# Konfiguration der Prestige 3xx Serie fuer Internet-Verbindungen (ISP-Routing)

Um den **Teledat DSL Komfort**, **Prestige 310/314**, **312** oder **316** mittels der **Telnet-Console** zu programmieren, gehen Sie bitte wie folgt vor: Starten Sie das Programm „*Telnet*“ und stellen eine Verbindung zur **IP-Adresse** Ihres Routers her.

Anhand folgender Bildschiminhalte soll ein Beispiel gegeben werden, wo sich welche Einstellungen befinden um diverse Filter, Sicherheits und ISP-Einstellungen vorzunehmen.

**Liste der behandelten Protokolle:**

```
1     ICMP        Internet Control Message           [RFC792]
http://www.iana.org/assignments/icmp-parameters

6     TCP         Transmission Control               [RFC793]
17    UDP         User Datagram                    [RFC768,JBP]
http://www.iana.org/assignments/tcp-parameters
```

**Liste des/der behandelten Ports:**

```
Domain            53/tcp    Domain Name Server
Domain            53/udp    Domain Name Server
#                           Paul Mockapetris PVM@ISI.EDU

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
#                           Jon Postel postel@isi.edu

snmp             161/tcp    SNMP
snmp             161/udp    SNMP
snmptrap         162/tcp    SNMPTRAP
snmptrap         162/udp    SNMPTRAP
#                           Marshall Rose mrose@dbc.mtview.ca.us

router           520/udp    local routing process (on site);
#                           uses variant of Xerox NS routing
#                           information protocol – RIP
```

Zunaechst sehen Sie nach dem **Login**, durch Eingabe Ihres Passwortes: **1234** – das Hauptmenu des Routers.

**Haupt-Menu:**

```
              Copyright (c) 1994 - 2002 ZyXEL Communications Corp.

                              Prestige 3xx Main Menu
                        (Teledat DSL Router Komfort Main Menu)

     Getting Started                       Advanced Management
       1. General Setup                      21. Filter Set Configuration
       2. WAN Setup                          22. SNMP Configuration
       3. LAN Setup                          23. System Password
       4. Internet Access Setup              24. System Maintenance
                                             26. Schedule Setup


     Advanced Applications
       11. Remote Node Setup
       12. Static Routing Setup
       15. NAT Setup

                                             99. Exit


                               Enter Menu Selection Number:
```

Im **Menu-3** finden Sie zum einen die **TCP/IP** und **DHCP** Einstellungsmoeglichkeit Ihres Routers, welche sich rein auf das **LAN** (*Lokal-Area-Network*) bezieht. Hier kann man z.B. die IP-Adresse des Router entsprechend Ihrem **Subnetz** anpassen, sowie den **DHCP-Pool** aendern um den einzelnen **Clients** in Ihrem Subnetz (also den einzelnen Rechnern) automatisch alle Informationen wie **IP-Adresse**, **Gateway** und **DNS** (*Domain-Name-Server zur Namensaufloesung von Internetnamen* wie etwa www.zyxel.de) zu zuweisen.

Im **LAN Port Filter Setup** besteht die Moeglichkeit zur Eingabe von Programmierten **Filter-SET**s, welche im **Menu-21** zu programmieren und korrekt einzustellen sind.

**Menu-3:**

```
                        Menu 3 - LAN Setup

                  1. LAN Port Filter Setup
                  2. TCP/IP and DHCP Setup









                        Enter Menu Selection Number:
```

Hier im **Menu-3.1** findet sich ein als default vorgegebener Eintrag. Dieser Eintrag ist als **Input Filter Set** angegeben und wird somit aus Sicht vom **LAN** (also von den lokalen Rechnern kommend) zum Router und darueber hinaus in das **WAN** (*Wide-Area-Network*) betrachtet. Ein in diesem Menu angegebener Output Filter Set behandelt daher Daten kommend vom Router zum **LAN**.

**Menu-3.1:**

```
                     Menu 3.1 - LAN Port Filter Setup

                Input Filter Sets:
                  Protocol filters= 2
                    device filters=
                Output Filter Sets:
                  Protocol filters=
                    device filters=









                Press ENTER to Confirm or ESC to Cancel:
```

**Menu-21:**

```
                    Menu 21 - Filter Set Configuration

    Filter                                  Filter
    Set #        Comments                   Set #        Comments
    ------  -----------------               ------  -----------------
      1      NetBIOS_WAN                      7      _________________
      2      NetBIOS_LAN                      8      _________________
      3      _________________                9      _________________
      4      ARP-Broadcast                   10      _________________
      5      SNMPTRAP_RIP                    11      _________________
      6      _________________               12      _________________


                    Enter Filter Set Number to Configure= 0

                    Edit Comments= N/A

                    Press ENTER to Confirm or ESC to Cancel:
```

Der Filter im **Menu-21.2** bewirkt bzw. **verhindert** aus Sicht **vom LAN kommend** alle **Anfragen** von Rechner ueber das **Protokoll-17 (UDP) durch Port-137 (NETBIOS Name Service) an Port-53 (DNS)**, welche ggf. nicht vom Router behandelt werden koennen und somit eine Daten- bzw. Onlineverbindung des Routers zur Folge haetten. Da dies im Regelfall ueberhaupt nicht erwuenscht wird, gehoeren derartige Anfragen gefiltert.

**Menu-21.2:**

```
                        Menu 21.2 - Filter Rules Summary

# A Type                        Filter Rules                              M m n
- - ---- ------------------------------------------------------------ - - -
1 Y IP   Pr=17, SA=0.0.0.0, SP=137, DA=0.0.0.0, DP=53                  N D F
2 N
3 N
4 N
5 N
6 N




                  Enter Filter Rule Number (1-6) to Configure:
```

**Menu-21.2.1 (Protokoll-17: UDP / Port-137: NETBIOS Name Service zu Port-53: DNS):**

```
                          Menu 21.2.1 - TCP/IP Filter Rule

                    Filter #: 2,1
                    Filter Type= TCP/IP Filter Rule
                    Active= Yes
                    IP Protocol= 17    IP Source Route= No
                    Destination: IP Addr= 0.0.0.0
                                 IP Mask= 0.0.0.0
                                 Port #= 53
                                 Port # Comp= Equal
                         Source: IP Addr= 0.0.0.0
                                 IP Mask= 0.0.0.0
                                 Port #= 137
                                 Port # Comp= Equal
                    TCP Estab= N/A
                    More= No           Log= None
                    Action Matched= Drop
                    Action Not Matched= Forward

                    Press ENTER to Confirm or ESC to Cancel:
```

Im **Menu-11** finden Sie die **Erweiterten Einstellungsmoeglichkeiten**, wie etwa fuer Oesterreich die Angabe des fuer **PPtP**-Verbindungen benoetigte **VPN-Tunnel IP-Adressen**. Bei **PPPoE** Verbindungen wie etwa in Deutschland, der Schweiz und Teilen Frankreichs sind diese Einstellung der Tunnelung nicht notwendig und deshalb auch ausgeblendet, wenn die Encapsulation PPPoE ausgewaehlt wurde.

Begeben Sie sich **mittels CURSOR oder ENTER-Taste** zum Eintrag **Edit Filter Sets** und stellen diesen mittels der **LEER-Taste** (auch **SPACE-Taste** genannt) auf **Yes**. Eine **erneute betaetigung** der **Enter** oder Cursor-Taste bringt Sie dann in das **Untermenu 11.5**.

**Menu-11:**

```
                    Menu 11.1 - Remote Node Profile

Rem Node Name= xDSL                    Route= IP
Active= No

Encapsulation= PPPoE (PPTP)            Edit IP= No
Service Type= Standard                 Telco Option:
Service Name= N/A                        Allocated Budget(min)= 0
Outgoing:                                Period(hr)= 0
  My Login= 1111111111122222222222#+   Schedules=
  My Password= ********                  Nailed-Up Connection= No
  Authen= CHAP/PAP
                                       Session Options:
PPTP:                                    Edit Filter Sets= No
  My IP Addr= 10.0.0.140                 Idle Timeout(sec)= 300
  Server IP Addr= 10.0.0.138
  Connection ID/Name=                  Edit Traffic Redirect= No

                Press ENTER to Confirm or ESC to Cancel:
```

Hier im **Menu-11.5** finden sich mehrere als default vorgegebene Eintraege. Diese Eintrage werden als **Input Filter Set**, **Output Filter Set** bzw. **Call Filter Set** angegeben und sind somit aus Sicht vom Router zum **WAN** (also in das Internet abgehend) zu betrachten. Ein in diesem Menu angegebener **Call** oder **Output Filter Set** behandelt daher Daten vom Router abgehend zum **WAN** bzw. als **Input Filter Set** hereinkommend vom **WAN**.

Sollen nun Datenpakete, welche vom LAN kommend nicht gefiltert wurden und somit in das WAN (Internet) zu transportieren sind, gefiltert werden – sind diese hier als Filter-Set entsprechend dem Menu-21 anzugeben.

Eintragungen im Feld **Call Filter Set verhindern** das **Onlineverbindungen** hergestellt werden.
Besteht jedoch schon eine Verbindung zum Internet/WAN, beinhaltet der **Call Filter Set** keine Funktion.
Eintragungen im Feld **Output Filter Set verhindern den Transport** zu filternder Datenpakete **zum Internet**.
Eintragungen im Feld **Input Filter Set verhindern Datenanfragen** kommend von aussen, also in den Router und somit ggf. **in das LAN**.

**Menu-11.5:**

```
                    Menu 11.5 - Remote Node Filter

                Input Filter Sets:
                  protocol filters= 5, 1
                    device filters= 4
                Output Filter Sets:
                  protocol filters= 1
                    device filters=
                Call Filter Sets:
                  protocol filters= 1
                    device filters=




                 Enter here to CONFIRM or ESC to CANCEL:
```

Die hier nachfolgend angegebenen Filter bewirken, das **Anfragen aus dem Internet kommend** ueber das **Protokoll 17 (UDP)** durch die **Ports 162 (SNMP-Trap) sowie 520 (LRP) auf keinen Fall zum Router und somit auch nicht in das LAN** gelangen. Der **Filter-5** beinhaltet u.a. auch das **Protokoll-1 (ICMP)** und **verhindert dadurch Anfragen durch den Port-8 (Echo-Request/PING)**, was dazu fuehrt das man den Router WAN-Seitig nicht mehr anpingen kann *(z. B. bei der Einstellung SUA/None notwendig)*. Dieser **ICMP/PING-Filter** ist hier **absichtlich aktiviert**, obwohl in den aktuellen Firmware-Versionen der Prestige 300er Serie dies **mittels Internet-Browser im Advanced/SUA-NAT Menu einstellbar** – nicht aber nicht im Teledat. Die bildliche Darstellung zum Advanced/SUA Browser-Menu finden Sie am Ende dieses Dokumentes!

**Menu-21:**

```
                  Menu 21 - Filter Set Configuration

    Filter                                Filter
    Set #        Comments                 Set #        Comments
    ------  -----------------             ------  -----------------
      1      NetBIOS_WAN                     7      _________________
      2      NetBIOS_LAN                     8      _________________
      3      _________________               9      _________________
      4      ARP-Broadcast                  10      _________________
      5      SNMPTRAP_RIP                   11      _________________
      6      _________________              12      _________________


                   Enter Filter Set Number to Configure= 0

                   Edit Comments= N/A

                   Press ENTER to Confirm or ESC to Cancel:
```

**Menu-21.5:**

```
                       Menu 21.5 - Filter Rules Summary

# A Type                        Filter Rules                              M m n
- - ---- ------------------------------------------------------------- - - -
1 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=162                         N D N
2 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=520                         N D N
3 Y IP   Pr=1, SA=0.0.0.0, DA=0.0.0.0, DP=8                            N F N
4 N
5 N
6 N









                  Enter Filter Rule Number (1-6) to Configure:
```

**Menu-21.5.2 (Protokoll-17: UDP / Port-162: SNMP-Trap):**

```
                       Menu 21.5.2 - TCP/IP Filter Rule

                   Filter #: 5,2
                   Filter Type= TCP/IP Filter Rule
                   Active= Yes
                   IP Protocol= 17    IP Source Route= No
                   Destination: IP Addr= 0.0.0.0
                                IP Mask= 0.0.0.0
                                Port #= 162
                                Port # Comp= Equal
                        Source: IP Addr= 0.0.0.0
                                IP Mask= 0.0.0.0
                                Port #=
                                Port # Comp= None
                   TCP Estab= N/A
                   More= No           Log= None
                   Action Matched= Drop
                   Action Not Matched= Check Next Rule

                   Press ENTER to Confirm or ESC to Cancel:
```

**Menu-21.5.3 (Protokoll-17: UDP / Port-520: LRP):**

```
Menu 21.5.3 - TCP/IP Filter Rule

                    Filter #: 5,3
                    Filter Type= TCP/IP Filter Rule
                    Active= Yes
                    IP Protocol= 17    IP Source Route= No
                    Destination: IP Addr= 0.0.0.0
                                 IP Mask= 0.0.0.0
                                 Port #= 520
                                 Port # Comp= Equal
                         Source: IP Addr= 0.0.0.0
                                 IP Mask= 0.0.0.0
                                 Port #=
                                 Port # Comp= None
                    TCP Estab= N/A
                    More= No           Log= None
                    Action Matched= Drop
                    Action Not Matched= Check Next Rule

                    Press ENTER to Confirm or ESC to Cancel:
```

**Menu-21.5.5 (Protokoll-1: ICMP / Port-8: PING):**

```
Menu 21.5.5 - TCP/IP Filter Rule

                    Filter #: 5,5
                    Filter Type= TCP/IP Filter Rule
                    Active= No
                    IP Protocol= 1     IP Source Route= No
                    Destination: IP Addr= 0.0.0.0
                                 IP Mask= 0.0.0.0
                                 Port #= 8
                                 Port # Comp= Equal
                         Source: IP Addr= 0.0.0.0
                                 IP Mask= 0.0.0.0
                                 Port #=
                                 Port # Comp= None
                    TCP Estab= N/A
                    More= No           Log= Action Matched
                    Action Matched= Forward
                    Action Not Matched= Check Next Rule

                    Press ENTER to Confirm or ESC to Cancel:
```

Fuer **Oesterreich** gibt es eine leidige Sonderheit, naemlich den sogenannten **ARP-Filter** **(ARP = Adress-Resolution-Protokoll / MAC-Adress Aufloesung zur IP-Adresse)**, der **bei Nichtanwendung** dazu fuehrt das **keine brauchbaren Datenuebertragungen** stattfinden. Kommt es zu dem erwaehnten Problem, sollte dieser **Filter-Set-4** im **Menu-21.4** als **Input Device Filter** im **Menu-11.5** Anwendung finden und als default vorgegeben werden.

**Menu-21:**

```
Menu 21 - Filter Set Configuration

     Filter                              Filter
     Set #        Comments               Set #        Comments
     ------  -----------------           ------  -----------------
       1      NetBIOS_WAN                  7      ________________
       2      NetBIOS_LAN                  8      ________________
       3      ________________             9      ________________
       4      ARP-Broadcast               10      ________________
       5      SNMPTRAP_RIP                11      ________________
       6      ________________            12      ________________


                    Enter Filter Set Number to Configure= 0

                    Edit Comments= N/A

                    Press ENTER to Confirm or ESC to Cancel:
```

**Menu-21.4:**

```
Menu 21.4 - Filter Rules Summary

 # A Type                      Filter Rules                              M m n
 - - ---- ------------------------------------------------------------ - - -
 1 Y Gen  Off=12, Len=2, Mask=ffff, Value=0806                         Y N N
 2 Y Gen  Off=0, Len=6, Mask=ffffffffffff, Value=ffffffffffff          N D F
 3 N
 4 N
 5 N
 6 N









                  Enter Filter Rule Number (1-6) to Configure:
```

**Menu-21.4.1 (*ARP-Broadcast*):**

```
Menu 21.4.1 - Generic Filter Rule

                    Filter #: 4,1
                    Filter Type= Generic Filter Rule
                    Active= Yes
                    Offset= 12
                    Length= 2
                    Mask= ffff
                    Value= 0806
                    More= Yes          Log= None
                    Action Matched= N/A
                    Action Not Matched= N/A









                    Press ENTER to Confirm or ESC to Cancel:
```

**Menu-21.4.2 (*ARP-Broadcast*):**

```
Menu 21.4.2 - Generic Filter Rule

                    Filter #: 4,2
                    Filter Type= Generic Filter Rule
                    Active= Yes
                    Offset= 0
                    Length= 6
                    Mask= ffffffffffff
                    Value= ffffffffffff
                    More= No            Log= None
                    Action Matched= Drop
                    Action Not Matched= Forward




                    Press ENTER to Confirm or ESC to Cancel:
```

Der **Filter-Set-1** im **Menu-21.1** filtert die **Ports 137** bis **139** in Verbindung der Protokolle **6 (TCP)** und **17 (UDP)**, weil NetBIOS-Aufrufe z.b. unter Windows eine sehr stoerende Eigenschaft haben, sollten diese moeglichst LAN-Seitig bleiben um keine unnoetigen Onlineverbindungen herzustellen (**Call Filter Set**) oder falls eine Verbindung in das Internet besteht (**Output Filter Set**), diese nicht unnoetig aufrecht zu halten.

Da auch eingehende NetBIOS-Aufrufe seitens dem WAN eine Online-Verbindung aufrecht halten kann, findet der **Filter-Set-1** im **Menu-11.5** auch als **Input Filter Set** seine Anwendung.

**Menu-21:**

```
Menu 21 - Filter Set Configuration

     Filter                              Filter
     Set #        Comments               Set #        Comments
     ------  -----------------           ------  -----------------
       1      NetBIOS_WAN                  7      _________________
       2      NetBIOS_LAN                  8      _________________
       3      _________________            9      _________________
       4      ARP-Broadcast               10      _________________
       5      SNMPTRAP_RIP                11      _________________
       6      _________________           12      _________________


                    Enter Filter Set Number to Configure= 0

                    Edit Comments= N/A

                    Press ENTER to Confirm or ESC to Cancel:
```

**Menu-21.1**

```
Menu 21.1 - Filter Rules Summary

 # A Type                        Filter Rules                              M m n
 - - ---- ------------------------------------------------------------- - - -
 1 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=137                          N D N
 2 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=138                          N D N
 3 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=139                          N D N
 4 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=137                         N D N
 5 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=138                         N D N
 6 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=139                         N D F




                  Enter Filter Rule Number (1-6) to Configure:
```

**Menu-21.1.1 (Protokoll-6: TCP / Port-137: NETBIOS Name Service):**

```
Menu 21.1.1 - TCP/IP Filter Rule

                    Filter #: 1,1
                    Filter Type= TCP/IP Filter Rule
                    Active= Yes
                    IP Protocol= 6     IP Source Route= No
                    Destination: IP Addr= 0.0.0.0
                                 IP Mask= 0.0.0.0
                                 Port #= 137
                                 Port # Comp= Equal
                         Source: IP Addr= 0.0.0.0
                                 IP Mask= 0.0.0.0
                                 Port #=
                                 Port # Comp= None
                    TCP Estab= No
                    More= No           Log= None
                    Action Matched= Drop
                    Action Not Matched= Check Next Rule

                    Press ENTER to Confirm or ESC to Cancel:
```

**Menu-21.1.2 (Protokoll-6: TCP / Port-138: NETBIOS Datagram Service):**

```
Menu 21.1.2 - TCP/IP Filter Rule

                    Filter #: 1,2
                    Filter Type= TCP/IP Filter Rule
                    Active= Yes
                    IP Protocol= 6     IP Source Route= No
                    Destination: IP Addr= 0.0.0.0
                                 IP Mask= 0.0.0.0
                                 Port #= 138
                                 Port # Comp= Equal
                         Source: IP Addr= 0.0.0.0
                                 IP Mask= 0.0.0.0
                                 Port #=
                                 Port # Comp= None
                    TCP Estab= No
                    More= No           Log= None
                    Action Matched= Drop
                    Action Not Matched= Check Next Rule

                    Press ENTER to Confirm or ESC to Cancel:
```

**Menu-21.1.3 (Protokoll-6: TCP / Port-139: NETBIOS Session Service):**

```
Menu 21.1.3 - TCP/IP Filter Rule

                    Filter #: 1,3
                    Filter Type= TCP/IP Filter Rule
                    Active= Yes
                    IP Protocol= 6     IP Source Route= No
                    Destination: IP Addr= 0.0.0.0
                                 IP Mask= 0.0.0.0
                                 Port #= 139
                                 Port # Comp= Equal
                         Source: IP Addr= 0.0.0.0
                                 IP Mask= 0.0.0.0
                                 Port #=
                                 Port # Comp= None
                    TCP Estab= No
                    More= No           Log= None
                    Action Matched= Drop
                    Action Not Matched= Check Next Rule

                    Press ENTER to Confirm or ESC to Cancel:
```

**Menu-21.1.4 (Protokoll-17: UDP / Port-137: NETBIOS Name Service):**

```
Menu 21.1.4 - TCP/IP Filter Rule

                    Filter #: 1,4
                    Filter Type= TCP/IP Filter Rule
                    Active= Yes
                    IP Protocol= 17    IP Source Route= No
                    Destination: IP Addr= 0.0.0.0
                                 IP Mask= 0.0.0.0
                                 Port #= 137
                                 Port # Comp= Equal
                         Source: IP Addr= 0.0.0.0
                                 IP Mask= 0.0.0.0
                                 Port #=
                                 Port # Comp= None
                    TCP Estab= N/A
                    More= No           Log= None
                    Action Matched= Drop
                    Action Not Matched= Check Next Rule

                    Press ENTER to Confirm or ESC to Cancel:
```

**Menu-21.1.5 (Protokoll-17: UDP / Port-138: NETBIOS Datagram Service):**

```
Menu 21.1.5 - TCP/IP Filter Rule

                    Filter #: 1,5
                    Filter Type= TCP/IP Filter Rule
                    Active= Yes
                    IP Protocol= 17    IP Source Route= No
                    Destination: IP Addr= 0.0.0.0
                                 IP Mask= 0.0.0.0
                                 Port #= 138
                                 Port # Comp= Equal
                         Source: IP Addr= 0.0.0.0
                                 IP Mask= 0.0.0.0
                                 Port #=
                                 Port # Comp= None
                    TCP Estab= N/A
                    More= No           Log= None
                    Action Matched= Drop
                    Action Not Matched= Check Next Rule

                    Press ENTER to Confirm or ESC to Cancel:
```

**Menu-21.1.6 (Protokoll-17: UDP / Port-139: NETBIOS Session Service):**

```
Menu 21.1.6 - TCP/IP Filter Rule

                    Filter #: 1,6
                    Filter Type= TCP/IP Filter Rule
                    Active= Yes
                    IP Protocol= 17    IP Source Route= No
                    Destination: IP Addr= 0.0.0.0
                                 IP Mask= 0.0.0.0
                                 Port #= 139
                                 Port # Comp= Equal
                         Source: IP Addr= 0.0.0.0
                                 IP Mask= 0.0.0.0
                                 Port #=
                                 Port # Comp= None
                    TCP Estab= N/A
                    More= No           Log= None
                    Action Matched= Drop
                    Action Not Matched= Forward

                    Press ENTER to Confirm or ESC to Cancel:
```

Eine wichtige Eigenschaft sei hier noch erwaehnt, naemlich die Funktion **Forward**, **Drop** und **Check Next Rule** in den einzelnen Filter-Sets. **Drop** steht fuer **Verwerfen**, **Forward** fuer **Weiterleiten** und **Check next Rule** fuer **Naechste Regel pruefen**.

Jedes ein/ausgehendes Datenpaket wird geprueft und trifft eine Regel nicht zu (Action Not Matched), wird diese entweder in der naechsten Regel geprueft oder an den Router bzw. ins WAN oder falls anders herum ins LAN weitergeleitet.

Betrachtet man das Menu-11.5 findet man hier jeweils immer nur einen angegebenen Filter-Set.
Allerdings befinden sich beim **Input Filter Set** zwei Filter-Sets durch Komma voneinander getrennt.

```
Input Filter Sets:
  protocol filters= 5, 1
```

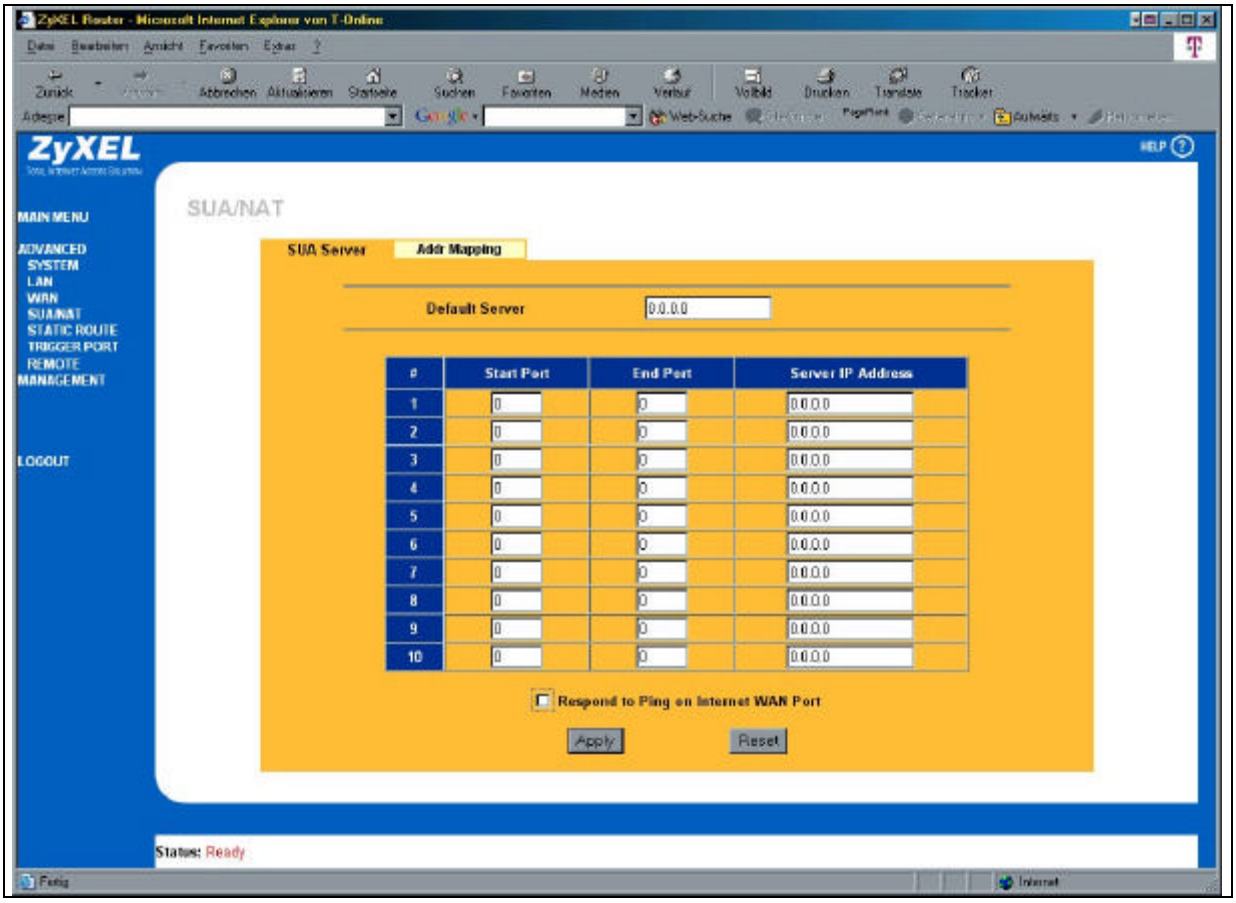
Da im **Filter-Set-1** die **letzt zu pruefende Regel immer auf Forward** (Weiterleiten) steht, sollten die durch Komma getrennt angegebenen Filter-Sets und somit vor der Ziffer 1 stehend immer den Eintrag Check Next Rule beinhalten, da sonst der nach einer Ziffer stehende Filterset nicht beruecksichtigt und abgearbeitet wird.

```
Action Matched= Drop
Action Not Matched= Forward

Action Matched= Drop
Action Not Matched= Check Next Rule.
```

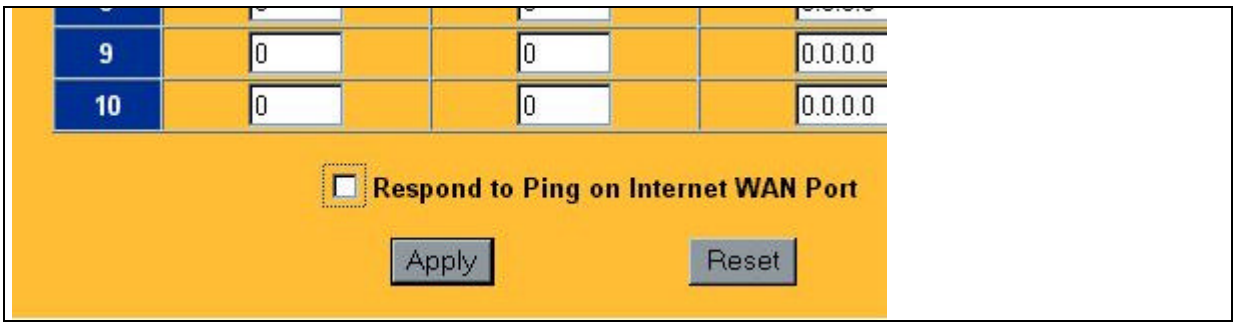
**„ICMP/PING“ am WAN-Port vom Internet aus verhindern/erlauben.**

Mittels Internet-Brownser koennen Sie den Ping unterbinden oder erlauben, je nach dem ob sich ein Haeckchen beim Punkt „Resond to Ping on Internet WAN Port“ befindet oder nicht.
Dieser Menupunkt befindet sich jedoch nicht in allen Firmware-Versionen, so z. B. die Firmware vom Teledat DSL Komfort Routers der Telekom. In einen solchen Fall ist im Menu-21.5.5 der ICMP-Filter auf active = Yes zu stellen, was bei vorgefertigten Romfiles schon entsprechend definiert ist.

```
5 Y IP   Pr=1, SA=0.0.0.0, DA=0.0.0.0, DP=8                    N D N
```




Wenn man nun beim Feld „Respond to Ping Internet WAN Port“ das haeckchen setzt und dies mittels Apply bestaetigt, werden PINGs – welche von aussen an Ihren WAN-Port/Router ankommen – auch beantwortet.



**„IP Antiprobe 1“ ab Firmware v3.25.xx**

Eine weitere Besonderheit stellt im Menu-24.8 der Command Interpreter Mode zur Verfügung.
Mittels dem Befehl „**sys edit autoexec.net**“ laesst sich naemlich die Bootfunktion des Routers anpassen.
Ab der Firmware Version 3.25.xx kann der Befehl „**ip antiprobe 1**“ mittels dem Buchstaben ´i´ fuer Insert eingefügt und mittels dem Buchstaben ´x´ zum speichern und verlassen des Editors, in der autoexec.net gesichert werden. Somit steht auch nach einem Neustart vom Router die Antiprobe-Funktion dauerhaft zur Verfuegung.

Die Funktion Antiprobe sorgt bei einem Port-Scan am WAN-Port (also vom Internet aus gesehen) dazu, das nur die freigeschalteten Ports (im Falle von NAT im Menu-15.2 anzugebene Ports) als sichtbar gelten, sofern der eigentliche Server im LAN auch antwortet (http://scan.sygatetech.com).

```
                        Menu 24 - System Maintenance

                      1.  System Status
                      2.  System Information and Console Port Speed
                      3.  Log and Trace
                      4.  Diagnostic
                      5.  Backup Configuration
                      6.  Restore Configuration
                      7.  Upload Firmware
                      8.  Command Interpreter Mode
                      9.  Call Control
                      10. Time and Date Setting
                      11. Remote Management Setup




                        Enter Menu Selection Number: 8


teledat> sys edit autoexec.net
EDIT cmd: q(uit) x(save & exit) i(nsert after) d(elete) r(eplace) n(ext)
sys errctl 0
sys trcl level 5
sys trcl type 1180
sys trcp cr 96 128
sys trcl sw on
ip tcp mss 512
ip tcp limit 2
ip tcp irtt 65000
ip tcp window 2
ip tcp ceiling 6000
ip rip activate
ip rip merge on
ip icmp disc enif0 off
ip antiprobe 1
ppp ipcp com off
sys mbuf debug off
sys wdog sw on
EOF
teledat>
```

**„IP NAT Loopback On“ ab Firmware v3.25.xx**

Mittels dem Befehl „**sys edit autoexec.net**“ die Bootfunktion des Routers anpassen.
Ab der Firmware Version 3.25.xx kann der Befehl „**ip nat loopback on**“ mittels dem Buchstaben ´i´ fuer Insert eingefügt und mittels dem Buchstaben ´x´ fuer speichern und verlassen des Editors, in der autoexec.net gesichert werden. Somit steht auch nach einem Neustart vom Router die Loopback-Funktion dauerhaft zur Verfuegung.

Die Funktion Loopback sorgt bei Verwendung eines interen Webservers dafuer (im SUA/NAT den Port: 80 bis 80 auf die lokale Webserver IP-Adresse eingestellt und deaktivierten Sicherheitsfilter im Menu-21 bzw. korrekt eingestellter Firewall-ACL: WAN zu LAN), das wenn man im Internetbrowser die WAN IP-Adresse oder den eigenen „hostname.dyndns.org“ (Dynamic DNS Menu-1.1) angibt, auch der Lokale Webserver erreicht wird und nicht der Lokale Router bzw. dessen Webkonfiguration.

```
teledat> sys edit autoexec.net
EDIT cmd: q(uit) x(save & exit) i(nsert after) d(elete) r(eplace) n(ext)
sys errctl 0
sys trcl level 5
sys trcl type 1180
sys trcp cr 96 128
sys trcl sw on
ip tcp mss 512
ip tcp limit 2
ip tcp irtt 65000
ip tcp window 2
ip tcp ceiling 6000
ip rip activate
ip rip merge on
ip icmp disc enif0 off
ip antiprobe 1
ip nat loopback on
ppp ipcp com off
sys mbuf debug off
sys wdog sw on
EOF
teledat>
```

**„MTU und/oder MSS dauerhaft zur Verwendung von AOL/Compuserve und Freenet anpassen“**

Mittels dem Befehl „**sys edit autoexec.net**“ die Bootfunktion des Routers anpassen.
Um mittels AOL eine korrekte Internetverwendung zu erreichen, sollte der Befehl „**ip adjTcp wanif0 1360**“ mittels dem Buchstaben ´i´ fuer Insert an letzter Stelle eingefügt und mittels dem Buchstaben ´x´ zum speichern und verlassen des Editors, in der autoexec.net gesichert werden. Somit steht auch nach einem Neustart vom Router die korrekte Einstellung der MTU/MSS-Size fuer AOL dauerhaft zur Verfuegung.

Verwendet man im Router einen AOL-Account, so wird es bei aelteren Firmwareversionen vorkommen, das man diverse Internetseiten oder Server im allgemeinen nicht richtig oder vollstaendig erreichen kann.
Um den Router nun auch ueber AOL verwenden zu koennen, bedarf es der (*korrekte Schreibweise ist wichtig*)
Angabe von: **ip adjTcp wanif0 1360** (**AOL**), der Router verwendet die MTU: **1400** und eine MSS von **1360**.
Angabe von: **ip adjTcp wanif0 1414** (**Freenet**), der Router verwendet die MTU: **1454** und eine MSS von **1414**.
Angabe von: **ip adjTcp wanif0 1390** (**Telekom**), der Router verwendet die MTU: **1492** und eine MSS von **1390**.

```
teledat> sys edit autoexec.net
EDIT cmd: q(uit) x(save & exit) i(nsert after) d(elete) r(eplace) n(ext)
sys errctl 0
sys trcl level 5
sys trcl type 1180
sys trcp cr 96 128
sys trcl sw on
ip tcp mss 512
ip tcp limit 2
ip tcp irtt 65000
ip tcp window 2
ip tcp ceiling 6000
ip rip activate
ip rip merge on
ip icmp disc enif0 off
ip antiprobe 1
ip nat loopback on
ppp ipcp com off
sys mbuf debug off
sys wdog sw on
ip adjTcp wanif0 1360
EOF
teledat>
```

Ist der Router mit dem Internet verbunden (WANIF0), kann dies mit folgenden Befehlen gepfueft werden:
Geziehlte abfrage der MSS: *ip adjTcp wanif0*
Abfragen der MTU/MSS: *ip ifconfig wanif0*

```
Copyright (c) 1994 - 2003 ZyXEL Communications Corp.
Teledat> ip ifconfig wanif0
wanif0: mtu 1400        mss 1360
    inet 217.84.11.33, netmask 0xffffffff, broadcast 255.255.255.255
    RIP RX:None, TX:None,
    [InOctets     331667855] [InUnicast    435548] [InMulticast            0]
    [InDiscards           0] [InErrors          0] [InUnknownProtos         0]
    [OutOctets    103587449] [OutUnicast   320827] [OutMulticast           0]
    [OutDiscards          0] [OutErrors         0]

teledat> ip adjTcp wanif0
adjust TCP mss on wanif0 to 1360

teledat> ip adjTcp
Usage: adjTcp <iface> [<mss>]
teledat>
```

**„Dynamic DNS Configuration“**

Ist der Router im Internet eingewaehlt, erhaellt er beim Internetprovider fuer gewoehnlich eine Dynamische erteilte IP-Adresse am WAN-Device. Um diese nun bis zur naechsten Trennung durch die eingestellte IDLE-Time bzw. der Zwangstrennung des Internetproviders auf einen Hostnamen im Internet zu binden, gibt es das Menu-1.1 zur Angabe eines bei www.dyndns.org erstellten DNS-Accounts. Dies hat den Vorteil das man die am WAN zugeteilte Internet IP-Adresse mittels einem Ping auf den angegebenen „hostnamen.dyndns.org“ erreicht. Ein im Lokalen LAN/Netz befindlichen Webserver kann man nun so aus dem Internet immer anhand des Hostnamens erreichen. Natuerlich nur wenn dies entsprechend im SUA/NAT angegeben wurde und keine Filter oder Firewall-ACL die Erreichbarkeit des Ports bzw. lokalen Servers verhindern.

```
                Copyright (c) 1994 - 2003 ZyXEL Communications Corp.

                          Prestige ??????? Main Menu

Getting Started                         Advanced Management
  1. General Setup                        21. Filter Set Configuration
  3. LAN Setup                            22. SNMP Configuration
  4. Internet Access Setup                23. System Password
                                          24. System Maintenance
Advanced Applications                     25. IP Routing Policy Setup
  11. Remote Node Setup                   26. Schedule Setup
  12. Static Routing Setup
  15. NAT Setup
                                          99. Exit
```

```
                          Menu 1 - General Setup

                System Name=
                Location=
                Contact Person's Name=
                Domain Name=
                Edit Dynamic DNS= Yes

                Route IP= Yes
                Bridge= No
```

```
                      Menu 1.1 - Configure Dynamic DNS

Service Provider= WWW.DynDNS.ORG
Active= Yes
Host= hostname.dyndns.org
EMAIL= alias@domain.de
USER= username
Password= ********
Enable Wildcard= Yes
```

```
                      Menu 1.1 - Configure Dynamic DNS

Service Provider= WWW.DynDNS.ORG
Active= Yes
DDNSType= DynamicDNS
Host1= hostname.dyndns.org
Host2=
Host3=
USER= username
Password= ********
Enable Wildcard= Yes
Offline= N/A
Edit Update IP Address:
  Use Server Detected IP= No
  User Specified IP Address= No
  IP Address= N/A


                Press ENTER to Confirm or ESC to Cancel:
```

**Menu-24.10 „Time and Date Setting“ ab Firmware v3.25.xx**

Der Router besitzt keine Echtzeituhr und muss so seine Systemzeit aus dem Internet mittels Protokoll...

**Daytime (RFC-867)**
**Time (RFC-868)**
**NTP (RFC-1305)**

...bei einem entsprechenden Zeit/Datums-Server abgleichen.

Fuer Deutschland/Oesterreich gilt z. B. die Time Zone „*GMT+0100*“ bei einer Sommer/Winterzeit vom 31.03. bis 31.10. Dessen Schreibweise in „*MM-DD*“ (Monat-Tag) beim Router einzutragen ist.

**Menu-24.10 (Protokoll-6: `TCP / Port-123:` NTP (RFC-1305)):**

```
            Menu 24.10 – System Maintenance - Time and Date Setting

          Use Time Server when Bootup= NTP (RFC-1305)
          Time Server Address= 212.16.32.200

          Current Time:                          07 : 11 : 49
          New Time (hh:mm:ss):                   07 : 07 : 57

          Current Date:                          2000 - 01 – 01
          New Date (yyyy-mm-dd):                 2000 - 01 – 01

          Time Zone= GMT+0100

          Daylight Saving= Yes
          Start Date (mm-dd):                          03 – 31
          End Date (mm-dd):                            10 – 27


                     Press ENTER to Confirm or ESC to Cancel:
```

Um ohne Angabe eines GMT und Daylight-Saving time zu arbeiten, genuegt die Verwendung eines Daytime Servers wie z.b. unter „`129.206.119.11`“ erreichbar.

**Menu-24.10 (Protokoll-6: `TCP / Port-13:` Daytime (RFC-867)):**

```
            Menu 24.10 – System Maintenance - Time and Date Setting

          Use Time Server when Bootup= Daytime (RFC-867)
          Time Server Address= 129.206.119.11

          Current Time:                          07 : 11 : 49
          New Time (hh:mm:ss):                   07 : 07 : 57

          Current Date:                          2000 - 01 – 01
          New Date (yyyy-mm-dd):                 2000 - 01 – 01

          Time Zone= GMT

          Daylight Saving= No
          Start Date (mm-dd):                          03 – 31
          End Date (mm-dd):                            10 - 27


                     Press ENTER to Confirm or ESC to Cancel:
```

**Menu-24.11 „Remote Management Setup“ ab Firmware v3.25.xx**

Das Remote-Management Menu ersetzt die Filter fuer Telnet, FTP und WEB und kann entsprechend dazu verwendet werden um z. B. nur spezielle IP-Adressen das Administrieren/Konfigurieren vom Routers zu erlauben. Die Einstellungen koennen hierbei „*LAN only*“, „*WAN only*“, „*ALL*“ oder „*Disable*“ sein.

Gibt man beim Feld „*Secure Client IP*“ eine IP-Adresse an, kann nur diese den entsprechend eingestellten Port zur Routerkonfiguration/Administration verwenden. Dabei ist die entsprechende Richtung zu beruecksichtigen, aus der die eingestellte IP-Adresse den Kontakt zur Verbindungsaufnahme versucht.
Im Falle „*LAN only*“ kann es sich dabei immer nur um Adressen aus dem eigenen LAN/Netzwerk (Local Area Network) handeln.
Im Falle „*WAN only*“ hingegen kann es immer nur um Adressen aus dem fernen WAN/Internet (Wide Area Network) handeln.
Die Auswahl „*ALL*“ definiert LAN/Netzwerk und WAN/Internet, „*Disable*“ deaktiviert den Port und somit dessen Nutzung zur Konfiguration. Deaktiviert man alle RouterDienste, kann nur noch mittels Serieller Verbindung ueber den Console-Anschluss konfiguriert werden.

```
                  Menu 24.11 - Remote Management Control

    TELNET Server:     Port = 23         Access = LAN only
                       Secured Client IP = 0.0.0.0

    FTP Server:        Port = 21         Access = LAN only
                       Secured Client IP = 0.0.0.0

    Web Server:        Port = 80         Access = LAN only
                       Secured Client IP = 0.0.0.0

    SNMP Service:      Port = 161        Access = LAN only
                       Secured Client IP = 0.0.0.0

    DNS Service:       Port = 53         Access = LAN only
                       Secured Client IP = 0.0.0.0


                  Press ENTER to Confirm or ESC to Cancel:
```

**Menu-24.3.2 „UNIX Syslog“**

Das Menu „*UNIX Syslog*“ dient zur Weiterleitung von Routerinformationen wie z. B. das „auf- & wieder ab-bauen von Internet-Verbindungen“ oder „Paketfilter“, welche z. B. in der Filterregel auf „*Log= Action Matched*“ gestellt wurden. Um diese Funktion zu nutzen, genuegt es die IP-Adresse des Lokalen Computers anzugeben, auf dem ein sogenannter „*Syslog-Client*“ gestartet ist. Die auf dem angegebene Syslog-Software wird die ueber „*Port-514*“ uebertragenen Sysloginformationen vom Router annehmen und auswerten bzw. anzuzeigen.

Eine typisch verwendete Software fuer Windows waere der SysLOGdaemon von Kiwi Enterprises:
http://www.kiwi-enterprises.com/software_downloads.htm

**Menu-21.3.2**

```
                Menu 24.3.2 - System Maintenance - UNIX Syslog

                   Syslog:
                   Active= Yes
                   Syslog IP Address= 192.168.1.33
                   Log Facility= Local 1

                   Types:
                   CDR= Yes
                   Packet triggered= Yes
                   Filter log= Yes
                   PPP log= Yes




                   Press ENTER to Confirm or ESC to Cancel:
```

Um nun einen am WAN ankommenden ICMP/PING dazu zu bewegen, das diese Information im Falle eines solchen Versuches auch zum Syslog-Client uebermittelt wird, genuegt es die entsprechend definierte Regel im Menu-21.5.5 auf „*Log= Action Matched*“ zu stellen/confirmen.

**Menu-21.5.5 (Protokoll-1: ICMP / Port-8: PING):**

```
Menu 21.5.5 - TCP/IP Filter Rule

                   Filter #: 5,5
                   Filter Type= TCP/IP Filter Rule
                   Active= No
                   IP Protocol= 1     IP Source Route= No
                   Destination: IP Addr= 0.0.0.0
                                IP Mask= 0.0.0.0
                                Port #= 8
                                Port # Comp= Equal
                        Source: IP Addr= 0.0.0.0
                                IP Mask= 0.0.0.0
                                Port #=
                                Port # Comp= None
                   TCP Estab= N/A
                   More= No           Log= Action Matched
                   Action Matched= Drop
                   Action Not Matched= Check Next Rule

                   Press ENTER to Confirm or ESC to Cancel:
```

**„Syslog-Beispiel anhand ICMP/Ping“**
Hier ein Beispiel vom Versuch eines Ping von der IP-Adresse „*80.142.160.72*“ aus dem Internet welche durch den ICMP-Filter geblockt wurde. Diese Information bekommt der Syslog-Client vom Router gesandt, wenn der ICMP-Filter Menu-21.5.5 auf „*Log= Action Matched*“ gesetzt wurde.

```
13-05-2002   18:45:43   Local1.Notice   teledat.t-online.de   teledat: May 13 2002
18:45:57 IP[Src=80.142.160.72 Dst=192.168.1.1 ICMP]}S05>R05mD

13-05-2002   18:45:47   Local1.Notice   teledat.t-online.de   teledat: May 13 2002
18:46:01 IP[Src=80.142.160.72 Dst=192.168.1.1 ICMP]}S05>R05mD

13-05-2002   18:45:51   Local1.Notice   teledat.t-online.de   teledat: May 13 2002
18:46:05 IP[Src=80.142.160.72 Dst=192.168.1.1 ICMP]}S05>R05mD
```

Ermittelte Daten vom Pingenden mittels der Software „WS Ping Pro“ und Whois von „whois.ripe.net“:
http://www.ipswitch.com/downloads/index.html

```
% This is the RIPE Whois server.
% The objects are in RPSL format.
% Please visit http://www.ripe.net/rpsl for more information.
% Rights restricted by copyright.
% See http://www.ripe.net/ripencc/pub-services/db/copyright.html

inetnum:      80.128.0.0 - 80.146.159.255
netname:      DTAG-DIAL16
descr:        Deutsche Telekom AG
country:      DE
admin-c:      DTIP-RIPE
tech-c:       ST5359-RIPE
status:       ASSIGNED PA
remarks:      ***************************************************************
remarks:      * ABUSE CONTACT: abuse@t-ipnet.de IN CASE OF HACK ATTACKS,      *
remarks:      * ILLEGAL ACTIVITY, VIOLATION, SCANS, PROBES, SPAM, ETC.        *
remarks:      ***************************************************************
notify:       auftrag@nic.telekom.de
notify:       dbd@nic.dtag.de
mnt-by:       DTAG-NIC
changed:      auftrag@nic.telekom.de 20020108
source:       RIPE

route:        80.128.0.0/11
descr:        Deutsche Telekom AG, Internet service provider
origin:       AS3320
mnt-by:       DTAG-RR
changed:      bp@nic.dtag.de 20010807
source:       RIPE

person:       DTAG Global IP-Adressing
address:      Deutsche Telekom AG
address:      Postfach 900110
address:      D-90492 Nuernberg
address:      Germany
phone:        +49 911 68909856
e-mail:       ripe.dtip@telekom.de
nic-hdl:      DTIP-RIPE
mnt-by:       DTAG-NIC
changed:      auftrag@nic.telekom.de 20020311
source:       RIPE

person:       Security Team
address:      Deutsche Telekom AG
address:      Technikniederlassung Schwaebisch Hall
address:      D-89070 Ulm
address:      Germany
phone:        +49 731 100 84055
fax-no:       +49 731 100 84150
e-mail:       abuse@t-ipnet.de
nic-hdl:      ST5359-RIPE
notify:       auftrag@nic.telekom.de
notify:       dbd@nic.dtag.de
mnt-by:       DTAG-NIC
changed:      auftrag@nic.telekom.de 20010321
source:       RIPE

**complete**
```

**Menu-24.3.4 „Call-Triggering Packet – Anzeige einer ausloesenden Internetverbindung“**

Im Menu-24.3.4 laesst sich ersehen, welcher Client (z.B. Computer / Netzwerkdrucker, usw.) den Router zur Internetanwahl veranlasst hat. In dem unteren Beispiel hat ein Computer mit der IP-Adresse 192.168.120.12 eine Anfrage ueber ICMP und dem Protokoll-8 (Echo Request/PING) eine Anfrage an die IP-Adresse 141.1.1.1 gestellt.

Dies kann z. B. dann der Fall sein, wenn ein Anwender mittels „**PING 141.1.1.1**“ diese Anfrage selbst stellt oder aber eine Software im Hintergrund ein Update starten möchte, in einem solchen Fall dann die Destination IP jene Internetadresse enthaelt, auf dessen Server der Zugriff stattfinden soll/wird.

Meistens jedoch werden Ausloesende Internet-Anwahlen dadurch zustande kommen, weil eine Anfrage an den DNS stattfinden muss (Domain-Name-Server zur Namensaufloesung einer Internet-namens-Adresse), in einem derartigen Fall es dann die IP-Adresse des naechst zu erreichenden DNS-Servers sein wird und diese Anfrage ueber Protokoll-17 / Port-53 starttfindet.

```
IP Frame: ENET0-RECV   Size:  48/  48   Time: 02:06:25.978
 Frame Type:

   IP Header:
     IP Version              = 4
     Header Length           = 20
     Type of Service         = 0x00 (0)
     Total Length            = 0x003C (60)
     Idetification           = 0x1ADB (6875)
     Flags                   = 0x00
     Fragment Offset         = 0x00
     Time to Live            = 0x1E (30)
     Protocol                = 0x01 (ICMP)
     Header Checksum         = 0xBB2F (47919)
     Source IP               = 0xC0A8780C (192.168.120.12)
     Destination IP          = 0x8D010101 (141.1.1.1)

   ICMP Header:
     Type                    = 0x08 (Echo Request)
     Code                    = 0x0800 (Echo Request)
     Checksum                = 0x1B5C (7004)
-= Next page =-
   ICMP Data: (Length=24, Captured=24)
     0000: 05 00 2D 00 61 62 63 64-65 66 67 68 69 6A 6B 6C  ..-.abcdefghijkl
     0010: 6D 6E 6F 70 71 72 73 74                          mnopqrst

   RAW DATA:
     0000: 45 00 00 3C 1A DB 00 00-1E 01 BB 2F C0 A8 78 0C  E..<......./..x.
     0010: 8D 01 01 01 08 00 1B 5C-05 00 2D 00 61 62 63 64  .......\..-.abcd
     0020: 65 66 67 68 69 6A 6B 6C-6D 6E 6F 70 71 72 73 74  efghijklmnopqrst

Press any key to continue...
```

**Menu-24.8 „Command Interpreter Mode – Internet-Zugangs-Test ueber den Kommandozeilen-Modus“**

Um genauere Informationen fuer fehlschlagende Internetanwahlverbindungen zu erhalten, eignet sich der CI-Command-Mode am allerbesten dazu. – Mit den Befehlen „**poe debug 1**“ bzw. „**pptp debug 1**“ und „**dev dial 1**“ laesst sich ein solcher test manuell durchfuehren.

**Beispiel einer fehlschlagenden Internetanwahl-Verbindungen:**

```
teledat> poe deb 1 (pptp deb 1)
teledat> dev dial 1
Start dialing for node <T-Online>...
PoeNetCmdExe: chann poe0 event x420
poeChannDial: start session, peer<T-Online>
poeSendInitiation: srvcName  len = 0 36e824
bdcastInit: pch poe0
poePut1SrvcName: '' len 0 36e824
  host-uniq 31303030 len 4
putPoeHdr: ver 1 type 1 code x09 sess-id 0 len 12(x000C)
poePut1SrvcName: '' len 0 36e824
  host-uniq 31303030 len 4
putPoeHdr: ver 1 type 1 code x09 sess-id 0 len 12(x000C)
### Hit any key to continue.###
$$$ DIALING dev=6 ch=0.........
$$$ OUTGOING-CALL phone()
poeI/C: ver 1 type 1 code x07 sessId x0000 len 46(x002E)
poeCtrlI/C: pkt len 46
poeGetTags()
  AC-name AACX12-erx
  host-uniq 31303030 len 4
  service-name  36e8b4
  AC-cookie 1E86218C970D5D710A968D21E1C507C4 len 16
PADO recv'd, chann enet1
procPADO: for poe chann poe0
procPADO: requested svrc-name () len = 0 36e824
Chann poe0 sending request
poePut1SrvcName: '' len 0 36e824
  host-uniq 31303030 len 4
  AC-cookie 1E86218C970D5D710A968D21E1C507C4 len 16
putPoeHdr: ver 1 type 1 code x19 sess-id 0 len 32(x0020)
poeI/C: ver 1 type 1 code x65 sessId x0B24 len 12(x000C)
poeCtrlI/C: pkt len 40
poeGetTags()
  service-name  36e8fc
  host-uniq 31303030 len 4
PADS recv'd: chann enet1
procPADS: poe chann poe0 found
poeNotifyCM: event <423>
putPoeHdr: ver 1 type 1 code x00 sess-id 2852 len 16(x0010)
poeO/G: chann poe0 sess-id 2852
poeNetCmdExe: chann poe0 event x417
$$$ CALL CONNECT speed<512> type<6> chan<0>
poeI/C: ver 1 type 1 code x00 sessId x0B24 len 20(x0014)
putPoeHdr: ver 1 type 1 code x00 sess-id 2852 len 20(x0014)
poeO/G: chann poe0 sess-id 2852
poeI/C: ver 1 type 1 code x00 sessId x0B24 len 16(x0010)
putPoeHdr: ver 1 type 1 code x00 sess-id 2852 len 53(x0035)
poeO/G: chann poe0 sess-id 2852
poeNetCmdExe: chann poe0 event x417
$$$ LCP opened
$$$ PAP sending user/pswd
poeI/C: ver 1 type 1 code x00 sessId x0B24 len 26(x001A)
putPoeHdr: ver 1 type 1 code x00 sess-id 2852 len 6(x0006)
poeO/G: chann poe0 sess-id 2852
poeI/C: ver 1 type 1 code x00 sessId x0B24 len 6(x0006)
putPoeHdr: ver 1 type 1 code x00 sess-id 2852 len 6(x0006)
poeO/G: chann poe0 sess-id 2852
$$$ LCP closed
$$$ Recv'd TERM-REQ
poeI/C: ver 1 type 1 code x00 sessId x0B24 len 6(x0006)
poeNetCmdExe: chann poe0 event x424
poePut1SrvcName: '' len 0 36e824
  host-uniq 31303030 len 4
  AC-cookie 1E86218C970D5D710A968D21E1C507C4 len 16
putPoeHdr: ver 1 type 1 code xA7 sess-id 2852 len 32(x0020)
poeNotifyCM: event <425>
poeI/C: ver 1 type 1 code xA7 sessId x0B24 len 0(x0000)
poeCtrlI/C: pkt len 46
PADT recv'd, chann enet1
procPADT: chann enet1 not PPPoE; sess-id 2852
src 00:90:1A:40:09:BF
poeNetCmdExe: chann poe0 event x430
$$$ Recv'd TERM-ACK state 5
$$$ LCP stopped
```

Kommt die Meldung „*$$$ Recv'd TERM-ACK state 5*“, wurden die Login/Passwort-Daten abgelehnt!

**Beispiel einer funktionierenden Internetanwahl-Verbindung:**

```
Teledat> poe deb 1 (pptp deb 1)
teledat> dev dial 1
Start dialing for node <T-Online>...
PoeNetCmdExe: chann poe0 event x420
poeChannDial: start session, peer<T-Online>
poeSendInitiation: srvcName  len = 0 36ea1c
bdcastInit: pch poe0
poePut1SrvcName: '' len 0 36ea1c
  host-uniq 31303031 len 4
putPoeHdr: ver 1 type 1 code x09 sess-id 0 len 12(x000C)
poePut1SrvcName: '' len 0 36ea1c
  host-uniq 31303031 len 4
putPoeHdr: ver 1 type 1 code x09 sess-id 0 len 12(x000C)
### Hit any key to continue.###
$$$ DIALING dev=6 ch=0..........
$$$ OUTGOING-CALL phone()
poeI/C: ver 1 type 1 code x07 sessId x0000 len 46(x002E)
poeCtrlI/C: pkt len 46
poeGetTags()
  AC-name AACX12-erx
  host-uniq 31303031 len 4
  service-name  36eaac
  AC-cookie 1E86218C970D5D710A968D21E1C507C4 len 16
PADO recv'd, chann enet1
procPADO: for poe chann poe0
procPADO: requested svrc-name () len = 0 36ea1c
Chann poe0 sending request
poePut1SrvcName: '' len 0 36ea1c
  host-uniq 31303031 len 4
  AC-cookie 1E86218C970D5D710A968D21E1C507C4 len 16
putPoeHdr: ver 1 type 1 code x19 sess-id 0 len 32(x0020)
poeI/C: ver 1 type 1 code x65 sessId x0B99 len 12(x000C)
poeCtrlI/C: pkt len 40
poeGetTags()
  service-name  36eaf4
  host-uniq 31303031 len 4
PADS recv'd: chann enet1
procPADS: poe chann poe0 found
poeNotifyCM: event <423>
putPoeHdr: ver 1 type 1 code x00 sess-id 2969 len 16(x0010)
poeO/G: chann poe0 sess-id 2969
poeNetCmdExe: chann poe0 event x417
$$$ CALL CONNECT speed<10000000> type<6> chan<0>
poeI/C: ver 1 type 1 code x00 sessId x0B99 len 20(x0014)
putPoeHdr: ver 1 type 1 code x00 sess-id 2969 len 20(x0014)
poeO/G: chann poe0 sess-id 2969
poeI/C: ver 1 type 1 code x00 sessId x0B99 len 16(x0010)
putPoeHdr: ver 1 type 1 code x00 sess-id 2969 len 57(x0039)
poeO/G: chann poe0 sess-id 2969
poeNetCmdExe: chann poe0 event x417
$$$ LCP opened
$$$ PAP sending user/pswd
poeI/C: ver 1 type 1 code x00 sessId x0B99 len 7(x0007)
putPoeHdr: ver 1 type 1 code x00 sess-id 2969 len 24(x0018)
poeO/G: chann poe0 sess-id 2969
poeI/C: ver 1 type 1 code x00 sessId x0B99 len 12(x000C)
putPoeHdr: ver 1 type 1 code x00 sess-id 2969 len 12(x000C)
poeO/G: chann poe0 sess-id 2969
$$$ IPCP negotiation started
$$$ BACP stopped
poeI/C: ver 1 type 1 code x00 sessId x0B99 len 24(x0018)
putPoeHdr: ver 1 type 1 code x00 sess-id 2969 len 24(x0018)
poeO/G: chann poe0 sess-id 2969
$$$ IPCP neg' Primary DNS 212.185.249.84
$$$ IPCP neg' Primary DNS 194.25.2.129
poeI/C: ver 1 type 1 code x00 sessId x0B99 len 24(x0018)
$$$ IPCP opened
putPoeHdr: ver 1 type 1 code x00 sess-id 2969 len 10(x000A)
poeO/G: chann poe0 sess-id 2969
poeI/C: ver 1 type 1 code x00 sessId x0B99 len 10(x000A)
teledat> exit
```

Kommt es zu einem „*$$$ CALL CONNECT*“, ist der Zustand einer Leitungsverbindung zwischen Router ueber DSL-Modem zum DSLam (sozusagen ist der DSLam eine Art Vermittlungsstelle) gegeben.
Kommt die Meldung „*$$$ LCP opened*“, wurde das Layer-Control-Protocol zum Datenaustausch geoeffnet.
Kommt die Meldung „*$$$ PAP sending user/pswd*“, werden die Login/Passwort-Daten uebermittelt.
Kommt die Meldung „*$$$ IPCP negotiation started*“, wurde die Authentifizierung abgeschlossen und das Internet-Protocol/Control-Protocol zum weiteren Datenaustausch gestartet.
Kommt die Meldung „*$$$ IPCP opened*“, wurde eine verfuegbare Internetverbindung zum weiteren Datenaustausch geoeffnet. – Das Internet-Protocol/Control-Protocol transportiert nun Daten zum und vom Internet!

Kommt es zum Fehler wie im „**Beispiel einer fehlschlagenden Internetanwahl-Verbindungen**“ angefuehrten Verhalten, liegt das meistens an einem falsch angegebenen LOGIN, der meistens einem festen Format unterliegt.

**Menu-4 „Internet Access Setup“**

```
                        Menu 4 - Internet Access Setup

                    ISP's Name= T-Online
                    Encapsulation= PPPoE
                      Service Type= N/A
                      My Login= 111111111111222222222222#0001@t-online.de
                      My Password= ********
                      Idle Timeout= 100

                    IP Address Assignment= Dynamic
                      IP Address= N/A
                      IP Subnet Mask= N/A
                      Gateway IP Address= N/A
                    Network Address Translation= SUA Only
```

```
Die Angabe „ISP's Name“ dient lediglich zur eigenen Bezeichnung.
Die Angabe „Idle Timeout“ bezieht sich auf die Abwahlzeit bei keinem Traffic.
Die „Encapsulation“ muss in Deutschland auf „PPPoE“ eingestellt sein.
Das „IP Address Assignment“ muss auf „Dynamic“ eingestellt sein.
Die „Network Address Translation“ muss auf „SUA Only“ eingestellt sein.

Der Login zu T-Online bei einem Router eingegeben, ergibt sich in folgendem Format:

111111111111222222222222#0001@t-online.de

111111111111 - Anschlusskennung   = 12 Zeichen laenge.
222222222222 - T-Online Nummer    = 12 Zeichen laenge.
#            - die Raute (Hash)   = zwecks Abgrenzung zum Mitbenutzer-Suffix.
0001         - Mitbenutzer-Suffix = 4 Zeichen laenge.
@t-online.de - Domain-Name des Provider zwecks Rufzielrichtung.
```

```
                        Menu 4 - Internet Access Setup

                    ISP's Name= AOL
                    Encapsulation= PPPoE
                      Service Type= N/A
                      My Login= AOL-Name@de.aol.com
                      My Password= ********
                      Idle Timeout= 100

                    IP Address Assignment= Dynamic
                      IP Address= N/A
                      IP Subnet Mask= N/A
                      Gateway IP Address= N/A
                    Network Address Translation= SUA Only
```

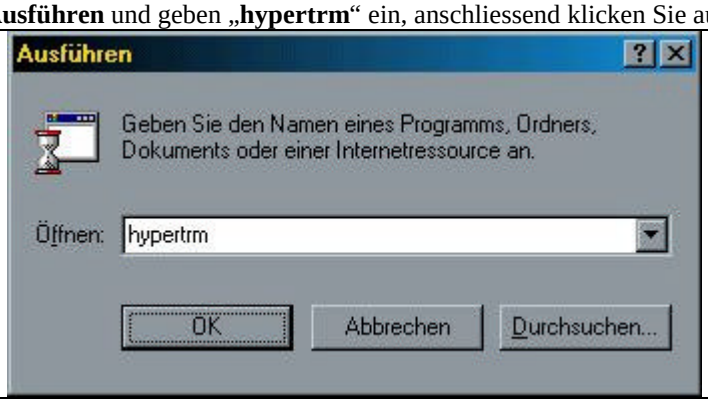
```
                        Menu 4 - Internet Access Setup

                    ISP's Name= 1&1
                    Encapsulation= PPPoE
                      Service Type= N/A
                      My Login= 1und1/1111-222@online.de
                      My Password= ********
                      Idle Timeout= 100

                    IP Address Assignment= Dynamic
                      IP Address= N/A
                      IP Subnet Mask= N/A
                      Gateway IP Address= N/A
                    Network Address Translation= SUA Only
```

**Flashen der Default-Konfiguration und Firmware mittels Serieller Verbindung:**

Um den Router in den Grund-/Werkszustand zu versetzen, kann es notwendig sein die „**Default-Konfiguration**“ und „**Firmware**“ – Datei mittels Terminalprogramm ueber den Seriellen „**Console-Anschluss**“ des Routers einzuspielen.

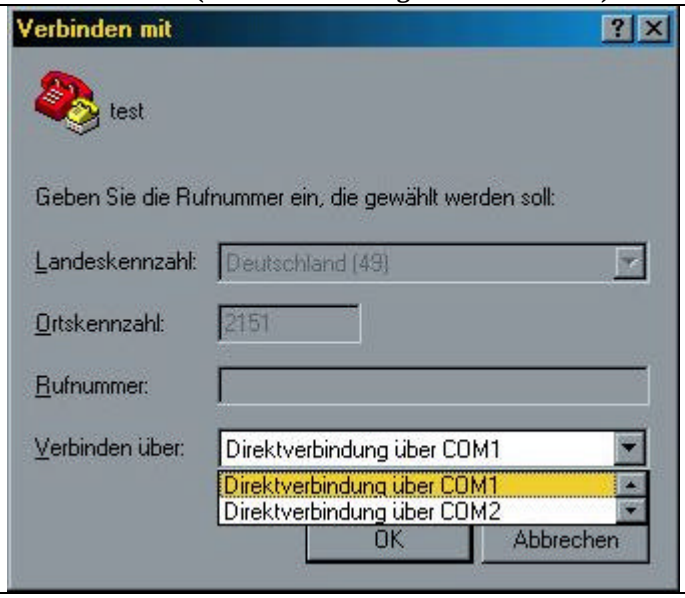
Dazu ist bei Windows wie folgt vorzugehen...

*Klicken Sie* auf **Start/Ausführen** und geben „**hypertrm**“ ein, anschliessend klicken Sie auf „**OK**“

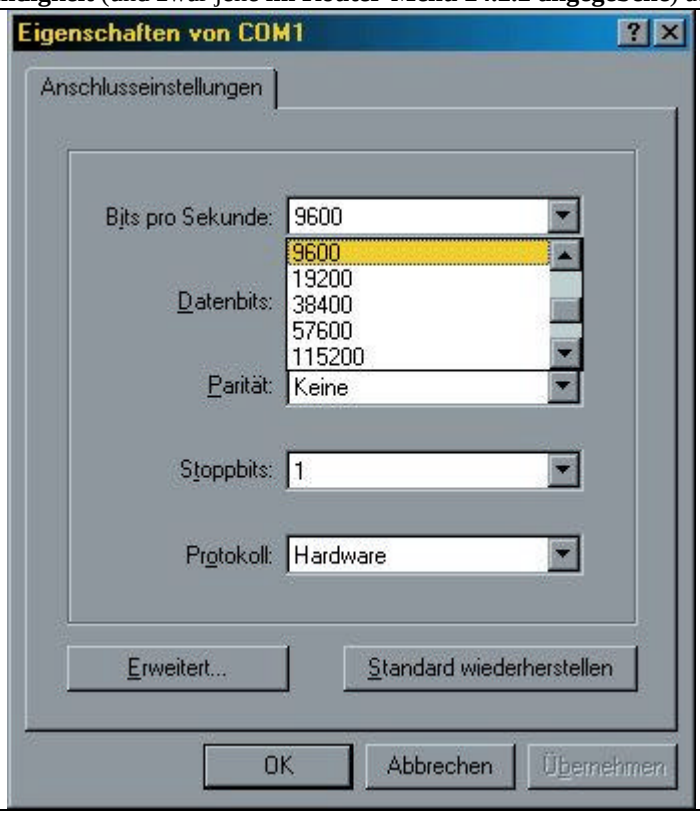



Daraufhin oeffnet sich ein Dialogfenster zur Angabe eines Bezeichnungs-Namens der Terminalverbindung:

Im naechsten Dialog werden Sie um eine **Auswahl der Verbindung** erfragt, in der keine Rufnummer anzugeben ist, sondern einfach **nur der Serielle Port (Direktverbindung über COM-Port) auszuwaehlen** ist.




Nachdem der Serielle Port an dem der Router angeschlossen ist ausgewaehlt wurde, muss noch die korrekt zu **verwendende Geschwindigkeit** (und zwar jene **im Router-Menu 24.2.2 angegebene**) ausgewählt sein.



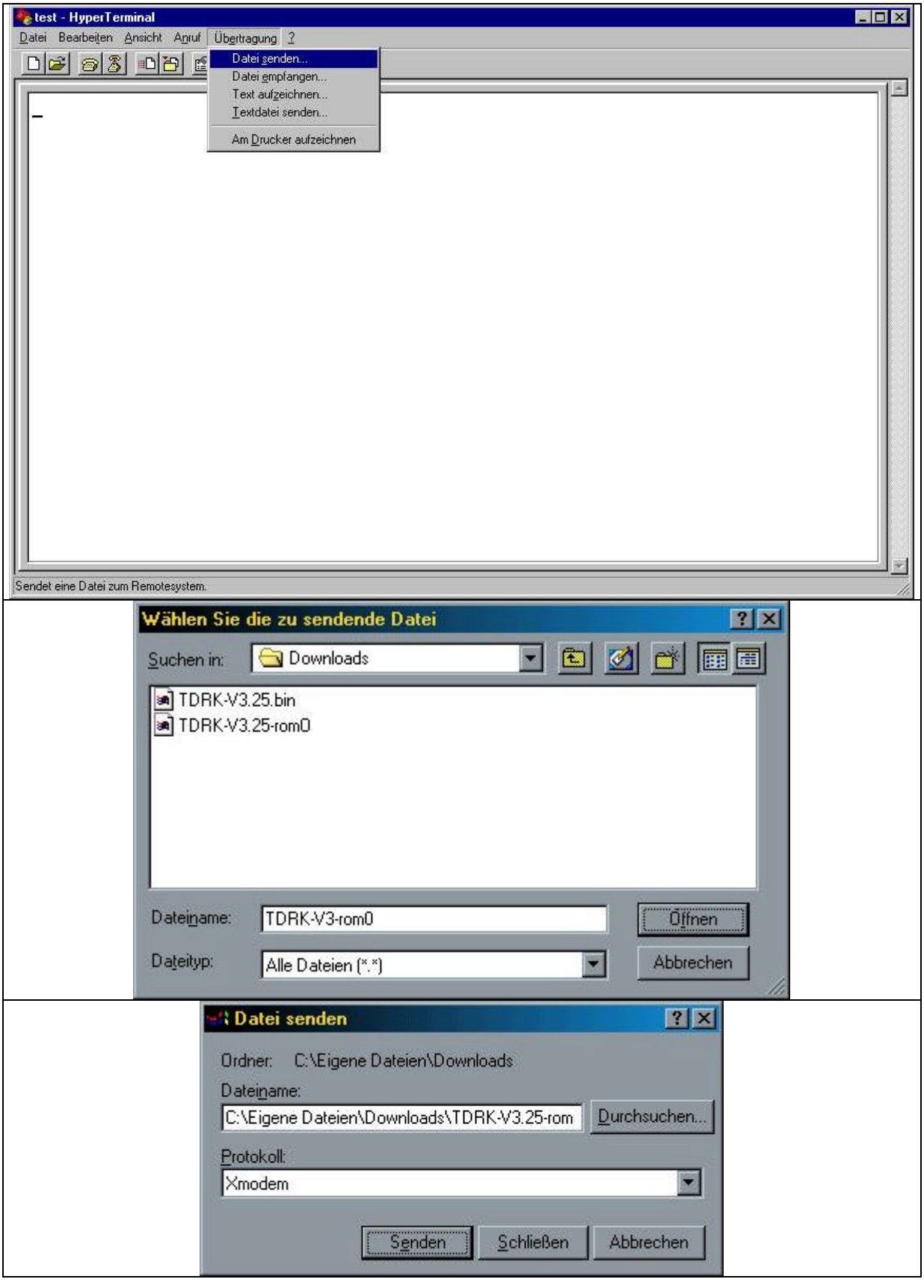
Schalten Sie nun den Router Aus/Ein, woraufhin bei korrekter Einstellung Ihres Terminalprogrammes eine Bootmeldung des Routers leserlich zu sehen sein sollte.

Unterbrechen Sie den Bootvorgang Ihres Router mittels betaetigung einer Taste (z. B. der SPACE- / Leer-Taste).

Mit **ATUR3** leiten Sie den **UpLoad-Prozess** zur Uebertragung der **Konfigurations-Datei *.ROM** ein.
Mit **ATUR** leiten Sie den **UpLoad-Prozess** zur Uebertragung der **Firmware-Datei *.BIN** ein.
Mit **ATHE** laesst sich eine **Hilfs-Seite** der verwendbaren **AT-Befehle** anzeigen.

```
Bootbase Version: V1.13 | 4/14/2000 13:48:37
RAM: Size = 4096 Kbytes
FLASH: Intel 8M

ZyNOS Version: V320(M.01) | 8/8/2000 11:55:33

Press any key to enter debug mode within 3 seconds.
.........
Enter Debug Mode
Athe
======= Debug Command Listing =======
AT just answer OK
ATHE print help
ATBAx change baudrate. ´x´= 1:38.4k, 2:19.2k, 3:9.6k 4:57.6k 5:115.2k
ATENx,(y) set BootExtension Debug Flag (y=password)
ATSE show the seed of password generator
ATTI(h,m,s) change system time to hour:min:sec or show current time
ATDA(y,m,d) change system date to year/month/day or show current date
ATDS dump RAS stack
ATDT dump Boot Module Common Area
ATDUx,y dump memory contents from address x for length y
ATRBx display the 8-bit value of address x
ATRWx display the 16-bit value of address x
ATRLx display the 32-bit value of address x
ATGO(x) run program at addr x or boot router
ATGR boot router
ATGT run Hardware Test Program
ATRTw,x,y(,z) RAM test level w, from address x to y (z iterations)
ATSH dump manufacturer related data in ROM
ATDOx,y download from address x for length y to PC via XMODEM
ATTD download router configuration to PC via XMODEM
ATUR upload router firmware to flash ROM

< press any key to continue >
ATUR3 upload router configuration file to flash ROM
ATLC upload router configuration file to flash ROM
ATXSx xmodem select: x=0: CRC mode(default); x=1: checksum mode

OK
atur3 (mittels XModem-Dateiuebertragungsprotokoll die zu sendende *.ROM-(Konfigurations)-Datei
in den Router uebertragen/flashen)
Starting XMODEM upload (CRC mode)....
C
Total 16384 bytes received.

Erasing..
....
OK
atur (mittels XModem-Dateiuebertragungsprotokoll die zu sendende *.BIN-(Firmware)-Datei in den
Router uebertragen/flashen)
Starting XMODEM upload (CRC mode)....
C
Total 1054720 bytes received.

Erasing
startBlk = 3, endBlk = 14
............
................................................................................
................................................................................
................................................................................
..............
OK
System Reboot...
Bootbase Version: V1.13 | 4/14/2000 13:48:37
RAM: Size = 4096 Kbytes
FLASH: Intel 8M

ZyNOS Version: V320(M.01) | 8/8/2000 11:55:33

Press any key to enter debug mode within 3 seconds.
.........................................................
Copyright (c) 1994 - 2000 ZyXEL Communications Corp.
initialize ch =0, ethernet address: 00:a0:c5:24:3f:08
initialize ch =1, ethernet address: 00:a0:c5:24:3f:09
Press ENTER to continue...
```

atur3 (die zu sendende *.ROM-(Konfigurations)-Datei in den Router uebertragen/flashen)



atur (die zu sendende *.BIN-(Firmware)-Datei in den Router uebertragen/flashen)