ISDN
PPP Troubleshooting

ISDN
POCKET GUIDE
No. **2**

Edition 3

WAVETEK
WANDEL
GOLTERMANN
Communications Test Solutions

Visit our Web site for regular updates
on our test and measurement solutions:
http://isdn.wwgsolutions.com
e-mail: isdn@wwgsolutions.com

Table of contents

Introduction

ISDN is a popular technology for internetworking and Internet access, providing the user with a flexible bandwidth together with an excellent quality of transmission.

The efficiency of all internetworking applications is strongly linked to the Customer Premises Equipment (CPE) configurations. These configurations may be complex due to the numerous options and functions available to users: an ISDN router may have more than 100 configuration parameters to be set in order to ensure that it functions properly (each dialer may have 30 parameters describing the ISDN connection mode as well as the remote LAN access conditions, data link parameters and IP parameters).

That means that the use of protocol analysis to determine these parameters and their on-line effects is a keypoint for troubleshooting such applications. The object of this booklet is to introduce the troubleshooting procedure for LAN interconnection, Internet access or any remote access through ISDN using a standardized technology which is the Point-to-Point Protocol (PPP).

This guide describes troubleshooting procedures step by step, illustrated with a case study using an ISDN Basic Rate Access, and highlights the benefit of protocol analysis through some troubleshooting cases. All measurements described hereafter are performed at the ISDN BRA interface.

The troubleshooting tool used to illustrate this case study is the Multiport Protocol Analyzer WWG DA-5 dedicated to troubleshooting datacommunications over WAN and ISDN. All procedures described in this booklet are also applicable to the WWG's Expert Protocol Analyzer DominoWAN ISDN.

Visit our Web site (www.wwgsolutions.com)!
Free download of PPP troubleshooting guide (Acrobat ™ file):
http://www.wwgsolutions.com/products/da5/da5.html

WWG DA-5 Multiport Protocol Analyzer

Troubleshooting solution for:
- ISDN BRA interface
- V interfaces

Applications:
- ➜ CPE configuration troubleshooting
- ➜ WAN service troubleshooting

Learn more: *http://www.wwgsolutions.com/products/da5/da5.html*

WWG DominoWAN ISDN Internetwork Analyzer

Expert troubleshooting solution for:
- ISDN BRA interface
- ISDN PRA interface
- V interfaces

Applications:
- ➜ LAN application over WAN troubleshooting
- ➜ Network management and optimization
- ➜ Expert support

Learn more: *http://www.wwgsolutions.com/products/domino/domino.html*

WWG IUM-10 U-Interface Monitor

Connection of the WWG DA-5 and WWG DominoWAN ISDN to the U (2B1Q) interface.
Applications:
- ➜ Maintenance from the central office
- ➜ Maintenance of ISDN CPEs including the NT1
- ➜ Layer 1 event monitoring over the local loop

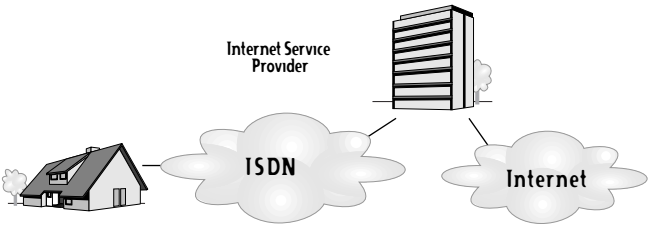
Learn more: *http://www.wwgsolutions.com/products/ium10/ium10.html*

1 User Application Overview

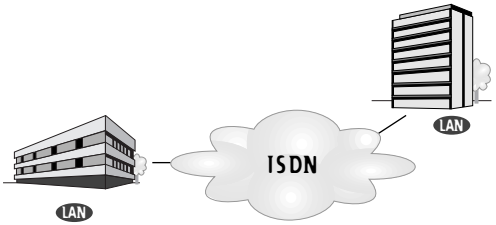
Internetworking over ISDN means interconnecting 2 data instruments through the ISDN network, using the ISDN B channel for data traffic.

The most common applications are:

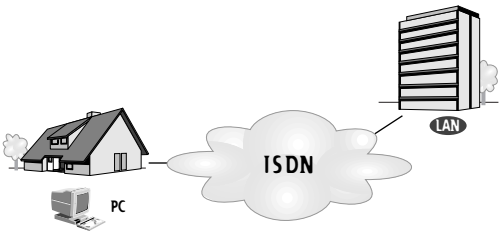
Internet access



LAN to LAN



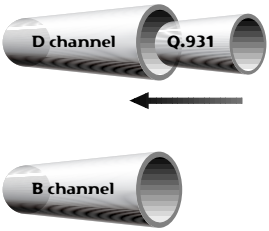
Remote access



2 Technology Overview

LAN-to-LAN traffic, Internet or any remote access through ISDN are performed in 3 main steps:

D-channel signaling for end-to-end B-channel connection

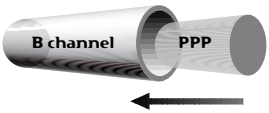


D-channel signaling for end-to-end B-channel connection with the data service.

➥ ***Troubleshooting requires D-channel analysis***

Datalink layer negotiation

Point-to-Point Protocol or Multilink Point-to-Point Protocol (PPP and PPP/MLP) are the datalink protocols used within ISDN B channels. Before sending data packets encapsulated in PPP frames, PPP negotiation takes place.

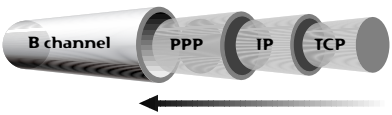


B channels are used as transparent 64-kbit/s pipes to send PPP negotiation for the configuration of end-to-end Customer Premises Equipment (CPE).

➥ ***Troubleshooting requires B-channel analysis***

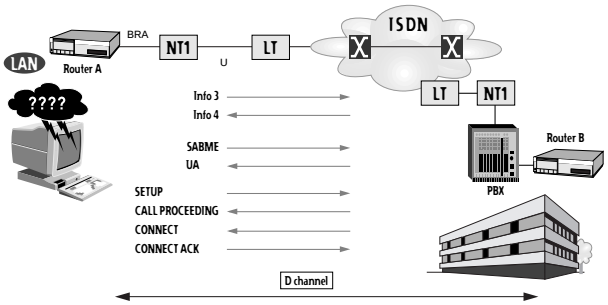
LAN traffic over datalink layer

The LAN traffic (IP/IPX packets) is sent encapsulated in PPP frames.



➥ ***Troubleshooting requires B-channel analysis.***

3 D-channel Troubleshooting



The aim of D-channel signaling is to establish an end-to-end B-channel connection between router A and router B. This is a step-by-step procedure starting with D-channel layer 1 activation up to D-channel layer 3.

Most of the D-channel problems can be fixed step by step by analyzing the following information:

- D-channel layer 1 is up if Info 3 and Info 4 are exchanged by the router and the NT1. The main layer 1 problems are caused by wrong cabling.
- D-channel layer 2 is up once the SABME and UA frames are exchanged by the router and the terminal.
- B-channel connection is done once the CONNECT message is received. If not, router A may receive the RELEASE COMPLETE or DISCONNECT message indicating the cause of the failure. Detailed decoding of these messages plus the associated SETUP message will diagnose the problem.

DA-5 diagnosis

The example below shows a failure in an outgoing call.

Frame summary provides overview of D-channel activity:

- Layer 1 information
- Layer 2 frames
- Layer 3 messages

Frame summary monitor

```
   TE: Info 0 - NT: Info 0 / PS1 On                          04:45:12001
   TE: Info 0 - NT: Info x / PS1 On                          04:45:46596
   TE: Info 0 - NT: Info 2 / PS1 On                          04:45:46597
   TE: Info 3 - NT: Info 2 / PS1 On                          04:45:46598
   TE: Info 3 - NT: Info 4 / PS1 On                          04:45:46600
←D   0   64 c SABME  p                                 3 G 04:45:46607
→D   0   64 r UA     f                                 3 G 04:45:46609
←D   0   64 c  I       08   4E  -  SETUP                29 G 04:45:46617
   Channel: B1       Calling: 7082       Called: 6067
←D   0   64 r RR        -   1                           4 G 04:45:46705
→D   0   64 c  I        1   0 08   4E  f  RELEASE COMPL.  8 G 04:45:46714
```

Diagnosis: All D-channel layers OK except layer 3; detailed analysis is needed for cause diagnosis.

Frame detail provides bit-to-bit decoding for complete diagnosis:

RELEASE COMPLETE detailed analysis

```
EDSS-1    : ------------------- ISDN layer 3 -------------------
EDSS-1    : Protocol Discriminator.. 08
EDSS-1    :  Call Reference:
EDSS-1    :       Length.....  1
EDSS-1    :       Flag.....  0
EDSS-1    :       Value.....  4Eh (78)
EDSS-1    : RELEASE COMPLETE
EDSS-1    :       CAUSE          Lg =      2
EDSS-1    :              Hex. value   : 87 9C
EDSS-1    :              Coding stand.: CCITT
EDSS-1    :              Location     : internat.netw.
EDSS-1    :              Cause Class  : normal
EDSS-1    :               uncomplete address
```

Diagnosis: The ISDN called address dialed by router A (6067) is incomplete. The network is not able to proceed with the call. The router B ISDN address has to be checked within the router A routing table.

4 Point-to-Point Protocol Overview

The Point-to-Point Protocol (PPP) is used to transmit the encapsulated LAN protocol (IP) over B channel(s). Before sending LAN traffic over PPP frames, PPP negotiation takes place just after the physical connection of the B channel: troubleshooting the B channel is also a step-by-step procedure.

- ***Link Control Protocol negotiation (LCP):***
  Negotiation of the router configuration parameters and options (such as multilink, authentication mode etc.) to be used.

- ***Authentication negotiation:***
  Password Authentication Protocol or Challenge Handshake Authentication Protocol (PAP or CHAP) or other proprietary access authentication negotiation.

- ***Network Control Protocol negotiation (NCP):***
  Negotiation of the transport protocol and its parameters (IP protocol, IP router addresses etc.).

- ***LAN traffic over B channel:***
  Once all PPP negotiations have been successfully completed, routers are able to start the LAN traffic encapsulated over PPP frames.

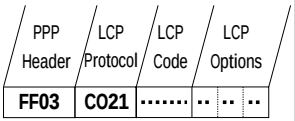
Learn more about RFC's (IETF Requests for Comments) for PPP and PPP/MLP at: *http://www.internic.net/ds/dspg1intdoc.html*

Protocol overview

Problems with PPP negotiations are solved using protocol analysis. Detailed protocol analysis of D+B1+B2 channels is required for complete diagnosis of the CPE configuration. Complete decoding means a full decode of PPP protocols as well as negotiated options which show the CPE configuration parameters.

Link Control Protocol negotiation

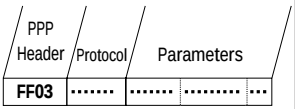
LCP Frame structure



Main LCP code:
Configuration Request
Configuration Acknowledge
Configuration Non Acknowledge
Configuration Reject
Echo Request
Echo Reply

Authentication negotiation

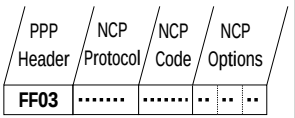
Authentication Frame structure



Main Authentication protocols:
Password Authentication Protocol (PAP)
Challenge Handshake Authentication Protocol (CHAP)

Network Control Protocol negotiation

NCP Frame structure



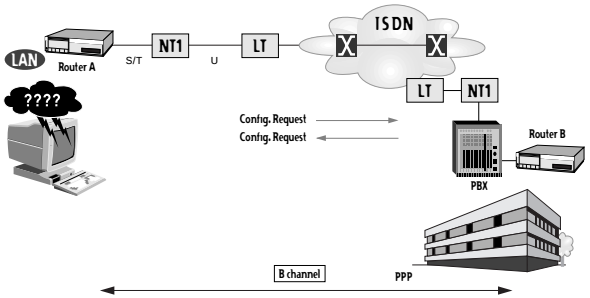
Main NCP protocols:
IPCP, IPXCP, Bandwidth Allocation Protocol (BACP)...

Main NCP code:
Configuration Request
Configuration Acknowledge
Configuration Non Acknowledge
Configuration Reject
Termin Request
Termin Acknowledge

Note: *In the case of terminal adapters or modems using bit rate adaptation, the PPP negotiation frames and LAN encapsulated traffic may be encapsulated into V.120 frames.*

5 LCP: Link Control Protocol

5.1 LCP negotiation overview



Once the B channel is physically connected, the LCP negotiation starts immediately (average delay is 80 ms): this makes simultaneous analysis of D and B channels mandatory for troubleshooting.

LCP Code	*Function*
Configuration Request	Initiate LCP negotiation, request of options to be negotiated (Authentication mode, Multilink option, security option etc.)
Configuration Acknowledge	Acknowledgement of the options negotiated by the configuration request
Configuration Non Acknowledge	Non-Acknowledgement of the option parameters of the configuration request
Configuration Reject	Reject of the options negotiated by the configuration request
Echo Request/ Echo Reply	Operation frames to check Quality of Service

Detailed analysis of the configure requests exchanged will provide routers with an initial diagnosis of the configuration (what are the options declared per dialer in the CPE configuration).

3 cases will be illustrated hereafter:

- LCP negotiation success
- Configuration Request rejected
- Configuration Request Non Acknowledge

DA-5 analysis overview

The DA-5 monitors the PPP protocol in both frame summary and frame detail modes:

Frame summary provides an overview of LCP negotiation status:

- Frame direction identification
- LCP frame ID and type identification
- Frame length and checksum diagnosis
- Time-stamping

Frame summary monitor

→	B1 PPP ID=1	Config-Req	LCP	12 G 00:01:44262
←	B1 PPP ID=1	Config-Req	LCP	22 G 00:01:44269

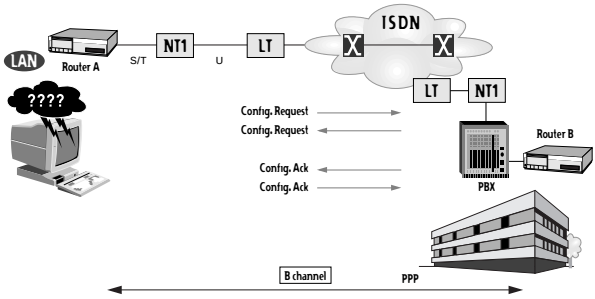
Frame detail provides identification and diagnosis of option negotiation:

- Header bit-to-bit decoding
- LCP options bit-to-bit decoding

Configuration Request detailed analysis

```
B1: NT<-TE --- Frame # 00000008 ---Length=0016    Time=00:01:45127
PPP       : ------------ Point-to-Point Protocol ------------
PPP       : PPP header..... FF 03
PPP       : Protocol code.. Not compressed
PPP       : Protocol..... LCP (C021)
PPP       : LCP Code..... Config-Req
PPP       : Identifier..... 2
PPP       : LCP Length..... 12
PPP       :
PPP       : Option 17      Lg =      4
PPP       : (MultiLink MRRU)
PPP       : Dec.value..... 1600
PPP       :
PPP       : Option 03      Lg =      4
PPP       : (Authentication-Protocol)
PPP       : Protocol..... PAP
```

5.2 LCP negotiation success



If the LCP negotiation is successful, each configuration request is acknowledged by the peer.

- Protocol analysis in frame summary mode at the S/T interface indicates whether the LCP negotiation has been successfully completed.
- Protocol analysis of Configuration Request frames in frame detailed mode at the S/T interface shows which options have been negotiated.

DA-5 diagnosis

Frame summary monitor

→	B1 PPP	ID=1	Config-Req	LCP	12 G 00:01:44262
←	B1 PPP	ID=1	Config-Req	LCP	22 G 00:01:44269
←	B1 PPP	ID=1	Config-Ack	LCP	12 G 00:01:44271
→	B1 PPP	ID=1	Config-Ack	LCP	14 G 00:01:45122

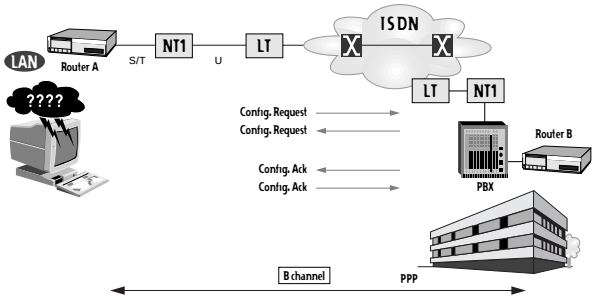
Diagnosis: LCP negotiation OK: both requests get acknowledgement

Configuration request detailed analysis

```
B1 : NT<-TE --- Frame # 00000109 --- Length=0062     Time=04:46:14473
PPP      : ------------ Point-to-Point Protocol ------------
PPP      : PPP header..... FF 03
PPP      : Protocol code.. Not compressed
PPP      : Protocol..... LCP (C021)
PPP      : LCP Code..... Config-Req
PPP      : Identifier..... 1
PPP      : LCP Length..... 30
PPP      :
PPP      : Option 01      Lg =     4
PPP      : (Maximum-Receive-Unit)
PPP      : Dec.value..... 1522
PPP      :
PPP      : Option 03      Lg =     8
PPP      : (Authentication-Protocol)
PPP      : Protocol..... Shiva authent.
PPP      : DUMP..... 01 00 00 02
PPP      :
PPP      : Option 05      Lg =     6
PPP      : (Magic_Number)
PPP      : Hex.value..... 55 99 F5 84
```

Diagnosis: The following options are negotiated because set in router dialer configuration:
• Maximum receive units • Shiva Authentication method • Magic number

5.3 LCP negotiation failure: Configuration Rejected



If LCP negotiation fails, the Configuration Request sent by router A receives a Configuration Reject by router B.

- Protocol analysis in frame summary mode at the S/T interface shows that the LCP negotiation has failed: router B rejects the router A Configuration Request, the requested option is not known to router B and cannot be performed.
- Protocol analysis of Configuration Reject frames in frame detailed mode shows which options have been rejected. Detailed analysis of both Configuration Request and Reject will pinpoint which option has been rejected and which parameter has to be changed inside the local router configuration.

Note: If no Configuration Request is sent, this means that no connection has been activated inside the router configuration.

DA-5 diagnosis

Frame summary monitor

→	B1 PPP	ID=1	Config-Req	LCP	12 G 00:01:44262
←	B1 PPP	ID=1	Config-Req	LCP	22 G 00:01:44269
←	B1 PPP	ID=1	Config-Ack	LCP	12 G 00:01:44271
→	B1 PPP	ID=1	Config-Rej	LCP	14 G 00:01:45122
←	B1 PPP	ID=1	Config-Req	LCP	12 G 00:01:45127
→	B1 PPP	ID=1	Config-Rej	LCP	14 G 00:01:45832

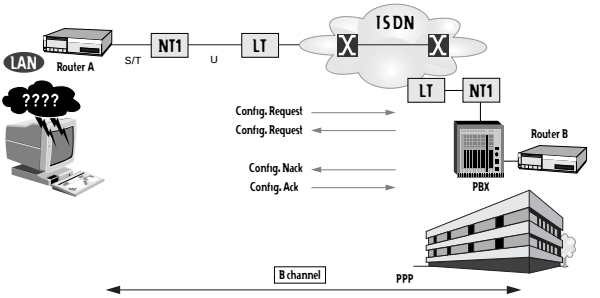
Diagnosis: LCP Negotiation KO, router B rejects router A Configuration Request.

Configuration Reject detailed analysis

```
B1 : NT->TE --- Frame # 00000112 --- Length=0114      Time=04:46:14526
PPP      : ------------ Point-to-Point Protocol ------------
PPP      : PPP header..... FF 03
PPP      : Protocol code.. Not compressed
PPP      : Protocol..... LCP (C022)
PPP      : LCP Code..... Config-Rej
PPP      : Identifier..... 1
PPP      : LCP Length..... 30
PPP      :
PPP      : Option 03      Lg =      8
PPP      : (Authentication-Protocol)
PPP      : Protocol..... Shiva authent.
PPP      : DUMP..... 01 00 00 02
```

Diagnosis: Shiva Authentication protocol cannot be performed by router B, the user has to change the router configuration to achieve a common authorized authentication protocol (PAP/CHAP, or other proprietary protocol).

5.4 LCP negotiation failure: Configuration Non Acknowledge



The LCP negotiation has failed, the Configuration Request sent by router A gets a Configuration Non Acknowledge by router B.

- Protocol analysis in frame summary mode at S/T interface shows that the LCP negotiation has failed: the router B does not acknowledge the local router Configuration Request, the requested option is known by the router B but negotiated with a wrong parameter.
- Protocol analysis of *Configuration Non Acknowledge* frame in frame detailed mode shows which options parameters are wrong. Detailed analysis of both Configuration Request and Reject will pinpoint which option is rejected and which parameter has to be changed inside the local router configuration. According to the CPE configuration, this change may be done dynamically by the CPE or manually by the user inside the CPE setting.

DA-5 diagnosis

Frame summary monitor

→	B1 PPP	ID=1	Config-Req	LCP	12 G 00:01:44262
←	B1 PPP	ID=1	Config-Req	LCP	22 G 00:01:44269
←	B1 PPP	ID=1	Config-Ack	LCP	12 G 00:01:44271
→	B1 PPP	ID=1	Config-Nack	LCP	14 G 00:01:45122
←	B1 PPP	ID=2	Config-Req	LCP	16 G 00:01:45127
→	B1 PPP	ID=2	Config-Nack	LCP	16 G 00:01:45832

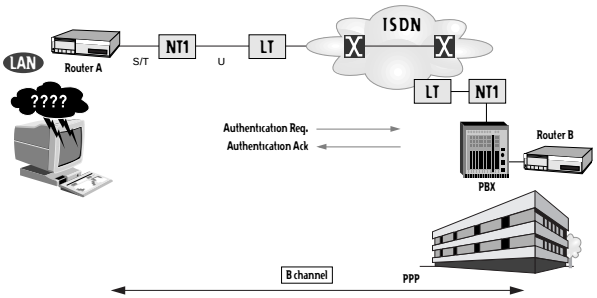
Diagnosis: LCP negotiation failure, router B does not acknowledge router A Configuration Request.

Configuration Non Acknowledge detailed analysis

```
PPP     : ---------- Point-to-Point Protocol ----------
PPP     : PPP header..... FF 03
PPP     : Protocol code.. Not compressed
PPP     : Protocol..... LCP (C021)
PPP     : LCP Code..... Config-Nack
PPP     : Identifier..... 1
PPP     : LCP Length..... 30
PPP     :
PPP     : Option 01      Lg =     4
PPP     : (Maximum-Receive-Unit)
PPP     : Dec. value..... 1522
```

Diagnosis: Router B is not able to negotiate a Maximum-Receive unit (maximum number by bytes per frame) over 1522. Router A sent the first request with a greater value.

6 Authentication Negotiation



Various authentication protocols are used: apart from the proprietary method, the best-known are:

- Password Authentication Protocol (PAP),
- Challenge Handshake Authentication Protocol (CHAP).

The following example is taken with PAP. In the case of PAP, the CPE which initiates the connection sends Authentication parameters to router B. If the Authentication Request is rejected, the parameters (user name and password) are wrong and must be changed inside the CPE configuration.

DA-5 diagnosis

Frame summary monitor

→	B1 PPP ID=1	Authent-Req	PAP	23 G 00:01:53943
←	B1 PPP ID=1	Authent-Ack	PAP	9 G 00:01:53950

Diagnosis: Authentication OK

→	B1 PPP ID=1	Authent-Req	PAP	23 G 00:01:53943
←	B1 PPP ID=1	Authent-Rej	PAP	9 G 00:01:53950

Diagnosis: Authentication KO.

If the Authentication is KO, detailed analysis is mandatory.

Authentication reject detailed analysis

```
B1 : NT->TE --- Frame # 00000031 --- Length=0023     Time=00:01:53943
PPP      : ---------- Point-to-Point Protocol ----------
PPP      : Protocol code.. Not compressed
PPP      : Protocol..... PAP (C023)
PPP      : PAP Code..... Authent. rej
PPP      : Identifier..... 1
PPP      : PAP Length..... 19
PPP      : Username Length   7
PPP      : Username ..... router1

PPP      : Password Length   6
PPP      : Password ..... secret
```

Diagnosis: Both router user name *"Router1"* and password *"secret"* are wrong. These parameters have to be changed inside the router configuration.

Refer to Appendix 1 for the list of Authentication Protocols decoded by the DA-5.

7
NCP: Network Control Protocol

7.1 NCP negotiation overview

PPP frames are designed to carry different types of protocols. NCP is responsible for the Layer 3 LAN protocol configuration. The CPEs have to configure themselves to be able to transmit the LAN protocol packets: therefore there are many Control Protocols each of them being dedicated to one specific LAN protocol: IP Control Protocol, IPX Control Protocol, AppleTalk Control Protocol etc.

NCP Code	***Function***
Configuration Request	Initiate NCP negotiation, request of LAN parameters to be negotiated (router WAN alias, router IPX node and network number...)
Configuration Acknowledge	Acknowledgement of the LAN protocol negotiated by the Configuration Request
Configuration Non Acknowledge	Non Acknowledgement of the LAN parameters negotiated by the Configuration Request
Configuration Reject	Reject of the LAN protocol negotiated by the Configuration Request
Termin Request	Optional code used to interrupt PPP traffic before B-channel disconnection
Termin Acknowledge	Acknowledgement of Termin Request.

3 cases will be illustrated hereafter:

- NCP negotiation success
- Configuration Request rejected
- Configuration Request Non Acknowledge

DA-5 analysis overview

The DA-5 monitors the PPP protocol in both frame summary and frame detail modes:

Frame summary provides an overview of NCP negotiation status:

- Frame direction identification
- NCP frame ID and type identification
- Frame length and checksum diagnosis
- Time-stamping

Frame summary monitor

→	B1 PPP	ID=5	Config-Req	IPCP	14 G 00:01:56129
←	B1 PPP	ID=2	Config-Req	IPCP	14 G 00:01:56323

Frame detail provides identification and diagnosis of option negotiation:

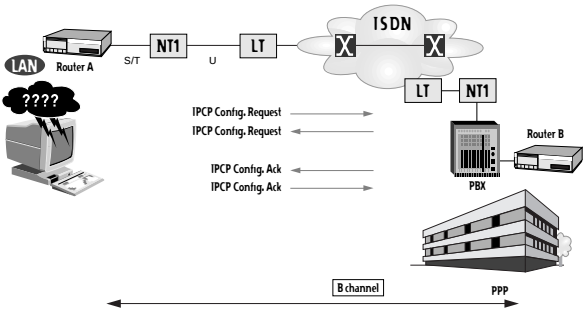
- Header bit-to-bit decoding
- NCP parameters bit-to-bit decoding

Configuration Request detailed analysis

```
B1 : NT<-TE --- Frame # 00000013 --- Length=0014     Time=00:01:53952
PPP      : ------------ Point-to-Point Protocol ------------
PPP      : PPP header..... FF 03
PPP      : Protocol code.. Not compressed
PPP      : Protocol..... IPCP (8021)
PPP      : IPCP Code..... Config-Req
PPP      : Identifier..... 1
PPP      : IPCP Length..... 10
PPP      :
PPP      : Option 03      Lg =      6
PPP      : (IP-Address)
PPP      : Hex.value.....8D A9 31 14
PPP      : Address.....141.169.49.20
```

Refer to Appendix 1 for the list of Control Protocols decoded by the DA-5.

7.2 NCP negotiation success



If the NCP negotiations are successful, each Configuration Request is acknowledged by the peer.

The 2 CPE's are ready to exchange IP packets.

- Protocol analysis in frame summary mode at the S/T interface indicates whether the NCP negotiations have been successfully completed.
- Protocol analysis of IPCP Configuration Request frames in frame detailed mode at the S/T interface shows which IP parameters have been negotiated.

DA-5 diagnosis

Frame summary monitor

→	B1 PPP	ID=5	Config-Req	IPCP	14 G 00:01:56129
←	B1 PPP	ID=5	Config-Ack	IPCP	14 G 00:01:56135
←	B1 PPP	ID=2	Config-Req	IPCP	14 G 00:01:56323
→	B1 PPP	ID=2	Config-Ack	IPCP	14 G 00:01:57089

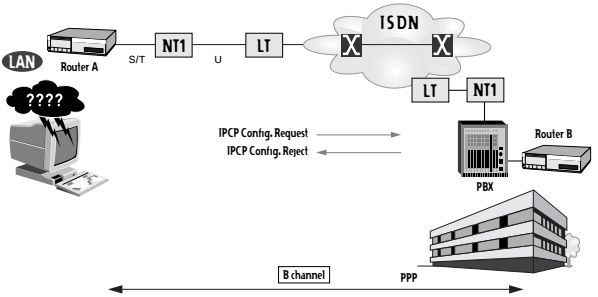
Diagnosis: IPCP negotiation OK.

IPCP Configuration Request detailed analysis

```
B1 : NT<-TE --- Frame # 00000039 --- Length=0014     Time=00:01:56323
PPP      : ------------ Point-to-Point Protocol ------------
PPP      : PPP header..... FF 03
PPP      : Protocol code.. Not compressed
PPP      : Protocol..... IPCP (8021)
PPP      : IPCP Code..... Config-Req
PPP      : Identifier..... 2
PPP      : IPCP Length..... 10
PPP      :
PPP      : Option 03      Lg =      6
PPP      : (IP-Address)
PPP      : Hex.value.....8D A9 31 14
PPP      : Address..... 141.169.49.20
```

Diagnosis: The parameter negotiated is the router A IP WAN address (also called WAN alias).

7.3 NCP negotiated failure: Configuration Rejected



The NCP negotiation has failed, the IPCP Configuration Request sent by router A is rejected by router B.

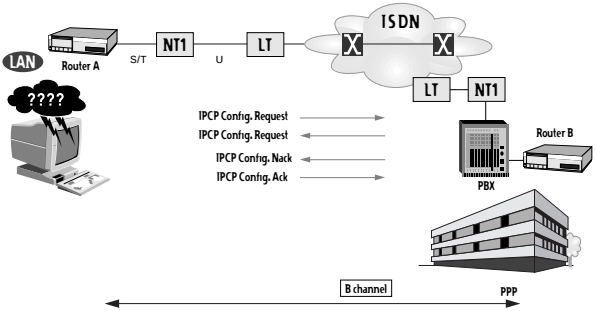
- Protocol analysis in frame summary mode at the S/T interface shows that the NCP has failed: router B rejects the local router Configuration Request, the requested protocol is not known to router B and cannot be performed. Moreover, router B is not sending any IPCP Configuration Request.

The IP protocol cannot be handled by router B, the router B configuration has to be changed.

DA-5 diagnosis

Frame summary monitor				
→	B1 PPP ID=1	Config-Req	IPCP	12 G 00:01:44262
←	B1 PPP ID=1	Config-Rej	IPCP	14 G 00:01:45122
Diagnosis: IPCP Negotiation KO, router B is not implemented to handle IP.				

7.4 NCP negotiated failure: Configuration Non Acknowledge



The NCP negotiation has failed, the Configuration Request sent by router A receives a Configuration Non Acknowledge from router B.

- Protocol analysis in frame summary mode at the S/T interface shows that the NCP negotiations have failed: router B does not acknowledge the local router configuration, the requested option is known to router B but negotiated with an incorrect parameter.

- Protocol analysis of the Configuration Non Acknowledge frame in frame detailed mode at the S/T interface shows which option parameters are wrong. Detailed analysis of both Configuration Request and Reject will pinpoint which option has been rejected and which parameter has to be changed inside the local router configuration. Depending on the CPE configuration, this change may be done dynamically by the CPE or manually (and a new Configuration Request sent) by the user inside the CPE setting.

Frame summary monitor

→	B1 PPP	ID=1	Config-Req	IPCP	12 G 00:01:44262
←	B1 PPP	ID=1	Config-Req	IPCP	22 G 00:01:44269
←	B1 PPP	ID=1	Config-Ack	IPCP	12 G 00:01:44271
→	B1 PPP	ID=1	Config-Nack	IPCP	14 G 00:01:45122
←	B1 PPP	ID=2	Config-Req	IPCP	16 G 00:01:45127
→	B1 PPP	ID=2	Config-Nack	IPCP	16 G 00:01:45832

Diagnosis: NCP negotiation failure.

Configuration Non Acknowledge detailed analysis

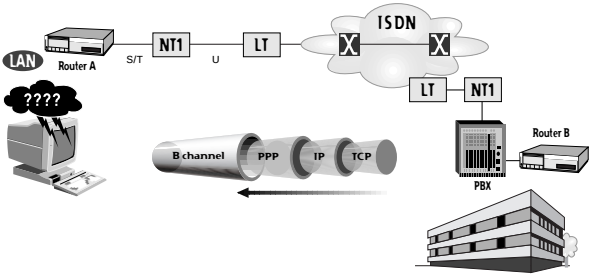
```
B1 : NT<-TE --- Frame # 00000049 --- Length=0012   Time=18:21:43592
PPP      : ------------ Point-to-Point Protocol ------------
PPP      : No PPP header
PPP      : Protocol code.. Not compressed
PPP      : Protocol..... IPCP (8021)
PPP      : IPCP Code..... Config-Nack
PPP      : Identifier..... 2
PPP      : IPCP Length..... 10
PPP      :
PPP      : Option 03      Lg =     6
PPP      : (IP-Address)
PPP      : Hex.value.....8D A9 22 97
PPP      : Address.....141.169.34.151
```

Diagnosis: IPCP address (14.169.34.151) negotiated in Configuration Request is wrong.

8 PPP Troubleshooting

8.1 LAN encapsulated protocol troubleshooting

Once the NCP layer has been passed, the B channel(s) can be used as virtual pipe(s) for LAN traffic encapsulated over PPP frames.



There are two main situations as regards the encapsulation of LAN protocols:

- Encapsulation over PPP frames if the LAN traffic to be transmitted needs a bandwidth lower than 64 kbit/s.
- Encapsulation over PPP/MLP (PPP Multilink) frames if the LAN traffic to be transmitted needs a bandwidth greater than 64 kbit/s.

In the case of PPP/MLP, all the procedures described above are still valid with the following variants:

- A second SETUP will be sent into the D channel to physically connect a second B channel.
- Multilink option will be negotiated at LCP layer in the 2 established B channels.
- IP packet will be split into 2 fragments and each fragment will be sent in a separate B channel over PPP/MLP frames.

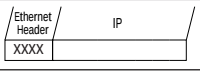
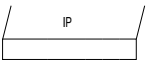
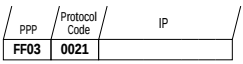
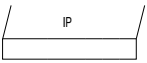
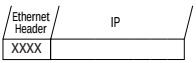
Note: The IP protocol will be taken to illustrate LAN encapsulation troubleshooting throughout this chapter.

Protocol overview

The LAN encapsulation is illustrated hereafter for IP packets to be sent from LAN A to LAN B.

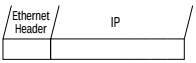
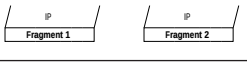
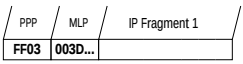
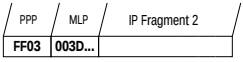
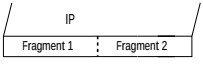
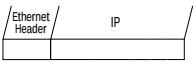
LAN traffic encapsulation over PPP

This encapsulation method is valid for LAN traffic which needs a bandwidth lower than 64 kbit/s.

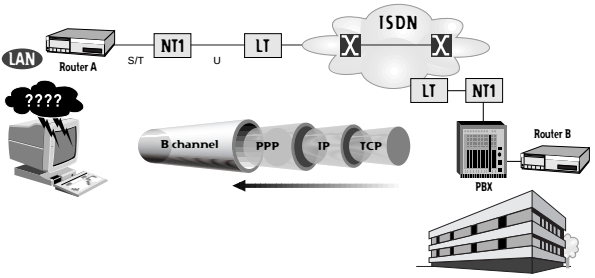
Location	*What*	*Frame structure*
LAN A	IP packet over Ethernet	
Router A	Extraction of IP packet	
ISDN B channel	Transmission of IP packet over PPP in one B channel	
Router B	Extraction of IP packet from PPP frames received	
LAN B	IP packet over Ethernet	

LAN traffic encapsulation over PPP/MLP

This encapsulation method is valid for LAN traffic which needs a bandwidth between 64 kbit/s and 128 kbit/s.

Location	*What*	*Frame structure*
LAN A	IP packet over Ethernet	
Router A	Extraction of IP packet which is then split into 2 IP fragments	
ISDN B1 channel	Transmission of IP fragment 1 over PPP/MLP	
ISDN B2 channel	Transmission of IP fragment 2 over PPP/MLP	
Router B	Reassembly of IP fragments received	
LAN B	IP packet over Ethernet	

8.2 IP over PPP troubleshooting



Protocol analysis of encapsulated protocols such as IP, TCP, UDP and ICMP provides useful information for troubleshooting by giving a diagnosis of CPE as well as LAN station configuration.

3 cases will be illustrated hereafter:

- Routing table checking
- ISDN usage and broadcast frame detection over ISDN
- IP packets time to live testing: number of remaining hops to check packet life time (an incoming packet on router A must have a number of hops greater than 1, while an outgoing packet must have the necessary number of hops to get to the peer).

DA-5 diagnosis

The DA-5 frame summary monitor provides easy identification of the encapsulated protocols and provides a quick means of locating the frames to be displayed in frame detailed mode for diagnosis.

Frame summary monitor

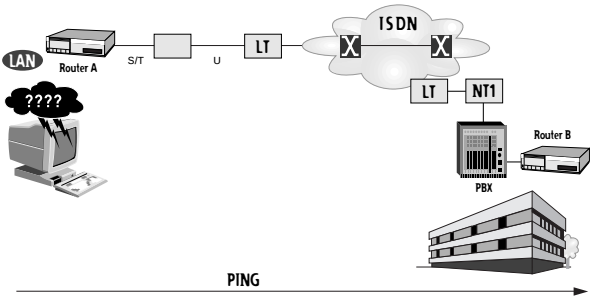
→	B1 MLP SEQ=1	Begin	IP (UDP)	25 G 00:02:08880
→	B2 MLP SEQ=2	End		20 G 00:02:08899
→	B1 MLP SEQ=1	Begin End	IP (TCP)	25 G 00:02:08900
→	B1 MLP SEQ=1	Begin End	IP (ICMP)	25 G 00:02:08980
←	B1 MLP SEQ=1	Begin End	IP (ICMP)	25 G 00:02:08990

Diagnosis: IP packets exchanged with the upper layer application identification.

- IP traffic using UDP ports over PPP/MLP, with IP fragmentation Begin in B1 and End in B2,
- IP traffic using TCP ports over PPP/MLP with no fragmentation (immediate required bandwidth less than 64 kbit/s),
- IP ICMP traffic in B1 channel (Case of ping echo request/echo reply).

Refer to Appendix 2 for the list of TCP/UDP ports decoded by the DA-5, and to Appendix 3 for the list of IP sub-identifiers supported by the DA-5.

8.3 Routing table checking



Monitoring router traffic or test traffic such as Ping, Telnet or FTP will provide diagnosis of routing table implementation. Routing tables associate groups of IP addresses with remote router ISDN and IP addresses.

The following test will show routing table validity:

- Detection of outgoing D-channel SETUP on the ISDN network: if an IP address is completely wrong, the router is not able to identify a remote peer and no SETUP will be sent.
- IP packet source and destination address checking.
- ICMP message sent by router B decoding may indicate any wrong or unknown IP address.

Simultaneous analysis of D+B1+B2 channels is mandatory to obtain all this information.

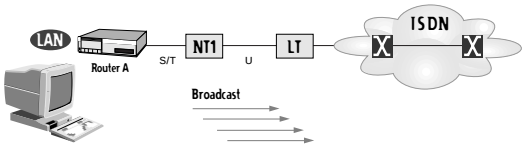
DA-5 diagnosis

B channel ICMP monitor (frame detail):

```
B2: NT->TE  ----  Frame # 00000088  ----  Length=0062      Time=18:21:54272
PPP     :---------- Point-to-Point Protocol ----------
PPP     :No PPP header
PPP     :Protocol code..... Not compressed
PPP     :Protocol..... IP (0021)
PPP     :
IP      :---------- Point-to-Point Protocol ----------
IP      :Header Length..... 20
IP      :Type Of Service..... 0
IP      :Total Length..... 60
IP      :Time To Live..... 32 hops
IP      :Protocol..... 1 (ICMP)
IP      :Checksum..... GOOD
IP      :Source Address..... 141.169.34.151
IP      :Destination Address..... 141.169.34.5
ICMP    :---------- Point-to-Point Protocol ----------
ICMP    :Type..... Network unreachable
ICMP    :Code..... 0
ICMP    :Checksum ..... GOOD (405Ch)
ICMP    :Identifier..... 256
ICMP    :Sequence Number..... 3072
```

Diagnosis: The ping was unsuccessful as shown by ICMP "Network unreachable" message. The IP address used for the ping is wrong.

8.4 ISDN usage and broadcast frames detection over ISDN



To prevent high telecommunications costs, there are two critical points:

- Identification of the LAN application over ISDN
- LAN broadcast frame detection over ISDN

Traffic linked with some LAN applications or routing protocols must not be sent over ISDN and concerns only local hosts (these applications usually generate broadcast frames). The router has to filter these frames in order to avoid non-useful traffic and unexpected telecommunications costs. The following applications or protocols are usually filtered by ISDN routers:

- RIP
- Netbios over IP

LAN broadcast frames have to be filtered by the router and not sent through the ISDN network. This is a critical point in terms of telecommunications costs: the ISDN B channel would never be available if the router did not filter broadcast frames. Broadcast frames usually have the following format:

IP address class	Broadcast address format
Class A	10.255.255.255
Class B	128.9.255.255
Class C	192.9.200.255

Warning: With some specific IP address masks, broadcast addresses may have different formats.

DA-5 diagnosis

The example hereafter shows application identification and broadcast detection.

IP Packet detailed analysis

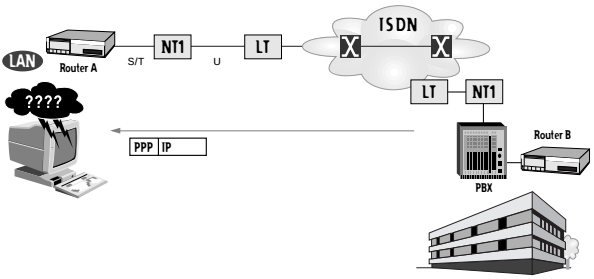
```
B1: NT<-TE  ----  Frame # 00000061  ----  Length=0037     Time=00:02:08880
PPP         :----------- Point-to-Point Protocol -----------
PPP         :PPP header..................... FF 03
PPP         :Protocol code.............. Not compressed
PPP         :Protocol....................... MLP (003D)
PPP         :Unfrag. Frame
PPP         :Seq. Number................ 0
PPP         :Protocol code.............. Not compressed
PPP         :Protocol....................... IP (0021)
IP          :----------------- IP Protocol -----------------
IP          :Header Length..... 20
IP          :Type Of Service..... 0
IP          :Total Length..... 96
IP          :Time To Live..... 32 hops
IP          :Protocol....................... 17 (UDP)
IP          :Checksum..... GOOD
IP          :Source Address..... 141.169.34.152
IP          :Destination Address... 141.169.255.255
UDP         :---------------- UDP Protocol ----------------
UDP         :Source Port..... 137 (NETBIOS Name Service)
UDP         :Destination Port.....137 (NETBIOS Name Service)
```

Diagnosis:

- DA-5 detailed analysis gives the user all the information required to identify the upper layer application thanks to UDP or TCP port decoding. This decoding capability, combined with the Find function and DA-5 long-term measurement capacity (real-time storage of data on PC hard disk) enables easy identification of any malfunction in application filtering.

- Decoding of the IP source and destination address combined with Find function (search for ".255") enables identification of broadcast frames.

8.5 IP packets time to live testing



IP packets have a predefined “time to live”, also called “number of hops”, which defines the number of networks the packet is allowed to go through before being suppressed: each time the IP packet goes through a router, the IP packet time to live is decremented.
If the number of hops defined is too small, the IP packet may never reach the destination host.

For example, an incoming IP packet on ISDN router A must have a number of hops greater than 1 to be able to go through router A and be transmitted to the LAN.

The time to live issue may be critical for Internet applications because IP packets will go through several routers.

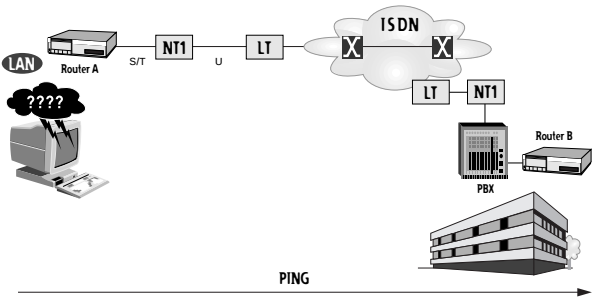
DA-5 diagnosis

IP Packet detailed analysis

```
B1: NT->TE  ----  Frame # 00000061  ----  Length=0037   Time=00:02:08880
PPP     :------------ Point-to-Point Protocol ------------
PPP     :PPP header..... FF 03
PPP     :Protocol code..... Not Compressed
PPP     :Protocol..... MLP (003D)
PPP     :Unfrag. Frame
PPP     :Seq. Number..... 0
PPP     :Protocol code..... Not Compressed
PPP     :Protocol..... IP (0021)
IP      :-------------------- IP Protocol --------------------
IP      :Header Length..... 20
IP      :Type Of Service..... 0
IP      :Total Length..... 96
IP      :Time To Live..... 1 hop
IP      :Protocol..... 17 (UDP)
IP      :Checksum..... GOOD
IP      :Source Address..... 141.169.34.152
IP      :Destination Address.... 141.169.15.452
```

Diagnosis: For this incoming IP packet, the number of hops is 1, this packet will not be transmitted to the LAN.

8.6 IP ping success



To summarize all the steps seen above for data connection establishment, the example hereafter shows the D- and B-channel activity required to complete an IP ping.

- D-channel activity for physical B-channel connection,
- PPP negotiation over ISDN B channel,
- IP ping over ISDN B channel.

DA-5 diagnosis

Complete monitoring of the IP ping starting from D-channel signaling to ICMP message exchange.

Frame summary

		TE: Info 0 - NT: Info 2 / PS1 On						18:21:39629
		TE: Info 3 - NT: Info 2 / PS1 On						18:21:39630
		TE: Info 3 - NT: Info 4 / PS1 On						18:21:39631
	D0	64 c SABME p						3 G 12:59:49050
→	D0	64 r UA f						3 G 12:59:49059
←	D	0	66 c I	16 25 08 01 -		SETUP		23 G 12:59:49061
		Channel: Any	Called: 41055					
→	D	0	66 r RR	- 17				4 G 12:59:49075
→	D	0	66 c I	25 17 08 01	f	SETUP ACK		11 G 12:59:49107
		Channel: B1						
←	D	0	66 r RR	- 26				4 G 12:59:49114
→	D	0	66 c I	26 17 08 01	f	CALL PROC		8 G 12:59:49698
←	D	0	66 r RR	- 27				4 G 12:59:49705
→	D	0	66 c I	27 17 08 01	f	ALERTING		8 G 12:59:53060
←	D	0	66 r RR	- 28				4 G 12:59:53067
→	D	0	66 c I	28 17 08 01	f	CONNECT		8 G 12:59:53844
←	D	0	66 r RR	- 29				4 G 12:59:53851
←	D	0	66 c I	17 29 08 01 -		CONNECT ACK.		8 G 12:59:53873
←	D	0	66 r RR	- 30				4 G 12:59:53881
→	D	0	66 r RR	- 18				4 G 12:59:53886
←	B1	PPP	ID = 1	Config-Req		LCP		38 G 12:59:54761
→	B1	PPP	ID = 1	Config-Req		LCP		34 G 12:59:57778
←	B1	PPP	ID = 1	Config-Ack		LCP		34 G 12:59:57813
→	B1	PPP	ID = 3	Config-Ack		LCP		31 G 12:59:57853
←	B1	PPP	ID = 1	Authent-Req		PAP		34 G 12:59:57882
→	B1	PPP	ID = 1	Authent-Ack		PAP		9 G 12:59:59478
←	B1	PPP	ID = 1	Config-Req		IPCP		44 G 12:59:59512
→	B1	PPP	ID = 1	Config-Req		IPCP		44 G 12:59:59515
←	B1	PPP	ID = 1	Config-Ack		IPCP		14 G 12:59:59520
→	B1	PPP	ID = 1	Config-Ack		IPCP		14 G 12:59:59525
←	B1	PPP				IP (ICMP)		62 G 12:59:59530
→	**B1**	**PPP**				**IP (ICMP)**		**62 G 12:59:59585**

Diagnosis: All steps are passed. Frame detail of ICMP sent by router B (last frame) will show that the ping is successful.

ICMP Frame detail

```
B1: NT->TE ---- Frame # 00000083 ---- Length=0062   Time=12:59:59585
PPP        :---------- Point-to-Point Protocol ----------
PPP        :No PPP header
PPP        :Protocol code ..............Not compressed
PPP        :Protocol ..................IP (0021)
PPP        :
IP         :-------------------- IP Protocol -------------------
IP         :Header Length..............20
IP         :Type Of Service ............0
IP         :Total Length ..............60
IP         :Time To Live ..............254 hops
IP         :Protocol ..................1 (ICMP)
IP         :Checksum ..................GOOD
IP         :Source Address ............141.169.34.5
IP         :Destination Address........141.169.34.151
ICMP       :------------------ ICMP Protocol ------------------
ICMP       :Type ......................Echo Reply (0)
ICMP       :Type ......................Echo Reply (0)
ICMP       :Code ......................0
ICMP       :Checksum ..................GOOD (4A5Ch)
ICMP       :Identifier ................256
ICMP       :Sequence Number ..........2560
           ----------------- Undecoded data -----------------
0          61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70   abcdefghijklmnop
16         71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69   qrstuvwabcdefghi
```

Diagnosis: Ping successful (echo reply). Comparison with ICMP echo request sent by router A will show the integrity of the data looped.

Conclusion

The examples presented in this booklet show the type of tools requested for Internet or LAN-to-LAN applications when troubleshooting on ISDN:

- D- and B-channel troubleshooting,
- Detailed decoding of D-channel signaling and B-channel protocols,
- Long-term measurement capacity.

90% of the difficulties will be solved at a similar level to the case studies detailed in the present document, i.e. troubleshooting CPE configuration or data service availability:

- D-channel troubleshooting,
- PPP negotiation troubleshooting,
- Transport layer troubleshooting (IP/IPX).

Therefore, these applications require 2 categories of protocol analyzers:

First-level protocol analyzers for ISDN BRA and V interfaces:

➜ CPE configuration troubleshooting
➜ WAN service troubleshooting

Expert troubleshooting solution for ISDN (BRA and PRA) and V interfaces:

➜ LAN application over WAN troubleshooting
➜ Network management and optimization
➜ Expert support

As a global provider in internetworking test solutions, WWG offers an homogeneous product line:

WWG DA-5 Multiport Protocol Analyzer

WWG IUM-10 U-Interface Monitor

WWG DominoWAN ISDN Internetwork Analyzer

Learn more about these products

http://www.wwgsolutions.com/products/da5/da5.html
http://www.wwgsolutions.com/products/domino/domino.html
http://www.wwgsolutions.com/products/ium10/ium10.html

Learn more about analyzing ISDN

Application Note 58: Maintenance of the CPE Primary Rate Interface
Application Note 63: Monitoring and Analysis at the U Interface
Application Note 69: AO/DI Turn-up and Maintenance

Appendix 1

Authentication and Control Protocols decoded by the DA-5

PROTOCOL NAMES	PROTOCOL LABEL	HEX VALUE	CONTROL PROTOCOL LABEL	HEX VALUE
802HP	802HP	0201		
AppleTalk	AT	0029	ATCP	8029
AppleTalk EDDP	AEDDB	0039		
AppleTalk SmartBufferred	ATSB	003B		
Ascend's MultiLink Protocol Plus (MP+)	MP+	0073		
Ascom Timeplex	ASC	0043	ASCCP	8043
Bandwidth Allocation	BAP	C02B	BACP	C02D
Banyan Vines	BAN	0035	BANCP	8035
Bridging PDU	BRI	0031	BRICP	8031
CallBack Control Protocol			CALCP	C029
Challenge Handshake Authentication Prot.	CHAP	C223		
Cisco Systems	CIS	0041	CISCP	8041
Compression	CP	00FD	CCP	80FD
Compression on Single Link in Mlk group	CSMLG	00FB	CSMCP	80FB
Container Control Protocol			CONCP	C081
DCA Remote LAN Network	DCA	0047	RLNCP	8047
DECnet Phase IV	DECNT	0027	DECCP	8027
DECST	DECST	0205		
Fujitsu Link Backup and Load Balancing	LBLB	0045	FUJCP	8045
IBMSR	IBMSR	0203		
Internet Protocol	IP	0021	IPCP	8021
Internet Protocol V6	IP	0057	IP6CP	8057
IP6 Header Compression	IP6HC	004F	IP6CP	804F
Link Control Protocol			LCP	C021
Link Quality Report	LQR	C025		
LUX	LUX	0231		
Multi-Link	MLP	003D	MLPCP	803D
NETBIOS Framing	NTB	003F	NTBCP	803F
Novell IPX	IPX	002B	IPXCP	802B
OSI Network Layer	OSI	0023	OSICP	8023
Padding Protocol	PADP	0001		
Password Authentication Protocol		PAP	C023	
PPP encryption	PPPE	0053		
Proprietary Authentication Protocol	PROAP	C281		
Proprietary Node ID Authentication Protocol	PNIAP	C481		
Serial Data Transport Protocol	SDTP	0049	SDCP	8049
Shiva Password Authentication Protocol	SDAP	C027		
Single Link PPP encryption	SLPE	0055		
SNA	SNA	004D	SNACP	804D
SNA over 802.2	SNA2	004B	SN2CP	804B
SNS	SNS	0233		
Stampede Bridging	SBR	006F	SBRCP	806F
Stampede Bridging Authorization Protocol	SBAP	C26F		
Stream Protocol (ST-II)	STR	0033	STRCP	8033
Van Jacobson Compressed TCP/IP	VJC	002D		
Van Jacobson Uncompressed TCP/IP	VJU	002F		
Xerox NS IDP	XEROX	0025	XRXCP	8025

Appendix 2

IP sub-protocol identifiers

The following table gives the list of protocols supported by the DA-5 when carried in IP. This list is a sub-set of the list given in the RFC 1700.

PROTOCOL VALUE	MNENONIC USED	PROTOCOL NAMES
1	ICMP	Internet Control Message
2	IGMP	Internet Group Management
6	TCP	Exterior Gateway Protocol
8	EGP	Transmission Control Protocol
17	UDP	User Datagram
22	XNS-IDP	XEROX NS IDP
29	ISO-TP4	ISO Transport Protocol Class 4
35	IDPR	Inter-Domain Policy Routing Protocol
37	DDP	Datagram Delivery Protocol
45	IDRP	Inter-Domain Routing Protocol
46	RSVP	Reservation Protocol
48	MHRP	Mobile Host Routing Protocol
54	NHRP	NBMA Next Hop Resolution Protocol
80	ISO-IP	ISO Internet Protocol
83	VINES	VINES
88	IGRP	IGRP
89	OSPF	OSPF
97	ETHERIP	Ethernet-within-IP Encapsulation

Appendix 3

Common TCP/UDP ports

The following table gives the list of ports known to the DA-5. Sub-set of the list is given in the RFC 1700.

Ftp-data	20/tcp	File Transfer [Default Data]
ftp-data	20/udp	File Transfer [Default Data]
ftp	21/tcp	File Transfer [Control]
ftp	21/udp	File Transfer [Control]
telnet	23/tcp	Telnet
telnet	23/udp	Telnet
smtp	25/tcp	Simple Mail Transfer
smtp	25/udp	Simple Mail Transfer
nameserver	42/tcp	Host Name Server
nameserver	42/udp	Host Name Server
login	49/tcp	Login Host Protocol
login	49/udp	Login Host Protocol
domain	53/tcp	Domain Name Server
domain	53/udp	Domain Name Server
sql*net	66/tcp	Oracle SQL*NET
sql*net	66/udp	Oracle SQL*NET
bootps	67/tcp	Bootstrap Protocol Server
bootps	67/udp	Bootstrap Protocol Server
bootpc	68/tcp	Bootstrap Protocol Client
bootpc	68/udp	Bootstrap Protocol Client
tftp	69/tcp	Trivial File Transfer
tftp	69/udp	Trivial File Transfer
gopher	70/tcp	Gopher
gopher	70/udp	Gopher
www-http	80/tcp	World Wide Web HTTP
www-http	80/udp	World Wide Web HTTP
sunrpc	111/tcp	SUN Remote Procedure Call
sunrpc	111/udp	SUN Remote Procedure Call
netbios-ns	137/tcp	NETBIOS Name Service
netbios-ns	137/udp	NETBIOS Name Service
netbios-dgm	138/tcp	NETBIOS Datagram Service
netbios-dgm	138/udp	NETBIOS Datagram Service
netbios-ssn	139/tcp	NETBIOS Session Service
netbios-ssn	139/udp	NETBIOS Session Service
news	144/tcp	NewS
news	144/udp	NewS
sql-net	150/tcp	SQL-NET
sql-net	150/udp	SQL-NET
sqlsrv	156/tcp	SQL Service
sqlsrv	156/udp	SQL Service
snmp	161/tcp	SNMP
snmp	161/udp	SNMP
snmptrap	162/tcp	SNMPTRAP
snmptrap	162/udp	SNMPTRAP
cmip-man	163/tcp	CMIP/TCP Manager
cmip-man	163/udp	CMIP/TCP Manager
cmip-agent	164/tcp	CMIP/TCP Agent
cmip-agent	164/udp	CMIP/TCP Agent
xdmcp	177/tcp	X Display Manager Control Protocol
xdmcp	177/udp	X Display Manager Control Protocol
bgp	179/tcp	Border Gateway Protocol
bgp	179/udp	Border Gateway Protocol
ipx	213/tcp	IPX
ipx	213/udp	IPX
netware-ip	396/tcp	Novell Netware over IP
netware-ip	396/udp	Novell Netware over IP
microsoft-ds	445/tcp	Microsoft-DS
microsoft-ds	445/udp	Microsoft-DS
rip	520/tcp	Routing Information Protocol

NOTES

Wavetek Wandel Goltermann
Worldwide

A closely linked network of 29 affiliated companies and more than 65 representatives ensures that our customers receive the best possible advice in solving specific measurement problems.

For all contacts in Western Europe:
Wandel & Goltermann GmbH & Co.
Vertriebsgesellschaft
PO Box 1155
72794 ENINGEN u.A. - GERMANY
Tel: +49 7121 9856 10
Fax: +49 7121 9856 12

For all contacts in Eastern Europe:
Wandel & Goltermann GmbH
Postfach 13
Elisabethstraße 36
A-2500 Baden - AUSTRIA
Tel: +43 2252 85521 0
Fax: +43 2252 80727

For all contacts in North America:
Wandel & Goltermann Inc.
PO Box 13585
1030 Swabia Court
Research Triangle Park
NC 27709-3585 - USA
Tel: +1 919 941 5730
Fax: +1 919 941 5751

For all contacts in Asia/Pacific:
Wandel & Goltermann Pty. Ltd.
PO Box 419
World Trade Centre
Melbourne
Victoria 3005 - AUSTRALIA
Tel: +61 3 9690 6700
Fax: +61 3 9690 6750

For all contacts in Latin America:
Wandel & Goltermann Instrumentaçao Ltda. & Cia.
Av. Eng. L. Carlos Berrini
936-9 Andar
04571-000 São Paulo, SP
BRAZIL
Tel: +55 11 5503 3800
Fax: +55 11 5505 1598

For any further information
or to get the address
of your local Sales Office,
please contact
Wavetek Wandel Goltermann
at the following address:
Wandel & Goltermann GmbH & Co.
Marketing International
PO Box 1262
D - 72795 ENINGEN u.A.
GERMANY
Tel: +49 7121 86 1616
Fax: +49 7121 86 1333

Or have a look at the Web site:
http://www.wwgsolutions.com
email: solutions@wwgsolutions.com

Edited and coordinated by:
Wandel & Goltermann CTS
Marketing Department
Rennes, France

Layout:
Soleil Rouge, Rennes

Order no.
LL/RN/PG02/1299/AE
Edition 3

December 1999