

1. Trace - Erweitertes Troubleshooting

Der Trace Befehl dient dazu, erweitertes Debugging und Troubleshooting durchzuführen. Im folgenden wird beschrieben, wie Sie sich Pakete im LAN anzeigen können, einen ISDN Verbindungsaufbau sowie einen PPPoE Aufbau samt PPP Verbindung anzeigen lassen können.

1.1 Allgemeines

Geben Sie an der Shell den Befehl **trace -?** ein, um die Optionen aufzulisten

```

r232bw:> trace -?
Usage:
WAN: trace [-h23aADfFiptvxXz] [-T <TEI>] [-c <cref>] <channel> <unit> <slot>
LAN: trace [-h23ilpxX] [-d dst mac filter] [-s src mac filter] [-l] 0 0 <slot>
  -h      hexadecimal output
  -2      layer 2 output
  -3      layer 3 output
  -a      asynchronous HDLC (B-Channel only)
  -v      strip V.120 encapsulation in async HDLC (B-Channel only)
  -F      FAX (B-Channel only)
  -A      FAX + AT Commands (B-Channel only)
  -D      delta time
  -p      PPP (WAN: B-Channel only, LAN: PPPoE)
  -f      Frame Relay (B-Channel only)
  -i      IP output
  -t      ascii text output (B-Channel only)
  -X      asynchronous PPP over X.75
  -x      raw dump mode
  -T      set TEI filter (D-Channel only)
  -c      set callref filter (D-Channel only)
  -s      set source MAC addr filter (LAN only)
  -d      set destination MAC addr filter (special: me,bc)
  -I [!]ipsrc:ipdst:proto:srcport:dstport  IPsession filter (LAN)
  -B [!]ip1:ip2:proto:port1:port2  bidirect IPsession filter (LAN)
  -o      filter logical or
  -l      set LLC2 filter (LAN only)
  -P      ATM Virtual Path Identifier (VPI)
  -C      ATM Virtual Channel Identifier (VCI)

<channel>      0      = D-Channel or X.21 Interface
                1..31 = Bx-Channel
<unit>         0..1
<slot>         1..3

Examples: trace -h23i 1 0 2 (ISDN-Interface)
          trace -ip <ifcname> (PPP Interface)
          trace -ip next (next used B-Channel)
          trace -2i -s me -d 0:a0:f9:0:5:1 0 0 1 (LAN AND filter)
          trace -d bc -o -d me 0 0 1 (LAN OR filter, broadcast/own)
          trace -I 1.1.1.10      all packets from
          trace -I :1.1.1.10    all packets to
          trace -B 1.1.1.10:1.1.1.20 all packets between
          trace -I ::6          all TCP packets
          trace -I :::17:::512  all UDP to port 512
          trace -vap <PPP Interface> (HSCSD PPP Trace)

r232bw:>

```

Die Syntax beim Trace Befehl wird in der Reihenfolge: Befehl, Optionen, Channel, Unit, Slot eingegeben. Folgende Erläuterung zu der Syntax:

Feld	Bedeutung
Befehl	Der Befehl lautet Trace .
Optionen	Geben Sie genau an, was Sie sich anzeigen lassen möchten.
Channel	Gibt an auf welchem Kanal Sie die Verbindung tracen möchten. Ethernet Interface haben keinen Kanal. Somit wählen Sie 0. Bei ISDN haben die B Kanäle Ihre feste Nummer.
Unit + Slot	Gibt die Position des physikalischen Interfaces im Gateway an. Die Tabelle biboadmboardtable gibt Ihnen Info über die Bestückung.

1.2 Ethernet Trace

Sie möchten im LAN auf der Ethernet Schnittstelle 1 Ihres R232bw die Ping Pakete von Ihrem Rechner zum Router anzeigen lassen. Geben Sie dazu folgenden Befehl an der Shell des Routers ein:

trace -hi2B 192.168.0.2:192.168.0.1:1 0 0 1&

Folgende Punkte sind hier relevant:

Feld	Bedeutung
h	Zeigt Ihnen die Ausgabe der Pakete im Hexadezimal-Format an.
i	Gibt IP-Pakete im Trace aus.
2	Zeigt Ihnen zusätzlich die MAC-Adressen aus der OSI-Schicht 2 an.
B	Filtert die Anzeige der IP-Pakete zwischen 2 Kommunikationspartnern.
192.168.0.2	Ist z.B. die IP-Adresse vom Rechner.
192.168.0.1	Ist z.B. die IP-Adresse vom Gateway.
:1	Gibt die Protokollnummer der IP-Paketinhalte zum Filtern an. Ping Pakete nutzen ICMP als Protokoll welches die Nummer 1 besitzt. (ICMP=1, TCP=6, UDP=17, ESP=50, AH=51)
0	Dies ist der Kanal der angezeigt werden soll. Beim Ethernet die 0.
0	Das ist die Unit des Ethernet Interfaces.
1	Das ist die Slot des Ethernet Interfaces.
&	Führt den Befehl im Hintergrund aus für weitere Eingaben an der Shell.

Nach dem Ausführen des Befehls und einem Ping von Ihrem Rechner zum Router, sollten sie folgende Ausgabe erhalten:

```
r232bw:> trace -hi2 -B 192.168.0.4:192.168.0.3:1 0 0 1&
r232bw:> 014446.937 R DATA[0078]
 0000: 00 a0 f9 09 6b fe 00 0f b0 68 bf 49 08 00 45 00 ...k...h.I...E.
 0010: 00 3c e3 62 00 00 80 01 d6 06 c0 a8 00 03 c0 a8 .<.b.....
 0020: 00 04 08 00 44 5c ....D\
DST=00:a0:f9:09:6b:fe SRC=00:0f:b0:68:bf:49 protocol 0x0800
IP-Packet from 192.168.0.2 to 192.168.0.1 protocol ICMP
ICMP-Message , type echo request

014446.945 X DATA[0074]
 0000: 00 0f b0 68 bf 49 00 a0 f9 09 6b fe 08 00 45 00 ...h.I...k...E.
 0010: 00 3c 03 12 00 00 3f 01 f7 57 c0 a8 00 04 c0 a8 .<....?..W.....
 0020: 00 03 00 00 4c 5c ....L\
DST=00:0f:b0:68:bf:49 SRC=00:a0:f9:09:6b:fe protocol 0x0800
IP-Packet from 192.168.0.1 to 192.168.0.2 protocol ICMP
ICMP-Message , type echo reply
```

Die erste Zeile eines jeden Pakets enthält jeweils als erstes den Zeitpunkt der Ausgabe gefolgt von der Information ob das Paket empfangen **R** oder gesendet **X** wurde.

1.3 ISDN Trace

Sie möchten einen ISDN Verbindungsaufbau Ihrer LAN Kopplung auf einem R232bw anzeigen lassen. Geben Sie dazu folgenden Befehl an der Shell des Routers ein:

trace -h23 0 0 4&

Folgende Punkte sind hier relevant:

Feld	Bedeutung
h	Zeigt Ihnen die Ausgabe der Pakete im Hexadezimal-Format an.
2	Zeigt den Layer 2 im ISDN D-Kanal an.
3	Zeigt den Layer 3 im ISDN D-Kanal an.
0	Dies ist der Kanal der angezeigt werden soll. Beim D-Kanal die 0.
0	Das ist die Unit des ISDN Interfaces.
4	Das ist der Slot des ISDN Interfaces.
&	Führt den Befehl im Hintergrund aus für weitere Eingaben an der Shell.

Nach dem Ausführen des Befehls und dem Aufbau einer ISDN Verbindung sollten sie Folgendes an der Shell des Routers erhalten:

Bei dem ersten Kontakt über das NTBA zur Vermittlungsstelle, erhalten Sie eine TEI für die Dauer der Kommunikation zugewiesen. Auf der Schicht 2 sieht man entsprechende Meldungen wie **SABME** für die Zuweisung:

```
018490.942 X #00000109 DATA[0008]
0000: fc ff 03 0f 6f c3 01 ff          ....o...
      SAPI=3F C/R=0   TEI=7F UI       P/F=0
      Identity Request      ri=28611 ai=127 (TEI=7f) e=1

018490.942 . #00000110 L1 F7
018490.957 R #00000111 DATA[0008]
0000: fe ff 03 0f 6f c3 02 93          ....o...
      SAPI=3F C/R=1   TEI=7F UI       P/F=0
      Identity Assigned    ri=28611 ai=73 (TEI=49) e=1

018490.957 X #00000112 DATA[0003]
0000: 00 93 7f                          ...
      SAPI=00 C/R=0   TEI=49 SABME P/F=1

018490.965 R #00000113 DATA[0003]
0000: 00 93 73                          ..s
      SAPI=00 C/R=0   TEI=49 UA       P/F=1
```

Auf der Schicht 3 im D-Kanal wird die ISDN Verbindung aufgebaut. So genannte Messages bestimmen die Art der Meldung und beinhalten Informationselemente mit den entsprechenden Verbindungsparametern. Die Message **SETUP** ist die erste Nachricht im D-Kanal, die die Verbindung initialisiert:

```
018490.972 X #00000114 DATA[0027]
0000: 00 93 00 00 08 01 01 05 04 02 88 90 18 01 83 6c .....1
0010: 04 80 31 34 33 70 04 80 31 35 31          ..143p..151
      SAPI=00 C/R=0   TEI=49 I       P/F=0 N(R)=00 N(S)=00
      PD=08 Orig CR=01 SETUP
      IE-Element   : Bearer capability
                    Coding Standard is CCITT
                    Information capability : unrestrict. digital info
                    Transfer Mode is circuit Mode
                    Information transfer rate is 64 kbit/s

      IE-Element   : Channel Identification :
                    Interface implicitly identified
                    Interface type S0
                    Channelnumber is preferred Channel
                    Identified Channel is not D-Channel
                    Selected Channel : Any Channel

      IE-Element   : Calling Party Number is 143
                    Type of Number is 0x0 , (unknown)
                    Numbering plan is 0x0 , (unknown)

      IE-Element   : Called Party Number is 151
                    Type of Number is 0x0 , (unknown)
                    Numbering plan is 0x0 , (unknown)
```

Nach einer SETUP Nachricht folgt optional ein **CALL PROCEEDING**, welches von der Vermittlungsstelle an das Endgerät ausgegeben wird um zu signalisieren, dass der Ruf weitergeleitet wird. Für die Verbindung wird bereits zu diesem Zeitpunkt ein freier B-Kanal reserviert:

```
018491.011 R #00000116 DATA[0011]
0000: 02 93 00 02 08 01 81 02 18 01 89 .....
SAPI=00 C/R=1 TEI=49 I P/F=0 N(R)=01 N(S)=00
PD=08 Dest CR=01 CALL PROCEEDING
IE-Element : Channel Identification :
Interface implicitly identified
Interface type S0
Channelnumber is exclusive (accept only this)
Identified Channel is not D-Channel
Selected Channel : B1-Channel
```

Wenn der Ruf an dem Zielgerät angekommen ist wird ein Klingeln signalisiert, den so genannten **ALERT**:

```
SAPI=00 C/R=1 TEI=49 I P/F=0 N(R)=01 N(S)=01
PD=08 Dest CR=01 ALERT
IE-Element : Channel Identification :
Interface implicitly identified
Interface type S0
Channelnumber is exclusive (accept only this)
Identified Channel is not D-Channel
Selected Channel : B1-Channel
IE-Element : Progress Indicator reports
In-band information now available
```

Nimmt das Zielgerät den Ruf entgegen meldet es einen **CONNECT**. In dieser Nachricht wird auch die Zeit und das Datum übermittelt, damit der Provider abrechnen kann und Sie die Uhr Zeit für Ihre Endgeräte automatisch empfangen lassen können:

```
018491.163 R #00000120 DATA[0024]
0000: 02 93 04 02 08 01 81 07 18 01 89 29 05 01 0c 11 .....))....
0010: 0a 30 4c 04 81 31 35 31 .0L..151
SAPI=00 C/R=1 TEI=49 I P/F=0 N(R)=01 N(S)=02
PD=08 Dest CR=01 CONNECT
IE-Element : Channel Identification :
Interface implicitly identified
Interface type S0
Channelnumber is exclusive (accept only this)
Identified Channel is not D-Channel
Selected Channel : B1-Channel
IE-Element : Date yy-mm-dd hh:mm : 06-08-17 10:48
IE-Element : Unknown IE-Element 0x4c in Codeset 0
```

Ein vollständiger Verbindungsaufbau wird von Ihrem Endgerät mit einem **CONNECT ACKNOWLEDGE** bestätigt. Ab diesem Zeitpunkt steht Ihnen ein B-Kanal für die Kommunikation oder PPP-Aushandlung zur Verfügung:

```
018491.178 X #00000121 DATA[0008]
0000: 00 93 02 06 08 01 01 0f .....
SAPI=00 C/R=0 TEI=49 I P/F=0 N(R)=03 N(S)=01
PD=08 Orig CR=01 CONNECT ACKNOWLEDGE
```

Bei einem Verbindungsabbau wird eine **DISCONNECT** Message gesendet. Diese enthält wie bei einem CONNECT üblicherweise das Datum und die Uhrzeit:

```
018516.713 X #00000127 DATA[0012]
0000: 00 93 04 06 08 01 01 45 08 02 80 90 .....E....
SAPI=00 C/R=0 TEI=49 I P/F=0 N(R)=03 N(S)=02
PD=08 Orig CR=01 DISCONNECT
IE-Element : Cause is 0x90 normal call clearing
```

Das Trennen der Verbindung wird durch eine **RELEASE** Meldung bestätigt. Ab diesem Zeitpunkt wird auf beiden Seiten der B-Kanal wieder freigesetzt:

```
018516.743 R #00000129 DATA[0012]
0000: 02 93 06 06 08 01 81 4d 08 02 81 90 .....M....
SAPI=00 C/R=1 TEI=49 I P/F=0 N(R)=03 N(S)=03
PD=08 Dest CR=01 RELEASE
IE-Element : Cause is 0x90 normal call clearing
```

Die RELEASE Meldung wird nochmals mit einem **RELEASE COMPLETE** bestätigt und somit vollständig abgebaut:

```
018516.759 X #00000130 DATA[0008]
0000: 00 93 06 08 08 01 01 5a .....Z
SAPI=00 C/R=0 TEI=49 I P/F=0 N(R)=04 N(S)=03
PD=08 Orig CR=01 RELEASE COMPLETE
```

1.4 PPPoE Trace

Um Ihre PPPoE (PPP Over Ethernet) Verbindung auf einem R232bw über das Ethernet Interface 5 zu aufzuzeichnen geben Sie Folgendes an der Shell ein:

trace -hp 0 0 1&

Folgende Punkte sind hier relevant:

Feld	Bedeutung
h	Zeigt Ihnen die Ausgabe der Pakete im Hexadezimal-Format an.
P	Gibt PPP und PPPoE Informationen aus.
0	Dies ist der Kanal der angezeigt werden soll. Beim Ethernet die 0.
0	Das ist die Unit des Ethernet Interfaces.
5	Das ist der Slot des Ethernet Interfaces.
&	Führt den Befehl im Hintergrund aus für weitere Eingaben an der Shell.

PPPoE wird als Verbindungsprotokoll in Deutschland bei DSL Zugängen ins Internet eingesetzt. Das Protokoll wurde entwickelt um über eine Ethernet Verbindung zwischen 2 Netzwerkgeräten eine virtuelle Verbindung aufzubauen und abzurechnen. Hier werden insgesamt 4 Nachrichten zwischen PPPoE Client und Server ausgetauscht.

Das erste ist ein **PADI** Paket (PPPoE Active Discovery Initiation.) womit eine Verbindung vom Client Initialisiert wird:

```
000004.890625 X DATA[0032]
0000: ff ff ff ff ff ff 00 a0 f9 02 32 0d 88 63 11 09 .....2..c..
0010: 00 00 00 0c 01 03 00 04 00 57 ff 70 01 01 00 00 .....W.p....
      PPP over Ethernet - discovery stage
      Version 1 Type 1 Session ID 0
      Active Discovery Initiation
      Host-Uniq 00 57 ff 70
      Service-Name <>
```

Das zweite Paket kommt vom PPPoE Server und heißt **PADO** (PPPoE Active Discovery Offer). Dies ist ein Angebot für den Verbindungsaufbau:

```

000004.898437 R DATA[0060]
0000: 00 a0 f9 02 32 0d 00 a0 f9 02 0f 19 88 63 11 07 .....2.....c..
0010: 00 00 00 19 01 02 00 09 58 34 30 30 30 5f 31 35 .....x4000_15
0020: 36 01 03 00 04 00 57 ff 70 01 01 00 00 00 00 00 6.....W.p.....
0030: 00 00 00 00 00 00 00 00 00 00 00 00 .....
      PPP over Ethernet - discovery stage
      Version 1 Type 1 Session ID 0
      Active Discovery Offer
      AC-Name <X4000_156>
      Host-Uniq 00 57 ff 70
      Service-Name <>
  
```

Das dritte Paket kommt vom PPPoE Client und heißt **PADR** (PPPoE Active Discovery Request). Dies ist die Anforderung des zuvor gesendeten Angebots für den Verbindungsaufbau:

```

000004.898437 X DATA[0032]
0000: 00 a0 f9 02 0f 19 00 a0 f9 02 32 0d 88 63 11 19 .....2...c..
0010: 00 00 00 0c 01 03 00 04 00 57 ff 70 01 01 00 00 .....W.p....
      PPP over Ethernet - discovery stage
      Version 1 Type 1 Session ID 0
      Active Discovery Request
      Host-Uniq 00 57 ff 70
      Service-Name <>
  
```

Das letzte und vierte Paket kommt vom PPPoE Server und heißt **PADS** (PPPoE Active Discovery Session-Confirmation). Dies ist die Zuordnung und Bestätigung einer Sitzung zu dem jeweiligen Client für die Verbindung:

```

000004.906250 R DATA[0060]
0000: 00 a0 f9 02 32 0d 00 a0 f9 02 0f 19 88 63 11 65 .....2.....c.e
0010: 00 18 00 19 01 02 00 09 58 34 30 30 30 5f 31 35 .....x4000_15
0020: 36 01 03 00 04 00 57 ff 70 01 01 00 00 00 00 00 6.....W.p.....
0030: 00 00 00 00 00 00 00 00 00 00 00 00 .....
      PPP over Ethernet - discovery stage
      Version 1 Type 1 Session ID 24
      Active Discovery Session-confirmation
      AC-Name <X4000_156>
      Host-Uniq 00 57 ff 70
      Service-Name <>
  
```

Nach dem PPPoE Verbindungsaufbau folgt die PPP Verbindung. In jedem Paket, welches über Ethernet während der Verbindung übertragen wird, befindet sich der 8 Byte große PPPoE Header.

1.5 PPP Trace

PPP (Point to Point Protocol) ist für den Aufbau und den Abbau einer Verbindung über ISDN oder Ethernet mittels PPPoE zuständig. Dazu wird PPP die Verbindung in 3 Phasen aufbauen. Grundsätzlich versuchen beide Parteien Vorschläge dem Partner zu übermitteln oder diese gezielt zu bestätigen bzw. abzulehnen.

In der **Phase 1** erfolgt die Aushandlung der Verbindungsparameter mit dem Protokoll **LCP** (Link Control Protocol) wie z.B. Paketgröße oder des Authentifizierungsprotokolls:

```

000004.914062 X DATA[0036]
0000: 00 a0 f9 02 0f 19 00 a0 f9 02 32 0d 88 64 11 00 .....2..d..
0010: 00 18 00 10 c0 21 01 01 00 0e 01 04 05 d4 05 06 .....!.....
0020: 4b 37 5d aa                                     K7].....
      PPP over Ethernet - session stage
      Version 1 Type 1 Session ID 24
      Compressed PPP packet protocol 0xc021 (LCP)
      ID 1 LCP Configure-Request
      MRU 1492;
      Magic-Number 0x4b375daa;

000004.914062 R DATA[0060]
0000: 00 a0 f9 02 32 0d 00 a0 f9 02 0f 19 88 64 11 00 ....2.....d..
0010: 00 18 00 15 c0 21 01 01 00 13 01 04 05 d4 03 05 .....!.....
0020: c2 23 05 05 06 a7 93 47 7c 00 00 00 00 00 00 00 .#.G|.....
0030: 00 00 00 00 00 00 00 00 00 00 00 00 .....
      PPP over Ethernet - session stage
      Version 1 Type 1 Session ID 24
      Compressed PPP packet protocol 0xc021 (LCP)
      ID 1 LCP Configure-Request
      MRU 1492;
      Authentication Protocol CHAP; Encrypt MD5;
      Magic-Number 0xa793477c;

000004.937500 R DATA[0060]
0000: 00 a0 f9 02 32 0d 00 a0 f9 02 0f 19 88 64 11 00 ....2.....d..
0010: 00 18 00 10 c0 21 02 01 00 0e 01 04 05 d4 05 06 .....!.....
0020: 4b 37 5d aa 00 00 00 00 00 00 00 00 00 00 00 00 K7].....
0030: 00 00 00 00 00 00 00 00 00 00 00 00 .....
      PPP over Ethernet - session stage
      Version 1 Type 1 Session ID 24
      Compressed PPP packet protocol 0xc021 (LCP)
      ID 1 LCP Configure-Ack
      MRU 1492;
      Magic-Number 0x4b375daa;

000004.945312 X DATA[0030]
0000: 00 a0 f9 02 0f 19 00 a0 f9 02 32 0d 88 64 11 00 .....2..d..
0010: 00 18 00 0a c0 21 03 01 00 08 03 04 c0 23 .....!.....#
      PPP over Ethernet - session stage
      Version 1 Type 1 Session ID 24
      Compressed PPP packet protocol 0xc021 (LCP)
      ID 1 LCP Configure-Nak
      Authentication Protocol PAP;
  
```

```

000004.945312 R DATA[0060]
0000: 00 a0 f9 02 32 0d 00 a0 f9 02 0f 19 88 64 11 00 ....2.....d..
0010: 00 18 00 14 c0 21 01 02 00 12 01 04 05 d4 03 04 .....!.....
0020: c0 23 05 06 f4 5d 11 35 00 00 00 00 00 00 00 00 .#...].5.....
0030: 00 00 00 00 00 00 00 00 00 00 00 00 .....
      PPP over Ethernet - session stage
      Version 1 Type 1 Session ID 24
      Compressed PPP packet protocol 0xc021 (LCP)
      ID 2 LCP Configure-Request
      MRU 1492;
      Authentication Protocol PAP;
      Magic-Number 0xf45d1135;

000004.953125 X DATA[0040]
0000: 00 a0 f9 02 0f 19 00 a0 f9 02 32 0d 88 64 11 00 .....2..d..
0010: 00 18 00 14 c0 21 02 02 00 12 01 04 05 d4 03 04 .....!.....
0020: c0 23 05 06 f4 5d 11 35 .#...].5
      PPP over Ethernet - session stage
      Version 1 Type 1 Session ID 24
      Compressed PPP packet protocol 0xc021 (LCP)
      ID 2 LCP Configure-Ack
      MRU 1492;
      Authentication Protocol PAP;
      Magic-Number 0xf45d1135;

```

In der **Phase 2** erfolgt die optionale Authentifizierung die z.B. mit den Protokollen PAP, CHAP oder MS-CHAP durchgeführt wird:

```

000004.960937 X DATA[0077]
0000: 00 a0 f9 02 0f 19 00 a0 f9 02 32 0d 88 64 11 00 .....2..d..
0010: 00 18 00 39 c0 23 01 01 00 37 2a 30 30 30 31 32 ...9.#...7*00012
0020: 33 34 35 36 37 38 39 30 31 32 33 34 30 31 32 33 3456789012340123
0030: 34 35 36 37 23 30 30 30 31 40 74 2d 6f 6e 6c 69 4567#0001@t-onli
0040: 6e 65 2e 64 65 07 31 32 33 34 35 36 37 ne.de.1234567
      PPP over Ethernet - session stage
      Version 1 Type 1 Session ID 24
      Compressed PPP packet protocol 0xc023 (PAP)
      ID 1 PAP Authenticate-Request Peer-ID 0001234567890123401234567#000
      1@t-online.de Password 1234567

000004.960937 R DATA[0060]
0000: 00 a0 f9 02 32 0d 00 a0 f9 02 0f 19 88 64 11 00 ....2.....d..
0010: 00 18 00 07 c0 23 02 01 00 05 00 00 00 00 00 00 .....#.....
0020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0030: 00 00 00 00 00 00 00 00 00 00 00 00 .....
      PPP over Ethernet - session stage
      Version 1 Type 1 Session ID 24
      Compressed PPP packet protocol 0xc023 (PAP)
      ID 1 PAP Authenticate-Ack Message <none>

```

In der **Phase 3** wird das NCP-Protokoll (Network Control Protocol) verwendet um die Netzwerk-Parameter auszuhandeln. Hier erfolgt die IP-Aushandlung der IP-Parameter mit dem Protokoll **IPCP** (Internet Protocol Configuration Protocol) welches z.B. eigene und remote IP-Adressen vergibt, DNS und WINS Server verteilt oder die IP Kompression aushandelt:

```

000004.968750 X DATA[0056]
0000: 00 a0 f9 02 0f 19 00 a0 f9 02 32 0d 88 64 11 00 .....2..d..
0010: 00 18 00 24 80 21 01 01 00 22 03 06 00 00 00 00 ...$.!...".....
0020: 81 06 00 00 00 00 82 06 00 00 00 00 83 06 00 00 .....
0030: 00 00 84 06 00 00 00 00 .....
      PPP over Ethernet - session stage
      Version 1 Type 1 Session ID 24
      Compressed PPP packet protocol 0x8021 (IPCP)
      ID 1 IPCP Configure-Request
      IP-Address 0.0.0.0;
      Primary DNS Server 0.0.0.0;
      Primary NBNS Server 0.0.0.0;
      Secondary DNS Server 0.0.0.0;
      Secondary NBNS Server 0.0.0.0;

000005.974375 R DATA[0060]
0000: 00 a0 f9 02 32 0d 00 a0 f9 02 0f 19 88 64 11 00 ....2.....d..
0010: 00 18 00 18 80 21 02 04 00 16 03 06 d4 01 01 01 .....!.....
0020: 81 06 c0 a8 c8 06 83 06 c0 a8 c8 77 00 00 00 00 .....w....
0030: 00 00 00 00 00 00 00 00 00 00 00 00 .....
      PPP over Ethernet - session stage
      Version 1 Type 1 Session ID 24
      Compressed PPP packet protocol 0x8021 (IPCP)
      ID 4 IPCP Configure-Ack
      IP-Address 212.1.1.1;
      Primary DNS Server 192.168.200.6;
      Secondary DNS Server 192.168.200.119;

000004.984375 X DATA[0056]
0000: 00 a0 f9 02 0f 19 00 a0 f9 02 32 0d 88 64 11 00 .....2..d..
0010: 00 18 00 24 80 21 01 02 00 22 03 06 d4 01 01 01 ...$.!...".....
0020: 81 06 c0 a8 c8 06 82 06 00 00 00 00 83 06 00 00 .....
0030: 00 00 84 06 00 00 00 00 .....
      PPP over Ethernet - session stage
      Version 1 Type 1 Session ID 24
      Compressed PPP packet protocol 0x8021 (IPCP)
      ID 2 IPCP Configure-Request
      IP-Address 212.1.1.1;
      Primary DNS Server 192.168.200.6;
      Secondary DNS Server 192.168.200.119;
      Primary NBNS Server 0.0.0.0;
      Secondary NBNS Server 0.0.0.0;

000004.992187 R DATA[0060]
0000: 00 a0 f9 02 32 0d 00 a0 f9 02 0f 19 88 64 11 00 ....2.....d..
0010: 00 18 00 12 80 21 04 02 00 10 82 06 00 00 00 00 .....!.....
0020: 84 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0030: 00 00 00 00 00 00 00 00 00 00 00 00 .....
      PPP over Ethernet - session stage
      Version 1 Type 1 Session ID 24
      Compressed PPP packet protocol 0x8021 (IPCP)
      ID 2 IPCP Configure-Reject
      Primary NBNS Server 0.0.0.0;
      Secondary NBNS Server 0.0.0.0;
  
```

Wenn die Verbindung aufgebaut wurde, können Sie einen Ping über die PPP Verbindung senden. Die Pakete samt aller Header Informationen werden Ihnen im Trace angezeigt:

```

000004.022437 X DATA[0105]
0000: 00 a0 f9 02 0f 19 00 a0 f9 02 32 0d 88 64 11 00 .....2...d..
0010: 00 18 00 56 00 21 45 00 00 54 0e ed 00 00 3e 01 ...V.!E..T....>.
0020: 57 c7 d4 01 01 01 3e 92 02 61 08 00 61 a4 80 06 W.....>..a..a...
0030: 00 00 3e 19 47 79 00 09 e4 f5 10 11 12 13 14 15 ..>.Gy.....
0040: 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 ..... !"#$$%
0050: 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 &'()*+,-./012345
0060: 36 37 38 39 3a 3b 3c 3d 3e 3f 6789:;<=>?
      PPP over Ethernet - session stage
      Version 1 Type 1 Session ID 24
      Compressed PPP packet protocol 0x21 (TCP/IP)
      IP-Packet from 212.1.1.1 to 62.146.2.97 protocol 0x1
      ICMP-Message , type echo request

000005.023437 R DATA[0106]
0000: 00 a0 f9 02 32 0d 00 a0 f9 02 0f 19 88 64 11 00 ....2.....d..
0010: 00 18 00 56 00 21 45 00 00 54 4f a1 40 00 ed 01 ...V.!E..TO.@...
0020: 28 12 3e 92 02 61 d4 01 01 01 00 00 69 a4 80 06 (.>..a.....i...
0030: 00 00 3e 19 47 79 00 09 e4 f5 10 11 12 13 14 15 ..>.Gy.....
0040: 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 ..... !"#$$%
0050: 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 &'()*+,-./012345
0060: 36 37 38 39 3a 3b 3c 3d 3e 3f 6789:;<=>?
      PPP over Ethernet - session stage
      Version 1 Type 1 Session ID 24
      Compressed PPP packet protocol 0x21 (TCP/IP)
      IP-Packet from 62.146.2.97 to 212.1.1.1 protocol 0x1
      ICMP-Message , type echo reply
  
```