

Konfiguration der Prestige 2xx Serie fuer Internet-Verbindungen (ISP-Routing) Sowie RAS- und LAN-LAN Verbindungen.

Um einen **Prestige 202 und 480** 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 Bildschirmhalte soll ein Beispiel gegeben werden, wo sich welche Einstellungen befinden um diverse Filter, Sicherheits und ISP- sowie RAS- und LAN-LAN Einstellungen vorzunehmen.

Liste der behandelten Protokolle:

1	ICMP	Internet Control Message	[RFC792]
6	TCP	Transmission Control	[RFC793]
17	UDP	User Datagram	[RFC768, JBP]

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 - 2000 ZyXEL Communications Corp.	
Prestige 202 DSS1 Main Menu	
Getting Started	Advanced Management
1. General Setup	21. Filter Set Configuration
2. ISDN Setup	22. SNMP Configuration
3. Ethernet Setup	23. System Security
4. Internet Access Setup	24. System Maintenance
Advanced Applications	26. Schedule Setup
11. Remote Node Setup	
12. Static Routing Setup	
13. Default Dial-in Setup	
14. Dial-in User 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-SETs**, welche im **Menu-21** zu programmieren und korrekt einzustellen sind.

Menu-3:

```
Menu 3 - Ethernet Setup

1. General 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 - General Ethernet 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 Set #      Comments      Filter Set #      Comments
-----
 1 NetBIOS_WAN      7
 2 NetBIOS_LAN     8
 3 TEL_FTP_WAN     9
 4                10
 5 LRP_SNMP_PING  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** (entsprechender Speicherplatz) finden Sie die **Erweiterten Einstellungsmoeglichkeiten**.

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= ChangeMe	Edit PPP Options= No
Active= No	Rem IP Addr= 0. 0. 0. 0
Call Direction= Outgoing	Edit IP= No
Incoming:	Telco Option:
Rem Login= N/A	Transfer Type= 64K
Rem Password= N/A	Allocated Budget (min)=
Rem CLID= N/A	Period(hr)=
Call Back= N/A	Schedules=
Outgoing:	Carrier Access Code=
My Login= ChangeMe	Nailed-Up Connection= No
My Password= *****	Toll Period(sec)= 0
Authen= CHAP/PAP	Session Options:
Pri Phone #= 1234	Edit Filter Sets= No
Sec Phone #=	Idle Timeout(sec)= 100

Press ENTER to Confirm or ESC to Cancel:

Hier im **Menu-11.5** finden sich mehrere als default vorgegebene Eintraege. Diese Eintraege 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 **in das LAN**.

Menu-11.5:

Menu 11.5 - Remote Node Filter	
Input Filter Sets:	
protocol filters= 3, 5, 1	
device filters=	
Output Filter Sets:	
protocol filters= 1	
device filters=	
Call Filter Sets:	
protocol filters= 1	
device filters=	

Press ENTER 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 161 (SNMP), 162 (SNMP-Trap) sowie 520 (LRP) auf keinen Fall zum Router und somit auch nicht in das LAN** gelangen. Der **Filter-4** bezieht sich auf das **Protokoll-1 (ICMP)** und **verhindert Anfragen durch den Port-8 (PING)**, was dazu fuehrt das man den Router WAN-Seitig nicht mehr anpingen kann. Dieser **ICMP/PING-Filter** ist hier **absichtlich nicht auf „Drop“ gestellt**, da in vielen Faellen eine Erreichbarkeit zwecks Pruefung mittels einem PING eine ersichtliche Erleichterung bringt. Darueber hinaus laesst sich so **mittels Syslog genauer erkennen**, wann es einen eingehenden PING gegeben hat und von wem.

Menu-21:

```

Menu 21 - Filter Set Configuration

Filter Set #      Comments      Filter Set #      Comments
-----
1      NetBIOS_WAN      7      _____
2      NetBIOS_LAN      8      _____
3      TEL_FTP_WAN      9      _____
4      _____      10     _____
5      LRP_SNMP_PING   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=161      N D N
2 Y IP Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=162      N D N
3 Y IP Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=520      N D N
4 Y IP Pr=1, SA=0.0.0.0, DA=0.0.0.0, DP=8      N F N
5 N
6 N

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

```

Menu-21.5.1 (Protokoll-17: UDP / Port- 161: SNMP):

```

Menu 21.5.1 - TCP/IP Filter Rule

Filter #: 5,1
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 #= 161
              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-21.5.2 (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-21.5.4 (Protokoll-1: ICMP / Port- 8: PING):

```
Menu 21.5.4 - TCP/IP Filter Rule

Filter #: 5,4
Filter Type= TCP/IP Filter Rule
Active= Yes
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:
```

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 störende Eigenschaft haben, sollten diese möglichst LAN-Seitig bleiben um keine unnötigen Onlineverbindungen herzustellen (**Call Filter Set**) oder falls eine Verbindung in das Internet besteht (**Output Filter Set**), diese nicht unnötig 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 Set #      Comments      Filter Set #      Comments
-----
1      NetBIOS_WAN      7      _____
2      NetBIOS_LAN      8      _____
3      TEL_FTP_WAN      9      _____
4      _____      10     _____
5      LRP_SNMP_PING  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:
```

Menu21-1.4 (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 erwähnt, nämlich die Funktion **Forward**, **Drop** und **Check Next Rule** in den einzelnen Filter-Sets. **Drop** steht für **Verwerfen**, **Forward** für **Weiterleiten** und **Check next Rule** für **Nächste Regel prüfen**.

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

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

Input Filter Sets:
protocol filters= 3, 5, 1

Da im **Filter-Set-1** die **letzt zu prüfende 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 berücksichtigt und abgearbeitet wird.

Action Matched= Drop
Action Not Matched= Forward

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

Eine Ausnahme bildet eine „absichtlich als Forward“ eingestellte Funktion, um z. B. wie beim ICMP-Filter den PING von aussen zu zulassen und somit zum Router weiterzuleiten. Damit lassen sich Funktionen wie etwa „**LOG= Action Matched**“ für einen Syslog-Client/Programm wie KIWI-Syslog auswerten und anzeigen.

Action Matched= Forward
Action Not Matched= Check Next Rule.

Steht die Regel auf „**Action Matched= Drop**“, wird der PING nicht zugelassen/beantwortet aber die Funktion „**LOG= Action Matched**“ zeigt im Syslog den entsprechenden Versuch an.

Menu-24.10 „Time and Date Setting“

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+0200“ waerend der Sommerzeit vom 31.03. bis 27.10 und in der Winterzeit die Time Zone „GMT+0100“.

Menu-24.10 (Protokoll-6: UDP / Port- 123: NTP (RFC-1305)):

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

Use Time Server when Bootup= NTP (RFC-1305)
Time Server IP 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+0200

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 IP 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

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

UNIX 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
POTS 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-21.5.4 (Protokoll-1: ICMP / Port-8: PING):

```
Menu 21.5.4 - TCP/IP Filter Rule

Filter #: 5,4
Filter Type= TCP/IP Filter Rule
Active= Yes
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:
```

„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 Local 1. Notice Router: t-online.de Router: 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 Local 1. Notice Router: t-online.de Router: 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 Local 1. Notice Router: t-online.de Router: 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/ripenc/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:      Technikerlassung 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)
  Identification     = 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  mmopqrst

  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  efghijklmmopqrst

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 dem Befehl „dev dial 1“ laesst sich ein solcher test manuell durchfuehren.

Beispiel einer fehlschlagenden Internetanwahl-Verbindungen:

```
Router> dev dial 3
Start dialing for node <BckUpISP>...
### Hit any key to continue.###
$$$ DIALING dev=2 ch=0.....
$$$ OUTGOING-CALL phone(010700192070)
$$$ CALL CONNECT speed<64000> type<2> chan<0>
$$$ LCP opened
$$$ CHAP login to remote failed
$$$ LCP closed
$$$ Recv'd TERM-REQ
$$$ Recv'd TERM-ACK state 5
$$$ LCP stopped
Router> exit
```

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

Beispiel einer funktionierenden Internetanwahl-Verbindung:

```
Router> dev dial 3
Start dialing for node <BckUpISP>...
### Hit any key to continue.###
$$$ DIALING dev=2 ch=0.....
$$$ OUTGOING-CALL phone(010700192070)
$$$ CALL CONNECT speed<64000> type<2> chan<0>
$$$ LCP opened
$$$ CHAP login to remote OK
$$$ IPCP negotiation started
$$$ CCP negotiation started
$$$ IPCP opened
Router> exit
```

Kommt es zu einem „\$\$\$ CALL CONNECT“, ist der Zustand einer Leitungsverbindung zwischen Router ueber ISDN-Leitung zum Ziel gegeben.

Kommt die Meldung „\$\$\$ LCP opened“, wurde das Layer-Control-Protocol zum Datenaustausch geoeffnet.

Kommt die Meldung „\$\$\$ CHAP/PAP login to remote OK“, wurden Login/Passwort korrekt 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 gerade bei T-Online einem festen Format unterliegt.

Menu-4 „Internet Access Setup“

```
Menu 4 - Internet Access Setup

ISP' s Name= T-Online
Pri Phone #= 0191011
Sec Phone #=
My Login= 11111111111222222222220001
My Password= *****
My WAN IP Addr= 0.0.0.0

NAT= SUA Only
Address Mapping Set= N/A

Telco Options:
Transfer Type= 64K

Multilink= Off
Idle Timeout= 100

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

Die Angabe „ISP's Name“ dient lediglich zur eigenen Bezeichnung.
Die Angabe „Idle Timeout“ bezieht sich auf die Abwahlzeit bei keinem Traffic.
Der „Transfer Type“ bezieht sich auf „64K“ (Wahl-) oder „Leased“ (Miet-Leitung)
Die „My WAN IP Addr.“ muss auf „0.0.0.0“ eingestellt sein!
Die „Network Address Translation / NAT“ muss auf „SUA Only“ eingestellt sein.

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

Aktuelles Format / neuere Kennungen:

1111111111112222222222220001
111111111111 - Anschlusskennung = 12 Zeichen laenge.
222222222222 - T-Online Nummer = 12 Zeichen laenge.
0001 - Mitbenutzer-Suffix = 4 Zeichen laenge.

Altes Format / aeltere Kennungen:

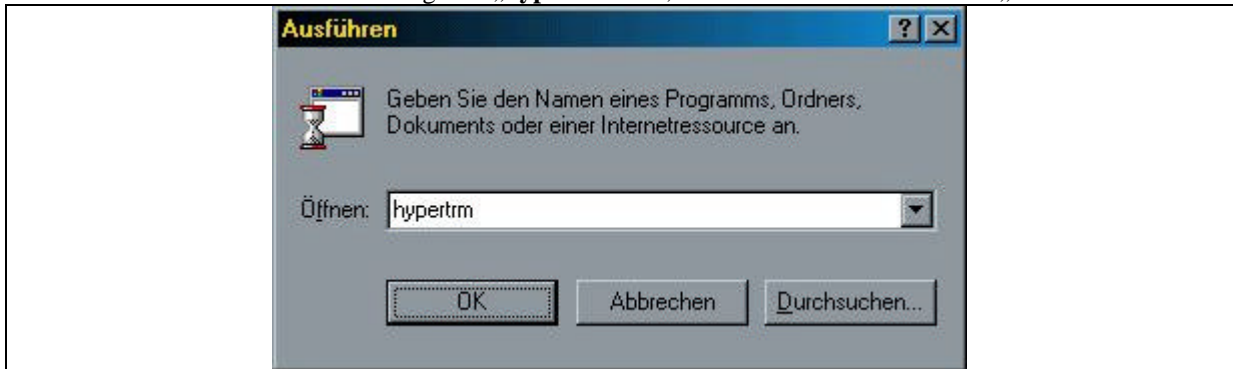
1111111111110123456789#0001
111111111111 - Anschlusskennung = 12 Zeichen laenge.
0123456789 - T-Online Nummer = weniger als 12 Zeichen laenge.
- die Raute (Hash) = zwecks Abgrenzung zum Mitbenutzer-Suffix.
0001 - Mitbenutzer-Suffix = 4 Zeichen laenge.

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...

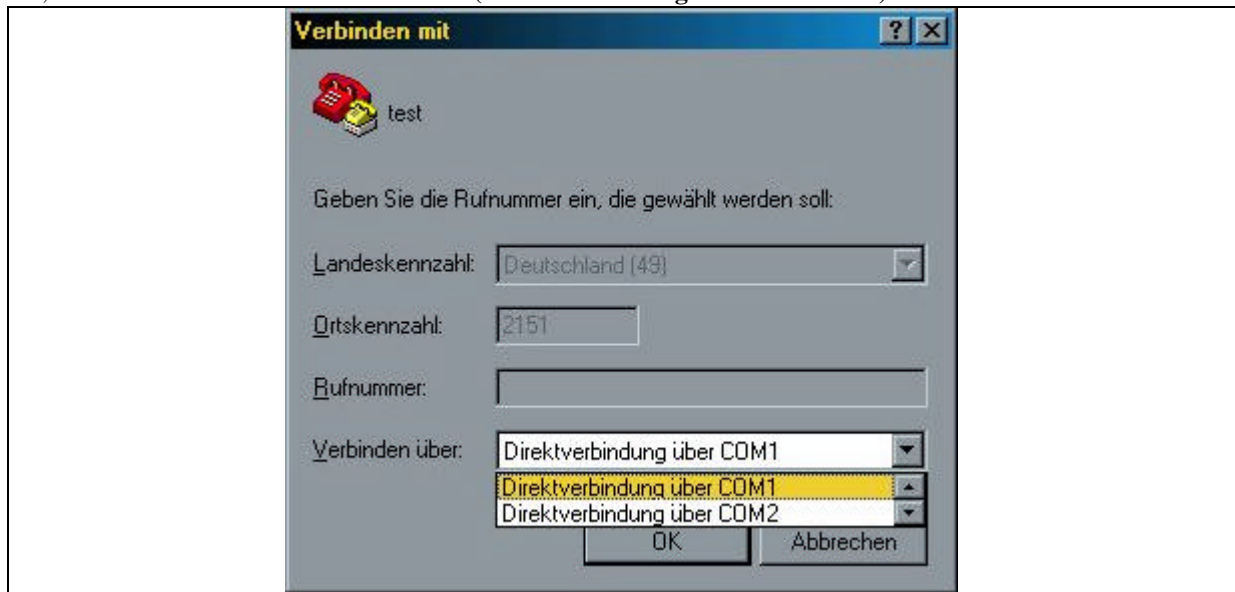
*Klicken Sie auf **Start/Ausführen** und geben „**hypertrm**“ ein, anschliessend klicken Sie auf „**OK**“*



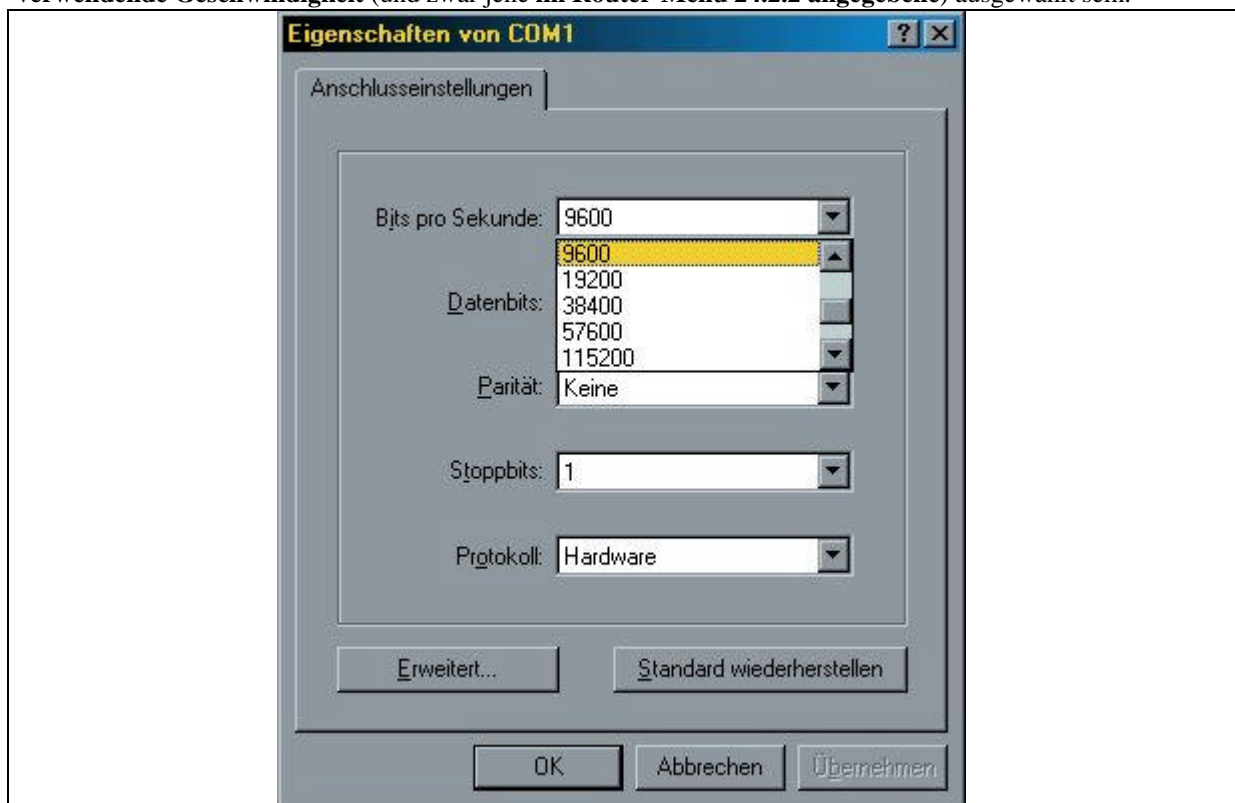
Daraufhin oeffnet sich ein Dialogfenster zur Angabe eines Bezeichnungs-Namens der Terminalverbindung:



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-Menü 24.2.2 angegebene**) ausgewaehlt 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: V1.11 | 7/28/1999 15:02:46
RAM Size = 4096 Kbytes
FLASH: Intel 8M

ZyNOS Version: V2.50(N.04) | 12/26/2001 15:03:08

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 firmware 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-Datei uebertragungsprotokoll die zu sendende *.ROM- (Konfigurations)-Datei
in den Router uebertragen/flaschen)
Starting XMODEM upload (CRC mode)....
C
Total 16384 bytes received.

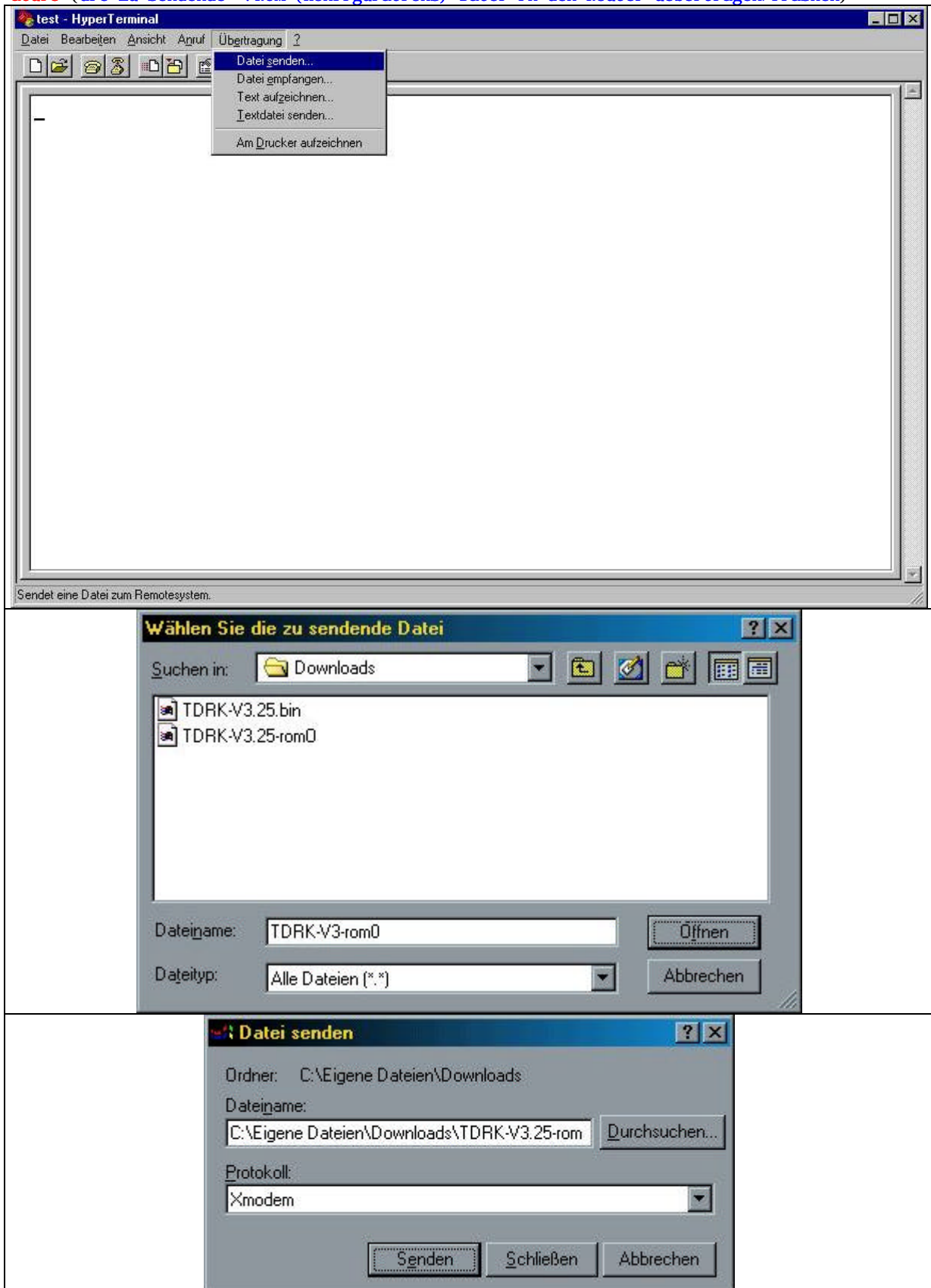
Erasing..
.....
OK
atur (mittels XModem-Datei uebertragungsprotokoll die zu sendende *.BIN- (Firmware)-Datei in den
Router uebertragen/flaschen)
Starting XMODEM upload (CRC mode)....
C
Total 1001472 bytes received.

Erasing.....
.....
.....
.....
OK
System Reboot...
Bootbase Version: V1.11 | 7/28/1999 15:02:46
RAM Size = 4096 Kbytes
FLASH: Intel 8M

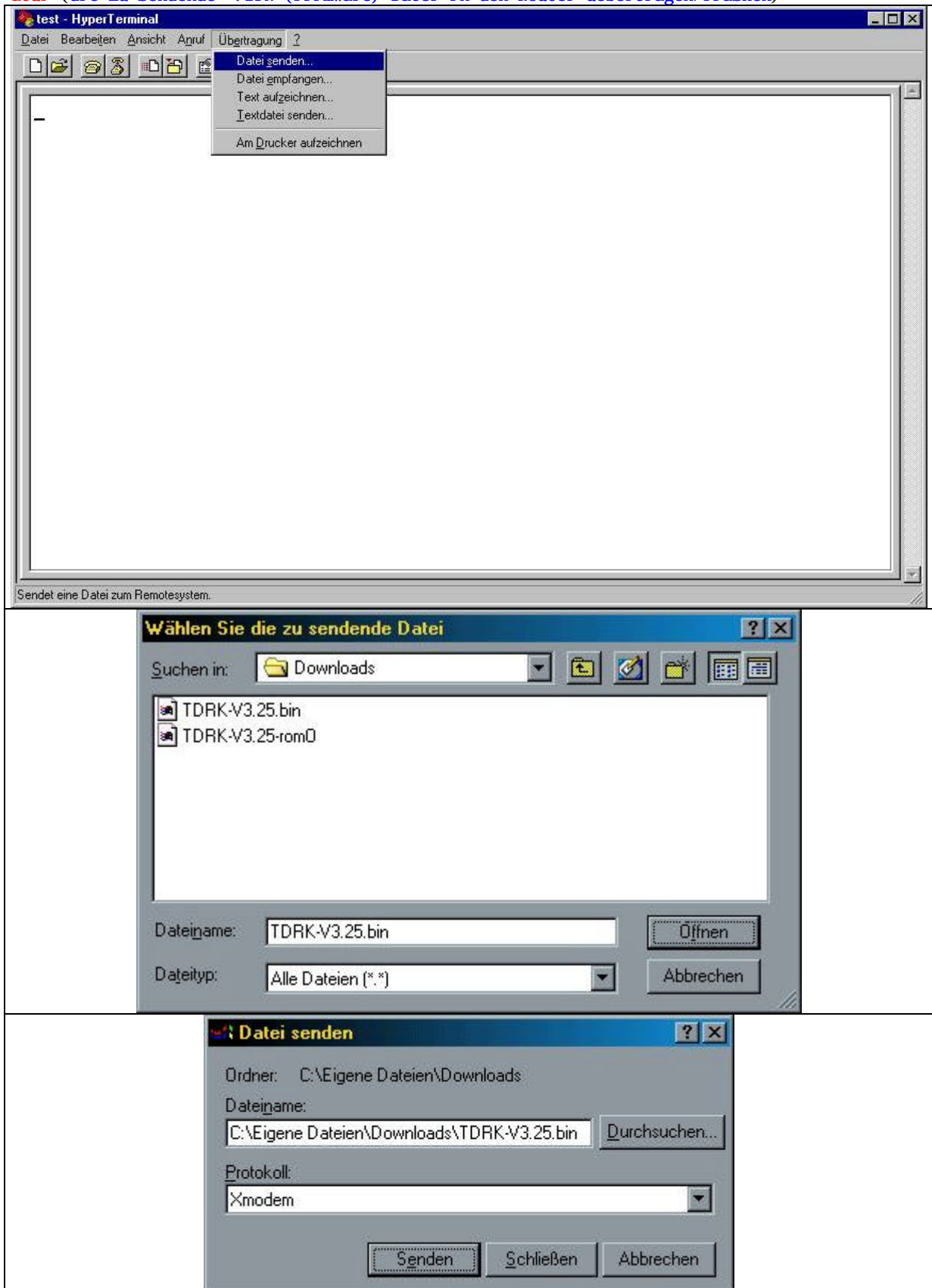
ZyNOS Version: V2.50(N.04) | 12/26/2001 15:03:08

Press any key to enter debug mode within 3 seconds.
.....
Copyright (c) 1994 - 2000 ZyXEL Communications Corp.
Initialize ch =0, ethernet address: 00:a0:c5:23:54:ed
(2) DSS1:
Resetting ISDN .....
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/flaschen)



Menu 2 - ISDN Setup

Switch Type: DSS-1
B Channel Usage= Switch/Switch

Incoming Phone Numbers:
ISDN Data = 28 Subaddress=
A/B Adapter 1 = Subaddress=
A/B Adapter 2 = Subaddress=

Incoming Phone Number Matching= Multiple Subscriber Number (MSN)
Analog Call Routing= N/A
Global Analog Call= N/A

Edit Advanced Setup = No
Edit NetCAPI Setup = No

Press ENTER to Confirm or ESC to Cancel:

Menu 2.1 - ISDN Advanced Setup

Phone 1 Call Waiting= Enable
Phone 2 Call Waiting= Enable
Calling Line Indication= Enable

PABX Outside Line Prefix=
PABX Number (Include S/T Bus Number) for Loopback=

Outgoing Calling Party Number:
ISDN Data = 28
A/B Adapter 1 =
A/B Adapter 2 =

Hangup Silence Time(sec)= 0
Data Link Connection= point-to-multipoint

Press ENTER to Confirm or ESC to Cancel:

Menu 2.2 - NetCAPI Setup

Active= No

Max Number of Registered Users= 5
Incoming Data Call Number Matching= NetCAPI

Access List:

Start IP	End IP	Operation
0.0.0.0	0.0.0.0	None
0.0.0.0	0.0.0.0	None
0.0.0.0	0.0.0.0	None
0.0.0.0	0.0.0.0	None
0.0.0.0	0.0.0.0	None
0.0.0.0	0.0.0.0	None
0.0.0.0	0.0.0.0	None
0.0.0.0	0.0.0.0	None
0.0.0.0	0.0.0.0	None
default		Both

Press ENTER to Confirm or ESC to Cancel:

Menu 11 - Remote Node Setup

1. - ChangeMe (ISP, NAT)
2. - BckupISP (NAT)
3. - LAN-LAN
4. - LAN-RAS (NAT)
5. _____
6. _____
7. _____
8. _____

Enter Node # to Edit:

Menu 11.1 - Remote Node Profile

Rem Node Name= BckupISP
Active= No
Call Direction= Outgoing

Edit PPP Options= No
Rem IP Addr= 1.1.1.1
Edit IP= No

Incoming:

Rem Login= N/A
Rem Password= N/A
Rem CLID= N/A
Call Back= N/A

Telco Option:

Transfer Type= 64K
Allocated Budget(min)=
Period(hr)=
Schedules=

Outgoing:

My Login= arcort
My Password= internet
Authen= CHAP/PAP
Pri Phone #= 0010700192070
Sec Phone #= 00101901929

Carrier Access Code=
Nailed-Up Connection= No
Toll Period(sec)= 0

Session Options:

Edit Filter Sets= No
Idle Timeout(sec)= 60

Press ENTER to Confirm or ESC to Cancel:

Menu 11.2 - Remote Node PPP Options

Encapsulation= Standard PPP
Compression= Yes
BACP= Enable

Multiple Link Options:

BOD Calculation= Transmit or Receive
Base Trans Rate(Kbps)= 64
Max Trans Rate(Kbps)= 128
Target Utility(Kbps)= 48-52

Add Persist(sec)= 180
Subtract Persist(sec)= 15

Press ENTER to Confirm or ESC to Cancel:

Menu 11.3 - Remote Node Network Layer Options

Rem IP Addr: 1.1.1.1
Rem Subnet Mask= 0.0.0.0
My WAN Addr= 0.0.0.0

NAT= SUA Only
Address Mapping Set= N/A

Metric= 2
Private= Yes
RIP Direction= None
Version= RIP-1

Press ENTER to Confirm or ESC to Cancel:

Menu 11.5 - Remote Node Filter

Input Filter Sets:
protocol filters= 3, 5, 1
device filters=

Output Filter Sets:
protocol filters= 1
device filters=

Call Filter Sets:
protocol filters= 1
device filters=

Press ENTER to Confirm or ESC to Cancel:

Menu 11 - Remote Node Setup

1. - ChangeMe (ISP, NAT)
2. - BckupISP (NAT)
3. - LAN-LAN
4. - LAN-RAS (NAT)
5. _____
6. _____
7. _____
8. _____

Enter Node # to Edit:

Menu 11.1 - Remote Node Profile

Rem Node Name= LAN-LAN
Active= No
Call Direction= Both

Edit PPP Options= No
Rem IP Addr= 192.168.2.0
Edit IP= No

Incoming:

Rem Login= test
Rem Password= test
Rem CLID=
Call Back= No

Telco Option:

Transfer Type= 64K
Allocated Budget(min)=
Period(hr)=
Schedules=
Carrier Access Code=
Nailed-Up Connection= N/A
Toll Period(sec)= 0

Outgoing:

My Login= test
My Password= test
Authen= CHAP/PAP
Pri Phone #= 38
Sec Phone #=

Session Options:

Edit Filter Sets= No
Idle Timeout(sec)= 60

Press ENTER to Confirm or ESC to Cancel:

Menu 11.5 - Remote Node Filter

Input Filter Sets:
 protocol filters=
 device filters=
Output Filter Sets:
 protocol filters=
 device filters=
Call Filter Sets:
 protocol filters=
 device filters=

Press ENTER to Confirm or ESC to Cancel:

Menu 11.3 - Remote Node Network Layer Options

Rem IP Addr: 192.168.2.0
Rem Subnet Mask= 255.255.255.0
My WAN Addr= 0.0.0.0

NAT= None
Address Mapping Set= N/A

Metric= 2
Private= No
RIP Direction= None
Version= RIP-1

Press ENTER to Confirm or ESC to Cancel:

Menu 11.2 - Remote Node PPP Options

Encapsulation= Standard PPP
Compression= Yes
BACP= Enable

Multiple Link Options:
BOD Calculation= Transmit or Receive
Base Trans Rate(Kbps)= 64
Max Trans Rate(Kbps)= 128
Target Utility(Kbps)= 32-48

Add Persist(sec)= 60
Subtract Persist(sec)= 10

Press ENTER to Confirm or ESC to Cancel:

Menu 11 - Remote Node Setup

1. - ChangeMe (ISP, NAT)
2. - BckupISP (NAT)
3. - LAN- LAN
4. - LAN- RAS (NAT)
5. _____
6. _____
7. _____
8. _____

Enter Node # to Edit:

Menu 11.1 - Remote Node Profile

Rem Node Name= LAN- RAS
Active= No
Call Direction= Outgoing

Edit PPP Options= No
Rem IP Addr= 192.168.55.1
Edit IP= No

Incoming:
Rem Login= N/A
Rem Password= N/A
Rem CLID= N/A
Call Back= N/A
Outgoing:
My Login= test
My Password= *****
Authen= CHAP/PAP
Pri Phone #= 21
Sec Phone #=

Telco Option:
Transfer Type= 64K
Allocated Budget(min)=
Period(hr)=
Schedules=
Carrier Access Code=
Nailed-Up Connection= No
Toll Period(sec)= 0
Session Options:
Edit Filter Sets= No
Idle Timeout(sec)= 60

Press ENTER to Confirm or ESC to Cancel:

Menu 11.5 - Remote Node Filter

Input Filter Sets:
 protocol filters=
 device filters=
Output Filter Sets:
 protocol filters=
 device filters=
Call Filter Sets:
 protocol filters=
 device filters=

Press ENTER to Confirm or ESC to Cancel:

Menu 11.3 - Remote Node Network Layer Options

Rem IP Addr: 192.168.55.1
Rem Subnet Mask= 255.255.255.0
My WAN Addr= 192.168.55.2

NAT= SUA Only
 Address Mapping Set= N/A

Metric= 2
Private= Yes
RIP Direction= None
 Version= RIP-1

Press ENTER to Confirm or ESC to Cancel:

Menu 11.2 - Remote Node PPP Options

Encapsulation= Standard PPP
Compression= Yes
BACP= Enable

Multiple Link Options:
 BOD Calculation= Transmit or Receive
 Base Trans Rate(Kbps)= 64
 Max Trans Rate(Kbps)= 128
 Target Utility(Kbps)= 32-48

 Add Persist(sec)= 60
 Subtract Persist(sec)= 10

Press ENTER to Confirm or ESC to Cancel:

Menu 13 - Default Dial-in Setup

Telco Options:

CLID Authen= Preferred

PPP Options:

Recv Authen= CHAP/PAP

Compression= Yes

Mutual Authen= No

O/G Username=

O/G Password= *****

Multiple Link Options:

Max Trans Rate(Kbps)= 128

Callback Budget Management:

Allocated Budget(mi n)=

Period(hr)=

IP Address Supplied By:

Dial-in User= Yes

IP Pool= Yes

IP Start Addr= 192. 168. 1. 31

IP Count(1, 2)= 2

Session Options:

Edit Filter Sets= No

Press ENTER to Confirm or ESC to Cancel:

Menu 13.1 - Default Dial-in Filter

Input Filter Sets:

protocol filters=

device filters=

Output Filter Sets:

protocol filters=

device filters=

Press ENTER to Confirm or ESC to Cancel:

Menu 14 - Dial-in User Setup

1. -gast
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____

Enter Menu Selection Number:

Menu 14.1 - Edit Dial-in User

User Name= gast
Active= No
Password= *****
Callback= No
 Phone # Supplied by Caller= N/A
 Callback Phone #= N/A
Rem CLID=
Idle Timeout= 300

Press ENTER to Confirm or ESC to Cancel:

Menu 22 - SNMP Configuration

SNMP:
Get Community= public
Set Community= public
Trusted Host= 0.0.0.0
Trap:
 Community= public
 Destination= 192.168.1.33

Press ENTER to Confirm or ESC to Cancel: