
 Avoid RIP dial-up Disable
 Multilink PPP Enable Bundle: 5
 Callback Disable
 Backup Disable
PPP Config>
```

The available MPPP interface in the device operates on traffic demand, i.e. activates or deactivates the multilink B channels depending on the defined traffic thresholds. The threshold definition is carried out in the required MPPP interface and is explained below.

2. MPPP Parameter Configuration

The PPP Multilink protocol implementation in the router has the following characteristics:

1. It is only possible to aggregate ISDN basic access B channels. (It is possible to configure MPPP in PPP serial lines, but only in order to permit fragmentation, i.e. each pipeline has a unique serial line).
2. The addition and subsequent removal of the B channels can be carried out at anytime depending on the PPP Multilink session's on demand bandwidth parameters.
3. When two or more B channels are established, the PPP traffic alternates between them.
4. If the Multilink session is configured as pre-emptive, MPPP session's B channels can be dynamically excluded when a PPP Dial interface over ISDN needs to send a call and all the device's B channels are busy.

The PPP Multilink session's characteristic parameters which determine its behavior are described below. The first five adapt their responses to the bandwidth on demand pattern, i.e. subsequent B channels are established and released depending on the existing traffic in the Multilink session. The last one has the possibility of configuring the MPPP session as pre-emptive as described above.

1. **Activation threshold**. MPPP occupation percentage in order to activate the other B channel in the Multilink. I.e. if during the activation period the average occupation of the active B channels is superior to this value, an additional B channel is activated should it be available. The parameter's default value is 90%.
2. **Deactivation threshold**. B channel occupation percentage in order to deactivate the Multilink B channel. I.e. if during the deactivation period the average occupation of the B channels do not reach this value, the B channel is deactivated. The parameter's default value is 50%.
3. **Interval of activation**. If during the time (in seconds) indicated in this parameter, the average occupation of the MPPP surpasses the threshold activation, a new B channel is activated should it be available. This parameter is measured in seconds and the default value is 120.
4. **Interval of deactivation**. If during the time (in seconds) indicated in the parameter, the average occupation of the B channels does not reach the deactivation threshold, the B channel is deactivated. This parameter is measured in seconds and the default value is 300.
5. **Direction of load**. This indicates the direction of the considered traffic in order to calculate the average load of the channels. This can be incoming (from the external network towards the device), outgoing (from the device towards the external network) or both. Under normal conditions for accessing an external network e.g. Internet, where the majority of the traffic is incoming, it is recommended that an incoming value is configured. The default value is incoming.
6. **Pre-emptive.** This is the property which determines if the B channels used in the Multilink session can be dynamically excluded by the PPP Dial interfaces in cases when they need to send traffic and there are no free B channels available in the device. The default value is non pre-emptive.

7. **Fragmentation.** The VOICE-IP fragmentation fixes the maximum MPPP frame length. All longer frames are fragmented and the shorter ones are sent with PPP encapsulated to interleave the voice frames with the data frame fragments. This option is disabled by default.

In order to configure the MPPP interface's bandwidth parameters, you need to enter in the MPPP interface:

```
Config>NETWORK 5

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

The available commands are:

? (HELP)

This allows you to view the options available from the configuration menu you are located in, at any time. By following a command you can see what options are available for this command. The following options are available in the MPPP interface configuration menu:

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

LIST

Allows you to view the MPPP parameters programmed in the interface.

```
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

This allows you to configure the on demand bandwidth parameters for traffic and the pre-emptive and fragmentation properties.

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

SET THRESHOLD

Permits you to configure the activation and the deactivation threshold for the on demand bandwidth due to traffic.

```
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

Permits you to configure the activation and the deactivation period for the on demand bandwidth due to traffic.

```
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

Permits you to configure the direction of the load affecting the on demand bandwidth due to traffic.

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

SET PRE-EMPTION

Permits you to configure pre-emptive quality in the MPPP interface.

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

NOTE: The pre-emptive property is not compatible with Multilink B channels configured as permanent.

SET FRAGMENTATION

Permits you to enable fragmentation in the MPPP interface.

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

EXIT

Return to general configuration menu.

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

Chapter 4
Configuration Examples for access trough ISDN

1. Connection to Internet through ISDN

The following explains the chains of commands needed to configure the router in order to access the Internet network through ISDN.

The configuration process is carried out in two parts.

1. First you need to aggregate the PPP interface over an ISDN line and assign any one of the IP addresses. You can also aggregate a route so the Teldat server can be accessed through this interface. In cases where the ISDN call is not established, this permits IP traffic, i.e. why datagrams appear with a 195.53.0.x destination address. Similarly you need to assign an Ethernet interface in order to connect the router to the network. Once this operation has been carried out, you must re start the device.

```
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
---      2 Node->Router                         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
---      4 Node->Router                         0             0
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>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>                                                                    <CTRL-P>
*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


*
```

If you check the ISDN base interface configuration you will see that the default connection is switch making further configuration is unnecessary.

```
*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. Secondly you need to configure the PPP interface. The main parameters which need to be configured are:
    - Destination Address: This is the number of the ISP access node you wish to use.
    - Permitted outgoing calls.
    - User and password in order to access ISP.
    - IP number assignment request.

The command sequence is as follows:

```
*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:    []? internet
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>                                                                   <CTRL-P>
*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. With this configuration, the ISDN call is established for traffic. Finally you can check that the interface is correctly configured through a ping. You need to establish the ISDN call and receive a response to the sent pings. The command sequence is as follows:

```
*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        ffffff00  1    0    Eth/0
 Dir(1)   192.6.3.0        ffffff00  1    0    PPP/0
 Dir(1)   192.168.252.0    ffffff00  1    0    R->N/0
Stat(1)   195.53.0.0       ffffff00  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        ffffff00  1    0    Eth/0
 Dir(1)   192.168.252.0    ffffff00  1    0    R->N/0
Sbnt(0)   193.153.67.0     ffffff00  1    0    None
 Dir(1)   193.153.67.59    ffffffff  1    0    PPP/0
Stat(1)   195.53.0.0       ffffff00  1    0    193.153.67.59


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

You can see how a new address for the PPP interface has been dynamically assigned (**193.153.67.59**). You can also see how all the ping packets carried out are lost. This is due to the fact that the IP packets sent have the PPP interface address as a source address before carrying out the IPCP handshake (192.6.3.1), an unknown address within Internet. If you subsequently execute the ping, the packets are correctly received as the source IP address is obtained from the ISP (193.153.67.59) which is valid.

NOTE: When you do not use the configuration generation from the Teldat Router quick configuration menu, you must remember to configure the DNS server's IP address in the terminal. For Internet, this address is supplied by the ISP.

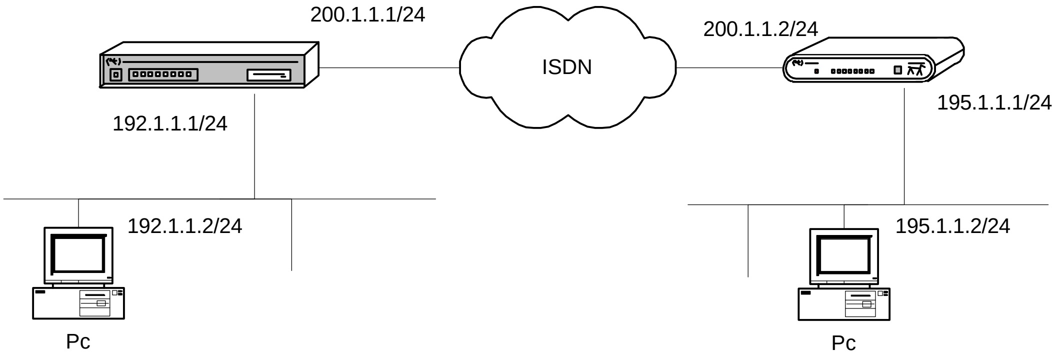
2. Permanent ISDN connection mode

In some cases the carrier offers the possibility of contracting permanent ISDN connections between two ISDN line subscribers using one or various basic access B channels. In these cases it is not necessary to carry out a call and the connections acts as a point to point line.

Please note that in order to take advantage of this possibility, two elements are necessary:

- Contract a permanent ISDN service with the carrier between the two ends.
- To have two routers which support permanent ISDN operation mode and place them at both ends of the permanent ISDN connection.

In this section a configuration example is shown joining two remote IP networks through PPP over an ISDN permanent link using a B1 channel at both extremes (this may not be your specific case). The configuration process is carried out in two parts: firstly by creating the PPP interface over ISDN and secondly configuring the IP. The connection diagram is as following:



a) PPP interface creation: The PPP interface is created and the basic ISDN interface is configured as permanent over the B1 channel (the data is provided by the carrier). Encapsulated PPP configuration is used by default so further configuration is unnecessary in this example. This step should be repeated for both routers.

```
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
---      2 Node->Router                         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
---      4 Node->Router                         0             0
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>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



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>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
```

```
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) IP address assignment for the interfaces and the routes. In this example, the router situated on the left of the figure is configured (200.1.1.1/24 for the PPP interface and 192.1.1.1/24 for the LAN interface). The other router is configured in the same way but with the following addresses: 200.1.1.2/24 for the PPP interface and 195.1.1.1/24 for the LAN interface with a route to the 192.1.1.0/24 through the 200.1.1.1. address.

```
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>                                                                      <CTRL-P>
*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


*
```

Once both devices have been configured, you can check the connection by sending pings from both places: from the routers themselves (through the IP monitoring process as explained in secion 1) or from the PC's or other devices located in the LANs at both ends: in order to carry this out, you need to aggregate the corresponding access routes to the remote IP networks.

Chapter 5
Configuration Example (Internet-Access through PSTN)

1. Configuration Example (Internet-Access through PSTN)

Here the command chain required to configure the router is shown in order to permit Internet network access through PSTN over an AT command interface. This permits you to manage an external modem to carry out the connection.

The configuration process is carried out in four parts. Three for configuration and one to establish and check the connection.

1. Firstly you need to aggregate the asynchronous PPP interface over an AT commands interface and assign any one of the IP addresses. You also need to establish the route so all the datagrams addressed to the 193.53.0.x network exit via this interface. In cases where the ISDN call is not established, this permits establishment by IP traffic, i.e. why datagrams appear with a 193.152.x.x destination address. In the same way you need to assign an Ethernet interface in order to connect the router to the network. Once this operation has been carried out, you must re start the device.

```
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>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
```

```


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


*
```

2. The next step is to configure the PPP interface. The main parameters to configure are the following:
   - Destination Address: This is the Access Node Number from the ISP you wish to use.
   - Line speed. This is speed at which the dialing and configuration commands are sent to the modem.
   - LCP parameters for connection in asynchronous mode. ACCM, protocol and control field Compression and the address for the frame and Magic Number.
   - Login and password in order to access Internet (e.g. remoteuser1-password1).
   - IP number assignment request.

The command sequence is as follows:

```
*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. Thirdly, you need to configure the AT commands interface which is going to be used in managing the modem. Modem management from a **Teldat Router** is carried out through commands and signal management. In order to control the call establishment and release, the **Teldat Router** just checks the status of the interface signals. This means that these must be programmed in the modem so they activate according to the norm and not from a fixed mode. The following table indicates the configurable parameters for the external modem and the default values taken:

Command	**Value**	**Meaning**

Connection Mode	C	Command Mode
Dial Mode	T	Dual Tone Multi Frequency (DTMF)
DCD control command	&C1	Data Carrier Detect signal - 109 follows the status of the on-line carrier
DSR control command	&S1	Data Set Ready signal - 107 through V.24. ON after having detected answer tone after dialing
DTR control command	&D2	Drop in Data Terminal Ready circuit - 108 makes the modem disconnect and disables automatic answer.
CTS control command	&R1	Clear To Send signal -106 must be in OFF position if required by flow control
V.42/V.42 bis command	&Q5	Modem tries to negotiate a connection with error correction and data compression
Flow control command	&K3	Flow control selected through hardware (RTS/CTS)
Automatic answer	dis	Disable automatic answer

Although the default commands are used by most modem manufacturers, it is possible that some of the above are not implemented in the modem used.

If any of the above needs modifying, the option chosen according to a set of implemented modem commands must comply with:

- **Connection mode** to be used by the modem, command dialing or DTR (Data Terminal Ready). If the connection mode is carried out through DTR, when the **Teldat Router** needs to establish a call, the interface 108 circuit (DTR) will be activated. If the mode required is through commands, the dialing command (ATD) will also be sent followed by the programmed number.
- **Dial mode** to be used by the modem, tones or pulses. It will depend on the type of access to the Public Switched Telephone Network (PSTN) employed by the user.
- **DCD control command**. Must be selected so that the 109 circuit (DCD) works through V.24, i.e. when the 109 circuit signals the status of the on-line carrier.
- **DSR control command**. Must be selected so that the 107 circuit (DSR) works through V.24. Will be activated when detecting answer from the remote end.
- **DTR control command**. Must be selected so that the modem hangs up in the absence of 108 (DTR) circuit. When the **Teldat Router** wishes to disconnect in the absence of traffic, the terminal-to-modem 108 circuit will be disabled. This permits the modem not to answer incoming calls when disconnected.
- **CTS control command**. Must be selected so that the modem supplies the 106 circuit (CTS) while in command mode. The 106 signal will be disabled only when required by the flow control.
- **V.42/V.42bis norm activation command**. Must be selected so that the connection is carried out with data compression and correction. Although correction and compression may not be required, it is advisable to chose this option, as it may obtain a better throughput in the link.
- **Modem flow control selection command**. Hardware flow control (RTS/CTS) must always be selected.
- **Automatic answer**. This permits the ATDIAL interface to accept incoming calls. If this option is enabled you must use modems which support AT commands as the device does not monitor the

V.24 RI125 signal. Furthermore, only one of the ends must have the destination number configured in the PPPAT interface. This is to avoid collisions being produced both in the incoming and outgoing calls. When this option is enabled, the ATDIAL interface can be used as a backup interface between the two line ends, one end being the caller and the other answering.

The command sequence to program is as follows:

```
*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>                                                                   <CTRL-P>
*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


*
```

With this configuration, the AT commands call towards the modem is established for traffic. Finally you can check that the interface is correctly configured through a ping. You need to establish the PSTN call and receive a response to the sent pings. The command sequence is as follows:

```
*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        ffffff00  1    0    Eth/0
 Dir(1)   192.168.1.0      ffffff00  1    0    PPP/0
 Dir(1)   192.168.252.0    ffffff00  1    0    R->N/0
Stat(1)   195.53.0.0       ffffff00  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        ffffff00  1    0    Eth/0
 Dir(1)   192.168.252.0    ffffff00  1    0    R->N/0
Sbnt(0)   193.153.66.0     ffffff00  1    0    None
 Dir(1)   193.153.66.40    ffffffff  1    0    PPP/0
Stat(1)   195.53.0.0       ffffff00  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>
```

You can see a new address for the PPP interface has been dynamically assigned (**193.153.66.40**). This must correspond to the ISP pool of addresses.

NOTES: Establishing a connection to Internet using a modem requires more connection time than for ISDN. If browsers are being used from terminals connected to the LAN network, should the call not be established (although it is correctly established for traffic), it's possible that the pages will not be updated correctly. This is due to the fact that the datagrams which have been sent are discarded until the connection is correctly established. It is therefore advisable to spend some time in manually updating.

When you do not use the configuration generation from the Teldat Router quick configuration menu, you must remember to configure the DNS server's IP address in the terminal. For Internet, this address is supplied by the ISP.

Chapter 6
PPP Interface Monitoring

1. PPP Interface Statistics

In order to view the interface statistics, enter the **DEVICE** command from the monitoring prompt (+) and indicate the interface number to obtain the statistics required. The information obtained depends on the physical method used as support.

In cases of a PPP interface over a synchronous line, the information displayed is:

```
+DEVICE 1

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

For cases of a PPP interface over an asynchronous line, the information displayed is:

```
+DEVICE 2

                                 Auto-test   Auto-test     Maintenance
Ifc  Interface     CSR    Vect      valids    failures        failures
2    PPP/1     F001620      9d           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
+
```

For cases of a PPP interfaces over an ISDN basic access, the information displayed is:

```
+DEVICE 5

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


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

For cases of a PPP interface over an AT commands interface, the information displayed is:

```
+DEVICE 2

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


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

2. PPP Console

Enter from the monitoring prompt (+):

```
+NETWORK 1

-- PPP Console --
PPP>
```

? (HELP)

This allows you to view the options available from the console menu you are located in, at any time. By following a command you can see what options are available for this command. The following options are available in the PPP interface console menu:

```
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>
```

This permits you to monitor the options transmitted and received when establishing the link such as the current state of the PPP protocol.

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>
```

Permits you to monitor the options transmitted and received when establishing the protocol at NETWORK level. In cases where dynamic assignment is used, the assigned IP number can be checked. In the same way the remote end IP number can be monitored if this has been received.

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>
```

This permits you to monitor the number of LCP frames received and sent via this interface as well as the number of bytes and frames received and transmitted.

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>
```

Permits you to monitor the number of NCP frames received and sent via this interface.

CLEAR

```
PPP>CLEAR
PPP>
```

Re starts all the interface statistics.

RESET-link

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

Resets the PPP link over an ISDN B channel or an AT commands interface.

EXIT

```
PPP>EXIT
+
```

Exits the PPP interface monitoring mode.

Chapter 7
PPP Protocol Events

1. PPP Protocol Events Monitoring

This permits real time monitoring of events that occur over one or more PPP interfaces where the events system is enabled for this protocol.

This is enabled from the configuration menu as follows:

```
*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>
```

This can also be configured from the monitoring menu in the same way at any time without this having to be stored in the configuration. This is carried out as follows:

```
*PROCESS 3
Console Operator
+EVENT

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

The events list available for the PPP protocol is as follows:

PPP.001

Level: Common informational comment, C-INFO

Short Syntax:

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

Long Syntax:

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

Description:

ppp_prinit routine called by the IP protocol.

PPP.002

Level: Common informational comment, C-INFO

Short Syntax:

PPP.002 Srl prt up nt *network ID*

Long Syntax:

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

Description:

pppslfts2 ends the driver selftest. Driver initialized.

PPP.003

Level: Common informational comment, C-INFO

Short Syntax:

PPP.003 Mnt nt *network ID*

Long Syntax:

PPP.003 Doing maint on network *network ID*

Description:

pppmnt maintenance being effected.

PPP.004

Level: Common informational comment, C-INFO

Short Syntax:

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

Long Syntax:

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

Description:

pppout function called by the IP protocol without being in an OPEN state. The IPCP protocol establishment has not been completed.

PPP.005

Level: Unusual external error, UE-ERROR

Short Syntax:

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

Long Syntax:

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

Description:

IP packet received with CRC error.

PPP.006

Level: Common external error, CE-ERROR

Short Syntax:

PPP.006 I_ERR on rcv nt *network ID*

Long Syntax:

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

Description:

pppin function has detected a packet with I_ERR bit.

PPP.007

Level: Unusual external error, UE-ERROR

Short Syntax:

PPP.007 Rcv Bd fr addr 0x*Address* nt *network ID*

Long Syntax:

PPP.007 Received packed with bad frame address = 0x*Address*, on network *network ID*

Description:

pppin function has detected a packet with an invalid address field, no 0xFF.

PPP.008

Level: Unusual external error, UE-ERROR

Short Syntax:

PPP.008 Rcv Bd fr cntrl 0x*Control_Field* nt *network ID*

Long Syntax:

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

Description:

pppin function has detected a packet with an invalid control field, no 0x03 (UI).

PPP.009

Level: Unusual external error, UE-ERROR

Short Syntax:

PPP.009 Rcv inv prtcl 0x*Protocol* nt *network ID*

Long Syntax:

PPP.009 Received packed with invalid protocol = 0x*Protocol*, on network *network ID*

Description:

pppin function has detected a packet with an unknown protocol.

PPP.010

Level: Common external error, CE-ERROR

Short Syntax:

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

Long Syntax:

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

Description:

pppin function has detected a protocol packet which is not in an OPEN state.

PPP.011

Level: Common external error, CE-ERROR

Short Syntax:

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

Long Syntax:

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

Description:

pppin function has detected NCP frames without the LCP being in an OPEN state.

PPP.012

Level: Common external error, CE-ERROR

Short Syntax:

PPP.012 PAP nt supp nt *network ID*

Long Syntax:

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

Description:

pppin function has detected unexpected PAP packet.

Cause:

An authentication packet has been received even though this option was not indicated during the LCP negotiation.

PPP.013

Level: Common external error, CE-ERROR

Short Syntax:

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

Long Syntax:

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

Description:

pppin function has detected a protocol packet which has not been implemented.

PPP.014

Level: Unusual external error, UE-ERROR

Short Syntax:

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

Long Syntax:

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

Description:

pppas_in function cannot detect the frame end flag.

Cause:

In asynchronous operating mode, a frame has been received which does not have the expected end flag. This is due to the fact it is longer than indicated in the MRU negotiation.

PPP.015

Level: Unusual internal error, UI-ERROR

Short Syntax:

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

Long Syntax:

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

Description:

Call carried out to the status machine with a packet containing a code error.

PPP.016

Level: Per packet trace, P-TRACE

Short Syntax:

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

Long Syntax:

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

Description:

Call carried out to the status machine. Indicates the type of frame that has been sent.

PPP.017

Level: Per packet trace, P-TRACE

Short Syntax:

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

Long Syntax:

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

Description:

Call carried out to the status machine. Indicates the type of frame that has been received.

PPP.018

Level: Common external error, CE-ERROR

Short Syntax:

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

Long Syntax:

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

Description:

The number of retries for the transmission of a frame type has been exceeded without receiving the correct response from the remote end.

PPP.019

Level: Per packet trace, P-TRACE

Short Syntax:

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

Long Syntax:

PPP.019 SCRIPT: Begin script on network *network ID*

Description:

Scrip execution begun after receiving the network connection.

PPP.020

Level: Per packet trace, P-TRACE

Short Syntax:

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

Long Syntax:

PPP.020 SCRIPT: received match *matched_item* on network *network ID*

Description:

A character sequence has been received which coincides with the current script element.

PPP.021

Level: Per packet trace, P-TRACE

Short Syntax:

PPP.021 SCRIPT: wt *wait_tmp* sec nt *network ID*

Long Syntax:

PPP.021 SCRIPT: waiting *wait_tmp* sec(s) on network *network ID*

Description:

Waiting the time corresponding to the current script element. This trace corresponds to a script 'wait and send' element.

PPP.022

Level: Per packet trace, P-TRACE

Short Syntax:

PPP.022 SCRIPT: no match, drp pkt nt *network ID*

Long Syntax:

PPP.022 SCRIPT: no match, drop packet on network *network ID*

Description:

The packet is discarded as it does not coincide with the current script element. This trace usually corresponds to the suppliers responses which are irrelevant from the script's point of view.

PPP.023

Level: Per packet trace, P-TRACE

Short Syntax:

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

Long Syntax:

PPP.023 SCRIPT: send *resp_item* on nnetwork *network ID*

Description:

The response corresponding to the current script element has been sent. If the element is a PASSWORD then the word “PASSWORD” is displayed instead of the response actually sent.

PPP.024

Level: Per packet trace, P-TRACE

Short Syntax:

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

Long Syntax:

PPP.024 SCRIPT: End of script on network *network ID*

Description:

The script has finished executing. The PPP will begin in the interface.

PPP.025

Level: Common informational comment, C-INFO

Short Syntax:

PPP.025 Add PPP to bundle nt *network ID*

Long Syntax:

PPP.025 Add PPP to multilink PPP bundle net *network ID*

Description:

A PPP net has been added to a multilink bundle due to traffic on demand

PPP.026

Level: Common informational comment, C-INFO

Short Syntax:

PPP.026 Excl PPP from bundle nt *network ID*

Long Syntax:

PPP.026 Excluded PPP from multilink PPP bundle net *network ID*

Description:

A PPP net has been excluded from a multilink bundle due to traffic on demand

PPP.027

Level: Unusual external error, UE-ERROR

Short Syntax:

PPP.027 Excl PPP from bundle nt *network ID*

Long Syntax:

PPP.027 Excluded PPP from multilink PPP bundle net *network ID*

Description:

A PPP net has been excluded from a multilink bundle due to authentication or IPCP errors.

Cause:

Additional PPP calls added to a multilink PPP bundle are having authentication or IPCP problems

Action:

Check IPCP and authentication parameters of the PPP net

PPP.028

Level: Per packet trace, P-TRACE

Short Syntax:

PPP.028 rx sec *rx_seq* exp *exp_seq* nt *network ID*

Long Syntax:

PPP.028 received sequence *rx_seq*, expected *exp_seq*, net *network ID*

Description:

Received and expected multilink PPP sequence on PPP net

PPP.029

Level: Per packet trace, P-TRACE

Short Syntax:

PPP.029 tx seq *tx_seq* nt *network ID*

Long Syntax:

PPP.029 transmited seq *tx_seq* net *network ID*

Description:

Multilink PPP sequence transmited on PPP net

PPP.030

Level: Common operation trace, C-TRACE

Short Syntax:

PPP.030 dlyd seq *dly_seq* exp *exp_seq* nt *network ID*

Long Syntax:

PPP.030 delayed sequence *dly_seq*, expected *exp_seq*, net *network ID*

Description:

Received and expected multilink PPP sequence on PPP net. Received sequence id greater than expected sequence, so reception is delayed and the packet is queued until we can process it.

PPP.031

Level: Unusual external error, UE-ERROR

Short Syntax:

PPP.031 rx sec *rx_seq* exp *exp_seq* nt *network ID*

Long Syntax:

PPP.031 received seq *rx_seq* less than expected *exp_seq*, net *network ID*

Description:

Received multilink PPP sequence is less than expected on PPP net. Strictly increasing number rule is broken. Packet is discarded. Remote peer could have problems.

PPP.035

Level: Per packet trace, P-TRACE

Short Syntax:

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

Long Syntax:

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

Description:

MRU option being made for the LCP negotiation.

PPP.036

Level: Per packet trace, P-TRACE

Short Syntax:

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

Long Syntax:

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

Description:

ACMM option being made for the LCP negotiation.

PPP.037

Level: Per packet trace, P-TRACE

Short Syntax:

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

Long Syntax:

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

Description:

PAP option being made for the LCP negotiation.

PPP.038

Level: Per packet trace, P-TRACE

Short Syntax:

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

Long Syntax:

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

Description:

Magic Number option being made for the LCP negotiation.

PPP.039

Level: Per packet trace, P-TRACE

Short Syntax:

PPP.039 mk pfc nt *network ID*

Long Syntax:

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

Description:

PFC option being made for the LCP negotiation.

PPP.040

Level: Per packet trace, P-TRACE

Short Syntax:

PPP.040 mk acfc nt *network ID*

Long Syntax:

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

Description:

ACFC option being made for the LCP negotiation.

PPP.041

Level: Per packet trace, P-TRACE

Short Syntax:

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

Long Syntax:

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

Description:

Quality Protocol option being made for the LCP negotiation.

PPP.042

Level: Per packet trace, P-TRACE

Short Syntax:

PPP.042 mk fcs nt *network ID*

Long Syntax:

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

Description:

FCS length (CRC) option being made for the LCP negotiation.

PPP.044

Level: Per packet trace, P-TRACE

Short Syntax:

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

Long Syntax:

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

Description:

Processing the MRU option received during the LCP negotiation.

PPP.045

Level: Per packet trace, P-TRACE

Short Syntax:

PPP.045 ck accm 0x*Asynchronous_Control_Character_Map* nt *network ID*

Long Syntax:

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

Description:

Processing the ACCM option received during the LCP negotiation.

PPP.046

Level: Per packet trace, P-TRACE

Short Syntax:

PPP.046 ck auth 0x*Authenticate_Protocol* nt *network ID*

Long Syntax:

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

Description:

Processing the PAP option received during the LCP negotiation.

PPP.047

Level: Per packet trace, P-TRACE

Short Syntax:

PPP.047 ck mag 0x*Magic_Number* nt *network ID*

Long Syntax:

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

Description:

Processing the Magic Number option received during the LCP negotiation.

PPP.048

Level: Per packet trace, P-TRACE

Short Syntax:

PPP.048 ck pfc nt *network ID*

Long Syntax:

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

Description:

Processing the PFC option received during the LCP negotiation.

PPP.049

Level: Per packet trace, P-TRACE

Short Syntax:

PPP.049 ck acfc nt *network ID*

Long Syntax:

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

Description:

Processing the ACFC option received during the LCP negotiation.

PPP.050

Level: Per packet trace, P-TRACE

Short Syntax:

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

Long Syntax:

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

Description:

Processing the Quality Protocol option received during the LCP negotiation.

PPP.051

Level: Per packet trace, P-TRACE

Short Syntax:

PPP.051 ck fcs nt *network ID*

Long Syntax:

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

Description:

Processing the FCS length (CRC) option received during the LCP negotiation.

PPP.052

Level: Per packet trace, P-TRACE

Short Syntax:

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

Long Syntax:

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

Description:

Unknown processing option received during the LCP negotiation.

Cause:

An option has been received during the LCP negotiation which is not implemented.

PPP.053

Level: Common informational comment, C-INFO

Short Syntax:

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

Long Syntax:

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

Description:

An LCP Identification packet has been received. This packet report about the remote end.

PPP.054

Level: Unusual external error, UE-ERROR

Short Syntax:

PPP.054 Bd *network ID*

Long Syntax:

PPP.054 Bad *network ID*

Description:

lcprsmsg function detects a frame with an invalid id.

Cause:

The response id does not coincide with the frame’s configure request or terminate request with the expected id.

PPP.055

Level: Unusual external error, UE-ERROR

Short Syntax:

PPP.055 Bd *network ID*

Long Syntax:

PPP.055 Bad *network ID*

Description:

lcprsmsg function has detected a frame with an invalid length.

Cause:

A frame has been received where the number of received data does not coincide with the length indicated for them.

PPP.056

Level: Unusual external error, UE-ERROR

Short Syntax:

PPP.056 Msmtchd *network ID*

Long Syntax:

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

Description:

lcprsmsg function has detected a frame with unexpected data.

Cause:

Acknowledgments have been received for negotiation options which were not sent.

PPP.057

Level: Unusual external error, UE-ERROR

Short Syntax:

PPP.057 Bd *network ID*

Long Syntax:

PPP.057 Bad *network ID*

Description:

lcprsmsg function has detected a nak frame with an invalid id.

Cause:

The reject frame for LCP negotiation options has been received containing an id which does not coincide with the one expected.

PPP.058

Level: Unusual external error, UE-ERROR

Short Syntax:

PPP.058 Bd *network ID*

Long Syntax:

PPP.058 Bad *network ID*

Description:

lcprsmsg function has detected a nak frame with an invalid length

Cause:

The reject frame for LCP negotiation options has been received and the length does not coincide with the one expected.

PPP.059

Level: Common informational comment, C-INFO

Short Syntax:

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

Long Syntax:

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

Description:

The authentication process for the indicated user has been successfully completed.

PPP.060

Level: Common informational comment, C-INFO

Short Syntax:

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

Long Syntax:

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

Description:

The authentication process for the indicated user has not been completed successfully.

Cause:

The user-password is unknown.

Action:

Reprogram the user and password options for PAP. If this problem persists, consult your service access supplier.

PPP.061

Level: Per packet trace, P-TRACE

Short Syntax:

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

Long Syntax:

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

Description:

MRRU option is being made for the LCP negotiation.

PPP.062

Level: Per packet trace, P-TRACE

Short Syntax:

PPP.062 mk ssnfh nt *network ID*

Long Syntax:

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

Description:

SSNHF option is being made for the LCP negotiation.

PPP.063

Level: Per packet trace, P-TRACE

Short Syntax:

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

Long Syntax:

PPP.063 making endpoint discrimator whit value *Endpoint_Discrimator_Class* on network *network ID*

Description:

ENDPD option is being made for the LCP negotiation.

PPP.066

Level: Per packet trace, P-TRACE

Short Syntax:

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

Long Syntax:

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

Description:

Addresses option is being made for the IPCP negotiation.

PPP.067

Level: Per packet trace, P-TRACE

Short Syntax:

PPP.067 mk cmp 0x*comp_protocol*, slt=0x*slot*, slt_cmp=0x*slot_comp* nt *network ID*

Long Syntax:

PPP.067 making compression option 0x*comp_protocol* slot=0x*slot*, slot_comp=0x*slot_comp* on network *network ID*

Description:

IP compression option is being made for the IPCP negotiation.

PPP.068

Level: Per packet trace, P-TRACE

Short Syntax:

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

Long Syntax:

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

Description:

Addresses option is being made for the IPCP negotiation.

PPP.069

Level: Per packet trace, P-TRACE

Short Syntax:

PPP.069 mk ipcp unk nt *network ID*

Long Syntax:

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

Description:

Initializing the buffer in order to store the IPCP negotiation options received and unknown or not implemented..

PPP.070

Level: Per packet trace, P-TRACE

Short Syntax:

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

Long Syntax:

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

Description:

Processing the addresses option received during the IPCP negotiation.

PPP.071

Level: Per packet trace, P-TRACE

Short Syntax:

PPP.071 ck cmp 0x*comp_protocol* slt=0x*slot*, slt_cmp=0x*slot_comp* nt *network ID*

Long Syntax:

PPP.071 checking compression option 0x*comp_protocol* slot=0x*slot*, slot_cmp=0x*slot_comp* on network *network ID*

Description:

Processing the IP compression option received during the IPCP negotiation.

PPP.072

Level: Per packet trace, P-TRACE

Short Syntax:

PPP.072 ck ad *ip_address* nt *network ID*

Long Syntax:

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

Description:

Processing the address option received during the IPCP negotiation.

PPP.073

Level: Per packet trace, P-TRACE

Short Syntax:

PPP.073 ck ipcp unk 0x*unk_option* nt *network ID*

Long Syntax:

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

Description:

Processing the unknown option received during the IPCP negotiation.

PPP.074

Level: Per packet trace, P-TRACE

Short Syntax:

PPP.074 ck mrru *Max_Receive_Reconstructed_Unit* nt *network ID*

Long Syntax:

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

Description:

Processing the MRRU option received during the LCP negotiation.

PPP.075

Level: Per packet trace, P-TRACE

Short Syntax:

PPP.075 ck ssnfh nt *network ID*

Long Syntax:

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

Description:

Processing the SSNHF option received during the LCP negotiation.

PPP.076

Level: Per packet trace, P-TRACE

Short Syntax:

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

Long Syntax:

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

Description:

Processing the ENDPD option for the LCP negotiation.

PPP.078

Level: Common informational comment, C-INFO

Short Syntax:

PPP.078 Mdm Chg 0x*network ID*

Long Syntax:

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

Description:

Change in the interface signals status.

PPP.079

Level: Unusual external error, UE-ERROR

Short Syntax:

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

Long Syntax:

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

Description:

A protocol reject has been received.

Cause:

Packets containing a protocol which has not been implemented or is unknown have been received by the remote end.

PPP.080

Level: Unusual external error, UE-ERROR

Short Syntax:

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

Long Syntax:

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

Description:

A sequence has been lost at reception when the buffer available for re ordering the received frames has been detected as full.

Cause:

A packet has been lost or errors provoking the loss of a frame at reception have been received.

PPP.081

Level: Unusual external error, UE-ERROR

Short Syntax:

PPP.081 rc bd mgc 0x*rcv_mag_num*, ours 0x*our_mag_num*, nt *network ID*

Long Syntax:

PPP.081 Received bad magic number 0x*rcv_mag_num*, ours 0x*our_mag_num*, on network *network ID*

Description:

A frame containing a magic number which does not coincide with the one indicated during the LCP negotiation has been received.

PPP.083

Level: Common informational comment, C-INFO

Short Syntax:

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

Long Syntax:

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

Description:

A call to the indicated address is carried out.

PPP.084

Level: Common informational comment, C-INFO

Short Syntax:

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

Long Syntax:

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

Description:

A call to the indicated address has been successfully established.

PPP.085

Level: Common informational comment, C-INFO

Short Syntax:

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

Long Syntax:

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

Description:

A call has been disconnected due to absence of traffic during the indicated period of time. The maintenance packets (echo) are not taken into account when considering periods without traffic.

PPP.086

Level: Common informational comment, C-INFO

Short Syntax:

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

Long Syntax:

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

Description:

The call to the indicated address has not been established as no response has been detected from the remote end.

PPP.087

Level: Per packet trace, P-TRACE

Short Syntax:

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

Long Syntax:

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

Description:

This is only for testing to see who activates the call.

PPP.088

Level: Common informational comment, C-INFO

Short Syntax:

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

Long Syntax:

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

Description:

Call to the indicated address is released.

PPP.089

Level: Common informational comment, C-INFO

Short Syntax:

PPP.089 In Call cmp nt *network ID*

Long Syntax:

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

Description:

Response to an incoming call successfully completed

2. Examples of PPP protocol events

A typical events trace for a connection through ISDN is displayed below:

```
*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 0xFFFFC023 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 0xFFFFC023 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>
*
```