

**Siemensstraße 18  
84051 Essenbach**

Tel +49 8703 929-00  
Fax +49 8703 929-201  
Web [www.tdt.de](http://www.tdt.de)  
E-Mail [support@tdt.de](mailto:support@tdt.de)

**C1500 – Serie  
C1550 – Serie  
C2000 – Serie  
M3000 – Serie  
G5000 – Serie  
L3000 – L5000**

DocID: Handbuch C-, M-, G-, L-Serie

Rev.: 9.20.0 – 12.06.2017 – SH

# Handbuch für C-, M-, G- und L-Serie

---

## Impressum

---

### Haftung

Die Zusammenstellung von Texten und Abbildungen für das Manual erfolgte mit größter Sorgfalt. Dennoch können Fehler nicht vollständig ausgeschlossen werden. Der Herausgeber übernimmt für fehlerhafte Angaben und deren Folge keinerlei Haftung. Änderungen an der Dokumentation und den darin beschriebenen Produkten bleiben jederzeit und ohne vorherige Ankündigung vorbehalten.

### Ansprechpartner

Als Ansprechpartner bei Problemen oder Fragen zu dieser Dokumentation steht Ihnen das TDT Expert Support Team gerne zur Verfügung.

### Copyright

TDT GmbH  
Siemensstraße 18  
84051 Essenbach

Tel.: +49 (8703) 929-00  
Fax: +49 (8703) 929-201  
Web: [www.tdt.de](http://www.tdt.de)  
Email: [support@tdt.de](mailto:support@tdt.de)

Viel Spaß und Erfolg wünscht Ihnen

**Ihr TDT Team**



# Inhaltsverzeichnis

---

<b>Impressum</b>	<b>2</b>
<b>Inhaltsverzeichnis</b>	<b>3</b>
<b>1 Erste Schritte</b>	<b>10</b>
1.1 Inbetriebnahme	10
1.2 Packungsinhalt	10
1.2.1 C1500 / C1550	10
1.2.2 C2000	10
1.2.3 M3000 / L3000	10
1.2.4 G5000 / L5000	11
1.3 Gerätebeschreibung mit Portbelegung	11
1.3.1 C1500, C1550 und C2000	11
1.3.1.1 Vorderseite C-Serie	11
1.3.1.1.1 Standard Konfiguration der LED's	12
1.3.1.1.2 C1500h/C1500l	12
1.3.1.1.3 C1500hw/C1500lw	12
1.3.1.1.4 C1550 und C2000	13
1.3.1.2 Rückseite C-Serie	14
1.3.2 M3000	15
1.3.2.1 Vorderseite	15
1.3.2.2 Rückseite	15
1.3.3 G5000	16
1.3.3.1 Vorderseite	16
1.3.3.2 Rückseite	17
1.3.4 Seriennummer	17
1.4 Zugangsdaten	18
1.5 Wie verbinde ich mich auf den Router?	19
1.5.1 Webinterface	19
1.5.2 Command Line Interface (CLI)	20
1.5.3 Serielle Verbindung mit einem PC	20
<b>2 Das Webinterface</b>	<b>23</b>
<b>3 Das Command Line Interface, die CLI</b>	<b>24</b>
<b>4 Systemverwaltung</b>	<b>25</b>
4.1 Bootup and Shutdown	25
4.2 Configuration Handling	25
4.3 Event-Handler	25
4.3.1 Event-Handler	25

4.3.1.1	<i>Health Checker</i>	26
4.3.1.2	<i>ICPM Checker</i>	26
4.3.1.3	<i>Beispielscript</i>	26
4.3.2	SMS-Handler	27
4.3.2.1	<i>Unterstützte Statusbefehle</i>	28
4.4	Firmware Update	29
4.5	LED Assignment (nur C-Serie)	29
4.5.1	Ethernet	29
4.5.2	WLAN	29
4.5.3	PPP und WWAN Schnittstellen	30
4.5.4	GSM Options	30
4.5.5	Connection Manager	31
4.5.6	IPSec Tunnel	31
4.5.7	Zertifikat	31
4.5.8	SIM Card	31
4.5.1	Blinkfrequenzen	31
4.6	Push Button Settings	32
4.6.1	Push Button Actions	32
4.6.2	Push Button Assignments	32
4.7	Scheduled Cron Jobs	33
4.7.1	Create a new scheduled cron job	33
4.7.2	Create a new environment variable	34
4.7.3	Control user access to cron jobs	34
4.8	System Time	34
4.9	Time Synchronisation	34
4.10	Webmin Configuration	35
4.10.1	IP Access Control	35
4.10.2	Port and Address	35
4.10.3	Logging	35
4.10.4	Language	36
4.10.5	Authentication	36
4.11	Webmin Users	37
<b>5</b>	<b>Netzwerkkonfiguration</b>	<b>38</b>
5.1	BIND DNS Server (nur M3000, G5000)	38
5.2	Certificate Management	38
5.2.1	Import-PKCS#12	39
5.3	Connection Management	39
5.3.1	Connection-Manager	39
5.3.1.1	<i>Connection-Dial-Entry</i>	39
5.3.1.1.1	<i>Inhibit</i>	40
5.3.1.1.2	<i>Interface- und Ping-Checker</i>	40
5.3.1.1.3	<i>Verbindungsübersicht</i>	40
5.3.1.1.4	<i>Add Connection (Connection-Dial-Entry Parameter)</i>	41
5.3.1.2	<i>Logical Subordinated Connections</i>	44
5.3.1.2.1	<i>Inhibit</i>	45

5.3.1.2.2	<i>Logical-Interface- und Ping-Checker</i>	45
5.3.1.2.3	<i>Add Connection (Connection-Logical-Entry Parameter)</i>	45
5.3.2	Static Connections	46
5.4	DHCP Server	46
5.5	DNS Server Update	47
5.6	DNSmasq	48
5.7	Dynamic DNS Update	48
5.8	IPSec VPN	49
5.8.1	Kommandozeilenbefehle (SSH)	49
5.9	L2TP	50
5.10	Linux Firewall (IPtables)	51
5.10.1	Tabellen (Tables)	51
5.10.2	Ketten (Chains)	52
5.10.3	Ziele (Targets)	53
5.10.4	Das Linux Firewall Menü	53
5.10.5	Erstellen einer neuen Regel	54
5.10.5.1	<i>Chain and action details</i>	54
5.10.5.2	<i>Condition details</i>	55
5.10.6	Beispiel: IP Forwarding einrichten	57
5.11	Network Configuration	58
5.11.1	Network Interfaces	58
5.11.1.1	<i>Bridge Settings</i>	59
5.11.1.2	<i>Tunnel Settings</i>	59
5.11.2	Routing and Gateways	60
5.11.3	DNS Client	61
5.11.4	Host Addresses	62
5.12	OpenVPN	62
5.12.1	Add new server/client	62
5.12.2	Edit existing peer	63
5.13	PPP	65
5.13.1	PPP Interfaces	65
5.13.1.1	<i>Basic PPP parameters for interface ppp#</i>	66
5.13.1.1.1	<i>ISDN PPP Interface Parameter</i>	66
5.13.1.1.2	<i>ISDN Dial-In PPP Interface Parameter</i>	67
5.13.1.1.3	<i>PPPoE Interface Parameter</i>	67
5.13.1.2	<i>Advanced PPP parameters for interface ppp#</i>	67
5.13.1.2.1	<i>ISDN PPP Interface Parameter</i>	68
5.13.1.2.2	<i>ISDN Dial-In PPP Interface Parameter</i>	68
5.13.1.2.3	<i>PPPoE interface Parameter</i>	68
5.13.1.2.4	<i>Globale Einstellungen</i>	69
5.13.1.2.5	<i>Logging Parameters</i>	69
5.13.1.2.6	<i>Networking Parameters</i>	70
5.13.1.2.7	<i>Authentication Parameters</i>	70
5.13.1.2.8	<i>Compression Parameters</i>	71
5.13.1.3	<i>Parameters for interface pppX when used in Static Connections</i>	71
5.13.2	PPP Accounts	72
5.13.2.1	<i>Create new PPP CHAP/PAP account</i>	72

5.14	Postfix Configuration (nur M3000, G5000)	72
5.15	QoS Control	73
5.15.1	Outgoing Interfaces	73
5.15.1.1	<i>Interface parameters</i>	73
5.15.1.2	<i>Root Qdisc Parameters</i>	73
5.15.1.2.1	<i>TBF (Token Bucket Filter)</i>	73
5.15.1.2.2	<i>SFQ (Stochastic Fairness Queueing)</i>	74
5.15.1.2.3	<i>BFIFO (Bytes First In First Out)</i>	74
5.15.1.2.4	<i>PFIFO Packet First In First Out</i>	74
5.15.1.2.5	<i>DSMARK</i>	75
5.15.1.2.6	<i>HTB (Hierarchical Token Bucket)</i>	75
5.15.1.2.7	<i>PRIQ (Filter)</i>	75
5.15.1.2.8	<i>PRIQ (Priomap)</i>	75
5.15.2	Incoming Interfaces	75
5.15.2.1	<i>Interface parameters</i>	75
5.15.3	Interface Statistics	76
5.16	SNMP	76
5.16.1	Access Control	76
5.16.2	Sysinfo Setup	77
5.16.3	Trap Control	77
5.16.3.1	<i>SNMP Create New Trap Control</i>	77
5.16.4	(Sub)Agent Configurations	77
5.16.4.1	<i>Common Settings</i>	77
5.16.4.2	<i>Monitor Running Processes</i>	78
5.16.4.2.1	<i>SNMP Agent Create Process Monitor</i>	78
5.16.4.3	<i>Monitor Disk Space</i>	78
5.16.4.4	<i>Monitor File Sizes</i>	78
5.16.4.5	<i>Monitor Load Average</i>	79
5.17	SSH Server	79
5.17.1	Authentication	79
5.17.2	Networking	80
5.17.3	Access Control	80
5.17.4	Miscellaneous Options	81
5.17.5	Client Host Options	81
5.17.6	User SSH Key Setup	82
5.18	SSL Tunnels	82
5.19	VRRP / Loadbalancer *	83
5.19.1	Funktionsweise VRRP	83
5.19.1.1	<i>Verhalten des VRRP-Routers im Backup-Zustand</i>	83
5.19.1.2	<i>Verhalten des VRRP-Routers im Master-Zustand</i>	84
5.19.2	Global Definitions	84
5.19.3	VRRP Instances	84
5.19.3.1	<i>Add VRRP Instance</i>	84
5.19.4	VRRP Synchronization Groups	86
5.19.4.1	<i>VRRP Create New Sync. Group</i>	86
5.19.5	Load Balancer Global Settings	86
5.19.6	Load Balancer Real Servers	87
5.19.7	Load Balancer Virtual Servers	88

5.20	WLAN	90
5.20.1	General settings	90
5.20.2	WPA/WPA2-PSK related settings	90
5.20.3	N-Standard settings (High Throughput Capabilities)	91
5.20.4	Advanced settings	91
5.20.5	WEP related settings	92
5.20.6	WPA/WPA2-EAP related settings	92
5.20.6.1	<i>Radius client configuration</i>	92
5.20.6.2	<i>Internal EAP server configuration</i>	93
5.20.6.2.1	<i>EAP User Einstellungen</i>	93
5.20.7	MAC Address Filtering	93
5.21	WWAN	94
5.21.1	Global	94
5.21.2	SIM1/2 Parameters	94
<b>6</b>	<b>Das Diagnose Menü</b>	<b>96</b>
6.1	Connection Manager	96
6.2	Distribution Information	96
6.3	GSM Modem State	96
6.4	IPSec VPN	96
6.5	Load Balancer	97
6.5.1	Load Balancer Statistics	97
6.5.2	Load Balancer Connections	97
6.6	Log File Rotation	97
6.7	PPP	97
6.8	Running Processes	98
6.9	System Information	98
6.10	System Logs	98
6.10.1	Logausgabe über eine SSH Verbindung	99
6.11	Webmin Actions Log	99
<b>7</b>	<b>Das Permanent Save Menü</b>	<b>100</b>
7.1	Save Config	100
7.2	Save System to USB (nur bei M- und G-Serie)	100
<b>8</b>	<b>Konfiguration sichern und wiederherstellen</b>	<b>101</b>
8.1	Konfiguration sichern	101
8.1.1	Webinterface	101
8.1.2	CLI	102
8.2	Konfiguration wiederherstellen	102
8.2.1	Webinterface	102
8.2.2	CLI	103
<b>9</b>	<b>Wiederherstellung des Auslieferungszustandes</b>	<b>104</b>
9.1	C-Serie	104

9.2	M3000 / G5000 / L-Serie	104
<b>10</b>	<b>Firmware Update</b>	<b>105</b>
10.1	Webinterface	105
10.2	CLI	106
<b>11</b>	<b>Das TDT_SupportInfo Skript</b>	<b>107</b>
<b>12</b>	<b>CLI Befehlsreferenz</b>	<b>108</b>
12.1	Hauptmenü - TDT(CLI)	108
12.1.1	Konfigurationsmenü - TDT(CLI/configuration)	109
12.1.1.1	Netzwerkmenü - TDT(CLI/configuration/network)	109
12.1.1.1.1	Interface-Menü - TDT(CLI/configuration/network/interface)	109
12.1.1.1.2	Connection-Manager - TDT(CLI/configuration/network/dialup)	114
12.1.1.1.3	SNMP Einstellungen - TDT(CLI/configuration/network/snmp)	118
12.1.1.1.4	NTP Einstellungen - TDT(CLI/configuration/network/ntp)	120
12.1.1.2	Allgemeine Einstellungen - TDT(CLI/configuration/general)	121
12.1.2	Statusmenü - TDT(CLI/status)	122
12.1.2.1	Show-Menü - TDT(CLI/status/show)	122
<b>13</b>	<b>Hardware</b>	<b>123</b>
13.1	C-Serie	123
13.1.1	Technische Daten	123
13.1.1.1	C1500xx	123
13.1.1.2	C1550xxx	123
13.1.1.3	ELW Router C1550lw	124
13.1.2	Hardware Module	124
13.1.3	DB9 / RS232 PIN- Belegung (DTE/V.24)	125
13.2	M3000	125
13.2.1	Unterstützte UMTS / GPRS Karten	125
13.2.2	Belegung des DSL/ISDN Y-Kabels	126
13.2.3	Ethernet 4 Port Karte	126
13.2.3.1	Pin Belegung der RJ45 PRI Stecker	127
<b>14</b>	<b>Wichtige Daten im Überblick</b>	<b>128</b>
14.1	C-, M-, G-, und L-Serie Standard	128
14.1.1	Passwort ändern	129
14.1.1.1	Webinterface	129
14.1.1.2	Kommandozeilen-Benutzer <b>root</b>	129
14.1.2	Arbeitsumgebung	130
14.1.3	Konformitätserklärung	130
14.2	Systemspezifische Daten	130
14.2.1	C-Router mit Mobilfunkmodul	130
14.2.1.1	GPS	131
14.2.1.1.1	GPS Daten auslesen	132
14.2.1.1.2	GPS Daten senden	132
14.2.2	C-Router mit WLAN	132
14.3	Software	132

---

<b>15 Link Übersicht</b>	<b>134</b>
15.1 Allgemeine Links	134
15.2 Wichtige Informationen	134
15.3 Empfohlene Software	134
15.4 Weiterführende Links	134

---

# 1 Erste Schritte

---

## 1.1 Inbetriebnahme

Öffnen Sie die Transportverpackung vorsichtig und kontrollieren Sie den Packungsinhalt.

Schließen Sie das gelieferte Gerät unter Verwendung des mitgelieferten Netzteils/Kaltgerätekabels an die 230V Spannungsversorgung an.

Verbinden Sie nun ihr Netzwerk mit dem mitgelieferten CAT5 Netzwerkkabel mit dem **eth1** Port des Routers.

### Hinweis

- Bitte beachten Sie, dass Sie den Router ca. 1 Stunde vor Inbetriebnahme aus der Verpackung nehmen und auf Raumtemperatur bringen müssen, um Beschädigungen durch Kondenswasser auszuschließen.
- Durch den Transport können sich verbaute Steckkarten aus den Steckplätzen lösen. Überprüfen Sie bitte den Ordnungsgemäßen Zustand der Karten, bevor Sie das Gerät in Betrieb nehmen.

## 1.2 Packungsinhalt

### 1.2.1 C1500 / C1550

- ◊ C1500 bzw. C1550
- ◊ Netzteil (12V DC / 1,8 A) mit Eurostecker
- ◊ CAT5 LAN Kabel
- ◊ Je nach Version zugehörige Antennen
- ◊ Handbuch auf USB-Stick

### 1.2.2 C2000

- ◊ C2000
- ◊ Kaltgerätekabel
- ◊ CAT5 LAN Kabel
- ◊ Je nach Version zugehörige Antennen
- ◊ Handbuch auf USB-Stick

### 1.2.3 M3000 / L3000

- ◊ M3000
- ◊ Kaltgerätekabel
- ◊ CAT5 LAN Kabel
- ◊ Je nach Version ein ISDN/DSL Kabel
- ◊ 1 USB Init-Stick (zum Zurücksetzen des Gerätes)
- ◊ Handbuch auf USB-Stick

## 1.2.4 G5000 / L5000

- ◊ G5000
- ◊ Kaltgerätekabel
- ◊ CAT5 LAN Kabel
- ◊ Je nach Hardwarekonfiguration zugehörige Kabel (z.B. Seriell, ISDN, usw.)
- ◊ 1 USB Init-Stick (zum Zurücksetzen des Gerätes)
- ◊ Handbuch auf USB-Stick

## 1.3 Gerätebeschreibung mit Portbelegung

### 1.3.1 C1500, C1550 und C2000

#### 1.3.1.1 Vorderseite C-Serie

Auf der Front des C1500 befinden sich drei LED Anzeigen zur Statusanzeige, C1550 und C2000 sind mit acht zusätzlichen Status LED's ausgestattet. Zudem sind auf der Vorderseite der Geräte ein Reset-Button und ein SIM Slot zu finden.



Abbildung 1: Vorderseite C1500

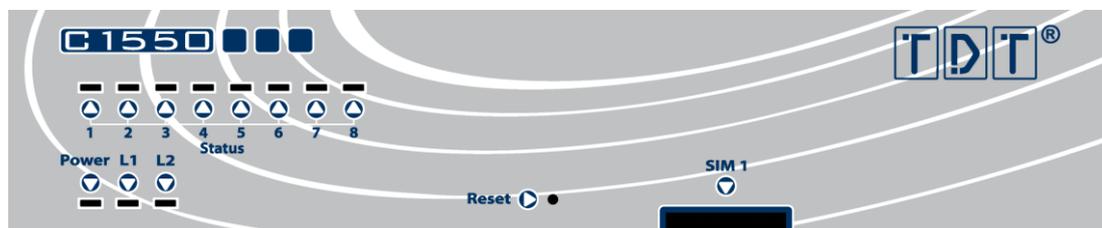


Abbildung 2: Vorderseite C1550

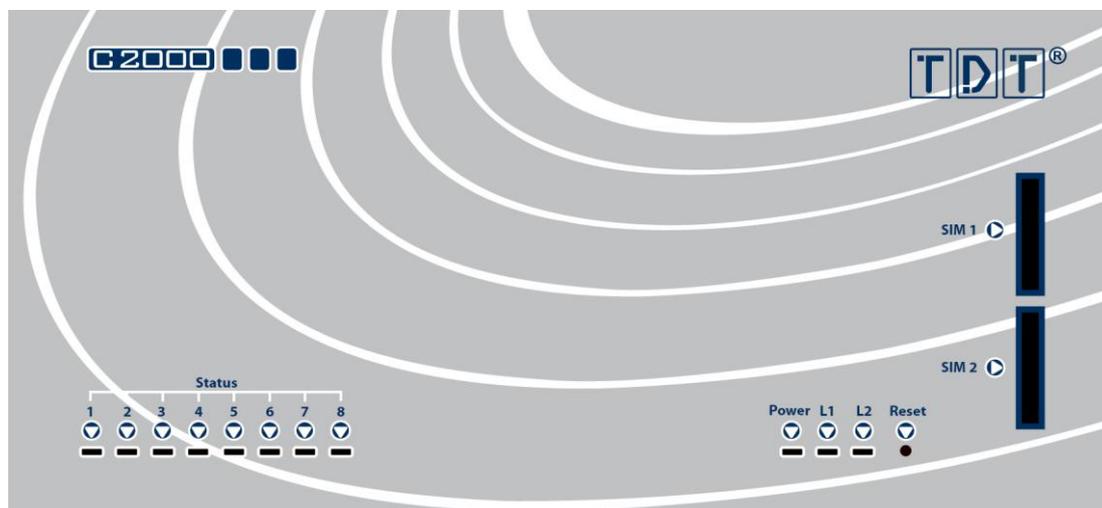


Abbildung 3: Vorderseite C2000

	Beschreibung
<b>Power - L2</b>	LED's zur Statusanzeige
<b>Status 1 - 8</b>	Zusätzliche LED's bei C1550 und C2000 zur Statusanzeige
<b>Reset-Button</b>	Funktion siehe Kapitel <a href="#">9.1</a>
<b>SIM 1</b>	SIM-Kartenslot für SIM1
<b>SIM 2</b>	SIM-Kartenslot für SIM2, nur bei C2000

### 1.3.1.1.1 Standard Konfiguration der LED's

Die LEDs der C-Serie Router sind frei konfigurierbar (siehe [4.5 LED Assignment \(nur C-Serie\)](#)). Einzig die Power LED ist fest belegt. Abhängig von Router/Ausstattung sind die LEDs von Werk ab vorkonfiguriert.

LED	Status	Beschreibung
<b>Power</b>	<b>aus:</b>	Gerät ist stromlos / ausgeschaltet
	<b>an:</b>	Router ist in Betrieb
	<b>langsam blinken:</b>	Bootvorgang
	<b>schnell blinken:</b>	Remote Access über SSH aktiv

### 1.3.1.1.2 C1500h/C1500l

LED	Wert	Status	Beschreibung
<b>L1</b>	<b>PPP3_UP_DOWN_DATA</b>	<b>aus:</b>	PPP3 Link down
		<b>an:</b>	PPP3 Link up
		<b>blinken:</b>	Datentransfer an PPPn (RX + TX)
<b>L2</b>	<b>WWAN0_UP_DOWN_DATA</b> Entspricht Mobilfunk	<b>aus:</b>	WWAN0 Link down
		<b>an:</b>	WWAN0 Link up
		<b>blinken:</b>	Datentransfer an /WWAN0 (RX + TX)

### 1.3.1.1.3 C1500hw/C1500lw

LED	Wert	Status	Beschreibung
<b>L1</b>	<b>WLAN0_ON_OFF_CONNECT</b>	<b>aus:</b>	WLAN0 inaktiv
		<b>an:</b>	WLAN0 aktiv
		<b>blinken:</b>	Ein oder mehr aktive Verbindungen
<b>L2</b>	<b>WWAN0_UP_DOWN_DATA</b> Entspricht Mobilfunk	<b>aus:</b>	WWAN0 Link down
		<b>an:</b>	WWAN0 Link up
		<b>blinken:</b>	Datentransfer an /WWAN0 (RX + TX)

### 1.3.1.1.4 C1550 und C2000

LED	Wert	Status	Beschreibung
L1	<b>WLAN0_ON_OFF_CONNECT</b>	aus:	WLAN0 inaktiv
		an:	WLAN0 aktiv
		blinken:	Mindestens eine aktive Verbindung
L2	<b>ETH0_UP_DOWN_DATA</b>	aus:	ETH0 Link down
		an:	ETH0 Link up
		langsam blinken:	Datentransfer an ETH0 (RX + TX)

LED	Wert	Status	Beschreibung
Status 1	<b>WWAN0_UP_DOWN_DATA</b> Entspricht Mobilfunk	aus:	WWAN0 Link down
		an:	WWAN0 Link up
		blinken:	Datentransfer an WWAN0 (RX + TX)
Status 2	<b>PPP2_UP_DOWN_DATA</b>	aus:	PPP2 Link down
		an:	PPP2 Link up
		blinken:	Datentransfer an PPP2 (RX + TX)
Status 3	<b>PPP3_UP_DOWN_DATA</b> Entspricht DSL	aus:	PPP3 Link down
		an:	PPP3 Link up
		blinken:	Datentransfer an PPP3 (RX + TX)
Status 4	<b>ACTIVE_SIM_CARD</b>	aus:	Keine SIM in Verwendung
		an:	SIM1 wird verwendet
		blinken:	SIM2 wird verwendet
Status 5	<b>GSM0_CONNECT_STATUS</b>	aus:	Keine Verbindung
		langsam blinken:	2G Signal (GPRS oder EDGE)
		schnell blinken:	3G Signal (UMTS/WCDMA oder HSPA)
		an:	4G Signal (LTE)
Status 6	<b>GSM0_SIGNAL1</b>	aus:	Kein Empfang (0%)
		an:	Signalqualität 1% - 33%
Status 7	<b>GSM0_SIGNAL2</b>	an:	Signalqualität 34% - 66%
Status 8	<b>GSM0_SIGNAL3</b>	an:	Signalqualität 67% - 100%

### 1.3.1.2 Rückseite C-Serie

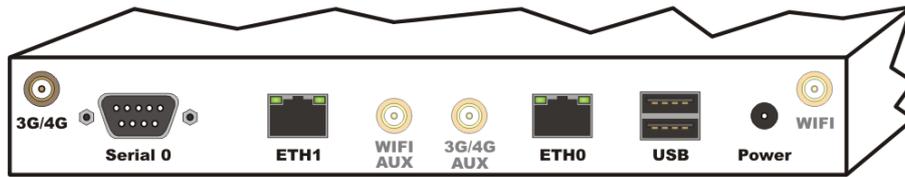


Abbildung 4: Rückseite C1500

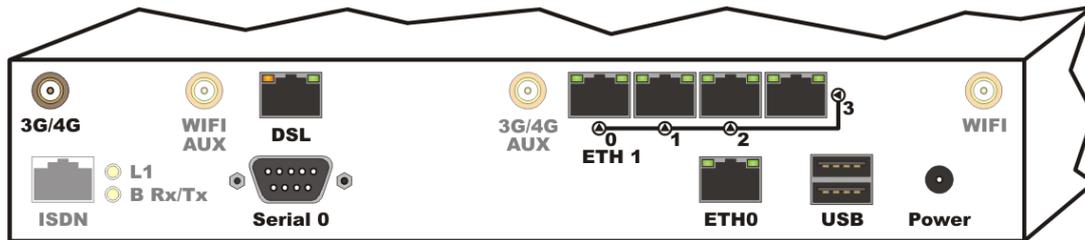


Abbildung 5: Rückseite C1550

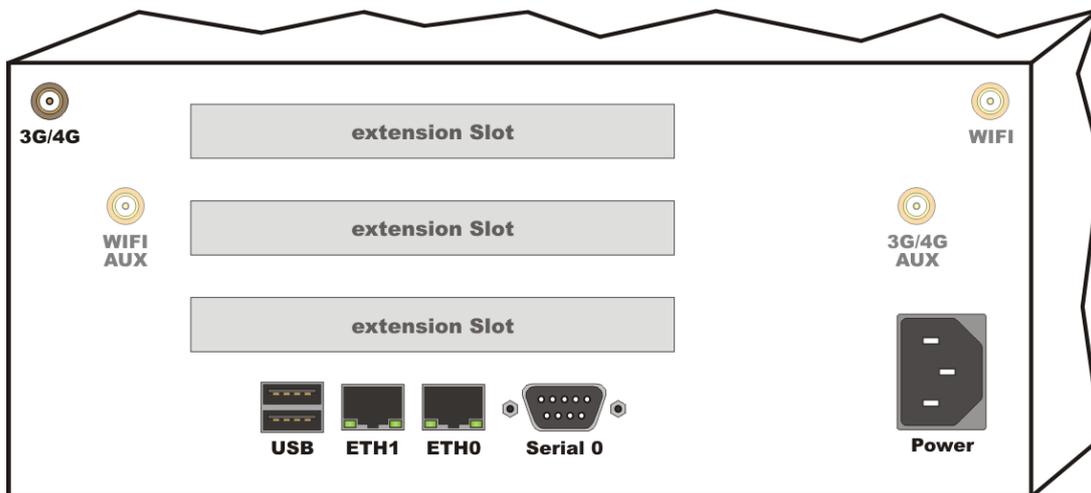


Abbildung 6: Rückseite C2000

Anschluss	Beschreibung
<b>3G/4G</b>	SMA Buchse zum Anschluss der Mobilfunk Antenne
<b>ISDN</b>	RJ45 Anschlussbuchse für ISDN
<b>L1</b>	ISDN Status LED aktive ISDN Layer 1 Verbindung
<b>B Rx/Tx</b>	ISDN Status LED statisch an: B Kanal Verbindung steht blinkt: Daten werden übertragen
<b>WiFi AUX</b>	RP-SMA Buchse zum Anschluss der zweiten WLAN Antenne für N Standard
<b>DSL</b>	RJ45 Anschlussbuchse für das integrierte DSL Modem mit Status LED's Grün blinkt: DSL Synchronisation läuft Grün + Orange an: DSL ist synchronisiert Orange blinkt: Daten werden übertragen
<b>Serial 0</b>	9-poliger RS-232 Seriell Port (Speed: 38400 (8N1))
<b>3G/4G AUX</b>	SMA Buchse zum Anschluss einer zweiten Mobilfunk

Anschluss	Beschreibung
<b>ETH1</b>	10/100BaseT Schnittstelle (bei C1550 mit integriertem 4 Port Switch) mit automatischer Erkennung von Geschwindigkeit und Kabeltyp (1:1 oder gekreuzt).
<b>ETH0</b>	10/100BaseT Schnittstelle, mit automatischer Erkennung von Geschwindigkeit und Kabeltyp (1:1 oder gekreuzt) <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Hinweis</b></p> <ul style="list-style-type: none"> <li>➤ Die Router C1500 und C1550 können über die eth0-Schnittstelle mittels »passive Power over Ethernet« mit Strom versorgt werden.</li> <li>➤ Hierfür wird ein PoE Converter benötigt.</li> </ul> </div>
<b>USB</b>	2 USB 2.0 Ports für externe Hardware
<b>Power</b>	Buchse für die Spannungsversorgung über das mitgelieferte Netzteil
<b>WiFi</b>	RP-SMA Buchse zum Anschluss der primären WLAN Antenne

### 1.3.2 M3000

#### 1.3.2.1 Vorderseite

Der M3000 ist für den Einbau in ein 19 Zoll Server Rack ausgelegt und benötigt 1 Höheneinheit.



Abbildung 7: Vorderseite M3000

Auf der Vorderseite finden sich folgende Anschlüsse und Schalter (von links nach rechts):

Anschluss	Beschreibung
<b>Power</b>	Taster zum Einschalten des Routers
<b>LED</b>	2 LED's zur Statusanzeige
<b>USB</b>	2 USB 2.0 Ports für externe Hardware
<b>COM</b>	9-poliger RS-232 Seriell Port (Speed: 38400 (8N1))

#### 1.3.2.2 Rückseite

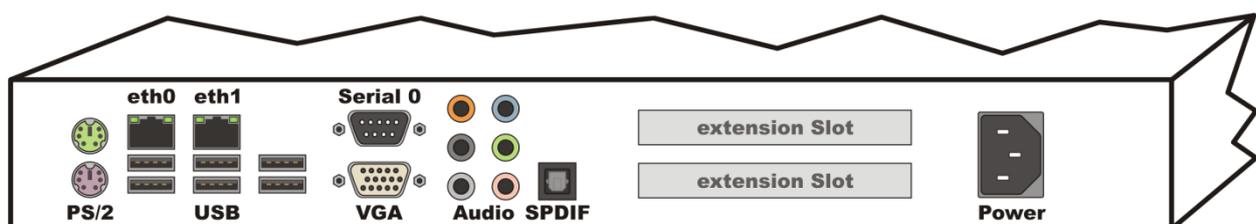


Abbildung 8: Rückseite M3000

Auf der Rückseite des M3000 sind folgende, für den Betrieb relevante Anschlüsse vorhanden:

Anschluss	Beschreibung
<b>PS/2</b>	Anschlüsse für Maus und Tastatur
<b>eth0 &amp; eth1</b>	10/100BaseT Schnittstelle, mit automatischer Erkennung von Geschwindigkeit und Kabeltyp (1:1 oder gekreuzt)
<b>USB</b>	6 USB 2.0 Ports für externe Hardware
<b>Serial 0</b>	9-poliger RS-232 Seriell Port (Speed: 38400 (8N1))
<b>VGA</b>	Monitoranschluss
<b>Audio &amp; SPDIF</b>	<i>Audio Anschlüsse</i>
<b>Extension Slot</b>	Je nach Hardwarekonfiguration des M3000 (z.B. DSL, ISDN, Ethernet Port(s))
<b>Power</b>	Kaltgerätebuchse für die Spannungsversorgung mit 230V Wechselstrom

### 1.3.3 G5000

#### 1.3.3.1 Vorderseite

Der G5000 ist für den Einbau in ein 19 Zoll Server Rack ausgelegt und dabei benötigt er 2 Höheneinheiten.



Abbildung 9: Vorderseite G5000

Die Front enthält unter der Klappe (von links nach rechts):

Anschluss	Beschreibung
<b>Power</b>	Wipptaster zum Einschalten des Routers
<b>Reset</b>	Wipptaster zum Neustart des Routers
<b>LED</b>	2 LED's zur Statusanzeige
<b>USB</b>	2 USB 2.0 Ports für externe Hardware
<b>PS/2</b>	Anschluss für Tastatur

### 1.3.3.2 Rückseite

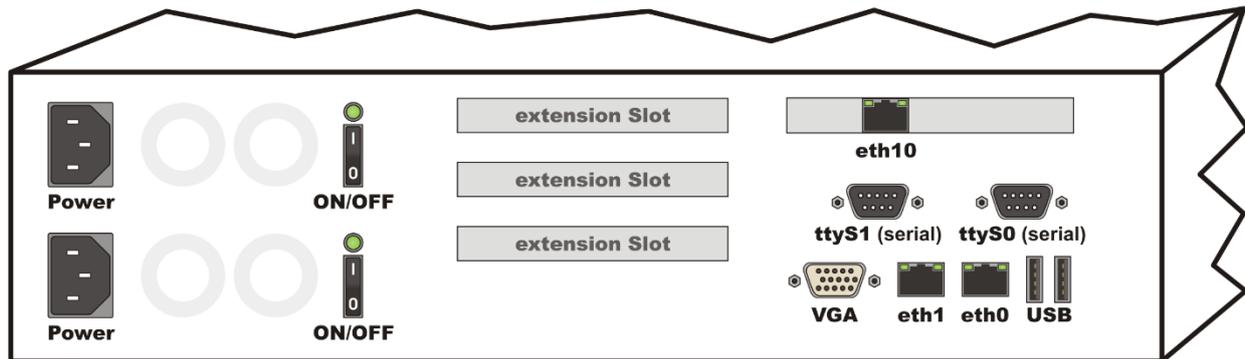


Abbildung 10: Rückseite G5000

Auf der Rückseite des G5000 sind folgende für den Betrieb relevanten Anschlüsse vorhanden:

Anschluss	Beschreibung
<b>Power</b>	Kaltgerätebuchse für die Spannungsversorgung mit 230V Wechselstrom
<b>ON/OFF</b>	Wippschalter zum Ein- und Ausschalten der Netzteile
<b>Extension Slot</b>	Je nach Hardwarekonfiguration des G5000 (z.B. DSL, ISDN, Ethernet Port(s))
<b>ttyS0, ttyS1</b>	9-polige RS-232 Seriell Ports (Speed: 38400 (8N1))
<b>eth0, eth1, eth10</b>	10/100/1000BaseT Schnittstelle, mit automatischer Erkennung der Geschwindigkeit, sowie Kabeltyps (1:1 oder gekreuzt)
<b>VGA</b>	Monitoranschluss
<b>USB</b>	2 USB 2.0 Ports für externe Hardware

### 1.3.4 Seriennummer

Die Seriennummer befindet sich auf der Geräteunterseite und auf dem Lieferschein. Diese ist jedem Gerät eindeutig zugewiesen. Bitte halten Sie die Seriennummer bei Support/Service und Reparaturanfragen bereit.

**Hinweis**

- Sollte das Gerät verbaut werden und die Seriennummer daher nicht mehr ablesbar sein, empfiehlt es sich diese zu dokumentieren.

## 1.4 Zugangsdaten

Bei allen C-, M-, G- und L-Geräten sind die hier aufgeführten Daten standardmäßig voreingestellt.

<b>Voreingestelltes LAN Schnittstelle</b>	IP-Adresse eth1	192.168.0.50
	Subnetzmaske für eth1	255.255.255.0
<b>Voreingestellte WAN Schnittstelle</b>	IP-Adresse eth0	10.99.99.99
	Subnetzmaske für eth0	255.255.255.0
<b>Voreingestellte WLAN Konfiguration</b>  für Geräte mit WLAN Modul	IP-Adresse wlan0	172.16.0.50
	Subnetzmaske für wlan0	255.255.255.0
	SSID	TDT-AP
	Pre Shared Key (ASCII)	tdt-Router
	Kanal	1 (2412 MHz)
<b>Webinterface</b>	Aufruf via SSL	<a href="https://&lt;Schnittstellen IP&gt;">https://&lt;Schnittstellen IP&gt;</a>
	Username	tdt
	Passwort	tdt
<b>SSH / CLI</b>	SSH Port	22
	CLI Port	2000
	Username	root
	Passwort	tdt
<b>Serial Port (RS232)</b>	Speed	38400 bit/s
	Datenbits	8
	Parität	keine
	Stoppbits	1
		<p><b>Hinweis</b></p> <p>➤ Zum Anschluss an einen PC ist ein Nullmodemkabel erforderlich.</p>

### **ACHTUNG!**

- **Aus Sicherheitsgründen sollten die Passwörter für das Webinterface und den SSH-Zugriff geändert werden!** (siehe [14.1.1 Passwort ändern](#))
- **Bei Modellen mit WLAN bitte unbedingt auch den Pre Shared Key ändern!**

## 1.5 Wie verbinde ich mich auf den Router?

Um den Router konfigurieren zu können stehen Ihnen das Webinterface (für die einfache Konfiguration im Browser) und die TDT CLI (Command Line Interface) zur Verfügung. Weiter besteht auch die Möglichkeit sich über SSH oder seriell auf den Router zu verbinden.

### Hinweis

- Um über LAN auf den Router zugreifen zu können, muss Ihr PC im selben Netz erreichbar sein wie der Router. In der Standard Konfiguration benötigen Sie eine IP-Adresse aus dem Bereich 192.168.0.0/255 (z.B. 192.168.0.1) und die Subnetzmaske 255.255.255.0.

### 1.5.1 Webinterface

Geben Sie in der Adressleiste Ihres Browsers die IP-Adresse des Routers ein. Im Auslieferungszustand ist die IP-Adresse von **eth1** auf **192.168.0.50** eingestellt.

Da das Webinterface nur über SSL zu erreichen ist, muss vor der IP-Adresse **https://** stehen.

### Beispiel:

**https://192.168.0.50**

Im nun erscheinenden Anmeldefenster müssen Sie den Benutzernamen und das zugehörige Passwort eingeben. Im Auslieferungszustand sind Username und Passwort **tdt** und **tdt**.



Welcome to C1550ldw



Please enter your login Username and Password

Username

Password

Login



TDT GmbH  
Siemensstr. 18  
Gewerbegebiet Altheim  
84051 Essenbach  
Web: [www.tdt.de](http://www.tdt.de)  
Mail: [info@tdt.de](mailto:info@tdt.de)

This product includes software developed by the Apache Group for use in the Apache HTTP server project (<http://www.apache.org/>).  
This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).  
[Licenses](#)

Abbildung 11: Die Eingabe des Passwortes wird aus Sicherheitsgründen mit Platzhaltern angezeigt

Auf der Login-Seite befindet sich rechts oben ein Handbuch Download Link.

### 1.5.2 Command Line Interface (CLI)

Mit einem SSH-Client, wie z.B. »PuTTY« (<http://www.chiark.greenend.org.uk/~sgtatham/putty>) können Sie eine Verbindung zu dem Router herstellen.

Zuerst wechseln Sie in **Category** auf **Terminal** > **Keyboard** und setzen bei The Backspace key den Parameter auf **Control-H**.

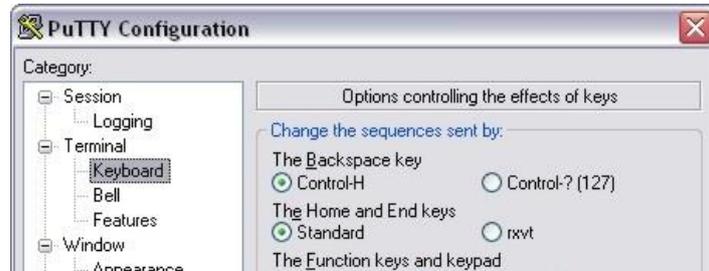


Abbildung 12: PuTTY Configuration Keyboard Einstellung

Danach wechseln Sie in **Category** zurück auf **Session** und öffnen eine SSH-Verbindung auf die IP des Routers unter Verwendung des CLI Ports. Im Auslieferungszustand sind die IP-Adresse von eth0 auf 192.168.0.50 und der CLI Port 2000 eingestellt.

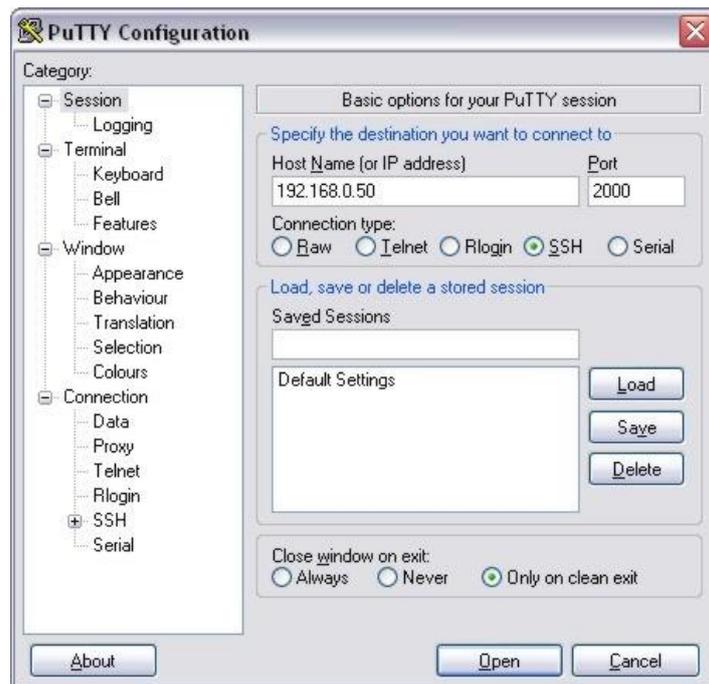


Abbildung 13: PuTTY Configuration für eine CLI-Verbindung

### 1.5.3 Serielle Verbindung mit einem PC

**Hinweis**

- Zum direkten Verbinden mit einem PC ist ein Nullmodemkabel (nicht im Lieferumfang enthalten) erforderlich.

Verbinden Sie das Nullmodemkabel mit der seriellen Schnittstelle (RS-232) des Routers und der seriellen Schnittstelle Ihres PCs.

Zur Einwahl verwenden Sie z.B. »PuTTY«.

Wählen Sie bei **Connection type: Serial**.

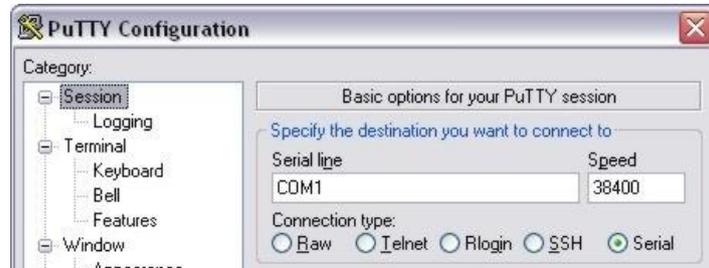


Abbildung 14: Serial auswählen

Wechseln Sie auf **Terminal > Keyboard** und setzen bei The Backspace key auf **Control-H**.

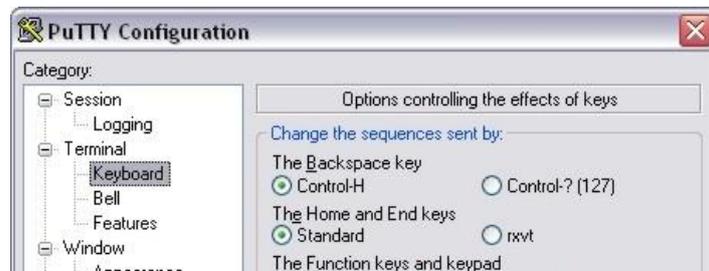


Abbildung 15: PuTTY Configuration Keyboard Einstellung

Unter **Category Connection > Serial** tragen Sie unter **Serial line to connect to** den verwendeten COM Port Ihres PCs (z.B. COM1) und bei **Speed (baud) 38400** ein. **Flow control** **None** auswählen und die Verbindung öffnen.

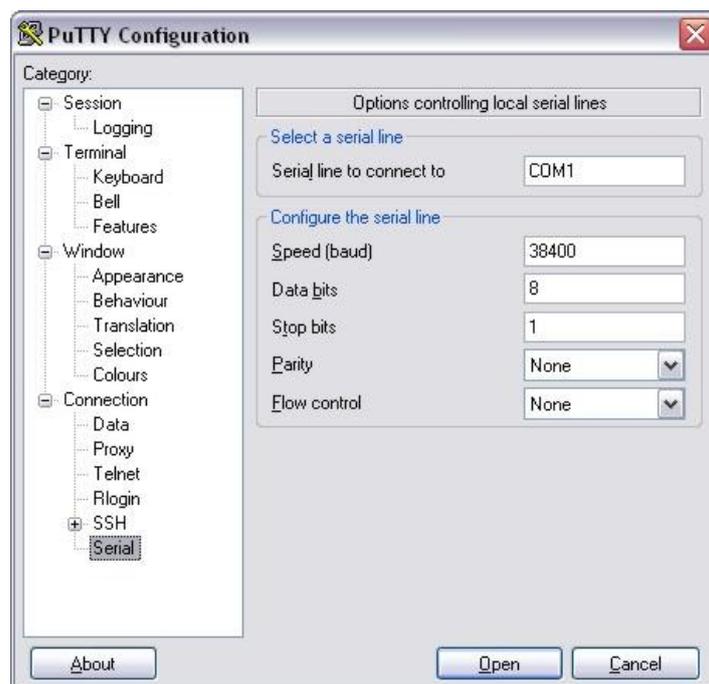


Abbildung 16: PuTTY Configuration für eine serielle Verbindung

In dem sich nun öffnenden Fenster einmal **[Enter]** drücken. Darauf erscheint die Login Abfrage. Melden Sie sich nun mit den SSH Login Daten an (Bei der Passworteingabe wird aus Sicherheitsgründen nichts angezeigt). Mittels des Befehls **cli** kann das Command Line Interface geöffnet werden.

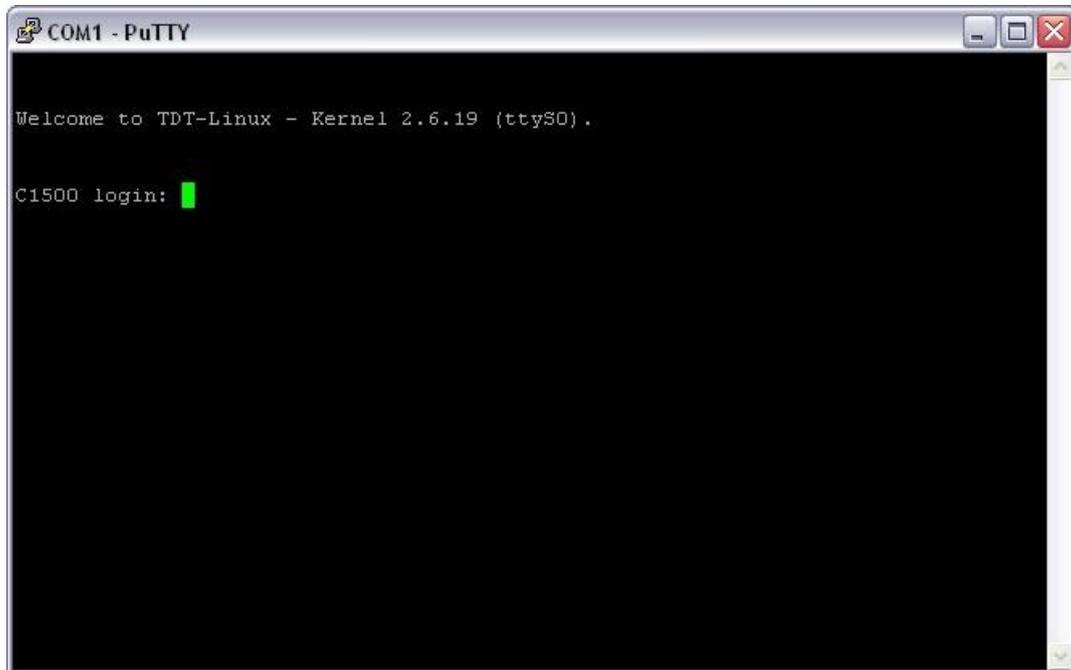


Abbildung 17: Router-Login

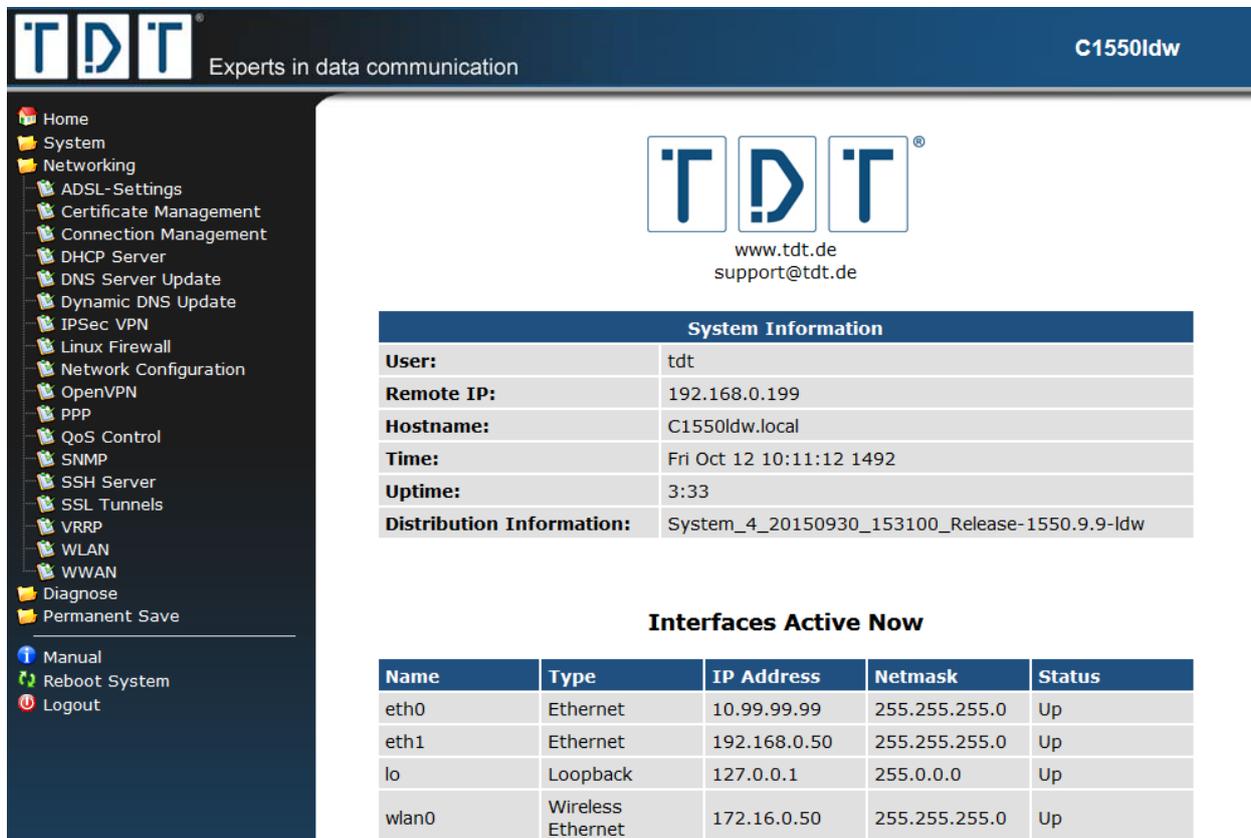
## 2 Das Webinterface

Da das Webinterface mit allen aktuellen Webbrowsern zusammenarbeitet ist diese grafische Benutzeroberfläche einer der bequemsten Wege die Router der C-, M-, G- und L-Serie remote, vom eigenen Arbeitsplatz aus zu administrieren und zu überwachen.

Zur besseren Übersicht ist das Menü in die 4 Punkte »System«, »Networking«, »Diagnose« und »Permanent Save« gegliedert die sich nach dem Login im linken Bereich der Seite finden. Zudem ist dort auch ein »Manual« Download Link, »Reboot System« Button und die »Logout« Schaltfläche zu finden.

Durch klicken auf die Menüpunkte klappt die Baumstruktur auf bzw. zu.

In den aufgeklappten Menüs finden sich die einzelnen Punkte zur Konfiguration des Routers.



The screenshot shows the TDT web interface for a C1550ldw router. The left sidebar contains a navigation menu with the following items: Home, System, Networking (expanded), ADSL-Settings, Certificate Management, Connection Management, DHCP Server, DNS Server Update, Dynamic DNS Update, IPSec VPN, Linux Firewall, Network Configuration, OpenVPN, PPP, QoS Control, SNMP, SSH Server, SSL Tunnels, VRRP, WLAN, WWAN, Diagnose, Permanent Save, Manual, Reboot System, and Logout. The main content area features the TDT logo and contact information (www.tdt.de, support@tdt.de). Below this is a 'System Information' table and an 'Interfaces Active Now' table.

System Information	
<b>User:</b>	tdt
<b>Remote IP:</b>	192.168.0.199
<b>Hostname:</b>	C1550ldw.local
<b>Time:</b>	Fri Oct 12 10:11:12 1492
<b>Uptime:</b>	3:33
<b>Distribution Information:</b>	System_4_20150930_153100_Release-1550.9.9-ldw

Interfaces Active Now				
Name	Type	IP Address	Netmask	Status
eth0	Ethernet	10.99.99.99	255.255.255.0	Up
eth1	Ethernet	192.168.0.50	255.255.255.0	Up
lo	Loopback	127.0.0.1	255.0.0.0	Up
wlan0	Wireless Ethernet	172.16.0.50	255.255.255.0	Up

Abbildung 18: Home Seite und Navigation mit ausgeklapptem Networking Menü

### Achtung!

- **Um die im Webinterface durchgeführten Änderungen dauerhaft zu übernehmen ist es immer nötig *Permanent Save* > *Save Config* auszuführen, da die Einstellungen sonst bei einem Router-Neustart verloren gehen.**

### 3 Das Command Line Interface, die CLI

Mit der von TDT entwickelten CLI steht eine weitere, einfache Konfigurationsmöglichkeit zur Verfügung.

Damit kann die aktuelle Konfiguration auf einem Blick angesehen werden und auf einfachem Wege die einzelnen Parameter überprüft oder geändert werden. Zudem ist auch eine Art Batch-Konfiguration möglich, mit der sich auf einfache Weise Konfigurationen aus einer Textdatei einfügen lassen.

Durch die Eingabe von Fragezeichen (siehe Beispiel1) können die Befehle der gerade aktiven Menü-Ebene angezeigt werden. Parameter lassen sich abfragen indem man dahinter ein Fragezeichen setzt (siehe Beispiel2).

**Beispiel1:**

**TDT(CLI): ?**

configuration	*enter configuration mode
status	*Status information
write	Save Configuration Permanent to
Flash	
save	Save Configuration as Textfile
to /tmp	
load	Load Configuration from
Textfile in /tmp and overwrite all existing configuration	
include	Include Configuration from
Textfile in /tmp and add it to existing configuration	
reboot	Reboot System
shutdown	Shutdown System
halt	Shutdown System immediately
exit	Exit CLI

**Beispiel2:**

**TDT(CLI/configuration/general): prompt ?**

prompt: TDT  
OK

Mit dem Befehl **quit** kann die CLI aus jeder Menü-Ebene komplett verlassen werden.

**Achtung!**

- **Um die in der CLI durchgeführten Änderungen dauerhaft zu übernehmen ist es immer nötig im Hauptmenü einen Permanent Save mit dem Befehl *write* durchzuführen, da die Einstellungen sonst bei einem Router-Neustart verloren gehen.**

Die Befehlsreferenz ist in Kapitel [12 CLI Befehlsreferenz](#) zu finden.

## 4 Systemverwaltung

Im **System** Menü des Webinterfaces werden grundlegende Einstellungen des Routers vorgenommen.

Zudem lassen sich viele Konfigurationsaufgaben auch in der Konsole mit Hilfe der CLI durchführen, um die Netzlast geringer zu halten.

### 4.1 Bootup and Shutdown

Im Bootup and Shutdown Menü befinden sich zwei Schaltflächen mit denen der Router neu gestartet bzw. ausgeschaltet werden kann. Außerdem kann das standardmäßig zu startende System (**System 1** oder **System 2**) ausgewählt werden. Hier wird zudem auch das aktuell laufende System angezeigt.

#### CLI-Äquivalent:

Im Hauptmenü der CLI lässt sich der Router optional mit den Befehlen **reboot** und **shutdown** neu starten bzw. ausschalten.

### 4.2 Configuration Handling

Im Configuration Handling können Sie zuvor gespeicherte Konfigurationsdateien des Routers wiederherstellen, bzw. die aktuelle Konfiguration des Routers in einer Konfigurationsdatei abspeichern. Während des Speicherns wird das komplette **/etc** Verzeichnis auf die Flashkarte geschrieben.

Mit Hilfe der integrierten Upload- und Download-Funktion können Konfigurationsdateien, die mit dem Configuration Handling erstellt wurden, auf den Router geladen oder vom Router heruntergeladen werden. (siehe Kapitel [8 Konfiguration sichern und wiederherstellen](#))

### 4.3 Event-Handler

#### 4.3.1 Event-Handler

Der Event-Handler bietet die Möglichkeit, bei bestimmten Ereignissen eine vordefinierte Aktion (Skript) auszuführen. Dazu pingt der Router ein Ziel an und löst je nach Ergebnis eine Aktion aus. Die Intervalle zwischen den Pings, sowie die Schwelle zum Auslösen des Skripts können genau festgelegt werden.

Kommando	Beschreibung
<b>Activate process-Monitoring</b>	aktiviert/deaktiviert die Selbstüberwachung des Event-Handlers
<b>Interval for process-Monitoring</b>	Zeitintervall in Sekunden in dem die Überprüfung durchgeführt wird
<b>Action to perform on missing process</b>	Aktion die bei einem fehlenden Prozess ausgeführt werden soll
<b>Activate Event-Handler</b>	aktiviert/deaktiviert den Event-Handler

#### Hinweis

➤ Ein Script kann erst erstellt werden, wenn der Event mit **Create** erstellt wurde.

#### 4.3.1.1 Health Checker

Kommando	Beschreibung
Health Check Target	zu überprüfendes Ziel
Health Check Port	zu überprüfender Port
Health Check Interval	Intervall zwischen den einzelnen Pings in Sekunden
Health Check Interval if one request failed	Intervall zwischen den einzelnen Pings, wenn ein Ping fehlschlägt
Health Check Timeout	Timeout für den Health Check Ping (Default: 60 Sekunden)
Maximum Failed Requests	maximale Anzahl der fehlgeschlagenen Pings bevor Befehl ausgeführt wird (Default: 1)
Action on success	Aktion die bei Erfolg ausgeführt werden soll
Action on failure	Aktion die bei einem Problem ausgeführt werden soll

#### 4.3.1.2 ICMP Checker

Kommando	Beschreibung
ICPM Check Target	zu überprüfendes Ziel
ICPM Check Interval	Intervall zwischen den einzelnen Pings in Sekunden
ICPM Check Interval if one request failed	Intervall zwischen den einzelnen Pings wenn ein Ping fehlschlägt
ICPM Check Timeout	Timeout für den ICMP Check Ping (Default: 5 Sekunden)
ICMP Check packet-size	ICMP Check Paketgröße in Bytes (Default: 4 Bytes)
Maximum Failed Requests	maximale Anzahl der fehlgeschlagenen Pings bevor Befehl ausgeführt wird (Default: 3)
ICPM Check Interface	Dropdown-Menü zur Auswahl des zu prüfenden Interfaces
Action on success	Aktion die bei Erfolg ausgeführt werden soll
Action on failure	Aktion die bei einem Problem ausgeführt werden soll

#### 4.3.1.3 Beispielscript

Bei Erreichbarkeit des Ziels, wird die DNAT Regel der Firewall gelöscht, Anfragen gehen weiterhin an die IP 192.168.100.51 mit dem Port 23966.

```
#OK script
#!/bin/sh
export
PATH=/usr/local/sbin:/usr/local/bin:/bin:/usr/bin:/sbin:/usr/sbin:/opt/TDT/bin
logger "deleting Firewall-Rule for DNAT..."
iptables -D OUTPUT -t nat -d 192.168.100.51 -dport 23966 -j DNAT --
to-destination 192.168.100.102:23966
logger DONE
```

Ist das Ziel nicht erreichbar, wird eine DNAT Regel hinzugefügt, welche alle Anfragen an die IP 192.168.100.51 und den Port 23966 auf die IP 192.168.100.102 und den Port 23966 umleitet.

```
#Bad script
#!/bin/sh
export
PATH=/usr/local/sbin:/usr/local/bin:/bin:/usr/bin:/sbin:/usr/sbin:/opt/TDT/bin
logger "adding Firewall-Rule for DNAT..."
iptables -A OUTPUT -t nat -d 192.168.100.51 -dport 23966 -j DNAT --to-destination 192.168.100.102:23966
logger DONE
```

### 4.3.2 SMS-Handler

Der SMS-Handler erlaubt das absetzen von Steuerbefehlen per SMS. Dazu muss eine SIM Karte in einen der beiden SIM Karten Slots eingelegt werden.

**Note**

- Wenn eine Datenverbindung besteht, wird die momentan aktive SIM Karte für den SMS-Handler verwendet.
- Wird keine Datenverbindung aufgebaut, wird standardmäßig der interne SIM Kartenslot (SIM2) verwendet. Dies kann aber geändert werden, siehe [5.21 WWAN](#).
- Ohne Datenverbindung kann die SIM Karte nur ohne PIN initialisiert werden

Um den Router per SMS steuern zu können müssen Telefonnummern definiert werden von denen aus das Gerät gesteuert werden darf. SMS von anderen Telefonnummern werden nicht bachtet.

Kommando	Beschreibung
<b>Accept SMS from phone-numbers</b>	In diesem Feld werden die erlaubten Telefonnummern mit Country Code aber ohne führende Nullen angegeben; mehrere Nummern werden durch Komma getrennt  <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p style="margin: 0;"><b>Beispiel</b></p> <p>➤ 4917xxxxxxxx,4916xxxxxxxx</p> </div>
<b>SMS command-separator</b>	Zum Senden mehrerer Befehle muss ein Steuerzeichen zum trennen verwendet werden, welches hier definiert wird (Default: CR,LF)
<b>send SMS reply</b>	Mit diesem Parameter wird definiert ob eine Antwort/Bestätigung per SMS zurückgesendet wird  <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p style="margin: 0;"><b>Hinweis</b></p> <p>➤ Sollen Statusabfragen per SMS erfolgen, muss hier <b>Yes</b> eingestellt werden</p> </div>
<b>Activate SMS-Handler</b>	Aktiviert/deaktiviert den SMS-Handler Dienst

Es werden alle Konfigurationsbefehle der CLI unterstützt (siehe [0 Hinweis](#))

*Bitte* senden Sie die erzeugte Datei bei Supportanfragen mithilfe des *Kontaktformulars* oder via Mail an *support@tdt.de* mit ein.

CLI Befehlsreferenz), ausgenommen sind hier Statusabfragen.

**Beispiel1**

**General prompt <prompt>**

**Beispiel2**

**Ethernet-eth0 ip 1.2.3.4**

### 4.3.2.1 Unterstützte Statusbefehle

**Hinweis**

- Es werden nicht alle Status-Befehle unterstützt. In dieser Tabelle finden Sie die Statusbefehle die per SMS gesendet werden können.

Kommando	Beschreibung
<b>modemstat</b>	listet die Statusangaben des integrierten GPRS-Moduls auf
<b>modem_signal</b>	Anzeige der Signalstärke
<b>modem_reg</b>	Ausgabe des Registrierungsstatus
<b>modem_net</b>	zeigt das Netz mit dem der Router verbunden ist (z.B. T-D1)
<b>modem_lac</b>	Der Location Area Code (Aufenthaltsbereichskennzahl) wird angezeigt
<b>modem_cell</b>	zeigt die aktuelle ID der Funkzelle an
<b>get_ip</b>	gibt die IP der aktiven Mobile Verbindung zurück
<b>ppp_disc &lt;interface&gt;</b>	trennt eine aktive PPP-Verbindung
<b>connection_deact</b>	Deaktiviert einen Connection-Entry des Connection-Managers
<b>pppstat &lt;interface&gt;</b>	zeigt den Status einer PPP-Verbindung
<b>ifconfig</b>	gibt den Status der Netzwerkschnittstellen aus
<b>sastat</b>	gibt den IPSec-SA-Status aus
<b>uptime</b>	zeigt die Laufzeit des Routers aus
<b>id</b>	zeigt die aktuelle Firmware-Version und die installierten Pakete an
<b>arp</b>	zeigt/löscht ARP-Einträge
<b>ping</b>	Sendet einen Ping Host mit angegeben Optionen (hierbei werden 5 Pingpakete gesendet)
<b>traceroute</b>	Ermittelt den zurückgelegten Weg zu einem Host (Wartezeit 10 sec)

Kommando	Beschreibung
<b>delete_sa</b> <SA-name>	Löscht die angegebene IPSec-SA
<b>date</b>	gibt Systemzeit und -datum aus
<b>cpu</b>	gibt die Prozessor- und Arbeitsspeicherauslastung aus
<b>write</b>	speichert die aktuelle Konfiguration auf das Flash
<b>reboot</b>	führt einen Neustart des Systems durch

## 4.4 Firmware Update

Auf dieser Seite befindet sich das Firmware Update, hiermit kann die Firmware des Gerätes aktualisiert werden. Die Beschreibung dazu finden Sie unter Kapitel [10 Firmware Update](#).

## 4.5 LED Assignment (nur C-Serie)

In diesem Menü kann die Konfiguration der LED's an der Gerätevorderseite eingesehen und frei konfiguriert werden. Hierzu können Sie eine Belegung wie folgt wählen.

<p><b>Hinweis</b></p> <p>➤ <b>n</b> wird durch die Interface/Modem Nummer ersetzt</p>
---

### 4.5.1 Ethernet

Wert	Status	Beschreibung
<b>ETHn_UP_DOWN</b>	<b>aus</b>	ETHn Link down
	<b>an</b>	ETHn Link up
<b>ETHn_DATA</b>	<b>aus</b>	Kein Datentransfer an ETHn
	<b>an</b>	Datentransfer an ETHn (RX + TX)
<b>ETHn_UP_DOWN_DATA</b>	<b>aus</b>	ETHn Link down
	<b>an</b>	ETHn Link up
	<b>blinken</b>	Datentransfer an ETHn (RX + TX)

### 4.5.2 WLAN

Wert	Status	Beschreibung
<b>WLANn_ON_OFF</b>	<b>aus</b>	WLANn inaktiv
	<b>an</b>	WLANn aktiv
<b>WLANn_CONNECT</b>	<b>aus</b>	Keine WLAN Clients verbunden
	<b>an</b>	Ein oder mehr WLAN Clients verbunden
<b>WLANn_ON_OFF_CONNECT</b>	<b>aus</b>	WLANn inaktiv
	<b>an</b>	WLANn aktiv

Wert	Status	Beschreibung
	<b>blinken</b>	Ein oder mehr WLAN Clients verbunden

### 4.5.3 PPP und WWAN Schnittstellen

Wert	Status	Beschreibung
<b>PPP<sub>n</sub>_UP_DOWN</b>	<b>aus</b>	PPP <sub>n</sub> Link down
	<b>an</b>	PPP <sub>n</sub> Link up
<b>PPP<sub>n</sub>_DATA</b>	<b>aus</b>	Kein Datentransfer an PPP <sub>n</sub>
	<b>an</b>	Datentransfer an PPP <sub>n</sub> (RX + TX)
<b>PPP<sub>n</sub>_UP_DOWN_DATA</b>	<b>aus</b>	PPP <sub>n</sub> Link down
	<b>an</b>	PPP <sub>n</sub> Link up
	<b>blinken</b>	Datentransfer an PPP <sub>n</sub> (RX + TX)
<b>WWAN<sub>n</sub>_UP_DOWN</b>	<b>aus</b>	WWAN <sub>n</sub> Link down
	<b>an</b>	WWAN <sub>n</sub> Link up
<b>WWAN<sub>n</sub>_DATA</b>	<b>aus</b>	Kein Datentransfer an WWAN <sub>n</sub>
	<b>an</b>	Datentransfer an WWAN <sub>n</sub> (RX + TX)
<b>WWAN<sub>n</sub>_UP_DOWN_DATA</b>	<b>aus</b>	WWAN <sub>n</sub> Link down
	<b>an</b>	WWAN <sub>n</sub> Link up
	<b>blinken</b>	Datentransfer an WWAN <sub>n</sub> (RX + TX)

### 4.5.4 GSM Options

Wert	Status	Beschreibung
<b>GSM<sub>n</sub>_CONNECT_STATUS</b>	<b>aus</b>	Keine Verbindung
	<b>langsam blinken</b>	2G Signal (GPRS oder EDGE)
	<b>schnell blinken</b>	3G Signal (UMTS/WCDMA oder HSPA)
	<b>an</b>	4G Signal (LTE)
<b>GSM<sub>n</sub>_REG_STATUS</b>	<b>aus</b>	Nicht registriert
	<b>an</b>	Registriert
<b>GSM<sub>n</sub>_GPRS_REG_ROAM</b>	<b>aus</b>	Nicht registriert
	<b>an</b>	Registriert, Home Network
	<b>blinken</b>	Registriert, Roaming Network
<b>GSM<sub>n</sub>_SIGNAL</b>	<b>aus</b>	Kein Empfang (0%)
	<b>langsam blinken</b>	1 - 25 %
	<b>mittel blinken</b>	26 - 50 %
	<b>schnell blinken</b>	51 - 75 %
	<b>sehr schnell blinken</b>	76 - 99 %

➤ Wenn nur eine LED

Wert	Status	Beschreibung
	<b>an</b>	Vollausschlag (100%)
<b>GSMn_SIGNAL</b>  <div style="border: 1px solid black; padding: 2px; display: inline-block;">➤ 2 oder mehr LEDs</div>	<b>an/off</b>	Signalqualität abhängig der Anzahl der konfigurierten LEDs ( <i>m</i> == Signal LED Nummer)

#### 4.5.5 Connection Manager

Wert	Status	Beschreibung
<b>CM_n_CONNECTED (NAME)</b>	<b>aus</b>	Connection-Managers Eintrag <i>n</i> nicht verbunden
	<b>an</b>	Eintrag <i>n</i> verbunden
	<b>blinken</b>	Eintrag <i>n</i> in der Initialisierungsphase

#### 4.5.6 IPsec Tunnel

Wert	Status	Beschreibung
<b>IPSEC_name_CONNECTED</b>	<b>aus</b>	IPsec Verbindung <i>name</i> nicht aufgebaut
	<b>an</b>	IPsec Verbindung <i>name</i> aufgebaut

#### 4.5.7 Zertifikat

Wert	Status	Beschreibung
<b>CERT_name_STATUS</b>	<b>aus</b>	Zertifikat <i>name</i> nicht vorhanden/defekt
	<b>an</b>	Zertifikat <i>name</i> vorhanden und gültig
	<b>blinken</b>	Zertifikat <i>name</i> vorhanden aber ungültig

#### 4.5.8 SIM Card

Wert	Status	Beschreibung
<b>ACTIVE_SIM_CARD</b>	<b>aus</b>	Keine SIM in Verwendung
	<b>an</b>	SIM1 wird verwendet
	<b>blinken</b>	SIM2 wird verwendet

#### 4.5.1 Blinkfrequenzen

Status	Frequenz
<b>langsam blinken:</b>	2000 ms
<b>mittel blinken:</b>	500 ms

Status	Frequenz
schnell blinken:	100 ms
sehr schnell blinken:	30 ms

## 4.6 Push Button Settings

Mit Hilfe des Reset-Buttons können bei der C-Serie verschiedene Funktionen, wie zum Beispiel ein Providerwechsel oder das Zurücksetzen auf den Auslieferungszustand des Routers ausgeführt werden.

Abhängig von der Zeit, die der Reset-Button gedrückt wird, führt dieser verschiedene Funktionen aus.

Beim Drücken des Reset-Buttons leuchten nacheinander die LED's **Power**, **L1** und **L2** auf. Je nach Kombination der LED's führt das Loslassen des Buttons verschiedene Funktionen aus.

In den Werkseinstellungen sind folgende Funktionen definiert:

Aktion	aktive LED	Zeit	Funktion
<b>1st action</b>	<b>Power</b>	0 - 3 Sekunden	Reboot des C1500.
<b>2nd action</b>	<b>Power, L1</b>	4 - 14 Sekunden	Der C1500 schaltet ab.
<b>3rd action</b>	<b>Power, L1, L2</b>	≥ 15 Sekunden	Wiederherstellung des Auslieferungszustandes (Factory Reset) und Reboot des Routers.

Die Aktionen **1st action** sowie **2nd action** können unter »Push Button Assignments« individuell konfiguriert werden.

### 4.6.1 Push Button Actions

Als erstes muss eine entsprechende Aktion erstellt werden. Diese kann unter **System > Push Button Settings > Push Button Actions** erstellt werden.

Parameter	Beschreibung
<b>Description</b>	Name, Kurzbeschreibung der zu definierenden Aktion.
<b>Associated action</b>	Linux-Kommando oder aufzurufendes Skript.  <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Hinweis</b></p> <p>➤ Der Befehl sollte in doppelten Hochkommata definiert werden.</p> </div>

### 4.6.2 Push Button Assignments

Über das Modul »Push Button Assignments« können den Aktionen **1st action** sowie **2nd action** die unter Push Button Actions definierten Aktionen zugewiesen werden.

Die **3rd action** ist nicht konfigurierbar und löst somit immer einen Factory Reset aus.

**ACHTUNG!**

➤ **Die Änderungen werden erst nach dem nächsten Router-Neustart aktiv!**

## 4.7 Scheduled Cron Jobs

Im Scheduled Cron Jobs Menü findet man die Zusammenstellung der Cronjobs. Es werden die Cronjobs für jeden Benutzer, sowie dessen Ausführungsstatus aufgelistet.

### 4.7.1 Create a new scheduled cron job

Über den Link **Create a new scheduled cron job** öffnet sich ein umfangreiches Formular, über das man Auftragsdetails sowie die zeitliche Steuerung eines neuen Cronjobs eintragen kann.

**Hinweis**

➤ Wenn Sie einen Dienst per Cronjob aktivieren (deaktivieren), vergessen Sie anschließend nicht einen Cronjob zu erstellen, welcher den Dienst wieder deaktiviert (aktiviert).

Kommando	Beschreibung
<b>Execute cron job as</b>	Benutzer, unter dem der Cronjob ausgeführt werden soll.
<b>Active</b>	Cronjob ist aktiviert/deaktiviert
<b>Command</b>	Auszuführender Unix-Befehl. Für unser Beispiel: <b><code>/etc/sysconfig/network-devices/ifup wlan0</code></b>
<b>Input to command</b>	Wurde der Befehl erfolgreich gestartet, werden die hier eingetragenen Befehle zur Laufzeit diesem übergeben.
<b>When to execute</b>	<b>Simple schedule:</b> Der Auftrag kann zu festgelegten Zeitpunkten ausgeführt werden. Mögliche Werte: Hourly, Daily (at midnight), Weekly (on Sunday), Monthly (on the 1st), Yearly (on 1st Jan), When system boots. <b>Times and dates selected below:</b> Der Auftrag wird zu den ausgewählten Zeitpunkten ausgeführt.
<b>Minutes, Hours, Days, Months, Weekdays</b>	<b>All:</b> der Cronjob wird zu allen aufgelisteten Punkten ausgeführt <b>Selected:</b> der Cronjob wird nur zu den ausgewählten Punkten ausgeführt.

Am folgenden Beispiel wird mit Hilfe der **Scheduled Cron Jobs** das WiFi-Interface immer Montag bis Freitag um 07:00 Uhr aktiviert.

## Create Cron Job

**Job Details**

Execute cron job as   Active?  Yes  No

Command

Input to command

---

**When to execute**

Simple schedule .. Hourly  Times and dates selected below ..

Minutes	Hours	Days	Months	Weekdays																																																																																																																								
<input type="radio"/> All <input checked="" type="radio"/> Selected ..	<input type="radio"/> All <input checked="" type="radio"/> Selected ..	<input checked="" type="radio"/> All <input type="radio"/> Selected ..	<input checked="" type="radio"/> All <input type="radio"/> Selected ..	<input checked="" type="radio"/> All <input type="radio"/> Selected ..																																																																																																																								
<table style="width: 100%; text-align: center;"> <tr><td>0</td><td>12</td><td>24</td><td>36</td><td>48</td></tr> <tr><td>1</td><td>13</td><td>25</td><td>37</td><td>49</td></tr> <tr><td>2</td><td>14</td><td>26</td><td>38</td><td>50</td></tr> <tr><td>3</td><td>15</td><td>27</td><td>39</td><td>51</td></tr> <tr><td>4</td><td>16</td><td>28</td><td>40</td><td>52</td></tr> <tr><td>5</td><td>17</td><td>29</td><td>41</td><td>53</td></tr> <tr><td>6</td><td>18</td><td>30</td><td>42</td><td>54</td></tr> <tr><td>7</td><td>19</td><td>31</td><td>43</td><td>55</td></tr> <tr><td>8</td><td>20</td><td>32</td><td>44</td><td>56</td></tr> <tr><td>9</td><td>21</td><td>33</td><td>45</td><td>57</td></tr> <tr><td>10</td><td>22</td><td>34</td><td>46</td><td>58</td></tr> <tr><td>11</td><td>23</td><td>35</td><td>47</td><td>59</td></tr> </table>	0	12	24	36	48	1	13	25	37	49	2	14	26	38	50	3	15	27	39	51	4	16	28	40	52	5	17	29	41	53	6	18	30	42	54	7	19	31	43	55	8	20	32	44	56	9	21	33	45	57	10	22	34	46	58	11	23	35	47	59	<table style="width: 100%; text-align: center;"> <tr><td>0</td><td>12</td></tr> <tr><td>1</td><td>13</td></tr> <tr><td>2</td><td>14</td></tr> <tr><td>3</td><td>15</td></tr> <tr><td>4</td><td>16</td></tr> <tr><td>5</td><td>17</td></tr> <tr><td>6</td><td>18</td></tr> <tr><td>7</td><td>19</td></tr> <tr><td>8</td><td>20</td></tr> <tr><td>9</td><td>21</td></tr> <tr><td>10</td><td>22</td></tr> <tr><td>11</td><td>23</td></tr> </table>	0	12	1	13	2	14	3	15	4	16	5	17	6	18	7	19	8	20	9	21	10	22	11	23	<table style="width: 100%; text-align: center;"> <tr><td>1</td><td>13</td><td>25</td></tr> <tr><td>2</td><td>14</td><td>26</td></tr> <tr><td>3</td><td>15</td><td>27</td></tr> <tr><td>4</td><td>16</td><td>28</td></tr> <tr><td>5</td><td>17</td><td>29</td></tr> <tr><td>6</td><td>18</td><td>30</td></tr> <tr><td>7</td><td>19</td><td>31</td></tr> <tr><td>8</td><td>20</td><td></td></tr> <tr><td>9</td><td>21</td><td></td></tr> <tr><td>10</td><td>22</td><td></td></tr> <tr><td>11</td><td>23</td><td></td></tr> <tr><td>12</td><td>24</td><td></td></tr> </table>	1	13	25	2	14	26	3	15	27	4	16	28	5	17	29	6	18	30	7	19	31	8	20		9	21		10	22		11	23		12	24		<input type="radio"/> All <input type="radio"/> Selected .. <ul style="list-style-type: none"> <li>January</li> <li>February</li> <li>March</li> <li>April</li> <li>May</li> <li>June</li> <li>July</li> <li>August</li> <li>September</li> <li>October</li> <li>November</li> <li>December</li> </ul>	<input checked="" type="radio"/> All <input type="radio"/> Selected .. <ul style="list-style-type: none"> <li>Sunday</li> <li>Monday</li> <li>Tuesday</li> <li>Wednesday</li> <li>Thursday</li> <li>Friday</li> <li>Saturday</li> </ul>
0	12	24	36	48																																																																																																																								
1	13	25	37	49																																																																																																																								
2	14	26	38	50																																																																																																																								
3	15	27	39	51																																																																																																																								
4	16	28	40	52																																																																																																																								
5	17	29	41	53																																																																																																																								
6	18	30	42	54																																																																																																																								
7	19	31	43	55																																																																																																																								
8	20	32	44	56																																																																																																																								
9	21	33	45	57																																																																																																																								
10	22	34	46	58																																																																																																																								
11	23	35	47	59																																																																																																																								
0	12																																																																																																																											
1	13																																																																																																																											
2	14																																																																																																																											
3	15																																																																																																																											
4	16																																																																																																																											
5	17																																																																																																																											
6	18																																																																																																																											
7	19																																																																																																																											
8	20																																																																																																																											
9	21																																																																																																																											
10	22																																																																																																																											
11	23																																																																																																																											
1	13	25																																																																																																																										
2	14	26																																																																																																																										
3	15	27																																																																																																																										
4	16	28																																																																																																																										
5	17	29																																																																																																																										
6	18	30																																																																																																																										
7	19	31																																																																																																																										
8	20																																																																																																																											
9	21																																																																																																																											
10	22																																																																																																																											
11	23																																																																																																																											
12	24																																																																																																																											

Note: Ctrl-click (or command-click on the Mac) to select and de-select minutes, hours, days and months.

[Return to cron list](#)

Abbildung 19: Beispielkonfiguration: WLAN starten

### 4.7.2 Create a new environment variable

Hier lassen sich Umgebungsvariablen für Cron Jobs definieren.

### 4.7.3 Control user access to cron jobs

Mittels der Zugriffskontrolle kann man User festlegen die Cron Jobs erstellen und starten dürfen. Dabei kann man die Zugriffskontrolle auf drei verschiedene Arten konfigurieren:

Kommando	Beschreibung
<b>Allow all users</b>	erlaubt allen Benutzern den Zugriff auf die Cron Jobs
<b>Allow only listed users</b>	nur die ausgewählten User dürfen Cron Jobs ausführen
<b>Deny only listed users</b>	den definierten Benutzern wird der Zugriff verweigert

## 4.8 System Time

In diesem Menü lassen sich System und Hardware Uhr stellen, die Zeitzone setzen und einen Network Time Protokoll Server (NTP Server) zur Zeitsynchronisation einrichten.

## 4.9 Time Synchronisation

Im NTP - Time Synchronisation Menü haben Sie die Möglichkeit einen oder mehrere Network Time Protokoll Server anzugeben. Sie können z.B. den NTP Server der Physikalisch-Technische Bundesanstalt (ptbtime1.ptb.de) als Server benutzen. Bitte beachten Sie dass die Eingabe von Domainnamen erst funktioniert, wenn der DNS Dienst konfiguriert und gestartet ist.

Bei allen C-Routern mit GPS kann die Zeit auch über den integrierten GPS-Receiver synchronisiert werden.

Dies funktioniert jedoch nur, wenn die am Router gültige Zeit nicht mehr als 4 Stunden abweicht. Als Server-Adresse muss dazu die pseudo IP-Adresse **127.127.20.0** angegeben werden.

## 4.10 Webmin Configuration

In diesem Menü können Sie verschiedene Einstellungen wie IP-Adressen Zugangskontrolle, Sprache, usw. festlegen.

### 4.10.1 IP Access Control

Im IP Access Control Menü haben Sie die Möglichkeit den Zugriff auf Webmin zu beschränken.

Kommando	Beschreibung
<b>Allow from all addresses (Default)</b>	Erlaubt allen IP Adressen den Zugriff auf das Webmin Interface
<b>Only allow from listed addresses</b>	Erlaubt nur den im nebenstehenden Fenster gelisteten IP Adressen den Zugriff auf das Webmin Interface
<b>Deny from listed addresses</b>	Erlaubt allen IP Adressen den Zugriff auf das Webmin Interface, <b>außer</b> den im nebenstehenden Fenster gelisteten IP Adressen
<b>Resolve hostnames on every request</b>	Löst einen eingegebenen Hostnamen bei jedem Zugriff erneut auf. Dies ist z.B. erforderlich wenn die Gegenstelle nur einen dynamischen DNS Namen hat, und sich dadurch die IP Adresse ändern kann

### 4.10.2 Port and Address

Hier können Sie die IP Adresse und die Portnummer eingeben, auf die das Webmin Interface reagieren soll.

Kommando	Beschreibung
<b>Listen on IP address (Default)</b>	Sofern der Router über mehrere IP Adressen verfügt, können Sie eine oder mehrere IP Adressen eingeben, die das Webmin Interface überwachen soll
<b>Listen on port</b>	Tragen Sie hier die Portnummer ein, die das Webmin Interface überwachen soll. Per Default ist die Portnummer 10000 eingetragen
<b>Listen for broadcasts on UDP port</b>	Tragen Sie hier die UDP Broadcast Portnummer ein, die das Webmin Interface überwachen soll. Per Default ist die Portnummer 10000 eingetragen

### 4.10.3 Logging

Webmin kann so konfiguriert werden, dass er eine Protokolldatei für Seitenanfragen im Standard-CLF-Protokolldateiformat schreibt. Wenn die Protokollierung aktiviert ist, können Sie wählen, ob IP-Adressen oder Host-Namen aufgezeichnet werden sollen und wie oft die Protokolldatei gelöscht wird. Wenn die Protokollierung aktiviert ist, schreibt Webmin das Protokoll in ***/var/webmin/miniserv.log***.

Bei aktiver Protokollierung kann Webmin auch ein detailliertes Protokoll in der Datei `/var/webmin/webmin.log` speichern. Dieses Protokoll kann mit der Webmin-Ereignisanzeige betrachtet und analysiert werden, um jede Aktivität aller Webmin-Benutzer zu beobachten.

Kommando	Beschreibung
<b>Disable logging</b>	deaktiviert die Log-Funktion
<b>Enable logging (Default)</b>	aktiviert die Log-Funktion
<b>Log resolved hostnames</b>	Webmin versucht die IP-Adresse in den Host Namen aufzulösen
<b>Clear logfiles every</b>	Gibt die Zeit in Stunden an, nachdem Webmin die Protokolldatei löscht
<b>Log actions by all users (Default)</b>	Alle User werden mitgeloggt
<b>Only log actions by ..</b>	Nur die angegebenen User werden mitgeloggt
<b>Log actions in all modules (Default)</b>	Alle Module werden mitgeloggt
<b>Only log actions in ..</b>	Nur die angegebenen Module werden mitgeloggt
<b>Log changes made to files by each action</b>	Dateiänderungen jedes Ereignisses werden protokolliert

#### 4.10.4 Language

In diesem Menu können sie die Sprache des Webmin Interface ändern. Die Default Sprache ist Englisch.

#### 4.10.5 Authentication

Hier können Sie Authentifizierung und Passwort-Timeouts einstellen. Passwort-Timeouts können den Webmin-Server vor sogenannten Brute-Force-Attacken schützen, indem eine, sich fortlaufend verlängernde Verzögerung, nach einem fehlgeschlagenen Anmeldeversuch eines Benutzers stattfindet. Bei aktiver Authentifizierung werden alle Sitzungen aller Benutzer von Webmin aufgezeichnet, so dass inaktive Benutzer automatisch abgemeldet werden können.

##### Hinweis

- Das Aktivieren oder Deaktivieren der Authentifizierung kann dazu führen, dass sich alle Benutzer neu anmelden müssen.

Kommando	Beschreibung
<b>Disable password timeouts</b>	Es können beliebig viele falsche Passwörter eingegeben werden, ohne dass eine Sperre erfolgt
<b>Enable password timeouts (Default)</b>	Die Sperre des Webmin Interface nach einer bestimmten Anzahl von inkorrekten Login Versuchen ist aktiviert
<b>Block hosts with more than <i>n1</i> failed logins for <i>n2</i> seconds. (Default: <i>n1</i>=5; <i>n2</i>=60)</b>	Legt maximale Anzahl falscher Login Versuche ( <b><i>n1</i></b> ) fest. Bei Überschreitung dieser Variable erlaubt das Webmin Interface kein Login für die in <b><i>n2</i></b> angegebene Zeit (Sekunden)
<b>Log blocked hosts, logins and authentication failures to syslog (Default)</b>	Hier können Sie festlegen ob blockierte Rechner, Anmelde- und Authentifizierungsfehler im syslog protokolliert werden sollen

Kommando	Beschreibung
<b>Disable session authentication</b>	Das Webmin Interface benötigt keine Authentifizierung
<b>Enable session authentication (Default)</b>	Das Webmin Interface benötigt eine Authentifizierung mit Benutzernamen und Passwort
<b>Auto-logout after n3 minutes of inactivity (Default=7)</b>	Nach der im Wert n3 angegebenen Zeit in der keinerlei Aktivitäten im Webmin unternommen wurden, beendet Webmin automatisch die Session
<b>Offer to remember login permanently?</b>	Hier können Sie angeben ob das Webmin Interface einen Cookie auf einem PC hinterlegen soll, um die Authentifizierung zu automatisieren
<b>Show hostname on login screen? (Default)</b>	Zeigt den Hostnamen des Routers im Webmin Interface an
<b>No pre-login page (Default)</b>	Es wird keine spezielle Seite oder Datei vor dem Login angezeigt.
<b>Show pre-login file</b>	Es wird eine spezielle Seite oder Datei auf dem Router vor dem Login angezeigt, die Sie im nachfolgenden Feld angeben können.

## 4.11 Webmin Users

Das Webinterface verfügt über eine leistungsfähige und flexible Benutzerverwaltung.

Über das Menü Webmin Users öffnet sich die Webmin eigene Benutzerverwaltung. Sie führt bereits eingerichtete Anwender auf. Außerdem erlaubt sie das Hinzufügen neuer Anwender und das Einstellen der Berechtigung auf den Modulzugriff.

Die Webmin-Oberfläche kann für die jeweilige Verbindung individuell angepasst werden (z.B. für GPRS-Verbindungen). Wechseln Sie dazu das Theme von Webmin unter dem Menüpunkt **System > Webmin Users > <USER> > Personal Theme**. Mit dem Theme **Simple Webmin Theme** erreichen Sie die schnellste Übertragung.

Um das Passwort zu ändern wird unter **System > Webmin Users > <USER>** der Parameter **Password** im Dropdown auf **Set to ..** und im nachfolgenden Textfeld das neue Passwort eingetragen und mit  gespeichert.

### Hinweis

- Hiermit wird **nicht** der Kommandozeilenbenutzer root geändert. Dieses Passwort wird über die Kommandozeile geändert. (siehe Kapitel [14.1.1 Passwort ändern](#))

## 5 Netzwerkkonfiguration

Im **Networking** Menü können sie alle netzwerkspezifischen Einstellungen des Routers vornehmen. Die möglichen Einstellungen variieren je nach Ausstattung des Routers.

### 5.1 BIND DNS Server (nur M3000, G5000)

BIND (Berkeley Internet Name Domain) ist ein Open Source DNS Server. Dieser Dienst ist nur bei Geräten der M und G Serie integriert.

Damit das Gerät für Clients als DNS Server agieren kann, muss der Dienst konfiguriert und gestartet sein.

Wird hier `The primary configuration file for BIND /etc/named/named.conf does not exist, or is not valid. Create it?` angezeigt ist der DNS Server nicht aufgesetzt.

Zum Erstellen der Konfiguration wird einer der folgenden Punkte ausgewählt und über den Button **[Create Primary Configuration File and Start Nameserver]** erzeugt.

Kommando	Beschreibung
<b>Setup nameserver for internal non-internet use only</b>	Hiermit wird ein Name Server erstellt, der nur für eine interne Nutzung ausgelegt ist. Es werden nur die Namen hinterlegter Einträge aufgelöst.
<b>Setup as an internet name server, and download root server information</b>	Setzt einen DNS Server auf, der sowohl lokal hinterlegte Namen als auch Internet Domains auflösen kann. Dazu wird eine »Root Zone« benötigt, die von rs.internic.net heruntergeladen wird  <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p><b>Hinweis</b></p> <p>➤ Hierzu wird eine aktive Internetverbindung benötigt.</p> </div>
<b>Setup as an internet name server, but use Webmin's older root server information</b>	Identisch zur vorhergehenden Beschreibung, allerdings wird hier keine bestehende Internetverbindung benötigt, da eine mit dem Router ausgelieferte »Root Zone« verwendet wird.

Eine nähere Beschreibung ist der offiziellen BIND Seite <https://www.isc.org/software/bind> zu entnehmen.

### 5.2 Certificate Management

Das Certificate Management bietet die Möglichkeit Zertifikate zu verwalten. Die vorhandenen Zertifikate werden im entsprechenden Bereich aufgeführt und können detailliert angezeigt werden. Zudem können Zertifikate hinzugefügt oder gelöscht werden.

Kommando	Beschreibung
<b>CA Certificates</b>	Zeigt alle vorhandenen »CA Zertifikate« (Certificate Authority) an
<b>Host Certificates</b>	Hier werden »Host Zertifikate« (Maschinenzertifikate) angezeigt, die auf dem Router hinterlegt sind
<b>Host Keys</b>	Listet auf dem Router vorhandene »Host Keys« auf
<b>Revocation Lists</b>	Die »Certificate Revocation List« ist eine Liste, die Informationen über die Unültigkeit von Zertifikaten enthält. Sie ermöglicht es, festzustellen, ob ein Zertifikat gesperrt/widerrufen wurde und warum

## 5.2.1 Import-PKCS#12

**PKCS** steht für **Public Key Cryptography Standards** und bezeichnet eine Reihe von kryptografischen Spezifikationen. Das PKCS#12 definiert ein Dateiformat, das dazu benutzt wird, private Schlüssel mit dem zugehörigen Zertifikat passwortgeschützt zu speichern. Die Import PKCS#12 Funktion des Routers ermöglicht es den öffentlichen und privaten Schlüssel und eventuell das CA Zertifikat aus der p12 Datei zu entpacken.

Kommando	Beschreibung
<b>Choose File To Upload</b>	Wählt die PKCS#12 Datei aus. Die Datei muss sich bereits auf dem Router befinden.
<b>Passphrase for PKCS#12</b>	Das Passwort für die PKCS#12 Datei.
<b>Host Key Name</b>	Der Name unter dem der private Key auf dem Router gespeichert wird. <b>Dieser muß zwingend auf .pem enden.</b>
<b>Passphrase for Host Key</b>	Das Passwort für den »private Key«.
<b>Verify Passphrase</b>	Das Passwort für den »private Key« zur Überprüfung.
<b>CA Certificate Name</b>	Der Name unter dem das root Zertifikat auf dem Router gespeichert wird. <b>Dieser muß zwingend auf .pem enden.</b>
<b>Host Certificate Name</b>	Der Name unter dem das »public« Zertifikat auf dem Router gespeichert wird. <b>Dieser muß zwingend auf .pem enden.</b>

## 5.3 Connection Management

Mit dem Connection Management werden vorhandene Verbindungen verwaltet.

Unter **Static Connections** werden Verbindungen einfach, ohne weitere Überprüfung gestartet.

Der **Connection-Manager** überwacht seine Verbindungen. Daher empfiehlt es sich immer mit dem Connection-Manager zu arbeiten. Zudem bietet der Connection-Manager auch die Möglichkeit Backup Szenarien zu realisieren.

### 5.3.1 Connection-Manager

Der Connection-Manager ermöglicht es, mehrere physikalische (ppp, eth, br, wlan, wwan) bzw. logische (IPSec) Verbindungen zu starten und zu überwachen.

Die Verbindungen sind anfangs alle gleichberechtigt. Mit Hilfe des »Inhibit Mode« lassen sich jedoch Abhängigkeiten definieren. Somit kann zum Beispiel, wenn bei einer dynamischen Prüfung ein Problem mit einer Verbindung festgestellt wird, ein zweiter Verbindungseintrag als Backup gestartet werden. Dadurch erreicht man eine höhere Ausfallsicherheit, die gerade bei sensibleren Anwendungen nötig ist.

#### 5.3.1.1 Connection-Dial-Entry

Ein Connection-Dial-Entry stellt eine physikalische Verbindung dar und kann

- ◊ mit mehreren statischen und default Routen arbeiten.
- ◊ mehrere untergeordnete logische Verbindungen, wie eine IPSec-Verbindung, überwachen.
- ◊ in Abhängigkeit des Status von jedem beliebigen anderen Connection-Dial-Entry stehen.
- ◊ unterstützt Scripts für jede interne Statusänderung.

Beim Systemstart holt sich der Connection-Dial-Entry seine Konfiguration und geht in die Abarbeitungsschleife. Wenn ein »Power Up Delay« gesetzt ist wird bis zum Ablauf der eingetragenen Zeit gewartet.

In der Abarbeitungsschleife startet der Eintrag, in Abhängigkeit seines internen Status, dem Status der anderen Dial-Entries und der Logical-Entries seinen Dienst.

#### 5.3.1.1.1 Inhibit

Bei jedem Zyklus der Abarbeitungsschleife überprüft jeder Connection-Dial-Entry den Status der konfigurierten Inhibit-Einträge. Wenn der Status eines Eintrages gleich oder größer ist wie unter »Inhibit Mode« eingestellt, wird der laufende Connection-Dial-Entry getrennt.

Ist der »Inhibit-Mode« von Connection-Dial-Entry 1 auf »Active« gesetzt und soll durch Connection-Dial-Entry 2 unterdrückt werden, wird Eintrag 1 deaktiviert, wenn Eintrag 2 einen Status wie folgt hat:

- ◊ Active
- ◊ Initializing
- ◊ Connected
- ◊ Disconnecting

Wenn Eintrag 2 einen Status wie folgt aufweist wird Eintrag 1 erlaubt:

- ◊ Power Up Delay
- ◊ Disconnectet

#### 5.3.1.1.2 Interface- und Ping-Checker

Der Interface-Checker wird während der Initialisierung für alle Einträge gestartet. Dabei überprüft er automatisch jede Sekunde den Status des Interfaces. Wenn das Interface, aus welchem Grund auch immer nicht funktioniert, wird der entsprechende Connection-Dial-Entry deaktiviert.

Wenn der Ping-Checker eingerichtet ist, startet dieser während der Initialisierungsphase. Der Ping-Checker sendet ICMP-Anfragen in dem konfigurierten Intervall und überprüft ob eine Antwort empfangen wird. Wird während der unter »Maximum failed Requests« definierten Anzahl an Versuchen keine Antwort empfangen, wird der entsprechende Eintrag deaktiviert.

##### **Hinweis**

- Ein Connection-Dial-Entry wird nicht auf den Status »disconnected« gesetzt solange noch ein Wählversuch aktiv ist. Er bleibt im Status »disconnecting« bis das Ende des »Redial-Delay« erreicht ist.

#### 5.3.1.1.3 Verbindungsübersicht

Alle Einträge die im Connection-Manager angelegt wurden, werden hier mit ihrem aktuellen Status angezeigt. Zur besseren Übersicht werden die Verbindungen entsprechend farbig hinterlegt.

Grau = inaktiv [Verbindungseintrag ist inaktiv], Blau = active [Power Up Delay, Verbindungsaufbau, Initialisierung], Grün = Connected [Verbindung aufgebaut], Rot = Disconnected [Verbindung getrennt, Inhibited durch anderen Verbindungseintrag]

Am Ende jeder Zeile findet sich ein **Reload** Link, der die Konfiguration des Eintrages neu einliest. Durch Drücken des Links wird die Verbindung getrennt, die Interface Parameter und Connection-Dial-Entry Konfiguration neu geladen und die Verbindung neu aufgebaut.

**Hinweis**

- Während eines **Reload** wird die Verbindung getrennt.
- Ein **Reload** der Konfiguration liest alle Verbindungsparameter, inklusive Interface Einstellungen (z.B. PPP, WWAN) neu ein.
- Änderungen an den Interface Einstellungen (PPP, WWAN) und im Connection-Manager werden erst nach einem **Reload** aktiv.

Unter den konfigurierten Verbindungseinträgen sind die Buttons **Add Connection** zum hinzufügen neuer Einträge, **Refresh** zum aktualisieren der Verbindungsübersicht/des Status sowie der **Reload All** zum neu einlesen der Parameter aller Verbindungen.

Hinter den »Advanced Functions« sind Buttons zur globalen Steuerung des Connection-Managers verborgen.

Button	Beschreibung
<b>Deactivate Connaction-Manager</b>	Dekativiert den Connection-Manager, der Connection-Manager Dienst wird beim Systemstart nicht gestartet. <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <p><b>Hinweis</b></p> <ul style="list-style-type: none"> <li>➤ Der Connection-Manager wird hierbei nicht gestoppt</li> </ul> </div>
<b>Activate Connaction-Manager</b>	Aktiviert den Connection-Manager, der Connection-Manager wird beim Systemstart gestartet. <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <p><b>Hinweis</b></p> <ul style="list-style-type: none"> <li>➤ Der Connection-Manager wird hierbei nicht gestartet</li> </ul> </div>
<b>Stop Connaction-Manager</b>	Stoppt den Connection-Manager Dienst, dabei werden auch alle eingetragenen Verbindungen beendet.
<b>Restart Connaction-Manager</b>	Beendet den Connection-Manager Dienst, stoppt alle eingetragenen Verbindungen und startet den Connection-Manager mit allen Verbindungseinträgen neu.

### 5.3.1.1.4 Add Connection (Connection-Dial-Entry Parameter)

In diesem Menü werden die Einstellungen für eine physikalische Verbindung festgelegt. Um die Konfiguration einfacher zu gestalten, wurde die Konfigurationsseite unterteilt. Standardmäßig werden dabei die »Advanced Connection Settings« nicht ausgeklappt dargestellt.

Kommando	Beschreibung
<b>Connection Name</b>	der zur Anzeige verwendete Name der Verbindung (z.B. »Main« oder »Backup«)
<b>Use Interface</b>	Auswahl der zu benutzenden Verbindung
<i>SIM card</i>	<i>gibt die zu verwendende SIM Karte an (nur bei Verwendung einer WWAN Schnittstelle)</i>
<b>Enable</b>	legt fest ob die Verbindung beim Start des Connection Manager aktiviert wird
<b>Update DynDNS entry</b>	Soll ein DynDNS Update durchgeführt werden, wenn die Verbindung aufgebaut ist wird dies hier mit Yes aktiviert.
<b>Use IPSec-Interface</b>	definiert die zu verwendende IPSec-Schnittstelle

### 5.3.1.1.4.1 Advanced Connection Settings

Kommando	Beschreibung				
<b>Power Up Delay</b>	wartet <i>n</i> Sekunden nach dem Systemstart mit dem Aufbau der Verbindung; mit dieser Option lässt sich eine Startreihenfolge der Einträge festlegen				
<b>Maximum Negotiation Timeout</b>	legt die maximale Wartezeit für den Aufbau einer Verbindung in Sekunden fest (default: 30 sec)				
<b>Add these DNS-Serves</b>	Hier angegebene DNS Server (mit Komma getrennt) werden hinzugefügt, wenn der Verbindungseintrag initialisiert wird.				
<b>Dial Attempts</b>	legt die Anzahl der Wählversuche fest bevor der Status auf »disconnected« geändert wird				
<b>Redial delay</b>	definiert wie viele Sekunden das Gerät zwischen den einzelnen Wählversuchen wartet				
<b>Synchronize Time</b>	führt eine Zeitsynchronisierung durch wenn die Verbindung aufgebaut wurde				
<b>NTP-Server</b>	Zeitserver zu dem nach einem erfolgreichen Verbindungsaufbau synchronisiert wird.				
<b>Update DNS Server</b>	legt fest ob ein DNS Server Update durchgeführt werden soll wenn das Interface in Betrieb geht				
<b>Debug Mode</b>	definiert den Debug-Modus für diese Verbindung fest				
<b>Reset</b>					
<b>Reset UMTS-Modem after this many failed connections</b>	legt die Anzahl der Wählversuche fest bevor das UMTS-Modem zurückgesetzt wird				
<b>Reboot after this many failed connections</b>	nach <i>n</i> fehlgeschlagenen Verbindungsversuchen wird ein Router-Neustart durchgeführt  <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p><b>Hinweis</b></p> <ul style="list-style-type: none"> <li>➤ Zähler wird bei einer erfolgreichen Verbindung zurückgesetzt</li> </ul> </div>				
<b>Reboot after this many deactivated connections</b>	nach <i>n</i> deaktivierten Verbindungsversuchen wird ein Router-Neustart durchgeführt  <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p><b>Hinweis</b></p> <ul style="list-style-type: none"> <li>➤ dieser Zähler wird erhöht, wenn eine bestehende Verbindung durch den Interface-Checker oder Ping-Checker deaktiviert wurde</li> </ul> </div>				
<b>Pre-Reboot Command</b>	Kommando das vor dem Reboot durchgeführt werden soll				
<b>Reboot Mode</b>	legt die Art des Neustarts fest				
	<table border="0" style="width: 100%;"> <tr> <td style="width: 15%;"><b>Normal</b></td> <td>das Gerät wird geregelt heruntergefahren und danach neu gestartet</td> </tr> <tr> <td><b>Forced</b></td> <td>Startet das Gerät direkt neu, die laufenden Prozesse werden dabei nicht geregelt beendet</td> </tr> </table>	<b>Normal</b>	das Gerät wird geregelt heruntergefahren und danach neu gestartet	<b>Forced</b>	Startet das Gerät direkt neu, die laufenden Prozesse werden dabei nicht geregelt beendet
<b>Normal</b>	das Gerät wird geregelt heruntergefahren und danach neu gestartet				
<b>Forced</b>	Startet das Gerät direkt neu, die laufenden Prozesse werden dabei nicht geregelt beendet				

Kommando	Beschreibung
<b>Connect time control</b>	
<b>Maximum Uptime</b>	Zeit in Sekunden die eine Verbindung maximal bestehen soll  <div style="border: 1px solid black; padding: 5px;"> <p><b>Hinweis</b></p> <ul style="list-style-type: none"> <li>➤ Die Verbindung wird unmittelbar in den Status »disconnected« versetzt, unabhängig von anderen laufenden Vorgängen</li> </ul> </div>
<b>Enable Daily Disconnect</b>	ermöglicht eine geregelte tägliche Unterbrechung der Verbindung
<b>Daily Stop Time</b>	Zeit zu der die Verbindung getrennt werden soll
<b>Daily Start Time</b>	Gibt die Zeit an zu der die Verbindung gestartet wird
<b>Add random minutes to Time</b>	Wählt beim Start des Connection Managers einmalig einen zufälligen Wert innerhalb des angegebenen Bereiches (0-n). Dieser wird zu <b>Daily Stop Time</b> und <b>Daily Start Time</b> addiert. Die Verwendung dieser Funktion empfiehlt sich für Außenstellen um bei größeren Netzen nicht alle Verbindungen zeitgleich neu aufzubauen, dadurch wird eine Entlastung der Zentralseite erzielt.
<b>Ping Health Checker</b>	
<b>Enable Ping-Checker</b>	der Ping-Checker wird aktiviert/deaktiviert  <div style="border: 1px solid black; padding: 5px;"> <p><b>Hinweis</b></p> <ul style="list-style-type: none"> <li>➤ Der Ping-Cecker überwacht die Verbindung aktiv</li> <li>➤ Empfiehlt sich besonders für den mobilen Einsatz und hochverfügbare Anbindungen</li> </ul> </div>
<b>Ping IP/Host</b>	gibt die IP oder den Host an, der zum Test gepingt wird
<b>Ping-Interface</b>	gibt die Schnittstelle an über die der Ping geschickt werden soll (notwendig für Ping-Recovery)
<b>Ping Gateway</b>	legt das zu benutzende Gateway fest (notwendig für Ping-Recovery)
<b>Ping Interval</b>	gibt das zu verwendende Ping Intervall an (Sekunden, z.B. 60)
<b>Ping Interval if one request failed</b>	Intervall in das nach einem unbeantworteten Ping gewechselt wird (Sekunden, z.B. 2)
<b>Ping Size</b>	Definiert die Größe des Ping-Paketes in Bytes. Der Standard 8-Byte ICMP Header wird hier hinzugerechnet. (z.B. 8 [+ 8 B ICMP- und 20 B IP-Header = 36 Bytes])
<b>Ping Timeout</b>	legt fest wie lange auf eine Ping-Antwort gewartet wird (Sekunden, z.B. 4)
<b>Maximum failed Requests</b>	maximale Anzahl der unbeantworteten Ping-Anfragen bevor der zugehörige Eintrag deaktiviert wird (default: 2)
<b>Perform Ping-Recovery</b>	aktiviert/deaktiviert die Ping-Recovery  <div style="border: 1px solid black; padding: 5px;"> <p><b>Hinweis</b></p> <ul style="list-style-type: none"> <li>➤ Mit Ping-Recovery wird bei der Initialisierung der Verbindung geprüft ob Daten übertragen werden</li> <li>➤ im Fehlerfall wird die Verbindung getrennt</li> </ul> </div>
<b>Ping Recovery Interval</b>	Zeit in Sekunden bis ein weiterer Ping durchgeführt wird
<b>Ping Recovery Timeout</b>	legt fest wie lange auf eine Ping-Antwort gewartet wird (Sekunden)

Kommando	Beschreibung										
<b>Ping Recovery Count</b>	Anzahl der maximal erlaubten Ping Recovery-Anfragen die unbeantwortet bleiben dürfen bevor der zugehörige Eintrag deaktiviert wird										
<b>Dependencies</b>											
<b>Go Out-of-Service</b>	dieser Verbindungseintrag soll (nicht) außer Betrieb genommen werden										
<b>Out-of-Service-Time</b>	Zeit in Sekunden bis der Verbindungseintrag reaktiviert wird										
<b>Inhibited by these Connections</b>	Legt die Verbindungen fest, die die aktuelle unterdrücken dürfen, wenn... <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Mode</th> <th></th> </tr> </thead> <tbody> <tr> <td><b>Active</b></td> <td>versucht wird diese Verbindung aufzubauen.</td> </tr> <tr> <td><b>Initializing</b></td> <td>die Verbindung steht, die Initialisierung, wie z.B. Route hinzufügen, noch nicht abgeschlossen ist.</td> </tr> <tr> <td><b>Connected</b></td> <td>die Verbindung steht und die Initialisierung abgeschlossen ist.</td> </tr> <tr> <td><b>OOS</b></td> <td>wenn die Verbindung »Out of Service« ist.</td> </tr> </tbody> </table>	Mode		<b>Active</b>	versucht wird diese Verbindung aufzubauen.	<b>Initializing</b>	die Verbindung steht, die Initialisierung, wie z.B. Route hinzufügen, noch nicht abgeschlossen ist.	<b>Connected</b>	die Verbindung steht und die Initialisierung abgeschlossen ist.	<b>OOS</b>	wenn die Verbindung »Out of Service« ist.
Mode											
<b>Active</b>	versucht wird diese Verbindung aufzubauen.										
<b>Initializing</b>	die Verbindung steht, die Initialisierung, wie z.B. Route hinzufügen, noch nicht abgeschlossen ist.										
<b>Connected</b>	die Verbindung steht und die Initialisierung abgeschlossen ist.										
<b>OOS</b>	wenn die Verbindung »Out of Service« ist.										
<b>Routing</b>											
<b>Default-Routing</b>	<table border="1" style="width: 100%; border-collapse: collapse;"> <tbody> <tr> <td><b>Interface</b></td> <td>das zu verwendende Interface (muss angegeben werden)</td> </tr> <tr> <td><b>Gateway</b></td> <td>Gateway für die Default Route</td> </tr> <tr> <td><b>Metric</b></td> <td>legt die Routingmetrik fest</td> </tr> </tbody> </table>	<b>Interface</b>	das zu verwendende Interface (muss angegeben werden)	<b>Gateway</b>	Gateway für die Default Route	<b>Metric</b>	legt die Routingmetrik fest				
<b>Interface</b>	das zu verwendende Interface (muss angegeben werden)										
<b>Gateway</b>	Gateway für die Default Route										
<b>Metric</b>	legt die Routingmetrik fest										
<b>Static Routing</b>	<table border="1" style="width: 100%; border-collapse: collapse;"> <tbody> <tr> <td><b>Destination</b></td> <td>die zu verwendende Zieladresse (muss angegeben werden)</td> </tr> <tr> <td><b>Gateway</b></td> <td>Gateway für die statische Route</td> </tr> <tr> <td><b>Interface</b></td> <td>das zu verwendende Interface (muss angegeben werden)</td> </tr> <tr> <td><b>Metric</b></td> <td>legt die Routing-Metrik fest</td> </tr> </tbody> </table>	<b>Destination</b>	die zu verwendende Zieladresse (muss angegeben werden)	<b>Gateway</b>	Gateway für die statische Route	<b>Interface</b>	das zu verwendende Interface (muss angegeben werden)	<b>Metric</b>	legt die Routing-Metrik fest		
<b>Destination</b>	die zu verwendende Zieladresse (muss angegeben werden)										
<b>Gateway</b>	Gateway für die statische Route										
<b>Interface</b>	das zu verwendende Interface (muss angegeben werden)										
<b>Metric</b>	legt die Routing-Metrik fest										
<b>State-Change-Scripts</b>	legt das Script fest das bei der jeweiligen Statusänderung ausgeführt werden soll <b>[Out-Of-Service,Active,Initialization,Connected, Disconnecting,Disconnected]</b>										

### 5.3.1.2 Logical Subordinated Connections

Kommando	Beschreibung
<b>Logical Subordinated Connections</b>	Übersicht über die untergeordneten logischen Verbindungen; über den Button <b>Add Connection</b> kann ein neuer Connection-Logical-Entry definiert werden

Eine »Logical Subordinated Connection« stellt eine logische Verbindung (z.B. IPSec-Verbindung) dar und kann

- ▷ in Abhängigkeit des Status jedes beliebigen anderen Connection-Logical-Entry gestellt werden.
- ▷ seinen übergeordneten Connection-Dial-Entry deaktivieren.

Beim Systemstart holt sich der Logical Subordinated Connection Eintrag seine Konfiguration und geht in die Abarbeitungsschleife wenn der übergeordnete Connection-Dial-Entry erfolgreich aufgebaut wurde. Wenn ein »Power Up Delay« gesetzt ist wartet der Eintrag bis zum Ablauf der Zeit.

In der Abarbeitungsschleife startet der Eintrag, in Abhängigkeit seines internen Status und dem Status der anderen logischen Einträge seinen Dienst.

Ein logischer Eintrag ist die einzige Instanz innerhalb des Connection-Managers die im Blocking-Modus läuft. Was bedeutet, dass jeder Systembefehl das Modul für andere Aufgaben blockiert.

#### 5.3.1.2.1 Inhibit

Bei jedem Zyklus der Abarbeitungsschleife überprüft jeder Connection-Logical-Entry den Status der konfigurierten Inhibit-Einträge. Wenn der Status eines Eintrages gleich oder größer ist wie unter „Inhibit Mode“ eingestellt, wird der laufende Connection-Logical-Entry getrennt.

Wenn zum Beispiel der »Inhibit-Mode« von Logical\_Connection\_2 auf »Logical\_Connection\_1, Mode Active« gesetzt ist, wird die zweite logische Verbindung deaktiviert, wenn die erste logische Verbindung einen Status wie folgt hat:

- ◊ Active
- ◊ Connected
- ◊ Disconnecting

Wenn logische Verbindung 1 einen Status wie folgt aufweist wird logische Verbindung 2 erlaubt:

- ◊ Power Up Delay
- ◊ Disconnectet

#### 5.3.1.2.2 Logical-Interface- und Ping-Checker

Der Logical-Interface-Checker wird während der Initialisierung für alle Einträge gestartet. Dabei überprüft er automatisch jede Sekunde den Status des Interfaces. Wenn das Interface, aus welchem Grund auch immer nicht funktioniert, wird der entsprechende Connection-Logical-Entry deaktiviert. Wenn es sich bei dem logischen Eintrag um eine IPSec-Verbindung handelt wird die aktuelle Phase 2-SA überprüft.

Wenn der Ping-Checker eingerichtet ist, startet dieser während der Initialisierungsphase. Der Ping-Checker sendet ICMP-Anfragen in dem konfigurierten Intervall und überprüft ob eine Antwort empfangen wird. Wird während der unter »Maximum failed Requests« definierten Anzahl an Versuchen keine Antwort empfangen, wird der entsprechende Eintrag deaktiviert.

##### **Hinweis**

- Ein Connection-Dial-Entry der durch einen logischen Eintrag mit der Funktion »Deactivate superordinated Connection« deaktiviert wird wechselt unmittelbar in den Status »disconnected«, auch wenn noch Wählversuche offen sind.

#### 5.3.1.2.3 Add Connection (Connection-Logical-Entry Parameter)

In diesem Menü werden die Einstellungen für eine logische Verbindung festgelegt. Die Optionen für eine logische Verbindung entsprechen weitestgehend denen der physikalischen (siehe [5.3.1.1.3 Verbindungsübersicht](#)), deshalb werden hier nur die Abweichungen aufgeführt.

Kommando	Beschreibung
<b>Use IPsec Connection</b>	Auswahl der zu benutzenden IPsec-Verbindung
<b>Deactivate superordinated Connection</b>	legt fest ob die übergeordnete Verbindung deaktiviert werden soll
<b>Change Power-Up-Delay of these Logical Connections if this Connection gets disconnected</b>	ändert das Power Up Delay für die ausgewählte Verbindung auf <b>n</b> Sekunden, wenn die Verbindung getrennt wurde

### 5.3.2 Static Connections

Im Gegensatz zum Connection-Manager findet bei der Static Connection keine Überwachung oder die Verwendung einer Backup Verbindung statt. Es können nur statische Verbindungen eingetragen werden.

#### Hinweis

- Die Static Connections empfehlen sich daher nur für Dial-on-Demand und Dial-In Verbindungen.

## 5.4 DHCP Server

Über das DHCP Server Menü ist die Konfiguration eines DHCP-Servers möglich. DHCP-Server stellen Clients Netzinformationen bereit und verwalten diese zentral. Zu den Netzinformationen gehören unter anderem die IP-Adresse, Netzmaske, Router und DNS-Adressen, DNS-Namen usw.

Neben einer komplett dynamischen Konfiguration des Netzwerkes können bestimmten Stationen (über deren MAC-Adresse) auch feste IP-Adressen zugewiesen werden. Dies ist sinnvoll, wenn einige Stationen aufgrund der IP-Adressen authentifiziert werden sollen. Natürlich ist auch Mischbetrieb beider Versionen möglich.

Über die Übersichtsseite der DHCP-Serverkonfiguration kann man neue Subnetze, gemeinsam genutzte Netzwerke und Host bzw. Hostgruppen definieren. Außerdem ist das Editieren der Client-Stationen und der Netzwerkschnittstelle möglich. Über den Button **Start Server** startet man den DHCP-Server.

Kommando	Beschreibung
<b>Subnet description</b>	Hier können sie eine Beschreibung des Subnetzes eintragen.
<b>Network address</b>	Tragen sie hier die IP-Adresse Ihres Netzes ein.
<b>Netmask</b>	Tragen sie hier die Netzmaske Ihres Netzes ein.
<b>Address ranges</b>	Hier können sie angeben innerhalb welchen Bereiches sich die automatisch vergebenen IP-Adressen befinden sollen (1-254)
<b>Dynamic BOOTP?</b>	Aktiviert das dynamische BOOTP (Bootstrap Protocol) welches eine Vorgängerversion von DHCP ist.
<b>Shared network</b>	Auswahl der Subnetze, die ein gemeinsames physikalisches Netzwerk verwenden.
<b>Boot filename</b>	Wenn sie BOOTP verwenden müssen sie hier den Namen des Boot-Image Files angeben.
<b>Boot file server</b>	Wenn sie BOOTP verwenden können sie hier angeben, ob der Router BOOTP anfragen direkt annehmen soll, oder ob diese an einen anderen Server weitergeleitet werden sollen.

Kommando	Beschreibung
<b>Lease length for BOOTP clients</b>	Vergabelänge für BOOTP-Clients in Sekunden.
<b>Dynamic DNS enabled?</b>	Ermöglicht Hostnamen an dynamische IP-Adressen zu vergeben.
<b>Dynamic DNS reverse domain</b>	Zu der angegebenen IP-Adresse, wird mit Hilfe des Domain Name System (DNS) versucht, einen entsprechenden Domainnamen aufzulösen.
<b>Allow unknown clients?</b>	Unbekannten Clients die Anwahl an den DHCP-Server erlauben oder keine IP-Adresse zuweisen.
<b>Hosts directly in this subnet</b>	Gruppen die sich direkt im Subnetz befinden.
<b>Default lease time</b>	Die Zeit in Minuten der Gültigkeit der zugewiesenen DHCP Konfiguration des Clients.
<b>Maximum lease time</b>	Angabe der maximalen Gültigkeit der zugewiesenen DHCP Konfiguration
<b>Server name</b>	Name des DHCP Servers.
<b>Lease end for BOOTP clients</b>	Dieser Wert gibt eine Zeit an, an dem alle BOOTP Einträge gelöscht werden. Der Defaultwert ist „Never“. Die Zeit muss im Format W YYYY/MM/DD HH:MM:SS (W=Wochentag 0=Sonntag bis 6=Samstag; YYYY=Jahr, MM=Monat; DD=Tag; HH=Stunden; MM=Minuten; SS=Sekunden) eingeben werden.
<b>Dynamic DNS domain name</b>	Angabe des Domain-Namen der den Hosts angefügt wird z.B.: testhost.M3000
<b>Dynamic DNS hostname</b>	Dieser Wert gibt an, ob der Hostname vom Client übernommen wird, oder ein fest eingestellter Hostnamen benutzt wird.

## 5.5 DNS Server Update

DNS Server Update führt mittels »DynDNS« ein Update auf einem festgelegten DNS Server aus.

DynDNS auch DDNS (dynamischer Domain-Name-System-Eintrag) ist ein System, das in Echtzeit Domain-Name-Einträge aktualisieren kann. Damit ist es möglich, ein Gerät welches über eine dynamische IP-Adresse verfügt, immer unter dem gleichen DNS-Namen anzusprechen.

Kommando	Beschreibung
<b>DNS server IP address</b>	Adresse des DNS Servers
<b>Zone</b>	Domain für das Update (z.B. <i>mycompany.com</i> )
<b>Name</b>	Name der aktualisiert werden soll (z.B. <i>site1</i> )
<b>Username</b>	Benutzername der vom DynDNS Service Provider zugeteilt wurde
<b>Password</b>	Passwort das vom DynDNS Service Provider zugeteilt wurde
<b>Confirm Password</b>	Passwort wiederholung zur Bestätigung
<b>Time to live</b>	gibt die Gültigkeit des Namenseintages in Sekunden an; nach dieser Zeit muß die Namensauflösung wiederholt werden
<b>Always delete previous records</b>	legt fest, ob die zuvor gespeicherten IP Adressen gelöscht werden sollen

## 5.6 DNSmasq

DNSmasq kommt bei Routern der C-Serie als DNS Relay zum Einsatz. Zudem stellt der Dienst vielfältige Möglichkeiten im Bereich DNS und DHCP zur Verfügung.

Auf der Menüseite können unter ***/etc/dnsmasq.conf*** alle relevanten Einstellungen direkt an der Konfigurationsdatei vorgenommen werden.

### Hinweis

- DNSmasq beantwortet in der ausgelieferten Konfiguration nur DNS Anfragen an lokalen Schnittstellen.

Änderungen an der Konfiguration werden mit dem Button **Save Configuration** gespeichert.

Ist der Dienst gestartet, lässt sich eine geänderte Konfiguration durch **Restart DNSmasq** übernehmen.

Zudem lässt sich DNSmasq

- ◊ starten **Start DNSmasq**
- ◊ stoppen **Stop DNSmasq**
- ◊ neustarten **Restart DNSmasq**

Und definieren ob der DNSmasq Dienst beim Booten des Routers gestartet werden soll.

- ◊ Aktivieren **Activate DNSmasq at boot time**
- ◊ Deaktivieren **Deactivate DNSmasq at boot time**

Unter <http://thekelleys.org.uk/dnsmasq/docs/dnsmasq-man.html> befindet sich eine ausführliche Dokumentation zu DNSmasq.

## 5.7 Dynamic DNS Update

Unter diesem Menüpunkt kann die Konfiguration des Dynamic DNS Update Dienstes ([www.dyndns.com](http://www.dyndns.com)) angepasst werden. Um diesen Dienst nutzen zu können, ist ein Konto bei [www.dyndns.com](http://www.dyndns.com) erforderlich.

Kommando	Beschreibung
<b>System</b>	Verwenden Sie folgende Einstellungen: <b>Dynamic DNS:</b> wenn der Router die IP-Adresse dynamisch zugewiesen bekommt. <b>Static DNS:</b> wenn der Router über eine statische IP-Adresse verfügt. <b>Custom DNS:</b> wenn Sie die Custom DNS – Option von <a href="http://www.dyndns.com">www.dyndns.com</a> nutzen.
<b>Hostname</b>	DynDNS-Adresse, welche bereits bei <a href="http://www.dyndns.com">www.dyndns.com</a> eingerichtet sein muss
<b>Username</b>	Benutzername für den DynDNS-Account
<b>Password</b>	Passwort für den DynDNS-Account
<b>Enable Wildcards</b>	Erlaubt es, weitere Subdomains vor der DynDNS-Adresse zu verwenden (z.B. <a href="http://ftp.aussenstelle1.dyndns.com">ftp.aussenstelle1.dyndns.com</a> )

Kommando	Beschreibung
<b>Use SSL</b>	<b>No:</b> es können keine SSL-Verbindungen über diese DynDNS-Adresse zum Router aufgebaut werden. <b>Yes:</b> es können SSL-Verbindungen über diese DynDNS-Adresse zum Router aufgebaut werden
<b>Mail Exchange</b>	A-Record eines Mailservers, welcher den Emailverkehr für die DynDNS-Adresse regelt (optional)
<b>Backup MX</b>	Gibt an, ob das Gerät z.B. als Secondary-MX arbeiten soll

## 5.8 IPsec VPN

Im IPsec VPN Menü können IPsec Verbindungen erstellt und verwaltet werden. Die IPsec Implementierung basiert auf dem Open Source Projekt strongSwan.

Auf der Menüseite können unter ***/etc/ipsec.conf*** alle relevanten Einstellungen direkt an der Konfigurationsdatei vorgenommen werden. Unter ***/etc/ipsec.secrets*** werden die Authentifizierungseinstellungen – wie zum Beispiel PreSharedKeys oder Zertifikatsinformationen – verwaltet. Eine ausführliche Dokumentation und Beispielkonfigurationen befinden sich unter <https://wiki.strongswan.org>.

Änderungen an der Konfiguration werden mit dem Button **Save Configuration** gespeichert.

Ist der IPsec Server gestartet, lässt sich mittels **Reload Configuration** die Konfiguration nach einer Änderung neu laden.

Zudem lässt sich hier der IPsec Server

- ◊ starten **Start IPsec VPN**
- ◊ stoppen **Stop IPsec VPN**
- ◊ neustarten **Restart IPsec VPN**

Und definieren ob der IPsec Dienst beim Booten des Routers gestartet werden soll.

- ◊ Aktivieren **Activate IPsec VPN at boot time**
- ◊ Deaktivieren **Deactivate IPsec VPN at boot time**

### Hinweis

- Für Außenstellen empfiehlt es sich IPsec durch den Connection Manager dynamisch verwalten zu lassen.
- Dazu wird an eine bestehende Verbindung (Connection-Dial-Entry) eine logische Verbindung (Logical Subordinated Connection) angehängt.

### 5.8.1 Kommandozeilenbefehle (SSH)

Nachfolgend ist eine kleine Auswahl an Befehlen für strongSwan zu finden, mit welchen der Dienst gesteuert und Analysen durchgeführt werden können.

Kommando	Beschreibung
<b>ipsec start</b>	Startet den IPsec Dienst und lädt die Verbindungsparameter. Ist bei einem <b>conn</b> -Eintrag <b>auto=start</b> angegeben wird dieser Tunnel aufgebaut.
<b>ipsec stop</b>	Stoppt den IPsec Dienst und alle Tunnel
<b>ipsec restart</b>	Führt einen Restart des IPsec Dienstes durch. Dabei werden alle bestehenden Verbindungen getrennt und wenn bei einem <b>conn</b> -Eintrag nicht <b>auto=start</b> angegeben ist wird dieser nicht wieder gestartet.
<b>ipsec reload</b>	Ist der IPsec Server gestartet, lässt sich hiermit die Konfiguration nach einer Änderung neu laden.
<b>ipsec up</b> <b>&lt;connectionname&gt;</b>	Initiiert den Verbindungsaufbau des angegebenen Tunnels.
<b>ipsec down</b> <b>&lt;connectionname&gt;</b>	Baut den angegebenen Tunnel ab.
<b>ipsec status</b> <b>&lt;connectionname&gt;</b>	Gibt den Tunnel-Status des angegebenen Tunnels, oder wenn keine Verbindung angegeben ist aller verbundenen Einträge aus.
<b>ipsec statusall</b> <b>&lt;connectionname&gt;</b>	Listet den Tunnel-Parameter und den Status des angegebenen Tunnels, oder wenn keine Verbindung angegeben ist aller Einträge auf.
<b>ipsec stroke loglevel</b> <b>ike 1</b>	Setzt das Loglevel für die IKE Ebene höher, um zum Beispiel beim Einrichten einer Verbindung bessere Diagnosemöglichkeiten zu haben. Default ist <b>0</b> .
<b>ip route list table</b> <b>220</b>	Zeigt die Routingeinträge der strongSwan eigenen Routingtabelle an.
<b>ip xfrm</b>	Das <b>xfrm</b> -Modul steuert den Paketfluss und kapselt die für einen IPsec-Tunnel bestimmten Pakete entsprechend.
<b>ip xfrm policy show</b>	Dieser Befehl zeigt die aktiven/installierten Policies.
<b>ip xfrm state</b>	Gibt den aktuellen <b>xfrm</b> -Status aus. (z.B. Protokoll, SPI)
<b>ip xfrm monitor</b>	Startet ein Monitoring über die durch <b>xfrm</b> behandelten Pakete.

## 5.9 L2TP

In diesem Menü wird L2TP (Layer 2 Tunneling Protocol) konfiguriert, ein VPN Protokoll zur Tunnelung von Daten der Sicherungsschicht (Schicht 2 des OSI Modells).

### Hinweis

- Da L2TP von sich aus keine Verschlüsselung liefert wird eine Kapselung via IPsec empfohlen.

Auf der Menüseite können unter **/etc/openl2tp.conf** alle relevanten Einstellungen direkt an der Konfigurationsdatei vorgenommen werden.

Änderungen an der Konfiguration werden mit dem Button **Save Configuration** gespeichert.

Ist der Dienst gestartet, lässt sich eine geänderte Konfiguration durch **Restart L2TP** übernehmen.

Zudem lässt sich openl2tp

- ◊ starten Start L2TP
- ◊ stoppen Stop L2TP
- ◊ neustarten Restart L2TP

Und definieren ob der openl2tp Dämon beim Booten des Routers gestartet werden soll.

- ◊ Aktivieren Activate L2TP at boot time
- ◊ Deaktivieren Deactivate L2TP at boot time

Eine weiterführende Dokumentation kann der Seite <http://www.openl2tp.org> entnommen werden.

## 5.10 Linux Firewall (IPtables)

Die Linux Firewall nimmt mittels der Firewall IPtables bestimmte Filterungen oder Reglementierungen im Datenverkehr vor. Der Paketfilter definiert Regeln, welche festlegen, ob einzelne oder zusammenhängende Pakete das Zugangsschutzsystem passieren dürfen oder abgeblockt werden. Eine solche Regel wäre zum Beispiel: verwerfe alle Pakete, die von der IP-Adresse 1.2.3.4 kommen.

Jedes Netzwerk Paket das zum Router gesendet, vom Router versendet oder weitergeleitet wird, durchläuft zuerst eine oder mehrere Ketten (Chains) von Verhaltensregeln (Rules) wie der Router mit dem Paket verfahren soll. Die einzelnen Regeln werden innerhalb des Ablaufes von oben nach unten abgearbeitet.

### 5.10.1 Tabellen (Tables)

Die IPtables-Architektur gruppiert die Regeln für die Verarbeitung von Netzwerk-Paketen gemäß ihrer Funktion in drei Tabellen.

#### Packet filtering (filter)

Die Standard-Tabelle, die immer dann verwendet wird, wenn keine Tabelle explizit angegeben wird. Diese Tabelle besteht aus den Ketten INPUT, FORWARD und OUTPUT. Eventuell lassen sich in dieser Tabelle weitere benutzerdefinierte Chains unterbringen.

#### Packet alteration (mangle)

In dieser Tabelle finden Sie die Ketten PREROUTING und OUTPUT und hier werden spezielle Änderungen an Paketen vorgenommen wie zum Beispiel die Änderung des ToS (Type of Service) oder der TTL (Time to life) Zeit des IP-Header.

#### Network address translation (nat)

Diese Tabelle ist für alle Arten von Adress-Umsetzungen oder Port-Forwarding verantwortlich und besteht aus den Ketten PREROUTING, OUTPUT und POSTROUTING. Die in dieser Tabelle befindlichen Ketten werden für jedes erste Paket einer neuen Verbindung aufgerufen und führen entsprechende Änderungen an den Port- oder IP-Nummern der Pakete durch.

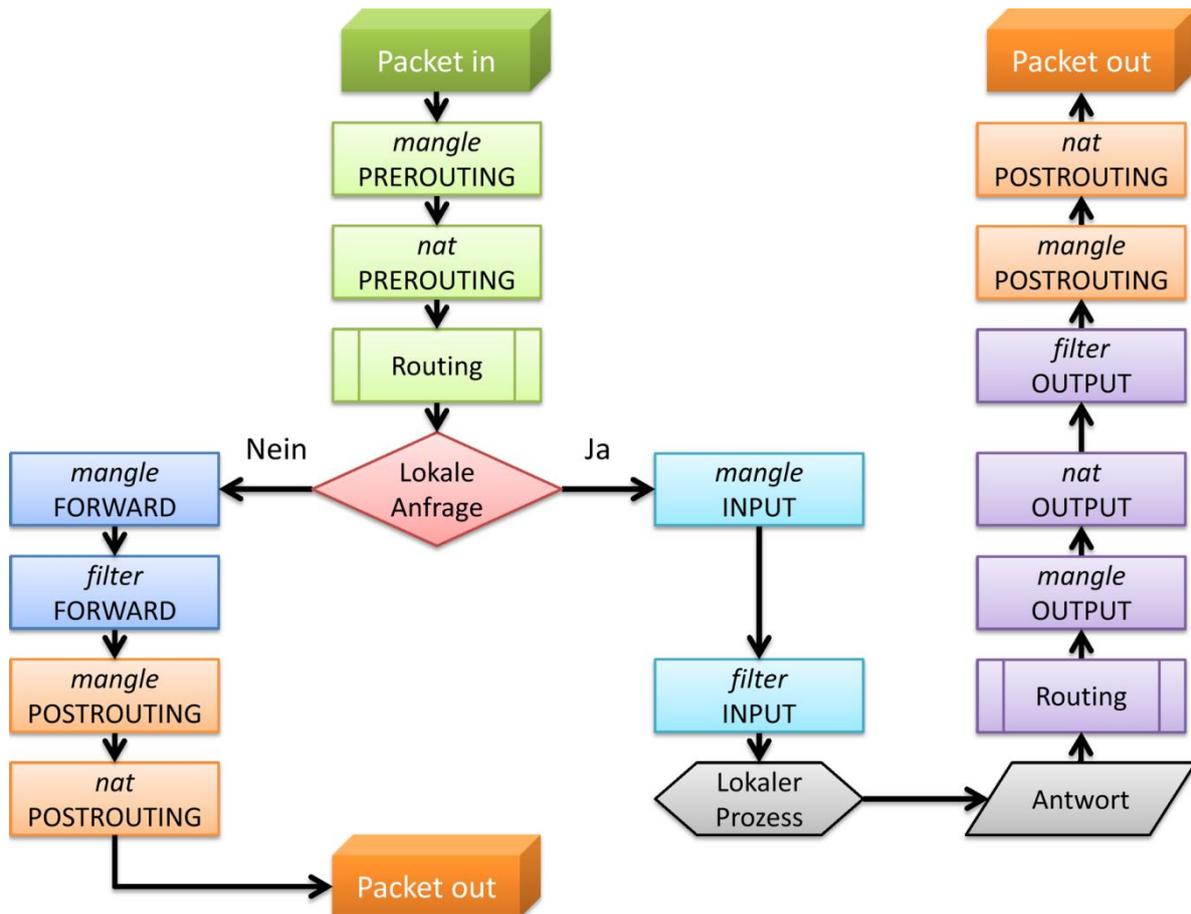


Abbildung 20: Darstellung wie die Firewall abgearbeitet wird

### 5.10.2 Ketten (Chains)

Iptables hat fünf fest vorgegebene Ketten (built-in chains) im Kernel eingebaut, welche wie nachfolgend aufgeführt abgearbeitet werden:

#### Packets before routing (PREROUTING)

Hier wird die Methode für Pakete eingestellt die unmittelbar vor der Routing-Entscheidung greift.

#### Incoming packets (INPUT)

Hier kann die Methode für alle eingehenden Pakete eingestellt werden.

#### Forwarded packets (FORWARD)

Hier kann die Methode für alle weiterzuleitenden Pakete eingestellt werden.

#### Outgoing packets (OUTPUT)

Hier kann die Methode für alle ausgehenden Pakete eingestellt werden.

#### Packets after routing (POSTROUTING)

Die Methode für alle lokalen und gerouteten Pakete wird hier eingetragen.

**Hinweis**

- IPtables arbeitet immer von Oben nach Unten
- Regeln (z.B. Destination NAT) die in dem Bereich »Pakets before routing (PREROUTING)« angegeben sind, werden umgehend verarbeitet und laufen **nicht** durch die Kette (Chain) »Incoming packets (INPUT)« oder eine der nachfolgenden

### 5.10.3 Ziele (Targets)

Jede Kette kann Regeln enthalten, welche dabei aus einer Filterspezifikation und einem Ziel (Target) bestehen. Das Ziel gibt letztendlich an, was mit einem Paket passiert. Ein Ziel kann eine benutzerdefinierte Kette, ein Standardziel oder ein erweitertes Ziel sein. Für die fest vorgegebenen Ketten kann man eine Default Policy definieren, die angewandt wird, wenn keine der Regeln greift. Eine Policy ist immer ein Standardziel, eine Übersicht über die Standardziele finden Sie in der Tabelle [Chain and action details](#) unter [Action to take](#). Default ist **ACCEPT**.

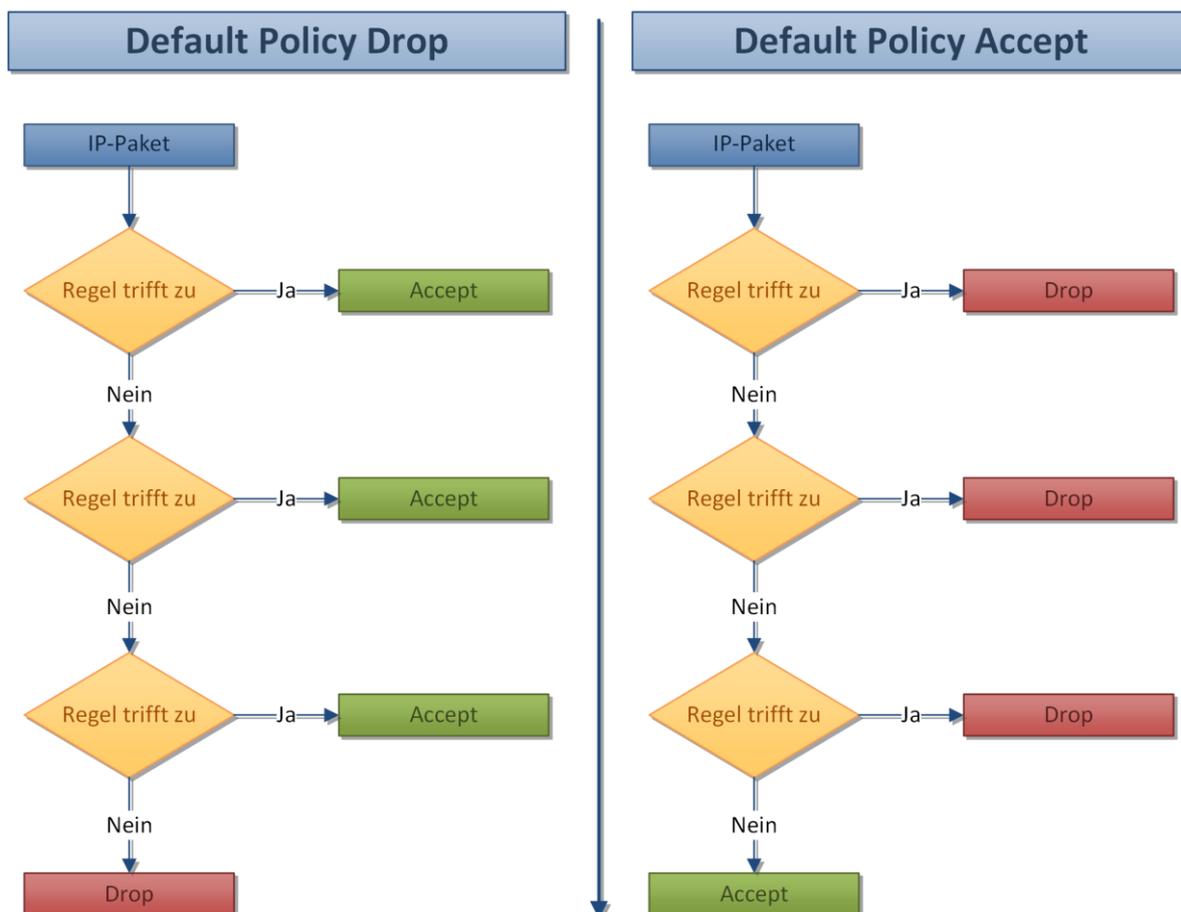


Abbildung 21: Abarbeitung einer Kette mit Default Policy Drop beziehungsweise Accept

### 5.10.4 Das Linux Firewall Menü

Wenn Sie das Menü das erste Mal öffnen und die IPtables Firewall noch nicht aufgesetzt ist erscheint ein Formular, mit dem schnell Grundeinstellungen für die Firewall gesetzt werden können.

Sind diese Einstellungen einmal durchgeführt erscheint das IPtables Menü.

## 5.10.5 Erstellen einer neuen Regel

Mit einem Klick auf den Button **Add Rule** können Sie neue Regeln innerhalb einer Kette erstellen.

### Hinweis

- IPtables arbeitet immer von Oben nach Unten
- Wenn mehrere Regeln auf ein Paket zutreffen wird das Paket entsprechend der ersten Regel behandelt die auf das Paket zutrifft und läuft **nicht** weiter durch die Regel Kette (Chain)
- Wird zum Beispiel ein Paket durch die 2. Regel von oben erlaubt, würde aber durch die 3. Regel geblockt werden wird das Paket entsprechend der 2. Regel zugelassen

### 5.10.5.1 Chain and action details

Kommando	Beschreibung
<b>Part of chain</b>	Anzeige innerhalb welcher Ablaufkette die Regel erstellt wird
<b>Rule comment</b>	Beschreibung der Regel
<b>Action to take</b>	Je nach ausgewähltem Ketten-Typ können folgende Ziele gewählt werden:
	<b>Do nothing:</b> es wird keine Aktion vorgenommen
	<b>Accept:</b> das Paket wird akzeptiert und verarbeitet
	<b>Drop:</b> das Paket wird ohne Rückantwort an den Sender verworfen
	<b>Reject:</b> das Paket wird verworfen und der Sender, wie unter »Reject with ICMP type« definiert darüber informiert
	<b>Userspace:</b> das Paket wird in die Warteschlange des Userprozesses gestellt
	<b>Exit chain:</b> die Ablaufkette wird verlassen
	<b>Log packet:</b> das Paket wird mit ausgewählten Informationen im Syslog aufgezeichnet und anschließend weiter durch die Kette geleitet
	<b>Run chain:</b> die angegebene Ablaufkette wird ausgeführt
	<b>Redirect:</b> Paket weiterleiten an »Target ports for redirect«
	<b>Destination NAT:</b> Paket weiterleiten an »IPs and ports for DNAT«
	<b>Source NAT:</b> Quell-Adresse wird durch »IPs and ports for SNAT« ersetzt
	<b>Masquerade:</b> Paket Quell-Adresse wird durch die Adresse der ausgehenden Schnittstelle ersetzt

Die ausgewählte Aktion wird nur bei zutreffen **aller** unter **Condition details** definierten Parameter ausgeführt, ansonsten wird die Kette verlassen und mit der Abarbeitung der Nächsten begonnen.

### 5.10.5.2 Condition details

Kommando	Beschreibung
<b>Source address or network</b>	<p><b>Ignored:</b> die Netzwerk Quell Adresse wird ignoriert</p> <p><b>Equals:</b> die Netzwerk Quell Adresse muss dem folgenden Wert entsprechen</p> <p><b>Does not equal:</b> die Netzwerk Quell Adresse muss ungleich dem folgenden Wert sein</p>
<b>Destination address or network</b>	<p><b>Ignored:</b> die Netzwerk Ziel Adresse wird ignoriert</p> <p><b>Equals:</b> die Netzwerk Ziel Adresse muss dem folgenden Wert entsprechen</p> <p><b>Does not equal:</b> die Netzwerk Ziel Adresse muss ungleich dem folgenden Wert sein</p>
<b>Incoming interface</b>	<p><b>Ignored:</b> die eingehende Netzwerkschnittstelle wird ignoriert</p> <p><b>Equals:</b> die eingehende Netzwerkschnittstelle muss dem folgenden Wert entsprechen</p> <p><b>Does not equal:</b> die eingehende Netzwerkschnittstelle muss ungleich dem folgenden Wert sein</p>
<b>Outgoing interface</b>	<p><b>Ignored:</b> die ausgehende Netzwerkschnittstelle wird ignoriert</p> <p><b>Equals:</b> die ausgehende Netzwerkschnittstelle muss dem folgenden Wert entsprechen</p> <p><b>Does not equal:</b> die ausgehende Netzwerkschnittstelle muss ungleich dem folgenden Wert sein</p>
<b>Fragmentation</b>	<p><b>Ignored:</b> Fragmente von IP Paketen werden ignoriert</p> <p><b>Is fragmented:</b> Bei Fragmenten von IP-Paketen gibt es keine Möglichkeit deren Quell- oder Ziel-IP oder -Port zu bestimmen. Deswegen greifen andere Bedingungen nicht und es ist nur mit diesem Parameter möglich die Regel auszuführen.</p> <p><b>Is not fragmented:</b> wenn die IP Pakete nicht fragmentiert sind, wird die Regel ausgeführt</p>
<b>Network protocol</b>	<p><b>Ignored:</b> das Protokoll wird ignoriert</p> <p><b>Equals:</b> das Protokoll muss dem folgenden Wert entsprechen</p> <p><b>Does not equal:</b> das Protokoll muss ungleich dem folgenden Wert sein</p>
<b>Source TCP or UDP port</b>	<p><b>Ignored:</b> der Quell Port wird ignoriert</p> <p><b>Equals:</b> der Quell Port muss dem folgenden Wert oder Bereich entsprechen</p> <p><b>Does not equal:</b> der Quell Port muss ungleich dem folgenden Wert oder Bereich sein</p>
<b>Destination TCP or UDP port</b>	<p><b>Ignored:</b> der Ziel Port wird ignoriert</p> <p><b>Equals:</b> der Ziel Port muss dem folgenden Wert oder Bereich entsprechen</p> <p><b>Does not equal:</b> der Ziel Port muss ungleich dem folgenden Wert oder Bereich sein</p>
<b>Source and destination port(s)</b>	<p><b>Ignored:</b> der Quell und Ziel Port wird ignoriert</p> <p><b>Equals:</b> der Quell und Ziel Port müssen dem folgenden Wert oder Bereich entsprechen</p> <p><b>Does not equal:</b> der Quell und Ziel Port müssen ungleich dem folgenden Wert oder Bereich sein</p>

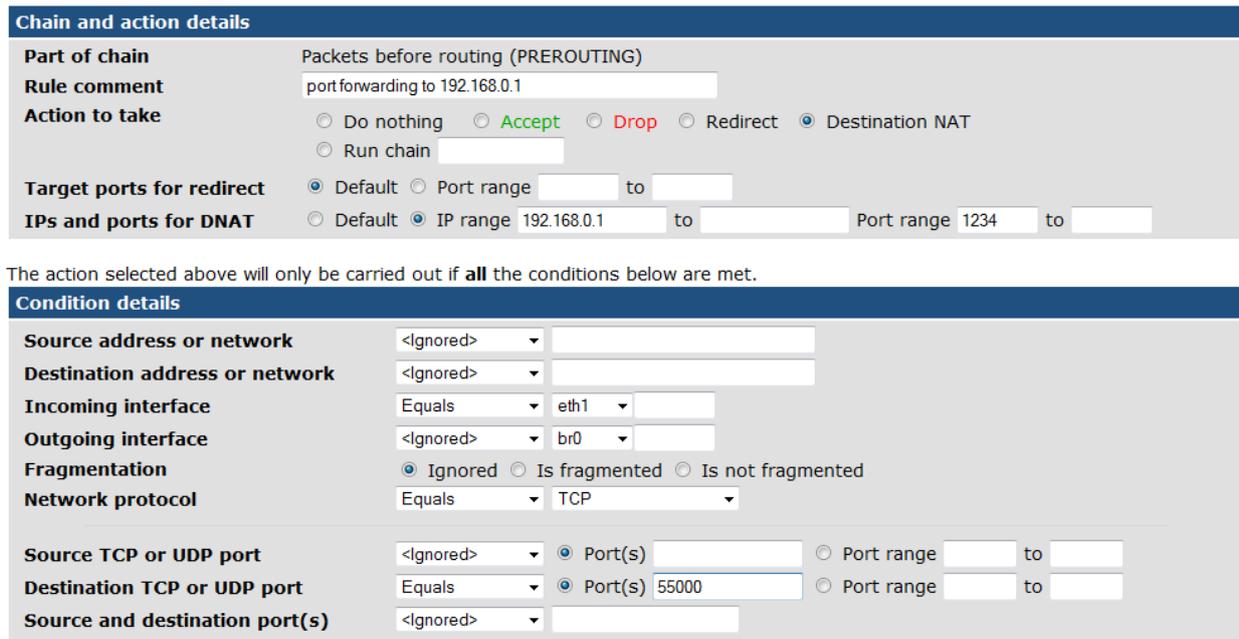
Kommando	Beschreibung
<b>TCP flags set</b>	wenn das TCP Flag ... <b>SYN:</b> ... SYN (Synchronisation) gesetzt ist, ... <b>ACK:</b> ... ACK (acknowledgement) gesetzt ist, ... <b>FIN:</b> ... FIN (final) gesetzt ist, ... <b>RST:</b> ... RST (reset) gesetzt ist, ... <b>URG:</b> ... URG (urgent) gesetzt ist, ... <b>PSH:</b> ... PSH (push) gesetzt ist, ... ... wird die Regel angewandt
<b>TCP option number is set</b>	<b>Ignored:</b> die TCP »option number« wird ignoriert <b>Equals:</b> die TCP »option number« muss dem folgenden Wert entsprechen damit die Regel angewandt wird <b>Does not equal:</b> die TCP »option number« muss ungleich dem folgenden Wert sein, damit die Regel angewandt wird
<b>ICMP packet type</b>	<b>Ignored:</b> das ICMP (Internet Control Messages Protocol) wird ignoriert <b>Equals:</b> das ICMP Protokoll muss dem folgenden Wert entsprechen damit die Regel angewandt wird <b>Does not equal:</b> das ICMP Protokoll muss ungleich dem folgenden Wert oder Bereich sein, damit die Regel angewandt wird
<b>Ethernet address</b>	<b>Ignored:</b> die Ethernet Adresse (MAC) wird ignoriert <b>Equals:</b> die Ethernet Adresse (MAC) muss dem folgenden Wert entsprechen damit die Regel angewandt wird <b>Does not equal:</b> die Ethernet Adresse (MAC) muss ungleich dem folgenden Wert sein, damit die Regel angewandt wird
<b>Packet flow rate</b>	<b>Ignored:</b> der Paketdurchsatz wird ignoriert <b>Below:</b> der Paketdurchsatz muss dem folgenden Wert unterschreiten, damit die Regel angewandt wird <b>Above:</b> der Paketdurchsatz muss größer dem folgenden Wert sein, damit die Regel angewandt wird
<b>Packet burst rate</b>	<b>Ignored:</b> der kurzzeitige Paketspitzenumsatz wird ignoriert <b>Below:</b> der Paketspitzenumsatz kann kurzzeitig den folgenden Wert unterschreiten, ohne dass die »Packet flow rate«-Regel angewandt wird <b>Above:</b> der Paketspitzenumsatz kann kurzzeitig den folgenden Wert überschreiten, ohne dass die »Packet flow rate«-Regel angewandt wird.
<b>Connection states</b>	<b>Ignored:</b> der Verbindungsstatus wird ignoriert <b>Equals:</b> der Verbindungsstatus muss dem folgenden Wert(en) entsprechen, damit die Regel angewandt wird <b>Does not equal:</b> der Verbindungsstatus muss ungleich dem folgenden Wert(en) sein, damit die Regel angewandt wird
<b>Type of service</b>	<b>Ignored:</b> der »Type of Service« Wert des IP Protokoll Headers wird ignoriert <b>Equals:</b> der »Type of Service« Wert des IP Protokoll Headers muss dem folgenden Wert entsprechen, damit die Regel angewandt wird <b>Does not equal:</b> der »Type of Service« Wert des IP Protokoll Headers muss ungleich dem folgenden Wert oder Bereich sein, damit die Regel angewandt wird
<b>Additional parameters</b>	Für künftige Anwendung

### 5.10.6 Beispiel: IP Forwarding einrichten

In dem Drop Down Menü hinter dem Button **Showing IPTable:** wählen Sie »Network address translation (nat)« aus und bestätigen mit dem Button.

Unter dem Punkt »Pakets before routing (PREROUTING)« fügen Sie über den Button **Add Rule** einen neuen Eintrag hinzu.

#### Add Rule



**Chain and action details**

**Part of chain** Packets before routing (PREROUTING)

**Rule comment** port forwarding to 192.168.0.1

**Action to take**

Do nothing  **Accept**  Drop  Redirect  Destination NAT

Run chain

**Target ports for redirect**  Default  Port range to

**IPs and ports for DNAT**  Default  IP range 192.168.0.1 to Port range 1234 to

The action selected above will only be carried out if **all** the conditions below are met.

**Condition details**

**Source address or network** <Ignored>

**Destination address or network** <Ignored>

**Incoming interface** Equals eth1

**Outgoing interface** <Ignored> br0

**Fragmentation**  Ignored  Is fragmented  Is not fragmented

**Network protocol** Equals TCP

**Source TCP or UDP port** <Ignored>  Port(s)  Port range to

**Destination TCP or UDP port** Equals  Port(s) 55000  Port range to

**Source and destination port(s)** <Ignored>

Abbildung 22: Beispielkonfiguration - IP Forwarding

Um die Übersicht zu behalten können Sie unter »Rule comment« eine Beschreibung für diesen Eintrag hinzufügen. Stellen Sie bei »Action to take« **Destination NAT** ein.

Die Ziel IP und den Ziel Port geben Sie unter »IPs and ports for DNAT« an. Soll nur eine IP oder ein Port weitergeleitet werden, so genügt die Angabe einmalig, es muss keine »range« definiert werden.

Nun erstellen Sie Bedingungen für die Portweiterleitung an die Zieladresse:

Setzen Sie unter »Incoming interface« die Bedingung **Equals** und im zweiten Drop Down Menü die Schnittstelle die das Original IP-Paket erhält (z.B. eth1).

Geben Sie bei »Network protocol« das gewünschte Protokoll (z.B. TCP) an.

Unter »Destination TCP or UDP Port« setzen Sie ebenfalls die Bedingung **Equals** und geben den Port an welcher umgesetzt werden soll. In dem Beispiel oben ist das der Port 55000.

Anschließend speichern Sie diese Regel mit dem Button **Create** und drücken Sie im Linux Firewall Menü auf **Apply Configuration**.

In diesem Beispiel werden alle TCP Pakete, die an der eth1 Schnittstelle mit dem Zielport 55000 ankommen an die Adresse 192.168.0.1 und den Port 1234 weitergeleitet.

## 5.11 Network Configuration

Hinter dem Menü Punkt Network Configuration findet man die Einstellungen für die einzelnen Netzwerkschnittstellen, Routing und Gateways, DNS-Client und Host Adressen.

Die Indexseite beinhaltet außerdem einen **Apply Configuration** Button, über den man die vorgenommenen Einstellungen zuweisen kann.

### Hinweis

- Trotz Übernahme der Einstellungen mit dem **Apply Configuration** Button ist ein **Permanent Save** unumgänglich, um die Einstellungen bei einem Neustart nicht zu verlieren.

### 5.11.1 Network Interfaces

Im Menü Punkt Network Interfaces können die physikalischen oder virtuellen Netzwerkschnittstellen konfiguriert und hinzugefügt werden.

### Hinweis

- Bei Änderungen an den Netzwerkschnittstellen kann es nötig sein sich mit der geänderten IP-Adresse erneut am Webinterface anzumelden.

Um eine neue Schnittstelle dauerhaft hinzuzufügen, klicken Sie bitte im Bereich **Interfaces Activated at Boot Time** auf **Add a new Interface**. Soll die Schnittstelle nur temporär sein, wird sie unter **Interfaces Active Now** hinzugefügt, ist diese dann nach einem Reboot oder »Apply Configuration« nicht mehr vorhanden.

In das folgende Formular müssen die Werte der Schnittstelle eingetragen werden:

### Create Bootup Interface

Boot Time Interface Parameters			
<b>Name</b>	<input type="text" value="eth1"/>	<b>IP Address</b>	<input type="radio"/> From DHCP <input checked="" type="radio"/> Static <input type="text" value="10.1.2.3"/>
<b>Netmask</b>	<input type="text" value="255.255.0.0"/>	<b>Broadcast</b>	<input type="text" value="10.1.255.255"/>
<b>MTU</b>	<input type="text"/>	<b>Activate at boot?</b>	<input checked="" type="radio"/> Yes <input type="radio"/> No
		<b>Activate on link?</b>	<input type="radio"/> Yes <input checked="" type="radio"/> No
		<b>Virtual interfaces</b>	0 (Add virtual interface)
		<b>VLAN interfaces</b>	0 (Add vlan interface)
<b>Bridge Settings:</b>			
<b>Should this be a bridge interface?</b>	<input type="radio"/> Yes <input checked="" type="radio"/> No		
<b>Bridged interface(s):</b>	<input type="checkbox"/> eth0 <input type="checkbox"/> eth1		
<b>Tunnel Settings:</b>			
<b>Should this be a tunnel interface?</b>	<input type="radio"/> Yes <input checked="" type="radio"/> No		
<b>Tunnel Mode</b>	GRE		
<b>Local Address</b>	<input type="text"/>	<b>Remote Address</b>	<input type="text"/>
<b>Serialize Packets*</b>	<input checked="" type="radio"/> None <input type="radio"/> Bothway <input type="radio"/> Incoming <input type="radio"/> Outgoing		
<b>Generate/Require Checksums*</b>	<input checked="" type="radio"/> None <input type="radio"/> Bothway <input type="radio"/> Incoming <input type="radio"/> Outgoing		
<b>Use Key*</b>	<input checked="" type="radio"/> None <input type="radio"/> <input type="text"/>		
<b>Type of Service (TOS)</b>	<input checked="" type="radio"/> inherit <input type="radio"/> CS0		
<b>Path MTU Discovery</b>	<input checked="" type="radio"/> Yes <input type="radio"/> No		
		<b>Time to Live (TTL)</b>	<input checked="" type="radio"/> inherit <input type="radio"/> <input type="text"/>
		<b>Bind to Device</b>	<input type="text"/>

\*only GRE tunnels

Abbildung 23: Beispielkonfiguration - Neues Interface hinzufügen

Kommando	Beschreibung								
<b>Name</b>	Bezeichnung der Schnittstelle z.B. eth1								
<b>IP Address</b>	Die IP-Adresse die der Schnittstelle zugewiesen werden soll.								
<b>Netmask</b>	Das Subnetz für die Schnittstelle (default: 255.255.255.0)								
<b>Broadcast</b>	Die Broadcastadresse der Schnittstelle. (default *.*.*.255)								
<b>MTU</b>	Maximum Transmission Unit. Die maximal zulässige Länge eines Datenpaketes bzw. die maximal zulässige Länge des Datenfeldes eines Datenpaketes bei paketvermittelter Datenkommunikation. Folgende Standardwerte gelten: <table style="margin-left: 40px;"> <tr> <td>X.25</td> <td>576</td> </tr> <tr> <td>Ethernet</td> <td>1500</td> </tr> <tr> <td>ATM (Ethernet)</td> <td>1500</td> </tr> <tr> <td>ATM (Classical IP)</td> <td>9180</td> </tr> </table>	X.25	576	Ethernet	1500	ATM (Ethernet)	1500	ATM (Classical IP)	9180
X.25	576								
Ethernet	1500								
ATM (Ethernet)	1500								
ATM (Classical IP)	9180								
<b>Activate at boot?</b>	Legt fest, ob das Interface beim Bootvorgang aktiviert wird								
<b>Activate on link?</b>	Aktiviert die Schnittstelle erst wenn ein Link besteht <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Hinweis</b></p> <p>➤ Kann im Zusammenhang mit Tunnels (z.B. IPSec) zu Problemen führen</p> </div>								
<b>Virtual interfaces</b>	Wurde das physikalische Interface angelegt, lassen sich hier virtuelle IP-Adressen für diese Schnittstelle vergeben. Die Werte entsprechen den hier genannten.								
<b>VLAN interfaces</b>	Nachdem die physikalische Schnittstelle angelegt wurde, können VLAN Interfaces konfiguriert werden. Die Werte entsprechen den hier genannten.								

### 5.11.1.1 Bridge Settings

Kommando	Beschreibung
<b>Should this be a bridge interface?</b>	dieses Interface als Bridge einrichten <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Hinweis</b></p> <p>➤ Wird zum Beispiel verwendet um WLAN und Ethernet logisch zu verbinden</p> </div>
<b>Bridged interface(s):</b>	Interfaces die in eine Bridge zusammengefasst werden sollen, werden hier definiert

### 5.11.1.2 Tunnel Settings

Kommando	Beschreibung
<b>Should this be a tunnel interface?</b>	dieses Interface als Tunnel einrichten
<b>Tunnel Mode</b>	Legt den Tunnel modus fest; <b>GRE</b> (Generic Routing Encapsulation) oder <b>IP/IP</b> (IP-to-IP Kapselung)
<b>Local Address</b>	gibt die feste lokale Adresse an
<b>Remote Address</b>	gibt die Adresse für das Tunnel Ziel an

Kommando	Beschreibung	
<b>Serialize Packets*</b>	<b>None</b>	keine Ablaufsteuerung der Pakete
	<b>Bothway</b>	ausgehende Pakete werden als sequenziert gesendet; eingehende Pakete müssen ebenfalls in serieller Reihenfolge eintreffen
	<b>Incoming</b>	eingehende Pakete müssen in serieller Reihenfolge erwartet
	<b>Outgoing</b>	ausgehende Pakete werden als sequenziert gesendet
<b>Generate/Require Checksums*</b>	<b>None</b>	Checksummen werden nicht berechnet
	<b>Bothway</b>	Checksummen werden für ausgehende Pakete berechnet und für eingehende benötigt
	<b>Incoming</b>	alle ankommenden Pakete müssen eine korrekte Checksumme aufweisen
	<b>Outgoing</b>	berechnet Checksummen für ausgehende Pakete
<b>Use Key*</b>	<b>None:</b> verschlüsselung wird nicht verwendet <b>String:</b> benutze einen verschlüsselten GRE Tunnel; der Key ist entweder eine Nummer oder eine punktgetrennte Vierergruppe (ähnlich einer IP Adresse)	
<b>Type of Service (TOS)</b>	<b>Inherit:</b> (Default) <b>Drop down menu:</b> legt den TOS für getunnelte Pakete fest	
<b>Time to Live (TTL)</b>	<b>Inherit:</b> (Default) <b>Integer:</b> gibt eine feste TTL für getunnelte Pakete an (1-255)	
<b>Path MTU Discovery</b>	Aktiviert/deaktiviert die dynamische Erkennung der Maximum Transmission Unit (MTU) <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Hinweis</b></p> <ul style="list-style-type: none"> <li>➤ Ein Tunnel mit einer festen TTL benutzt immer die PMTU Discovery</li> </ul> </div>	
<b>Bind to Device</b>	getunnelte Pakete werden immer über das hier festgelegte Device geroutet	

\*nur für GRE Tunnel Mode

## 5.11.2 Routing and Gateways

Über das Menü Routing and Gateways wird festgelegt welche Routen für das Erreichen bestimmter Hosts und Netzwerke verwendet werden sollen. Hier können die Geräte auch als Router zwischen verschiedenen Netzen konfiguriert werden.

Kommando	Beschreibung	
<b>Default routes</b>	<b>Interface</b>	geben Sie das Interface für die Route ein (z.B. eth0)
	<b>Gateway</b>	geben Sie hier das Gateway an, über das das Netzwerk erreichbar ist

Kommando	Beschreibung				
Act as router?	<b>Yes</b>	das Gerät arbeitet als Router laut der folgenden Liste			
	<b>No</b>	die Routing-Funktionalität ist deaktiviert			
Static routes	<b>Interface</b>	geben Sie das Interface für die Route ein (z.B. eth0)			
	<b>Network</b>	geben Sie hier das Netzwerk an, das erreicht werden soll (z.B. 192.168.5.0)			
	<b>Netmask</b>	geben Sie hier die Subnetzmaske des zu erreichenden Netzwerkes an (z.B. 255.255.255.0)			
	<b>Gateway</b>	geben Sie hier das Gateway an, über das das Netzwerk erreichbar ist			
Local routes	<b>Interface</b>	geben Sie das Interface für die Route ein (z.B. eth0)			
	<b>Network</b>	geben Sie hier das Netzwerk an, das erreicht werden soll (z.B. 192.168.5.0)			
	<b>Netmask</b>	geben Sie hier die Subnetzmaske des zu erreichenden Netzwerkes an (z.B. 255.255.255.0)			
	<b>Type</b>	<table border="0"> <tr> <td><b>host</b></td> <td>rutet zu einem Host</td> </tr> <tr> <td><b>unreachable</b></td> <td>setzt die Route als unerreichbar; sendet eine ICMP Meldung an die Quelladresse</td> </tr> </table>	<b>host</b>	rutet zu einem Host	<b>unreachable</b>
<b>host</b>	rutet zu einem Host				
<b>unreachable</b>	setzt die Route als unerreichbar; sendet eine ICMP Meldung an die Quelladresse				

**Hinweis**

- Um mehrere »Static routes« oder »Local routes« einzutragen muss zuerst die aktuelle Einstellung mit dem **Add** oder **Submit** Button gespeichert werden.

### 5.11.3 DNS Client

Über das Menü DNS Client konfiguriert man die Resolver-Einstellungen des Routers, die die Reihenfolge der Hostnamen Auflösung festlegt.

Kommando	Beschreibung	
<b>Hostname</b>	Hostname des Routers	
<b>DNS servers</b>	DNS Server die vom Router abgefragt werden, wenn ein unbekannter Hostname verwendet wird.	
<b>Resolution order</b>	Reihenfolge der Namensauflösung	
	<b>Host:</b>	der Router versucht den Namen selbst aufzulösen
	<b>DNS:</b>	der Router versucht den Namen über die in der DNS-Liste eingegebenen Server aufzulösen
	<b>NIS:</b>	der Router versucht den Namen über Network Information Services aufzulösen
<b>NIS+:</b>	der Router versucht den Namen über Network Information Services Plus aufzulösen	

Kommando	Beschreibung
<b>Search domains</b>	Die Search domains Liste beinhaltet eine Liste von lokalen Hostnamen, die erst nach der erfolglosen Abarbeitung der Namensauflösung die lokalen Namen auflöst z.B. M3000.local

### 5.11.4 Host Addresses

Unter dem Menü Host-Adressen werden die Hostnamen die unter **/etc/hosts** gespeichert sind angezeigt oder geändert. Durch Klicken auf **Add a new host address** wird eine neue Host Adresse hinzugefügt.

Kommando	Beschreibung
<b>IP Adress</b>	Geben Sie hier die IP-Adresse des Hosts an
<b>Hostname</b>	Hier definieren Sie den neuen Hostnamen

## 5.12 OpenVPN

Mit Hilfe von OpenVPN können VPN-Verbindungen über verschlüsselte TLS-Verbindungen hergestellt werden. Zur Verschlüsselung verwendet OpenVPN die Bibliotheken von OpenSSL. Zum Transport der Daten verwendet OpenVPN wahlweise UDP oder TCP.

### Hinweis

- Als erstes muss, soweit noch nicht vorhanden, ein neuer Server erstellt werden.

### 5.12.1 Add new server/client

Kommando	Beschreibung
<b>Peer name</b>	Name der Verbindung
<b>Port to use</b>	Port, der für die Verbindung verwendet werden soll
<b>Operating Mode</b>	<p><b>Routed VPN:</b> alle gängigen Netzwerkprotokolle auf IP-Basis werden transportiert (Layer 3). Zugriff auf das Netz „dahinter“ nicht möglich (Point-to-Point Verbindung).</p> <p><b>Bridged VPN (vollständiges Tunneln):</b> Layer 2 des Ethernet-Frames wird vollständig getunnelt, somit kann z.B. auch das Protokoll IPX geroutet werden. Clients bekommen von einem DHCP, der hinter dem VPN-Server steht eine Adresse zugewiesen.</p>
<b>Create appropriate Diffie-Hellman Random File</b>	<p>Wert = Länge des zu verwendenden Diffie-Hellman Schlüssels</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>➤ Je größer der Wert, desto länger dauert die Erstellung der Zufallsdatei.</p> </div>

### 5.12.2 Edit existing peer

Kommando	Beschreibung
<b>Peer name</b>	Name der Verbindung
<b>Operating Mode</b>	zeigt den verwendeten Operation mode an
<b>Port to use</b>	zeigt den Port für die OpenVPN-Verbindung an
<b>Protocol</b>	Verwendet das ausgewählte Protokoll (Default: UDP)
<b>TCP connection retry</b>	Zeit in Sekunden, die nach einem Verbindungsabbruch bis zum erneuten Wahlversuch gewartet wird (nur für Client)
<b>Internatl UDP fragmentation</b>	ermöglicht die interne Fragmentierung der Datenpakete; max. Datenpaketgröße in Bytes
<b>TCP send size to fit UDP</b>	Limitiert die Größe der Pakete in Senderichtung (Bytes)
<b>Network to assign client addresses</b>	Den Clients werden Adressen aus dem angegebenen Bereich zugewiesen. Der OpenVPN Server verwendet stets die .1 aus diesem Adressbereich. (z.B. 192.168.0.0/24) (nur bei Server)
<b>Netmask to assign client addresses</b>	Den Clients wird die Netzmaske aus dem angegebenen Bereich zugewiesen. (nur bei Server)
<b>Encrypt packets with cipher algorithm</b>	Verschlüsselt alle Pakete mit dem angegebenen Algorithmus
<b>Listen on IP</b>	<b>All:</b> akzeptiert Verbindungen über alle Netzwerkadressen <b>String:</b> akzeptiert Verbindungen nur über die angegebene IP-Adresse
<b>Authenticate packets with HMAC</b>	Die Authentifizierung der Pakete erfolgt mit dem angegebenen HASH-Algorithmus
<b>Keepalive</b>	<b>Ping:</b> werden <b>n</b> Sekunden keine Daten übertragen, wird ein Ping an die Gegenstelle gesendet, um die Verbindung aufrecht zu erhalten. <b>Ping-Restart:</b> empfängt der Server keine Antwort der Gegenstelle auf einen Ping innerhalb der festgelegten Zeit (in Sekunden), wird die Verbindung zurückgesetzt, und versucht, diese neu aufzubauen. (SIGUSR1 Signal) (Default: 120; Disable: 0;)
<b>Max. new connections</b>	Es dürfen maximal <b>n</b> Clients binnen <b>m</b> Sekunden eine Verbindung zum OpenVPN Server aufbauen (nur bei Server)
<b>Allow clients with same common name</b>	<b>No:</b> Clients müssen unterschiedliche Namen haben; Verbindet sich ein Client mit einem bereits eingeloggten Namen, so wird die Verbindung des „älteren“ Clients getrennt <b>Yes:</b> Clients dürfen den selben Namen verwenden (nur bei Server)
<b>Route client-to-client traffic</b>	<b>No:</b> Clients dürfen untereinander keine Daten austauschen <b>Yes:</b> Clients dürfen untereinander Daten austauschen (nur bei Server)
<b>Limit concurrent clients</b>	maximale Anzahl an gleichzeitiger Verbindungen zum OpenVPN-Server (nur bei Server)
<b>Allow remote to change IP and/or port</b>	Erlaubt dem Client, eine eigene IP-Adresse und Port anzugeben bzw. eine Vorgabe durch den Server zu verändern
<b>Enable Management</b>	<b>Yes:</b> startet einen TCP-Server auf dem angegebenen Port. Es wird aus Sicherheitsgründen empfohlen, die IP-Adresse auf 127.0.0.1 (localhost) zu setzen. (nur bei Server)

Kommando	Beschreibung
<b>Client's remote host(s)</b>	Legt die einzelnen Gegenstellen an (nur bei Client) <b>Priority:</b> Priorität des Servers <b>IP address:</b> IP-Adresse des Servers <b>Port:</b> Port des Servers
<b>Accept only host with X509 or common name</b>	nur Hosts mit X.509 oder dem angegebenen Common Namen zulassen (nur bei Client)
<b>TLS Cipher Algorithm</b>	Verschlüsselt die Pakete mit dem angegebenen Algorithmus
<b>TLS Retransmit Timeout (sec)</b>	Wird ein Kontrollpaket von OpenVPN an den Client gesendet, muss dieses innerhalb <b>n</b> Sekunden beantwortet werden. (Default: 2)
<b>Renegotiate Data Channel Key (sec)</b>	Der Schlüssel des Datenkanals wird alle <b>n</b> Sekunden neu ausgehandelt
<b>Use PKCS12 File</b>	Verwendet ein Zertifikat im PKCS12 Format
<b>Certification Authority</b>	gibt die Zertifizierungsstelle (CA) an
<b>Certificate</b>	Zertifikat im <b>.pem</b> Format
<b>Key</b>	gibt das private Zertifikat des Clients an
<b>Diffie-Hellman Random File</b>	Datei im <b>.pem</b> Format, welches die Diffie-Hellman-Parameter beinhaltet (nur bei Server)
<b>Certificate Revocation File</b>	Gibt die Zertifikats-Prüfdatei an, mit dem das Clientzertifikat auf seine Gültigkeit geprüft wird
<b>Enable username/password authentication</b>	Authentifizierung mit Benutzername und Passwort (nicht) zulassen
<b>Authentication script</b>	gibt den Pfad des Authentifizierungsscript an (nur bei Server)
<b>Require certificate authentication additionally</b>	<b>No:</b> kein zusätzliches Authentifizierungs-Zertifikat benötigt <b>Yes:</b> benötigt zusätzlich ein Authentifizierungs-Zertifikat (nur bei Server)
<b>Username</b>	Username für die OpenVPN-Verbindung (nur bei Client)
<b>Password</b>	Passwort für die OpenVPN-Verbindung (nur bei Client)
<b>Authentication file</b>	Pfad der Authentifizierungs-Datei (nur bei Client)
<b>'chroot' to dir after initialization</b>	<b>No:</b> (default) <b>String:</b> definiert das angegebene Verzeichnis als neues Toplevel-Verzeichnis. ( / )
<b>Change user after initialization</b>	<b>No:</b> (default) <b>Auswahl:</b> ändert die Benutzer-ID von OpenVPN auf den angegebenen User
<b>Change group after initialization</b>	<b>No:</b> (default) <b>Auswahl:</b> ändert die Gruppen-ID von OpenVPN auf die angegebene Gruppe
<b>Retain key files (persist-key)</b>	<b>No:</b> (default) <b>Yes:</b> bereits eingelesene Key-Files werden beibehalten und nicht erneut eingelesen
<b>Retain TUN/TAP devices (persist-tun)</b>	<b>Yes:</b> Aufgebaute Verbindungen werden nicht geschlossen und Start-/Stop Skripte werden nicht ausgeführt <b>No:</b> (default)
<b>Additional configurations</b>	OpenVPN unterstützt mehr Parameter als hier aufgelisteten. Falls Sie einen dieser Parameter benötigen, können Sie ihn hier eintragen.

Kommando	Beschreibung
<b>Script to execute after VPN is up</b>	Das angegebene Skript wird nach dem Starten einer OpenVPN-Verbindung ausgeführt. Läuft mit den Benutzerrechten des unter „Change user after initialization“ angegebenen Benutzers.
<b>Script to execute after VPN is down</b>	Das angegebene Skript wird nach dem Beenden einer OpenVPN-Verbindung ausgeführt. Läuft mit den Benutzerrechten des unter „Change user after initialization“ angegebenen Benutzers.
<b>Logging</b>	<b>Off:</b> die Log-Funktion ist deaktiviert <b>Truncate logfile at startup:</b> überschreibt eine vorhandene Log-Datei; ist diese nicht vorhanden, wird sie erzeugt <b>Append to logfile:</b> fügt Log an eine bestehende Log-Datei an; ist diese nicht vorhanden, wird sie erzeugt.
<b>Logfile</b>	Statusmeldungen von OpenVPN werden in der hier angegebenen Log-Datei gespeichert
<b>Log same consecutive messages</b>	Max. <i>n</i> Nachrichten desselben Nachrichtentyps werden gespeichert
<b>Output Verbosity</b>	Legt die Details der Ausgabe von OpenVPN fest. <b>0:</b> keine Ausgabe <b>1 - 4:</b> Normaler Gebrauch <b>5:</b> Read & Write für jedes Paket <b>6 - 11:</b> Debug Info Bereich.
<b>Write operational status to file</b>	<b>No:</b> speichert den OpenVPN nicht in eine Status-Datei <b>Yes:</b> Speichert den Status von OpenVPN in die unten angegebene Status-Datei
<b>Write status interval</b>	Alle <i>n</i> -Sekunden wird der Status gespeichert
<b>Status file</b>	Name der Status-Datei

## 5.13 PPP

In diesem Menü können Funktionen rund um das Point-to-Point Protocol (PPP) erstellt und verwaltet werden.

Zum Starten der hier erstellten Verbindungen wird das [Connection Management](#) (Kapitel: [5.3](#)) verwendet.

### Hinweis

- Bei Routern die mit einem LTE Modem ausgestattet (Cx~~xxx~~l) sind, ist ein Verbindungsaufbau mittels **Networking > WWAN** erforderlich.
- Bei Routern die mit einem HSPA Modem (Cx~~xxx~~h) ausgestattet sind empfiehlt sich aus Performancegründen der Verbindungsaufbau mittels **Networking > WWAN**.

### 5.13.1 PPP Interfaces

Unter dem Punkt Interfaces werden vorhandene PPP Verbindungen angezeigt, verwaltet und neue hinzugefügt. Folgende Daten werden in der Übersicht angezeigt:

Kommando	Beschreibung
<b>Name</b>	Name der ppp Verbindung
<b>Type</b>	Verbindungstyp der PPP Verbindung. Mögliche Typen: ADSL, ISDN, ISDN Dial In
<b>Phone Number(s)</b>	ISDN Rufnummer(n) bei ausgehenden ISDN Verbindungen
<b>APN</b>	Access Point Name
<b>Username</b>	Benutzername der Verbindung
<b>Local IP</b>	Gibt die lokale IP-Adresse wider
<b>Remote IP</b>	Zeigt die IP-Adresse der Gegenstelle an

Mit **Add a new PPP interface** wird eine neue Verbindung hinzugefügt.

Wählen Sie zunächst den Name und den Typ für die neue Verbindung aus und drücken den Button **Create**. Daraufhin erscheint die Konfigurationsseite für die Verbindung.

#### Hinweis

- Bei Routern die mit einem Mobilfunk-Modem ausgestattet sind (Cxxxxh oder Cxxxxl) wird der Verbindungskonfiguration mittels **Networking > WWAN** durchgeführt.
- Um eine Verbindung aufzubauen ist es nötig die konfigurierte PPP Schnittstelle über **Networking > Connection Management** zu starten.
- Für einen aktiven Verbindungsaufbau wird die Verwendung des **Connection Manager** empfohlen, da hier ein Monitoring der Verbindung möglich ist.

### 5.13.1.1 Basic PPP parameters for interface ppp#

Je nach verwendetem Verbindungstyp sind spezifische Einstellungen nötig, die nachfolgend aufgeführt werden.

#### 5.13.1.1.1 ISDN PPP Interface Parameter

Kommando	Beschreibung
<b>Phone number(s)*</b>	Legt die zu wählende(n) ISDN Nummern fest, die beim Verbindungsaufbau gewählt werden (kommagetrennt)
<b>Numberprefix</b>	Definiert das Präfix, welches jeder Nummer vorangestellt wird
<b>Outgoing MSN</b>	Legt die ausgehende Rufnummer fest, die der Gegenstelle übermittelt wird
<b>Username</b>	Feld für den vom Provider zugewiesenen Username
<b>Password</b>	Das Passwort für den Account
<b>Verify Password</b>	Passworteingabe zur Abgleich
<b>Ask for DNS server addresses</b>	Die Gegenstelle wird nach ihren DNS Servern gefragt. Die Server werden zur Namensauflösung am Router hinterlegt
<b>Maximum Transmit Unit</b>	Gibt die maximale Größe eines zu sendenden Datenpakets an
<b>Maximum Receive Unit</b>	Legt die maximale Größe eines zu empfangenden Datenpakets fest
<b>Protocol</b>	Definiert das Verbindungsprotokoll. Das Protokoll muss mit der Gegenstelle übereinstimmen

### 5.13.1.1.2 ISDN Dial-In PPP Interface Parameter

Kommando	Beschreibung
<b>Incoming MSN(s)*</b>	Legt die MSN(s) fest, die auf eingehende ISDN Anrufe überwacht werden. Ist keine MSN angegeben werden alle ankommenden Anrufe angenommen. (kommagetrennt)
<b>Accept Calls From*</b>	Den angegebenen Gegenstellen/Anrufern ist es erlaubt eine Verbindung aufzubauen, dazu werden die entsprechenden Nummern hier kommagetrennt angegeben. Ist das Feld leer, werden alle Gegenstellen/Anrufer erlaubt.
<b>Maximum Transmit Unit</b>	Gibt die MTU, die maximale Größe eines zu sendenden Datenpakets an
<b>Maximum Receive Unit</b>	Legt die MRU, die maximale Größe eines zu empfangenden Datenpakets fest
<b>Protocol</b>	Definiert das Verbindungsprotokoll. Das Protokoll muss mit der Gegenstelle übereinstimmen

### 5.13.1.1.3 PPPoE Interface Parameter

Kommando	Beschreibung
<b>Use Interface</b>	hier wird die physikalische Schnittstelle für die DSL Verbindung festgelegt
<b>Username</b>	Feld für den vom Provider zugewiesenen Username
<b>Password</b>	Das Passwort für den Account
<b>Verify Password</b>	Passworteingabe zur Abgleich
<b>Ask for DNS server addresses</b>	Die Gegenstelle wird nach ihren DNS Servern gefragt. Die Server werden zur Namensauflösung am Router hinterlegt
<b>Maximum Transmit Unit</b>	Gibt die maximale Größe eines zu sendenden Datenpakets an (Default: 1492)
<b>Maximum Receive Unit</b>	Legt die maximale Größe eines zu empfangenden Datenpakets fest (Default: 1492)

### 5.13.1.2 Advanced PPP parameters for interface ppp#

Für einen einfachen Verbindungsaufbau werden die **Advanced PPP parameters** nicht benötigt, spezielle Anwendungen können jedoch eine tieferegehende Konfiguration erfordern.

Nachfolgend werden die für den entsprechenden Verbindungstyp möglichen **Advanced PPP parameters** beschrieben.

Da sich die meisten Parameter wiederholen, werden die allgemein gültigen Einstellungen nach den spezifischen Verbindungstypen gelistet.

### 5.13.1.2.1 ISDN PPP Interface Parameter

Kommando	Beschreibung
<b>Wait for Callback</b>	Auf Rückruf warten
<b>Time to Wait For Callback</b>	Es wird <b>n</b> Sekunden auf den Rückruf gewartet (Default: 60 sec)
<b>Trys before giving up</b>	Im Fehlerfall werden <b>n</b> Verbindungsversuche durchgeführt (Default: 4)
<b>Timeout before giving up</b>	Es wird <b>n</b> Sekunden lang versucht die Verbindung aufzubauen, bevor der Aufbau abgebrochen wird. (Default: 60 sec)
<b>PPP multilink protocol</b>	Multilink PPP erlaubt die Bündelung mehrerer Kanäle zu einer logischen Verbindung (MLPPP)
	<b>No</b> die ISDN Kanäle werden nicht gebündelt
	<b>Yes</b> bündelt die ISDN B Kanäle
	<b>Auto</b> nutzt die Kanalbündelung, wenn möglich
<b>Short sequence numbers in MLPPP</b>	Ermöglicht die Benutzung von 12 bit großen Sequenznummern im Multilink PPP Header, standardmäßig werden 24 bit große Sequenznummern verwendet

### 5.13.1.2.2 ISDN Dial-In PPP Interface Parameter

Kommando	Beschreibung
<b>Do Callback</b>	Rückruf durchführen
<b>Callback Number(s)*</b>	Legt die zu wählende(n) ISDN Nummern fest, die bei einem Rückruf gewählt werden (kommagetrennt)
<b>Time To Wait Before Callback</b>	Der Rückruf wird mit einer Verzögerung von <b>n</b> Sekunden gestartet (Default: 60 sec)
<b>Trys before giving up</b>	Im Fehlerfall werden <b>n</b> Verbindungsversuche durchgeführt (Default: 4)
<b>Timeout before giving up</b>	Es wird <b>n</b> Sekunden lang versucht die Verbindung aufzubauen, bevor der Aufbau abgebrochen wird. (Default: 60 sec)
<b>PPP multilink protocol</b>	Multilink PPP erlaubt die Bündelung mehrerer Kanäle zu einer logischen Verbindung (MLPPP)
	<b>No</b> die ISDN Kanäle werden nicht gebündelt
	<b>Yes</b> bündelt die ISDN B Kanäle
	<b>Auto</b> nutzt die Kanalbündelung, wenn möglich
<b>Short sequence numbers in MLPPP</b>	Ermöglicht die Benutzung von 12 bit großen Sequenznummern im Multilink PPP Header, standardmäßig werden 24 bit große Sequenznummern verwendet

### 5.13.1.2.3 PPPoE interface Parameter

Kommando	Beschreibung
<b>PPPoE Access Concentrator Name</b>	PPPoE Access Concentrator Name (optional)
<b>PPPoE Service Name</b>	PPPoE Service Name (optional)

### 5.13.1.2.4 Globale Einstellungen

Kommando	Beschreibung
<b>On Demand Calling</b>	Legt fest, ob die Verbindung nur aufgebaut wird, wenn Daten gesendet werden (Yes), oder ob die Verbindung automatisch aufgebaut wird. (Default: No)
<b>Idle time before disconnect</b>	Die Verbindung wird nach <b>n</b> Sekunden getrennt, wenn keine Daten mehr gesendet oder empfangen werden.
<b>LCP-Echo-Failure</b>	Ist diese Option aktiviert, wird die PPP Verbindung getrennt, wenn auf <b>n</b> LCP-Echo-Requests keine Replys zurückgesendet wurde. Diese Überprüfung kann dazu verwendet werden, die Verbindung automatisch zu beenden, wenn die Gegenstelle nicht mehr erreichbar ist.
<b>LCP-Echo-Interval</b>	Dieser Parameter gibt das Intervall für die LCP Überprüfung in Sekunden an. Wird in Verbindung mit der <b>LCP-Echo-Failure</b> Option benutzt.
<b>Clamp MSS</b>	Mit dieser Funktion wird die Maximum Segment Size (MSS) definiert. Das ist nötig um Netze mit verschiedenen MTUs zu verbinden und dabei Übertragungsfehler durch eine eventuelle Fragmentierung zu vermeiden. Dafür wird die MSS entweder automatisch, anhand der »Path MTU« (PMTU, der kleinsten MTU für den aktiven Netzwerkpfad) bestimmt, oder auf einen vorgegeben Wert reduziert.
<b>Passive Mode</b>	Bei aktiviertem LCP »passive Mode« wird versucht eine PPP Verbindung aufzubauen. Antwortet die Gegenstelle nicht, wird passiv gewartet bis die Gegenstelle ein gültiges LCP Paket gesendet hat, anstatt die Verbindung zu trennen. (Default: No)
<b>Silent Mode</b>	Im Silent Mode wird mit dem Verbindungsaufbau gewartet, bis ein gültiges LCP Paket von der Gegenstelle empfangen wurde, ansonsten wird die Verbindung aktiv gestartet. (Default: No)
<b>Magic Number negotiation</b>	Aktiviert die Übertragung der »Magic Number«, einer zufällig generierten Nummer, die bei LCP Paketen zur Identifikation der Endpunkte einer PPP Verbindung verwendet wird. Ist dieser Parameter deaktiviert kann ein eventueller Loopback nicht identifiziert werden. (Default: Yes)

### 5.13.1.2.5 Logging Parameters

Kommando	Beschreibung
<b>Connection Debugging</b>	Aktiviert das Connection Debugging, um eine Fehlersuche zu vereinfachen. Dabei werden alle ppp Aktionen (Control packets) in der Datei <b>/var/log/messages</b> protokolliert. (Default: No)
<b>Additional Logfile (/var/log/ppp/&lt;type&gt;/pppX.log)</b>	Erstellt eine zusätzliche Log Datei für dieses PPP Verbindung. (z.B. /var/log/ppp/umts/ppp0.log) (Default: No)
<b>Show PAP password in log</b>	Standardmäßig wird in den Log Dateien das PAP Passwort nicht angezeigt. Ist die Ausgabe des Passwortes erforderlich, kann diese hier aktiviert werden. (Default: No)

### 5.13.1.2.6 Networking Parameters

Kommando	Beschreibung	
PPP IP addresses	<b>From peer</b>	Die IP Adresse wird von der Gegenstelle bezogen (Default)
	<b>Local IP</b>	IP Adresse für den Router und dessen Gegenstelle die vom Provider festgelegt ist
	<b>Remote IP</b>	
<b>Accept local IP address</b>	Die Gegenstelle darf dem Router die lokale IP Adresse zuweisen (Default: No)	
<b>Accept remote IP address</b>	Die Gegenstelle darf dem Router die remote IP Adresse zuweisen (Default: No)	
PPP interface netmask	<b>Based on Remote IP</b>	die Netzmaske wird anhand der remote IP Adresse definiert (Default)
	<b>String</b>	legt die Netzmaske für das PPP Interface fest
Force Local IP	<b>No</b>	(Default: No)
	<b>Yes, set to</b>	Erzwingt die angegebene Lokale IP

### 5.13.1.2.7 Authentication Parameters

Kommando	Beschreibung	
Require authentication	<b>No, but prevent routed IPs</b>	erlaubt nur IP Adressen, zu denen bisher noch keine Route besteht (Default)
	<b>Never</b>	die Gegenstelle muss sich nicht authentifizieren
	<b>Always</b>	eine Authentifikation ist immer erforderlich
<b>Refuse PAP</b>	Authentifizierungsanforderungen über PAP (Password Authentication Protocol) werden abgelehnt (Default: No)	
<b>Require PAP</b>	Die Gegenstelle muss sich via PAP authentifizieren (Default: No)	
<b>Refuse CHAP</b>	Authentifizierungsanforderungen über CHAP (Challenge Handshake Authentication Protocol) werden abgelehnt (Default: No)	
<b>Require CHAP</b>	Legt fest, dass eine Authentifizierung der Gegenstelle über CHAP erforderlich ist (Default: No)	
<b>Max. CHAP challenge transmissions</b>	Es wird <i>n</i> -mal versucht eine CHAP Authentifizierung durchzuführen (Default: 10)	
<b>CHAP restart interval</b>	Zwischen den CHAP challenge transmission liegen <i>n</i> Sekunden (Default: 3 sec)	
<b>Refuse MS-CHAP</b>	Lehnt die Authentifizierung über MS-CHAP ab (Default: Yes)	
<b>Refuse MS-CHAPv2</b>	MS-CHAPv2 Authentifizierungsanforderung werden abgelehnt (Default: Yes)	
<b>Refuse EAP</b>	Eine Authentifizierung über EAP wird abgelehnt (Default: No)	

Kommando	Beschreibung
<b>Append domain name</b>	Zur Authentifizierung wird der lokale Hostname zusammen mit dem hier angegebenen Domain Namen verwendet. (z.B.: Hostname <b>router1</b> und Domain Name <b>firma.com</b> ergibt für die Authentifizierung den »Fully Qualified Domain Name« <b>router1.firma.com</b> )

### 5.13.1.2.8 Compression Parameters

Kommando	Beschreibung
<b>VJ-Compression</b>	Aktiviert Van Jacobson TCP/IP Header-Kompression in beide Richtungen. (Default: Yes)
<b>VJ-Connection-ID Compression</b>	Aktiviert die Connection-ID Kompression in der Van Jacobson Compression, somit wird das Connection-ID-Byte komprimiert. (Default: Yes)
<b>Protocol Field Compression</b>	Definiert ob eine Übertragung der »protocol field compression« in Sende- und Empfangsrichtung durchgeführt wird. (Default: Yes)
<b>Address/Control Compression</b>	Die Address/Control Compression in beide Richtungen (senden und empfangen) wird hier aktiviert/deaktiviert. (Default: Yes)
<b>Predictor-1 Compression</b>	Erfordert »Predicator-1 Compression« bei Yes, bei No wird »Predicator-1 Compression« nicht zugelassen (Default: Auto)
<b>BSD Compression</b>	Aktiviert das BSD-Compression Schema, dabei fordert der Router von der Gegenstelle komprimierte Pakete mit einer maximalen Code Größe von <b>nr</b> Bits an. Ausgehende Pakete werden mit einer maximalen Kompression von <b>nt</b> Bits gesendet. Der Wert <b>0</b> deaktiviert die Kompression in der entsprechenden Richtung. Bei <b>No</b> wird die Kompression abgewiesen, <b>Auto</b> übernimmt die Einstellungen der Gegenstelle (Default: Auto)
<b>Deflate Compression</b>	Aktiviert das Deflate Compression Schema, dabei fordert der Router von der Gegenstelle komprimierte Pakete mit einer maximalen Fenstergröße Größe von <b>2**r</b> Bits an. Ausgehende Pakete werden mit einer maximalen Größe von <b>2**t</b> Bits gesendet. Der Wert <b>0</b> deaktiviert die Kompression in der entsprechenden Richtung. Bei <b>No</b> wird die Kompression abgewiesen, <b>Auto</b> übernimmt die Einstellungen der Gegenstelle (Default: Auto)
<b>Compression Control Protocol negotiation</b>	<b>No</b> deaktiviert das Compression Control Protocol bei der Übertragung. Diese Option sollte nur verwendet werden, wenn die Gegenstelle die CCP Übertragung nicht akzeptiert. (Default: Yes)

### 5.13.1.3 Parameters for interface pppX when used in Static Connections

<p><b>Achtung!</b></p> <ul style="list-style-type: none"> <li>➤ Die nachfolgenden Parameter <b>nicht</b> zusammen mit dem <b>Connection Manager</b> verwenden.</li> <li>➤ Diese Optionen können nur für ISDN Verbindungen verwendet werden.</li> </ul>
--

Kommando	Beschreibung
<b>Add a defaultroute</b>	Setzt nach dem Aushandeln/Aufbau der PPP Verbindung eine Default Route auf das PPP Interface
<b>PPP interface routing metric</b>	Legt die Routingmetrik des Interfaces fest
<b>Update DNS Server directly</b>	Führt ein DNS Server Update durch, wenn das Interface in Betrieb geht
<b>Update DynDNS entry</b>	Führt ein Dynamic DNS Update durch wenn das Interface in Betrieb geht

### 5.13.2 PPP Accounts

Im Menu PPP Accounts können CHAP (Challenge Handshake Authentication Protocol) oder PAP (Password Authentication Protocol) Benutzer erstellt und verwaltet werden.

#### 5.13.2.1 Create new PPP CHAP/PAP account

Kommando	Beschreibung	
<b>Username</b>	<b>Any</b>	Der Benutzername kann leer sein oder aus beliebigen ASCII Zeichen bestehen.
	<b>String</b>	Der eingetragene Benutzername muss verwendet werden
<b>Password</b>	<b>None</b>	Es wird keine Passwort Kontrolle bei der Einwahl durchgeführt.
	<b>From File</b>	Das Passwort wird mit dem, im angegebenen File, hinterlegten Passwort verglichen.
	<b>Set To</b>	Das Passwort wird auf den eingetragenen Wert gesetzt. Bitte beachten Sie Groß- und Kleinschreibung.
<b>Server</b>	<b>Any</b>	Es findet keine Kontrolle des eingehenden Servers statt.
	<b>String</b>	Eine Einwahl kann nur vom eingetragenen Server aus stattfinden
<b>Valid Addresses</b>	<b>Allow any</b>	Es wird keine Adressen Kontrolle bei der Einwahl durchgeführt.
	<b>Allow none</b>	Der Account ist gesperrt.
	<b>Allow listed</b>	Nur die eingetragenen Adressen dürfen sich einwählen.

## 5.14 Postfix Configuration (nur M3000, G5000)

Postfix ist ein Open Source Mail Transfer Agent. Dieser Dienst ist nur bei Geräten der M und G Serie integriert.

Die Beschreibung hierzu entnehmen Sie bitte der offiziellen POSTFIX Homepage unter <http://www.postfix.org>

## 5.15 QoS Control

Mit Quality of Service (QoS) ist es möglich, die verfügbare Bandbreite einer Verbindung zu regulieren und diese zum Beispiel auf verschiedene Ports oder IP's zu verteilen.

In Normalfall wird bei einer Internetverbindung mittels Modem jedes Paket der Reihe nach in eine sog. Packet-Queue (Queue = Schlange, Reihe) gespeichert. Die Größe der Packet-Queue übersteigt dabei die verfügbare Bandbreite der Internetverbindung. Alle dort gespeicherten Pakete werden der Reihe nach abgearbeitet. QoS verwaltet ebenfalls eine Packet-Queue, nur im Router selbst. Somit hat man die Möglichkeit, mit Hilfe von QoS-Regeln zu entscheiden, welche Pakete zuerst dürfen und welche sich noch etwas gedulden müssen. Sind diese Regeln alle richtig konfiguriert, sendet der Router die Pakete seiner Packet-Queue gerade so schnell an das Modem, dass diese Pakete nicht in der Packet-Queue des Modems landen. Das wäre so, als hätte man die Queue vom Modem in den Router geholt.

### 5.15.1 Outgoing Interfaces

#### 5.15.1.1 Interface parameters

Kommando	Beschreibung
<b>Interface</b>	Selektiert die eingehende Schnittstelle
<b>Enable Interface</b>	<b>Yes:</b> Schnittstelle wird aktiviert <b>No:</b> Schnittstelle ist nicht aktiv

#### 5.15.1.2 Root Qdisc Parameters

<p><b>Hinweis</b></p> <p>➤ Alle QoS-Regeln werden als User <b>root</b> ausgeführt.</p>
--

#### 5.15.1.2.1 TBF (Token Bucket Filter)

Aus der Funktionsweise des TBF ergeben sich drei Szenarien:

- ◊ Treffen die zu sendenden Netzwerkpakete mit der gleichen Rate ein, wie TBF neue Tokens erzeugt, darf die QDisc jedes Paket sofort senden.
- ◊ Treffen die Pakete schneller ein, müssen sie warten, bis wieder ausreichend Tokens vorhanden sind. Das drosselt die Senderate auf die Token-Rate.
- ◊ Erreichen die Pakete den TBF mit einer geringeren Rate oder kommen gar keine Pakete an, tröpfeln die überschüssigen Tokens wieder in den Bucket. Ist der irgendwann voll, fließen alle folgenden Tokens in den elektronischen Gully. Kommen nun wieder Pakete mit einer hohen Rate an, verbrauchen sie die angesammelten Tokens. Bis zur Bucketgröße darf die QDisc also mit einer höheren Rate senden, als dem TBF eigentlich zusteht. Es kommt zu einem so genannten Burst.

Kommando	Beschreibung
<b>Rate</b> (kbit/s)	gibt die maximale Verzögerung an, die sich ein Paket verspätet. (Aufenthalt in der Queue)
<b>Burst</b> (Bytes)	bestimmt die Bucketgröße und begrenzt damit die Datenmenge bei einem Burst.
<b>Latency</b> (ms)	gibt die maximale Zeit in ms an, welche sich ein Paket in der Queue befinden darf.
<b>Peakrate</b> (kbit/s)	gibt die maximale Bandbreite an, die während eines Bursts zur Verfügung steht. Die maximale Peakrate ergibt sich aus der durchschnittlichen Paketgröße multipliziert mit der Timerfrequenz.
<b>Mpu</b> (Bytes)	die „Minimum Packet Unit“ bestimmt die minimale Token Nutzung für ein Paket.
<b>Minburst</b> (Bytes)	bestimmt die Größe des Ausgangsbuckets

#### 5.15.1.2.2 SFQ (Stochastic Fairness Queueing)

Der SFQ (Stochastic Fairness Queueing) sorgt bei einer voll ausgelasteten Leitung für Fairness unter allen aktiven Verbindungen. Dafür werden 127 FIFO-Warteschlangen eingesetzt, welche abwechselnd senden. Ein Hashverfahren entscheidet, welche Verbindung in welcher Warteschlange landet. Jedoch müssen sich gelegentlich mehrere Verbindungen eine Warteschlange teilen, während andere eine Warteschlange alleine nutzen. Um diese Ungleichheit rasch auszugleichen, wechselt SFQ die Hashfunktion oft und garantiert so wenigstens eine stochastische Fairness.

Kommando	Beschreibung
<b>Perturb</b>	Bestimmt die Zeitspanne für die Hashfunktion-Wechsel
<b>Quantum</b>	Legt die Anzahl Bytes fest, die eine Warteschlange am Stück senden darf. Dieser Wert muss mindestens so groß sein wie die aktuelle Paketgröße (MTU). Andernfalls bleiben größere Pakete in der Queue hängen.

#### 5.15.1.2.3 BFIFO (Bytes First In First Out)

Kommando	Beschreibung
<b>Limit</b>	Menge an Bytes, die die Queue aufnehmen kann.

#### 5.15.1.2.4 PFIFO Packet First In First Out

Kommando	Beschreibung
<b>Limit</b>	Anzahl an Paketen, die die Queue aufnehmen kann.

### 5.15.1.2.5 DSMARK

DSMARK kontrolliert, überwacht oder ändert den Verkehr der Daten nicht. Es priorisiert nicht, verzögert nicht oder verwirft Pakete auch nicht. Es markiert lediglich das DS-Feldes der Pakete.

Kommando	Beschreibung
<b>Number of Indices</b>	Die Klassen sind nummeriert. <b>n</b> ist ein Parameter, der die Größe einer internen Tabelle definiert, welche die Rangfolge der zu durchlaufenden Queue festlegt.
<b>Default Index</b> (optional)	Pakete, die auf keine definierte Regel passen, werden in der default-Klasse abgearbeitet. Dieser Wert bestimmt diese default-Klasse.
<b>Set TC-Index</b>	<b>Yes:</b> Die Queue-Regel kopiert den TOS-Wert (Type of Service) des Pakets (DS-Wert).

### 5.15.1.2.6 HTB (Hierarchical Token Bucket)

Kommando	Beschreibung
<b>R2Q</b>	Der R2Q gibt eine Klasse an, die alle nicht klassifizierten Pakete erhält.

### 5.15.1.2.7 PRIO (Filter)

Kommando	Beschreibung
<b>Number of Bands</b>	Definiert eine Klasse. Je größer die Nummer, desto höher ist der Wert der Klasse.

### 5.15.1.2.8 PRIO (Priomap)

Kommando	Beschreibung
<b>Number of Bands</b>	Definiert eine Klasse. Je größer die Nummer, desto höher ist der Wert der Klasse.

## 5.15.2 Incoming Interfaces

Es gibt auch die Möglichkeit, den eingehenden Netzwerkverkehr mit Regeln zu steuern. Diese Implementation unterscheidet sich grundsätzlich von den anderen, da sich ankommende Pakete nicht vor der Schnittstelle anstauen. Folglich lässt sich eine Regel für eingehenden Verkehr nur mit Filtern und Policies verwenden.

### 5.15.2.1 Interface parameters

Kommando	Beschreibung
<b>Interface</b>	Selektiert die eingehende Schnittstelle
<b>Enable Interface</b>	Schnittstelle wird aktiviert/deaktiviert
<b>Attached Interface</b>	Gibt an, auf welche Schnittstelle(n) die neue QoS-Regel aktiviert werden soll.

Die Root Qdisc Parameter stimmen mit denen von Kapitel [5.15.1.2](#) überein.

### 5.15.3 Interface Statistics

Hier wird die Statistik der ankommenden und abgehenden QoS Interfaces angezeigt.

## 5.16 SNMP

Das Simple Network Management Protocol (SNMP) ist Teil der Internet Protokoll Familie. Es wurde entwickelt um Netzwerkelemente (Router, Server, Switches, usw.) von einer zentralen Managementstation aus überwachen und steuern zu können.

SNMP definiert ein Community-basierendes Administrations-Framework, um mit ihm die verschiedenen SNMP Elemente verwalten zu können. Jede SNMP-Community ist eine Gruppe von Geräten, die mindestens einen »Agent« und ein Management-System beinhaltet. Die Eigenschaften, die von einem Agenten über die gemanagte Netzwerkkomponente ausgelesen und verändert werden können, die so genannten »Managed Objects«, werden in der Management Information Base (MIB) festgelegt.

### 5.16.1 Access Control

Das SNMP Protokoll beinhaltet keine Zugriffs- oder Passwort-Mechanismen. Im SNMP Access Control Menü können Sie Communitys anlegen und deren Zugriffe und Berechtigungen reglementieren, die über SNMP ausgeführt werden.

Kommando	Beschreibung
<b>Community Name</b>	Name der SNMP Community, welcher der Router angehören soll. Einer SNMP Community muss mindestens ein SNMP Agent und ein gemanagtes System angehören. Sinnvollerweise werden in einer Community verschiedene Arbeitsgruppen (z.B. Internet, Drucker, Vertrieb, Marketing usw.) zusammengefasst. Einzelne SNMP Agents können aber auch in verschiedenen Communitys vertreten sein (z.B. Router).
<b>Source:</b>	<b>Default:</b> Alle SNMP Requests werden beantwortet <b>Hostname:</b> SNMP Requests vom angegebenen Host werden akzeptiert <b>Subnet:</b> SNMP Requests vom folgenden Netzwerk (IP-Adresse / Subnet z.B. 192.168.0.0 / 24) werden akzeptiert
<b>Restricted OID:</b>	<b>None:</b> Zugriff auf die gesamte MIB erlaubt <b>OID:</b> Der Wert OID (Object Identifier) regelt den Zugriff auf die MIB. Der Zugriff auf den MIB (Management Information Base) Baum wird nur unterhalb des eingegebenen Wertes erlaubt. In der MIB werden alle Eigenschaften, die über SNMP ausgelesen oder verändert werden können festgelegt.
<b>Access Mode:</b>	<b>Read Only:</b> Innerhalb der MIB ist nur ein Lesezugriff erlaubt. SNMP kann somit nur den jeweiligen Status oder die Eigenschaft abfragen, aber nicht verändern. <b>Read/Write:</b> Innerhalb der MIB sind Lese- und Schreibzugriffe erlaubt. SNMP kann somit nur den jeweiligen Status oder die Eigenschaft abfragen und verändern.
<b>Process:</b>	<b>Yes:</b> aktiviert diese Community <b>No:</b> deaktiviert diese Community

### 5.16.2 Sysinfo Setup

Die RFC1213-MIB Definition beinhaltet verschiedene managebare Objekte und Funktionsgruppen. Um diese Objekte und Funktionsgruppen übersichtlich gliedern zu können, können Sie im SNMP Sysinfo Setup die Werte sysLocation und SysContact für den Router festlegen.

Kommando	Beschreibung
<b>System Location</b>	Informative Angabe zum physikalischen Aufstellort.
<b>System Contact</b>	Informative Angaben zum System wie z. B. der Namen der Person, der Gruppe oder der Organisation die für die Wartung, Pflege usw. des Nodes verantwortlich ist.

### 5.16.3 Trap Control

Traps sind unangeforderte Nachrichten, die von einem »Agent« an ein Management-System gesendet werden, sobald etwas Unvorhergesehenes und für das Management-System interessantes geschieht.

#### 5.16.3.1 SNMP Create New Trap Control

Kommando	Beschreibung
<b>Symbolic Name</b>	Beschreibung der Trap Control
<b>Destination</b>	<b>Hostname:</b> Anfallende Traps werden an den folgenden Host gesendet <b>IP:</b> Anfallende Traps werden an die folgende IP-Adresse gesendet
<b>Community</b>	Name der Trap Community
<b>Type</b>	<b>SNMPv1 Trap Receiver:</b> SNMP Server empfängt SNMP Version 1 Traps <b>SNMPv2 Trap Receiver:</b> SNMP Server empfängt SNMP Version 2 Traps <b>SNMPv2 Inform Receiver:</b> SNMP Server empfängt SNMP Version 2 Inform Traps
<b>Process</b>	aktiviert/deaktiviert diese Trap Control

### 5.16.4 (Sub)Agent Configurations

In diesem Menü werden die Einstellungen für das SNMP-Monitoring vorgenommen.

#### 5.16.4.1 Common Settings

Kommando	Beschreibung
<b>Send trap on authentication failures:</b>	<b>Yes:</b> Der Router sendet einen Trap, wenn eine ungültige Authentifizierung stattgefunden hat. <b>No:</b> Der Router sendet keinen Trap, wenn eine ungültige Authentifizierung stattgefunden hat.
<b>Enable System Monitoring:</b>	<b>Yes:</b> aktiviert das Sub-Agent Monitoring <b>No:</b> deaktiviert das Sub-Agent Monitoring

## 5.16.4.2 Monitor Running Processes

### 5.16.4.2.1 SNMP Agent Create Process Monitor

Kommando	Beschreibung
<b>Process:</b>	Name des Prozesses, der überwacht werden soll.
<b>Max. running instances:</b>	Maximale Anzahl der erlaubten Instanzen. Wird kein Wert gesetzt oder der Wert 0 eingetragen, sind die erlaubten Instanzen unendlich.
<b>Min. running instances:</b>	Minimale Anzahl der erforderlichen Instanzen. Wird kein Wert gesetzt <b>und</b> der Wert Max. ist nicht gesetzt, dann wird der Wert 1 übernommen
<b>Process:</b>	Monitoring für diesen Prozess wird aktiviert/deaktiviert

### 5.16.4.3 Monitor Disk Space

Kommando	Beschreibung
<b>Disk mount path 1:</b>	Pfad des zu überwachenden freien Speicherplatzes von Device 1.
<b>Minimum limit</b>	Bei Unterschreitung dieses Wertes wird ein Trap versendet. <b>Bytes:</b> minimaler freier Speicherplatz in Bytes. <b>Percentage:</b> minimaler freier Speicherplatz in Prozent
<b>Disk mount path 2:</b>	Pfad des zu überwachenden freien Speicherplatzes von Device 2.
<b>Minimum limit</b>	Bei Unterschreitung dieses Wertes wird ein Trap versendet. <b>Bytes:</b> minimaler freier Speicherplatz in Bytes. <b>Percentage:</b> minimaler freier Speicherplatz in Prozent
<b>Disk mount path 3:</b>	Pfad des zu überwachenden freien Speicherplatzes von Device 3.
<b>Minimum limit</b>	Bei Unterschreitung dieses Wertes wird ein Trap versendet. <b>Bytes:</b> minimaler freier Speicherplatz in Bytes. <b>Percentage:</b> minimaler freier Speicherplatz in Prozent

### 5.16.4.4 Monitor File Sizes

Kommando	Beschreibung
<b>Destination</b>	Pfadangabe der zu überwachenden Datei (z.B.: <i>/var/log/messages</i> )
<b>Max. Size in Byte</b>	Maximale Größe der Datei in Bytes
<b>Process:</b>	<b>Yes:</b> die Datei wird überwacht <b>No:</b> die Datei wird nicht überwacht

#### Hinweis

- Die maximale Anzahl der zu definierenden Dateien beträgt 20!

### 5.16.4.5 Monitor Load Average

Kommando	Beschreibung
<b>Maximum load for 1 minute average:</b>	Maximal zulässiger Durchschnitt der CPU Auslastung innerhalb der letzten Minute. Bei Überschreitung des Wertes wird ein Trap gesendet.
<b>Maximum load for 5 minute average:</b>	Maximal zulässiger Durchschnitt der CPU Auslastung innerhalb der letzten fünf Minuten. Bei Überschreitung des Wertes wird ein Trap gesendet.
<b>Maximum load for 15 minute average:</b>	Maximal zulässiger Durchschnitt der CPU Auslastung innerhalb der letzten 15 Minuten. Bei Überschreitung des Wertes wird ein Trap gesendet.

## 5.17 SSH Server

SSH ist ein Protokoll, das Benutzern eine Anwahl zum Router ermöglicht, ähnlich Telnet. Jedoch werden alle SSH-Anschlüsse an beiden Enden verschlüsselt und zertifiziert, um zu verhindern, dass Angreifer Kennwörter oder übertragene Daten ausspionieren können.

### 5.17.1 Authentication

Alle SSH Anwendungen haben ähnliche Optionen wie sich Clients zu authentifizieren haben und wie Meldungen nach dem Login angezeigt werden. Die Einstellungen hierzu sind in diesem Menü durchzuführen.

Kommando	Beschreibung
<b>Allow authentication by password?</b>	<b>Yes (Default):</b> der Benutzer kann sich mit einem Passwort am Router anmelden <b>No:</b> Der Benutzer kann sich nur mit einem Public Key anmelden
<b>Allow login by root?</b>	<b>Yes (Default):</b> der Benutzer kann sich als root anmelden <b>No:</b> der Benutzer kann sich nicht als root anmelden <b>Only with RSA auth:</b> der Benutzer kann sich als root anmelden, wenn eine RSA Authentifizierung durchgeführt wurde <b>Only for commands:</b> der Benutzer kann sich als root anmelden, um Kommandos einzugeben
<b>Check permissions on key files?</b>	<b>Yes (Default):</b> die Berechtigungen des Benutzers werden anhand der hinterlegten Keys vergeben <b>No:</b> die Berechtigungen des Benutzers werden anhand des Benutzernamens vergeben
<b>Ignore users' known_hosts files?</b>	<b>Yes:</b> der SSH Daemon ignoriert die \$Home/.ssh/known_hosts während einer RSA Authentifizierung <b>No:</b> der SSH Daemon verarbeitet die \$HOME/.ssh/known_hosts während einer RSA Authentifizierung
<b>Pre-login message file</b>	<b>None (Default):</b> es wird keine Meldung vor dem Login ausgegeben <b>String:</b> die Textmeldung, in der angegebenen Datei, wird vor dem Login ausgegeben
<b>User authorized keys file</b>	<b>Default (~/.ssh/authorized_keys):</b> die Authentifizierungsschlüssel liegen im Default-Verzeichnis <b>String:</b> die Authentifizierungsschlüssel liegen im angegebenen Verzeichnis

Kommando	Beschreibung
<b>Permit logins with empty passwords?</b>	<b>Yes:</b> die Einwahl mit leerem Passwort wird erlaubt <b>No (Default):</b> zur Einwahl wird ein Passwort benötigt
<b>Allow RSA authentication?</b>	<b>Yes (Default):</b> die Einwahl mit RSA Authentifizierung wird erlaubt <b>No:</b> die Einwahl mit RSA Authentifizierung wird nicht erlaubt
<b>Display /etc/motd at login?</b>	<b>Yes (Default):</b> die Textmeldung, die unter /etc/motd gespeichert ist, wird nach dem Login ausgegeben <b>No:</b> es wird keine Meldung ausgegeben
<b>Allow login just by hosts.equiv and .rhosts?</b>	<b>Yes:</b> die Files hosts.equiv und .rhosts werden zur Authentifizierung benutzt (Sicherheitsrisiko) <b>No (Default):</b> die Files hosts.equiv und .rhosts werden nicht zur Authentifizierung benutzt
<b>Ignore .rhosts files?</b>	<b>Yes (Default):</b> der File .rhosts wird bei der Einwahl ignoriert <b>No:</b> der File .rhosts wird bei der Einwahl nicht ignoriert
<b>Check hosts.equiv and .rhosts for RSA authentication?</b>	<b>Yes (Default):</b> die Files hosts.equiv und .rhosts werden zur RSA Authentifizierung benutzt <b>No:</b> die Files hosts.equiv und .rhosts werden nicht zur RSA Authentifizierung benutzt

### 5.17.2 Networking

Der SSH Server verfügt über Konfigurationsmöglichkeiten zum Einstellen der überwachten IP-Adressen, zum Festlegen der benutzten Ports und verschiedene Protokolleinstellungen. Im Networking Menü können Sie diese Parameter einstellen.

Kommando	Beschreibung
<b>Listen on addresses</b>	<b>All addresses (Default):</b> alle IP Adressen des Routers werden auf eine eingehende SSH Verbindung überwacht <b>Entered below...:</b> nur die folgenden IP Adressen des Routers werden auf eine eingehende SSH Verbindung überwacht
<b>Listen on port</b>	<b>Default (22):</b> der Port 22 des Routers wird auf eine eingehende SSH Verbindung überwacht <b>String:</b> der angegebene Port des Routers wird auf eine eingehende SSH Verbindung überwacht
<b>Disconnect if client has crashed?</b>	<b>Yes (Default):</b> der Router beendet die Verbindung automatisch, wenn der Client getrennt wurde <b>No:</b> der Router beendet die Verbindung nicht, wenn der Client getrennt wurde
<b>Allow TCP forwarding?</b>	<b>Yes (Default):</b> Benutzer können TCP Verbindungen des Clients in das Netzwerk des Routers tunneln <b>No:</b> Benutzer können keine TCP Verbindungen des Clients in das Netzwerk des Routers tunneln
<b>Reverse-validate client IP addresses?</b>	<b>Yes (Default):</b> der Router vergleicht den Hostnamen mit der IP Adresse des DNS Servers <b>No:</b> der Router akzeptiert die IP Adresse ohne Rückfrage an den DNS Server

### 5.17.3 Access Control

Standardmäßig kann jeder auf dem Router konfigurierte User remote über SSH darauf zugreifen. Hier lassen sich User und Gruppen für den SSH Zugriff festlegen.

### 5.17.4 Miscellaneous Options

Dieses Menü enthält Optionen, die sich in keine der anderen Kategorien einordnen lassen.

<p><b>Hinweis</b></p> <p>➤ X11 ist <b>nicht</b> implementiert!</p>
--

Kommando	Beschreibung
<b>Allow X11 connection forwarding?</b>	<b>Yes:</b> ermöglicht Unix/Linux Usern X Anwendungen über SSH aufzurufen <b>No:</b> unterbindet den Aufruf von X Anwendungen
<b>X11 display offset</b>	<b>Default:</b> 10 <b>String:</b> Definiert das erste Display für das X11 Forwarding
<b>Full path to xauth program</b>	<b>Default:</b> /usr/X11R6/bin/xauth <b>String:</b> Hier wird der Pfad von <b>xauth</b> angegeben
<b>System log facility</b>	Der syslog-Service wird benutzt um Störungs- und Informationsanzeigen vom SSH-Benutzer zu loggen. Dieses kann in Verbindung mit dem Systemprotokollmodul verwendet werden. <b>Default:</b> alle Dienste geloggt <b>String:</b> nur der ausgewählte Dienst wird geloggt
<b>Logging level</b>	<b>Default:</b> der Logging-Level ist auf INFO gestellt <b>String:</b> der Logging Level ist auf den eingestellten Wert gesetzt, wobei <b>Quiet</b> den niedrigsten und <b>Debug</b> das höchste Logging-Level darstellt
<b>Server key size</b>	<b>Default:</b> die Authentifizierungs-Key Länge beträgt 128 Bit <b>String:</b> definiert die Länge des Authentifizierungs-Keys
<b>Server key regeneration interval</b>	<b>Default:</b> der SSH Key wird niemals aktualisiert <b>String:</b> der SSH Key wird alle <b>n</b> Sekunden aktualisiert
<b>PID file</b>	<b>Default:</b> die sshd.pid Datei liegt unter /var/run/sshd.pid <b>String:</b> definiert das Verzeichnis in dem die sshd.pid Datei liegt
<b>Use separate unprivileged process?</b>	<b>Yes:</b> der SSH Daemon startet verschiedene Prozesse <b>No:</b> der SSH Daemon läuft nur in einem Prozess

### 5.17.5 Client Host Options

Für einzelne Host's können hier spezifizierte Regelungen aufgestellt werden.

Kommando	Beschreibung
<b>Login as user</b>	Normally if no username is given on the ssh command line, the name of the current user is used to login to the remote SSH server. However, this option can be used to specify a different default username for a particular host or hosts.
<b>Escape character</b>	When making an interactive SSH login, the escape character can be used to break out of the connection and close or suspend it.
<b>Compress SSH traffic?</b>	If this option is enabled, the SSH client will compress all data sent to this host with the gzip algorithm. This can be useful if you are copying large files with scp over a slow link.

Kommando	Beschreibung
<b>Local ports to forward to server</b>	In this table you can enter local port numbers which will be forwarded to some host and port by the SSH server. This can be useful if your only access to some network is via SSH login to one machine on that network, and you want to access other services like web or POP servers.
<b>Server ports to forward to local</b>	In this table you can enter port numbers on the server which will be forwarded to some host and port on the client machine's network.

### 5.17.6 User SSH Key Setup

In diesem Menü können die SSH Optionen für neue lokale Benutzer des Routers festgelegt werden.

Kommando	Beschreibung
<b>Setup SSH key for new Unix users.</b>	Wenn die Option aktiviert ist, müssen alle neu angelegten lokalen Benutzer zuerst einen SSH Key generieren
<b>Copy new identify.pub to authorized_keys</b>	Der SSH Key wird im Home Verzeichnis des Benutzers im File <code>.ssh/authorized_keys</code> abgelegt
<b>Use password as key passphrase.</b>	Das Passwort des Benutzers wird als Key verwendet

### 5.18 SSL Tunnels

In diesem Menü können Verbindungen für den STunnel Dienst konfiguriert und editiert werden.

STunnel arbeitet als universaler SSL Tunnel zwischen Client und Router. Damit wird es möglich, auf einfache Weise beliebige TCP Verbindungen zu verschlüsseln.

Kommando	Beschreibung
<b>Service name</b>	legt den Namen für diesen SSL Tunnel fest
<b>TCP port</b>	Gibt den Port an von dem der Tunnel Verbindungen akzeptiert
<b>Active?</b>	aktiviert oder deaktiviert den SSL Tunnel
<b>Run inetd style program</b>	wenn der Tunnel ein inetd Programm starten soll; geben Sie bei <b>Path to program</b> den kompletten Pfad an; zur Parameterübergabe geben sie den Programmnamen und den Kommandozeilen Parameter bei <b>with arguments</b> an
<b>Run program in PTY</b>	wenn der Tunnel ein Programm im Terminal starten soll; geben Sie bei <b>Path to program</b> den kompletten Pfad an; zur Parameterübergabe geben sie den Programmnamen und den Kommandozeilen Parameter bei <b>with arguments</b> an
<b>Connect to remote host</b>	wenn sich der Tunnel zu einem Server verbinden soll geben Sie hier den <b>Remote hostname</b> und den <b>Remote port</b> an

Kommando	Beschreibung
<b>SSL certificate and key file</b>	wählen Sie <b>Use Webmin's cert</b> wenn das Webmin SSL Zertifikat verwendet werden soll; für ein selbst erstelltes Zertifikat wählen Sie <b>Use cert in file</b> und geben den vollen Pfad dazu an.  <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p><b>Hinweis</b></p> <ul style="list-style-type: none"> <li>➤ Laden Sie Ihr selbst erstelltes Zertifikat mit einem <a href="#">SCP Programm</a> auf den Router.</li> <li>➤ Benutzen Sie das Verzeichnis <b><i>/etc/stunnel</i></b>.</li> </ul> </div>
<b>TCP-wrappers name</b>	lassen Sie den TCP Wrapper Name mit <b>Automatic</b> automatisch erstellen, oder legen Sie ihn selbst fest
<b>Tunnel mode</b>	<b>Accept SSL and connect normally</b> Router arbeitet als Server; nimmt SSL Verbindungen entgegen und übermittelt sie „normal“ weiter
	<b>Accept normal and connect with SSL</b> Router arbeitet als Client; nimmt „normale“ Verbindungen entgegen und übermittelt sie SSL verschlüsselt weiter
<b>Outgoing source address</b>	geben Sie hier die Ausgehende IP Adresse an; mit <b>Automatic</b> wird die Router IP verwendet

## 5.19 VRRP / Loadbalancer \*

### 5.19.1 Funktionsweise VRRP

In diesem Menü können Sie VRRP (Virtual Router Redundancy Protocol) Geräte und Abhängigkeiten konfigurieren oder ändern.

Das VRRP sorgt dafür, dass mehrere Router als virtuelle Default Router eingesetzt werden können. Beim Ausfall eines sog. Master-Routers springt ein anderer sog. Backup-Router dynamisch (d.h. ohne manuelle Umschaltung) für den ausgefallenen Master-Router ein und übernimmt direkt dessen Aufgaben. Hierfür tauschen die Router sog. VRRP-Advertisements (RFC 3768) miteinander aus.

#### 5.19.1.1 Verhalten des VRRP-Routers im Backup-Zustand

Im Backup-Zustand überwacht der VRRP-Router, ob der Master-Router noch aktiv ist und regelmäßig seine VRRP-Advertisements sendet. Im Backup-Zustand verhält sich der Router folgendermaßen:

- ◊ Er darf keinen ARP-Request nach der virtuellen IP-Adresse beantworten.
- ◊ Er verwirft alle IP-Pakete, die die virtuelle IP-Adresse als Ziel-IP-Adresse haben.

Empfängt ein Router im Backup-Zustand ein VRRP-Advertisement mit der Priorität 0 bzw. läuft der Master\_Down\_Timer bei ihm ab, führt er folgendes aus:

- ◊ Der Router versendet seinerseits ein VRRP-Advertisement, in dem er sich als neuer Master-Router bekannt gibt.
- ◊ Er sendet eine ARP-Response, um die Zuordnung der virtuellen IP-Adresse zur neuen MAC-Adresse bekannt zu machen.
- ◊ Der Advertisement Timer wird gestartet.
- ◊ Der Router geht in den Master-Zustand über.
- ◊ Falls danach der Router (d.h. bereits im Master-Zustand) ein anderes VRRP-Advertisement
  - ◊ mit höherer Priorität empfängt, geht der Router wieder in den Backup-Zustand zurück.

- mit niedrigerer Priorität empfängt, wird das IP-Paket verworfen, und der Router bleibt weiter im Master-Zustand.

### 5.19.1.2 Verhalten des VRRP-Routers im Master-Zustand

Befindet sich ein VRRP-Router im Master-Zustand, ist er ab sofort für die Weiterleitung von IP-Paketen in andere IP-Subnetze zuständig. Somit fungiert er als Default Gateway. Im Master-Zustand verhält sich der Router wie folgt:

- Er versendet in regelmäßigen Abständen (standardmäßig 1 s) VRRP-Advertisements an die Backup-Router.
- Er beantwortet Requests die der virtuellen IP-Adresse entsprechen.
- Falls er nicht der "IP Address Owner" ist, verwirft er alle IP-Pakete, die die virtuelle IP-Adresse als Ziel-IP-Adresse haben.
- Empfängt der aktuelle Master-Router ein VRRP-Advertisement
  - mit höherer Priorität als die eigene, dann wird der Master\_Down\_Timer gestartet, und er geht in den Backup-Zustand über.
  - mit niedrigerer Priorität wird dieses VRRP-Advertisement von ihm ignoriert und verworfen.

### 5.19.2 Global Definitions

Hier wird eine Email Benachrichtigung aktiviert, welche eine Benachrichtigung versendet wenn eine der VRRP Instanzen ihren Status ändert.

Kommando	Beschreibung
<b>Router ID</b>	Bezeichnung des Routers zur Identifizierung
<b>Notify email address</b>	Email Adresse an die die Benachrichtigungen gesendet werden
<b>From email address</b>	Adresse die als Absender verwendet wird
<b>SMTP Server IP Address</b>	IP Adresse des Email Servers
<b>SMTP Server Connect Timeout</b>	Gibt eine Zeit an wie lange versucht wird den Server zu erreichen

### 5.19.3 VRRP Instances

Hier werden die eingerichteten VRRP Instanzen aufgelistet. Zudem können die Instanzen verwaltet und neue hinzugefügt werden.

#### 5.19.3.1 Add VRRP Instance

Kommando	Beschreibung				
<b>Instance Name</b>	Bezeichnung der VRRP Instanz. (z.B.: M3000_Master). Der Name sollte für jede VRRP Gruppe gleich sein.				
<b>Default State</b>	Startet die Instanz mit Master oder Backup Status.				
<b>Force Election</b>	<table border="0"> <tr> <td><b>Yes</b></td> <td>Nimmt der Maschine den Master Status.</td> </tr> <tr> <td><b>No</b></td> <td>Das Gerät mit der geringeren Priorität bleibt Master, wenn ein Partner mit höherer Priorität online kommt.</td> </tr> </table>	<b>Yes</b>	Nimmt der Maschine den Master Status.	<b>No</b>	Das Gerät mit der geringeren Priorität bleibt Master, wenn ein Partner mit höherer Priorität online kommt.
<b>Yes</b>	Nimmt der Maschine den Master Status.				
<b>No</b>	Das Gerät mit der geringeren Priorität bleibt Master, wenn ein Partner mit höherer Priorität online kommt.				

Kommando	Beschreibung
	<p><b>Delayed</b> Der Statuswechsel erfolgt erst nach <b>n</b> Sekunden (Range 0-1000; Default: 0)</p>
<b>Interface</b>	Die Entsprechende Schnittstelle, die die virtuelle IP im Störfall übernehmen soll. (z.B.: eth0)
<b>Traced Interfaces</b>	Mit überwachte Schnittstellen. Gerät wechselt in den FAULT Status, wenn ein der Schnittstellen down geht.
<b>Virtual Router ID</b>	Virtual Router ID (integer Wertebereich 1-255) einer VRRP Synchronisation Gruppe. Alle VRRP Geräte einer VRRP Gruppe müssen die gleiche VRID besitzen.
<b>Priority</b>	<p>Geben sie hier die Priorität (Wertebereich 1 bis 255) ein, die die Instanz in der VRRP Synchronisation Gruppe hat.</p> <div style="border: 1px solid black; padding: 5px;"> <ul style="list-style-type: none"> <li>➤ Der Master einer VRRP Synchronisation Gruppe muss die Priorität 255 erhalten</li> <li>➤ Backup Instanzen können im Bereich von 1 bis 254 liegen.</li> </ul> </div>
<b>Advert Intervall</b>	<p>Dieser Wert legt fest, in welchen Zeitabständen VRRP Nachrichten (Advertisements) verschickt werden. (Default: 1 sec)</p> <div style="border: 1px solid black; padding: 5px;"> <ul style="list-style-type: none"> <li>➤ Das Advertisement Intervall muss für alle Router mit der gleichen VRID den gleichen Wert haben</li> </ul> </div> <p>Der Wert wird auch zur Berechnung des »Master Down Intervalls« mit herangezogen.  Das »Master Down Intervall« berechnet sich wie folgt:  <math>(3 * \text{Advert Intervall}) + ((256 - \text{Priority}) / 256)</math>  Daraus ergibt sich folgendes: je höher die Priority des VRRP Routers ist, desto geringer das Master Down Intervall, desto schneller wird im Störfall vom Gerät reagiert.</p>
<b>Virtual IP (s)</b>	Die virtuelle(n) IP(s) die im Störfall übernommen werden soll(en). z.B.: 192.168.0.50 192.168.1.50
<b>Virtual Route(s)</b>	Die virtuelle(n) Route(n) die im Störfall übernommen werden soll(en).
<b>Default State:</b>	<p><b>Master:</b> legt fest, dass die Instanz als Master-Instanz arbeitet  <b>Backup:</b> legt fest, dass die Instanz als Backup-Instanz arbeitet</p>
<b>Auth. Mode:</b>	<p><b>None:</b> es wird keine Authentifizierung durchgeführt  <b>Pass:</b> zur Authentifizierung wird ein Passwort verwendet  <b>AH:</b> zur Authentifizierung wird ein Authentication Header verwendet</p>
<b>Auth. Password:</b>	<p>Geben Sie hier das Passwort ein, das für den Auth. Mode Pass verwendet wird.</p> <div style="border: 1px solid black; padding: 5px;"> <ul style="list-style-type: none"> <li>➤ Die Länge des Passwortes ist auf 8 Zeichen festgelegt. Wird ein Passwort mit mehr als 8 Zeichen verwendet, werden die restlichen Zeichen verworfen. Wird ein Passwort mit weniger als 8 Zeichen verwendet, werden die fehlenden Zeichen mit '0' aufgefüllt.</li> <li>➤ Bitte beachten Sie, dass das Passwort unverschlüsselt über das Netzwerk gesendet wird.</li> </ul> </div>

Kommando	Beschreibung
<b>Tracked Interface(s):</b>	Hier haben Sie die Möglichkeit Schnittstellen einzugeben, die überwacht werden (z.B. eth0). Geht die überwachte Schnittstelle down, schaltet die Instanz auch down und gibt den Mastermodus weiter.
<b>Notify Script:</b>	das hier angegebene Script wird bei einer Statusänderung ausgeführt
<b>Activate:</b>	Instanz aktivieren/deaktivieren

Nach dem Speichern der Konfiguration, muss der Dienst gestartet werden, um die virtuelle IP-Adresse zu übernehmen. Navigieren Sie hierzu in das Menü **Networking > VRRP (Loadbalancer)** und drücken dort den Button **Activate VRRP**. Wird der Slave vor dem Master gestartet, übernimmt er die Masterfunktion bis der Master verfügbar ist.

### 5.19.4 VRRP Synchronization Groups

In diesem Menü werden die Synchronisationsgruppen angezeigt und verwaltet.

#### 5.19.4.1 VRRP Create New Sync. Group

Kommando	Beschreibung
<b>Sync. Group</b>	Bezeichnung der Sync. Group
<b>Usable Instances</b>	Wählen Sie die Instanzen aus, die der Sync. Group angehören sollen.
<b>Activate:</b>	Aktiviert/deaktiviert die Sync-Group

### 5.19.5 Load Balancer Global Settings

Der Load Balancer ist ein »Lastverteiler«, der die Antwortzeiten und Auslastung einzelner Server beurteilen kann um eine Anfrage mit der bestmöglichen Performance zu bedienen. Dazu werden die Anfragen an verschiedene Server verteilt, was bei einem erhöhten Zugriff die Geschwindigkeit erheblich verbessert. Für den Benutzer bleibt dieser Vorgang jedoch verborgen.

Im Global Settings Menu werden allgemeine Einstellungen zum Load Balancing vorgenommen.

Kommando	Beschreibung
<b>Load Balancer Symbolic Name</b>	Name des Load Balancers
<b>Notify email address</b>	Bis zu fünf E-Mail Adressen, an die eine Benachrichtigung versendet wird sobald eine Statusänderung eines Realservers erkannt wird.
<b>From email address</b>	Absender E-Mail Adresse, mit der die E-Mails versendet werden.
<b>SMTP Server IP Address</b>	Die IP Adresse des Simple Mail Transfer Protocol Servers.
<b>SMTP Server Connect Timeout</b>	Der Wert gibt die Zeit in Sekunden an, wie lange versucht wird den SMTP Server zu erreichen. (default: 30 sec)

Kommando	Beschreibung
<b>Connection Synchronization</b>	<p><b>OFF:</b> Stoppt die Synchronisation.</p> <p><b>Master:</b> Der Router ist als Synchronization Master festgelegt und sendet Status Meldungen an die Gruppe.</p> <p><b>Backup:</b> Der Router arbeitet als Synchronization Backup Server und empfängt Statusmeldungen</p>
<b>Synchronization Multicast Interface</b>	Der Wert legt die Schnittstelle fest, an die der jeweilige Status der aktuell bestehenden Verbindungen als Multicast gesendet wird, wenn der Router als Master arbeitet. Diese Funktion dient dazu, dass die Backup Server der Sync. Gruppe jederzeit über bestehende Verbindungen informiert werden und die Verbindungen bei einem Ausfall des Masters weiter nutzen können. Wenn der Router als Backup arbeitet, werden über dieses Interface diese Multicasts empfangen.
<b>Create Load Balancer config on next startup</b>	Der Wert legt fest, ob der Router beim nächsten Start eine neue Konfigurationsdatei anlegt werden soll

### 5.19.6 Load Balancer Real Servers

Im Load Balancer Real Servers Menu können bestehende reale Server bearbeitet oder neue reale Server hinzugefügt werden.

Kommando	Beschreibung										
<b>IP Address</b>	Die IP Adresse, unter der der Real Server erreichbar ist.										
<b>Port</b>	Der IP Port auf, dem der Dienst läuft. Soll kein bestimmter Port verwendet werden, so ist dieses Feld leer zu lassen. Im Direct Routing oder Tunneling Modus müssen Port und der dazugehörige Dienst übereinstimmen.										
<b>Weight</b>	Der Wert legt die Gewichtung des Real Servers innerhalb einer Sync. Group fest. Je höher die Gewichtung desto mehr Anfragen werden an den Real Server geleitet. Server, die keine neue Anfragen mehr erhalten sollen, (z.B. wegen Wartungsarbeiten) werden mit der Gewichtung '0' angegeben. Sollen alle Anfragen gleichmäßig an alle Real Server verteilt werden, so müssen alle Server die gleiche Gewichtung besitzen. Die Gewichtung hat einen Wertebereich von 0 - 65535. Default: 1										
<b>Healthcheck</b>	<table border="1"> <tbody> <tr> <td><b>None</b></td> <td>Es findet kein Healthcheck statt.</td> </tr> <tr> <td><b>TCP</b></td> <td>Healthcheck wird über TCP mit den nachstehenden Werten durchgeführt.</td> </tr> <tr> <td><b>HTTP</b></td> <td>Healthcheck wird über HTTP mit den nachstehenden Werten durchgeführt.</td> </tr> <tr> <td><b>SSL</b></td> <td>Healthcheck wird über SSL mit den nachstehenden Werten durchgeführt.</td> </tr> <tr> <td><b>User Defined</b></td> <td>Healthcheck wird über eine eigene Funktion durchgeführt, die als Rückgabewert 0 oder -1 liefern muss.</td> </tr> </tbody> </table>	<b>None</b>	Es findet kein Healthcheck statt.	<b>TCP</b>	Healthcheck wird über TCP mit den nachstehenden Werten durchgeführt.	<b>HTTP</b>	Healthcheck wird über HTTP mit den nachstehenden Werten durchgeführt.	<b>SSL</b>	Healthcheck wird über SSL mit den nachstehenden Werten durchgeführt.	<b>User Defined</b>	Healthcheck wird über eine eigene Funktion durchgeführt, die als Rückgabewert 0 oder -1 liefern muss.
<b>None</b>	Es findet kein Healthcheck statt.										
<b>TCP</b>	Healthcheck wird über TCP mit den nachstehenden Werten durchgeführt.										
<b>HTTP</b>	Healthcheck wird über HTTP mit den nachstehenden Werten durchgeführt.										
<b>SSL</b>	Healthcheck wird über SSL mit den nachstehenden Werten durchgeführt.										
<b>User Defined</b>	Healthcheck wird über eine eigene Funktion durchgeführt, die als Rückgabewert 0 oder -1 liefern muss.										
<b>Connect Port</b>	Der Wert bestimmt den TCP Port, der zur Überprüfung verwendet wird.										

### 5.19.7 Load Balancer Virtual Servers

Kommando	Beschreibung
<b>IP Address</b>	Die IP Adresse, unter welcher der virtuelle Server erreichbar ist.
<b>Port</b>	Der IP Port des virtuellen Servers. Ein Port mit 0 als Adresse ist nur gültig, wenn der Dienst persistent angegeben worden ist. In diesem Fall ist es ein Wild- Card Port, zu den Verbindungen zu jedem Port zugelassen werden.
<b>Firewall Mark</b>	Der Wert ist eine Firewall Markierung, ein Ganzzahlwert größer als 0, um einen virtuellen Service anzudeuten anstatt einer Adresse, eines Ports und eines Protokolls (UDP oder TCP). Das markieren von Paketen mit einer Firewall Markierung wird konfiguriert mit der <code>-m --Markierungs</code> Option von IPtables. Sie kann benutzt werden, um einen virtuellen Service zu erstellen, der mit dem gleichen Real Server assoziiert wird, um mehrere IP Adressen, Ports und Protokoll tripplets zu umschreiben. Firewall markierte virtuelle Services ermöglichen eine bequeme Methode verschiedene IP Adressen, Ports und Protokolle zu einem einzigen Virtuellen Service zu gruppieren. Das ist nützlich für eine einfachere Konfiguration, wenn eine große Anzahl von virtuellen Diensten benötigt wird und Gruppenpersistenz wichtiger ist, als viele multiple virtuelle Dienste.
<b>Check Intervall</b>	Der Wert gibt die Zeit in Sekunden an, die zwischen den einzelnen Überprüfungen des Real Servers liegen.
<b>Persistence Timeout</b>	Der Wert gibt die Zeit in Sekunden an, die eine aufgebaute Verbindung an den bestehenden Server gebunden ist. Diese Option ist in Verbindung mit Protokollen wie SSL oder FTP sinnvoll, da es wichtig ist, dass die Clients konstant mit dem gleichen Real Server verbunden sind.
<b>Scheduling Method</b>	<p><b>Round Robin</b> Die eingehenden Anfragen werden nacheinander und regelmäßig den einzelnen Servern zugewiesen. Dieses Verfahren eignet sich nur, wenn alle Server identisch ausgerüstet sind. Es kann die unterschiedliche Auslastung der Server jedoch nicht verhindern.</p> <p><b>Weighted Round Robin</b> Bei diesem Verfahren wird der Leistungsfähigkeit der einzelnen Real Server Rechnung getragen. Schwächere Systeme werden bei der Verteilung sporadisch übersprungen und Server mit einem höheren Gewicht werden gelegentlich zweimal angewählt. Die Gewichtung bezieht sich auf den im Real Server eingetragenen Wert 'Weight'.</p> <p><b>Least-Connection</b> Die Vergabe einer neuen Verbindung erfolgt an den Server, der die geringste Zahl an offenen Verbindungen aufweist. Vor dem Hintergrund, dass nicht jede Session dieselbe Last erzeugt, kann es folglich trotzdem zur Überlast einzelner Server kommen.</p> <p><b>Weighted Least-Connection</b> Bei diesem Verfahren werden die offenen Verbindungen über eine Gewichtung normalisiert. Leistungsfähigere Server erhalten folglich mehr Verbindungen zugewiesen, als Server mit einer geringeren Kapazität. Die Gewichtung bezieht sich auf den im Real Server eingetragenen Wert 'Weight'.</p>

Kommando	Beschreibung
	<p><b>Source Hashing</b> Bei diesem Verfahren werden Jobs durch Nachschlagen in einer statischen Hash Tabelle, die der virtuelle Server anhand verschiedener Kriterien anlegt, aufgrund ihrer Quell IP-Adresse den einzelnen Servern zugewiesen. Das 'Source Hashing' kann bei Überschreitung der zulässigen Verbindungen (2*Weight) zum kompletten Ausfall des Systems führen.</p> <p><b>Destination Hashing</b> Bei diesem Verfahren werden Jobs durch Nachschlagen in einer statischen Hash Tabelle, die der virtuelle Server anhand verschiedener Kriterien anlegt, aufgrund ihrer Ziel IP-Adresse den einzelnen Servern zugewiesen. Das 'Destination Hashing' kann bei Überschreitung der zulässigen Verbindungen (2*Weight) zum kompletten Ausfall des Systems führen.</p> <p><b>Locality-Based Least-Connection</b> Weist Verbindungen, die in Richtung der gleichen IP-Adresse gehen, den gleichen Server zu, wenn der Server nicht mit Verbindungen überladen und verfügbar ist. Andernfalls weist der Algorithmus Verbindungen Servern mit weniger Verbindungen zu und nimmt diese Einstellung für zukünftige Zuordnungen.</p>
<b>Forwarding Method</b>	<p><b>NAT</b> Bei diesem Verfahren erfolgt die Ansteuerung der einzelnen Real Server via NAT. Das bedeutet, dass jedes Paket zwischen Client und Server den Load Balancer durchläuft: Auf dem Weg zum Server wird dabei die Ziel-Adresse des Datenpakets durch die IP eines Backend-Systems ausgetauscht. Auf dem Rückweg wird dagegen wieder die offizielle IP des Load Balancers als Absender-Adresse eingetragen. In den Real-Servern sollte eine Default-Route auf die IP des Load Balancers eingetragen werden.</p> <p><b>Direct Routing</b> Bei diesem Verfahren erhält der Load Balancer alle Pakete, die ein Client an einen Real Server schickt. Er ersetzt die Ziel-MAC-Adresse jedes Datenpaketes durch die MAC-Adresse des Real Servers und leitet damit jedes Paket direkt an den zuständigen Server weiter. Der so adressierte Real Server bearbeitet die Anfrage und sendet die Antwort-Pakete direkt zum Client zurück. Die IP-Stacks der Real Server müssen dabei so konfiguriert sein, dass sie <b>nicht!</b> auf ARP-Anfragen zur Service-IP antworten, nur der Load Balancer darf auf die Service-IP antworten.</p> <p><b>Tunneling</b> Bei diesem Verfahren passieren lediglich die Pakete in Richtung des Real Servers den Load Balancer. Die Weiterleitung der Pakete erfolgt bei diesem Verfahren durch IP-IP-Tunnel, die zwischen Load Balancer und Backend-Systemen aufgebaut werden.</p>
<b>Usable Real Servers</b>	Hier können Sie einen bestehenden Real Server auswählen.
<b>HTTP Virtualhost</b>	Der Wert gibt einen virtuellen HTTP Host an.
<b>Sorry Server IP</b>	IP des Servers, der die Verbindungen annehmen soll, wenn alle zur Verfügung stehenden Real-Server nicht verfügbar sind und keine Verbindungen mehr annehmen können.
<b>Sorry Server Port</b>	Port des Servers, der die Verbindungen annehmen soll, wenn alle zur Verfügung stehenden Real-Server nicht verfügbar sind und keine Verbindungen mehr annehmen können.
<b>Activate</b>	Der virtuelle Server ist aktiviert/deaktiviert.

## 5.20 WLAN

Unter **Networking** > **WLAN** kann die WLAN Schnittstelle auf Ihre Anforderungen angepasst werden. Auf der Menü Übersicht können neue/weitere WLAN Profile hinzugefügt, der Country Code gesetzt und der WLAN Dienst gestartet/gestoppt werden.

Voreingestellte WLAN Konfiguration	
SSID	TDT-AP
Channel	1 (2412 MHz)
Verschlüsselung	WPA+WPA2-PSK (AES/CCMP + TKIP)
Pre Shared Key (ASCII)	tdt-Router

### **ACHTUNG!**

➤ **Bitte aus Sicherheitsgründen unbedingt den Pre Shared Key ändern!**

### 5.20.1 General settings

Kommando	Beschreibung
<b>Networkname (SSID)</b>	Name über den das Netzwerk für Clients/Stations erreichbar ist
<b>Broadcast SSID</b>	Definiert ob die SSID für Clients/Stations sichtbar sein soll
<b>Enable IEEE 802.11d</b>	Wird IEEE 802.11d aktiviert, arbeitet der Router mit den, für den auf der WLAN Übersicht unter <b>Country Code</b> spezifizierten Bereich zugelassenen Standards
<b>Operation Mode</b>	Legt die Übertragungsgeschwindigkeit und das Frequenzband der WLAN-Verbindung fest. Verfügbare Modi: IEEE 802.11a (5GHz) IEEE 802.11b (2,4GHz) IEEE 802.11g (2,4GHz) IEEE 802.11g/n (2,4GHz withc N-capability) IEEE 802.11a/n (5GHz with N-capability)
<b>Channel Number</b>	Legt den Kanal für die Datenübertragung fest.
<b>Security System</b>	Legt die Art der WLAN-Verschlüsselung fest.

### 5.20.2 WPA/WPA2-PSK related settings

Kommando	Beschreibung
<b>PSK Format</b>	Legt das Format des geheimen Schlüssels fest
<b>PSK</b>	(Pre-Shared Key) geheimer Schlüssel. Bei dem PSK Format <b>HEX</b> wird eine Schlüssellänge von 64 Zeichen benötigt. Bei <b>ASCII</b> müssen mindestens 8 und maximal 63 Zeichen verwendet werden.

### 5.20.3 N-Standard settings (High Throughput Capabilities)

Kommando	Beschreibung						
<b>Supported channel width set</b>	Definiert den zu verwendenden Kanalabstand, bei HT40 (High-Throughput) können nur die unten angegebenen Kanäle bei <b>Channel Number</b> vergeben werden.						
	<b>20 MHz only</b>   Verwendet einen Kanalabstand von 20 MHz.						
	<b>HT40+</b>   Erhöht den Kanalabstand aufsteigend auf 40 MHz. <table border="1" style="margin-left: 20px;"> <thead> <tr> <th>Frequenz</th> <th>Kanäle</th> </tr> </thead> <tbody> <tr> <td>2.4 GHz</td> <td>1-7 (1-9 in Europa/Japan)</td> </tr> <tr> <td>5 GHz</td> <td>36,44,52,60</td> </tr> </tbody> </table>	Frequenz	Kanäle	2.4 GHz	1-7 (1-9 in Europa/Japan)	5 GHz	36,44,52,60
	Frequenz	Kanäle					
2.4 GHz	1-7 (1-9 in Europa/Japan)						
5 GHz	36,44,52,60						
<b>HT40-</b>   Erweitert den Kanalabstand absteigend auf 40 MHz <table border="1" style="margin-left: 20px;"> <thead> <tr> <th>Frequenz</th> <th>Kanäle</th> </tr> </thead> <tbody> <tr> <td>2.4 GHz</td> <td>5-13</td> </tr> <tr> <td>5 GHz</td> <td>40,48,56,64</td> </tr> </tbody> </table>	Frequenz	Kanäle	2.4 GHz	5-13	5 GHz	40,48,56,64	
Frequenz	Kanäle						
2.4 GHz	5-13						
5 GHz	40,48,56,64						
<b>Short GI for 40 MHz</b>	Verwendet ein kürzeres Guard Intervall und erhöht dadurch die Datenrate. Sollte bei Problemen deaktiviert werden						
<b>DSSS/CCK Mode in 40 MHz</b>	Erlaubt Clients/Stations DSSS bzw. CCK Modus zu verwenden						

### 5.20.4 Advanced settings

Kommando	Beschreibung
<b>Enable WDS (4-address frame) support</b>	Ermöglicht die Wireless Distribution System (WDS) Unterstützung für den Access Point. Dies wird zum Beispiel benötigt, wenn die WLAN Schnittstelle bei Access Point und Station mit anderen Interfaces zu einer Bridge zusammengefasst ist.
<b>Beacon Interval</b>	(Leitstrahl-Intervall) gibt die Zeitspanne vor, in der der Access Point den Clients mittels eines Broadcast die SSID mitteilt (Default: 100)
<b>DTIM period</b>	(Delivery Traffic Indication Message) informiert die Clients über die nächste Datensendung und deren Interfall, Beacon
<b>Maximum number of stations</b>	Definiert die Anzahl der maximal zugelassenen Clients/Stations für das aktuelle WLAN Profil. (1 - 2007; Default: 2007)
<b>RTS/CTS threshold</b>	Schwellenwert ab wann ein (RTS/CTS, Ready to Send/Clear to Send) Handshake-Signal zwischen Router und Client gesendet wird um Hidden-Station-Probleme zu vermeiden (Default: Disabled)
<b>Fragmentation threshold</b>	Definiert ab welcher Größe Datenpakete fragmentiert gesendet werden (Default: Disabled)
<b>Supported rates</b>	Hier werden die von der Hardware unterstützten Datenraten eingetragen
<b>Basic rate set</b>	Hier wird die Grundübertragungsrate festgelegt

### 5.20.5 WEP related settings

Kommando	Beschreibung
<b>Authentication</b>	<b>Open:</b> es findet keine Authentifizierung statt. <b>Shared:</b> Authentifizierung erfolgt mittels geheimen Schlüssel <b>Open/Shared:</b> beide Varianten können auf Clientseite verwendet werden.
<b>Key Index</b>	Laufende Nummer bei mehreren Schlüsseln
<b>Key Format</b>	Bestimmt das Schlüsselformat
<b>Key</b>	Netzwerkschlüssel. Die Schlüssellänge ist je nach Auswahl des Key Format unterschiedlich. <b>HEX</b> benötigt eine Länge von 10, 26 oder 32 Zeichen, bei <b>ASCII</b> werden 5, 13 oder 16 Zeichen

### 5.20.6 WPA/WPA2-EAP related settings

Kommando	Beschreibung
<b>IEEE 802.1X/EAPOL version</b>	hier wird die EAPOL Version (Extensible Authentication Protocol over LAN) festgelegt
<b>EAP Server</b>	legt fest ob ein externer RADIUS (Remote Authentication Dial-In User Service) Server oder der im Router integrierte EAP Server verwendet werden soll

#### 5.20.6.1 Radius client configuration

Kommando	Beschreibung
<b>Own IP address (used as NAS-IP)</b>	IP Adresse zum Identifizieren der NAS Anfrage
<b>NAS-Identifizier</b>	Name zum Identifizieren der NAS Anfrage
<b>Authentication server address</b>	IP Adresse des Authentication Servers
<b>Authentication server port</b>	Port des Authentication Servers (Default: 1812)
<b>Authentication server secrets</b>	tragen Sie hier den festgelegten »Shared Secret« Schlüssel des Authentication Servers ein
<b>Accounting server address</b>	IP Adresse des Accounting Servers
<b>Accounting server port</b>	Port des Accounting Servers (Default: 1813)
<b>Accounting server secrets</b>	tragen Sie hier den festgelegten »Shared Secret« Schlüssel des Accounting Servers ein
<b>Interim accounting update interval</b>	Zeitraum in Sekunden zwischen jeder Aktualisierung, die vom NAS gesendet wird

### 5.20.6.2 Internal EAP server configuration

Kommando	Beschreibung
<b>File path to CA certificate file</b>	geben Sie hier den vollständigen Pfad der CA Zertifikat Datei an
<b>File path to server certificate file</b>	Angabe des vollständigen Pfades der Server Zertifikat Datei
<b>File path to server private key file</b>	hier geben Sie den vollständigen Pfad der »Private Key« Datei an
<b>Password for private key file</b>	Passwort für die »Private Key« Datei

#### 5.20.6.2.1 EAP User Einstellungen

Kommando	Beschreibung
<b>Username / Identity</b>	Username / Identität des Benutzers
<b>Username / Identity match</b>	<b>exact match</b>   der Username muss exakt übereinstimmen
	<b>prefix match</b>   der Username muss mit dem angegebenen String beginnen
	<b>any (*)</b>   jeder Name wird akzeptiert
<b>EAP Method(s)</b>	wählen Sie hier die zu verwendende(n) Authentivizierungsverschlüsselung(en)
<b>Password</b>	Passwort für den Benutzer
<b>Phase</b>	wählen Sie die zu benutzende Phase

### 5.20.7 MAC Address Filtering

Durch eine Überprüfung der MAC Adresse kann der Zugriff per WLAN gewährt oder verweigert werden.

Kommando	Beschreibung
<b>Off</b>	keine Überprüfung der MAC-Adressen
<b>Deny unless MAC address is in the following accept list</b>	nur eingetragenen MAC-Adressen wird der Zugriff gewährt
<b>Accept unless MAC address is in the following deny list</b>	eingetragenen MAC-Adressen wird der Zugriff verweigert

Um MAC Adressen hinzuzufügen wird die Adresse angegeben und mit dem **[Add]** Button hinzugefügt. Optional kann auch eine Beschreibung angegeben werden um die MAC Adressen besser zuordnen zu können.

## 5.21 WWAN

Bei Routern die mit einem LTE Modem ausgestattet (Cxxxxl) sind ist ein Verbindungsaufbau mittels WWAN erforderlich.

Bei Routern die mit einem Mobilfunk-Modem ausgestattet sind (Cxxxxh oder Cxxxxl) wird der Verbindungskonfiguration mittels **Networking > WWAN** durchgeführt.

### Hinweis

- Um eine Verbindung aufzubauen ist es nötig die konfigurierte WWAN Schnittstelle über **Networking > Connection Management** zu starten.
- Für einen aktiven Verbindungsaufbau wird die Verwendung des **Connection Manager** empfohlen, da hier ein Monitoring der Verbindung möglich ist.

Die verfügbaren WWAN Module/Schnittstellen werden auf der Hauptseite angezeigt.

Auf der Interface Seite, erreichbar durch einen Klick auf die Bezeichnung des Interfaces, können die Global Parameters und die Parameter für SIM1 und SIM2 eingesehen und konfiguriert werden.

### 5.21.1 Global

Kommando	Beschreibung
<b>Active SIM after bootup</b>	<p>An dieser Stelle kann der SIM-Slot ausgewählt werden, der beim Systemstart zuerst initialisiert wird. (Default: SIM2) Das kann hilfreich sein, wenn der Router über ein Monitoring System überwacht wird.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Hinweis</b></p> <ul style="list-style-type: none"> <li>➤ Bei der Initialisierung wird keine WWAN Verbindung aufgebaut, dies geschieht erst durch den Connection Manager</li> <li>➤ Dieses Feature funktioniert nicht wenn die eingelegte SIM-Karte durch einen PIN geschützt ist.</li> </ul> </div>

### 5.21.2 SIM1/2 Parameters

Kommando	Beschreibung						
<b>Status</b>	Zeigt den Status der entsprechenden SIM Karte an						
<b>Network Technology</b>	<p>Definiert welche Technologien verwendet werden dürfen. Der Verbindungstyp wird nach Verfügbarkeit ausgewählt</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 10%;"><b>2G</b></td> <td>verwende 2G Verbindungen (GPRS/EDGE)</td> </tr> <tr> <td><b>3G</b></td> <td>verwende 3G Verbindungen (UMTS/WCDMA bis HSPA+)</td> </tr> <tr> <td><b>4G</b></td> <td>verwende 4G Verbindungen (LTE)</td> </tr> </table>	<b>2G</b>	verwende 2G Verbindungen (GPRS/EDGE)	<b>3G</b>	verwende 3G Verbindungen (UMTS/WCDMA bis HSPA+)	<b>4G</b>	verwende 4G Verbindungen (LTE)
<b>2G</b>	verwende 2G Verbindungen (GPRS/EDGE)						
<b>3G</b>	verwende 3G Verbindungen (UMTS/WCDMA bis HSPA+)						
<b>4G</b>	verwende 4G Verbindungen (LTE)						

Kommando	Beschreibung
<b>GSM Network Registration</b>	<p>Legt fest ob eine Registrierung im Sprachkanal durchgeführt werden soll oder nicht</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Hinweis</b></p> <ul style="list-style-type: none"> <li>➤ Hilfreich bei Verwendung von MultiSIM-Karten, da der Router bei »parallel ringing« Anrufe abweist</li> </ul> </div>
<b>PIN</b>	<p>Wenn nicht deaktiviert muss hier die PIN der SIM-Karte eingetragen werden  Nach erfolgreicher Authentifizierung der PIN kann diese hier deaktiviert/disabled oder geändert werden.  Sollte eine Eingabe der PUK erforderlich sein, kann dieser hier eingegeben werden.</p>
<b>Public Land Mobile Network</b>	<p>Mit diesem Parameter kann explizit ein Provider für die Verbindung definiert werden.  Dies kann nützlich, oder nötig sein, wenn mehre Provider zur Verfügung stehen um einen Wechsel zwischen den Providern zu unterbinden.  Die »Public Land Network Code« setzt sich auf dem dreistelligen Mobile Country Code (MCC) und dem zwei-/dreistelligen Mobile Network Code (MNC) zusammen und wird ohne Trenn- oder Leerzeichen angegeben. (siehe <a href="#">15.2 Wichtige Informationen</a>)</p>
<b>APN</b>	Access Point Name des Mobilfunk Providers
<b>Authentication</b>	Wenn eine Autentifizierung am APN erforderlich ist, wird der Authentifizierungstyp hier konfiguriert
<b>Auth. Username</b>	Feld für den vom Provider zugewiesenen Username
<b>Auth. Password</b>	Das Passwort für den Account

## 6 Das Diagnose Menü

### 6.1 Connection Manager

Das Connection Manager Diagnose Modul zeigt Statusinformationen zum Connection Manager Prozess an, sowie Informationen und Fehlermeldungen der Verbindungen. So können hier zum Beispiel die letzten, die Verbindung betreffenden, Fehlermeldungen ausgelesen werden.

### 6.2 Distribution Information

Im Distribution Information Menü werden die installierten Softwaremodule, Versionsnummern und optional das dazugehörige Konfigurationsfile angezeigt. Bitte halten Sie diese bei einem Anruf beim TDT Expert Support bereit.

#### *CLI-Äquivalent:*

Im **status** Menü gibt der Befehl **id** die Firmware und Softwaremodul Version aus.

### 6.3 GSM Modem State

Auf dieser Seite finden Sie Informationen zum aktuellen Status des GSM Modems. Je nach Modem Typ können unterschiedliche Informationen angezeigt werden.

Hier können IMEI und IMSI eingesehen werden. Zudem finden sich Informationen zum Registration Status, Netzbetreiber, Verbindungstyp, Location Area Code (LAC), Zell ID und die Signalstärke.

#### *CLI-Äquivalent:*

Das Kommando **modemstat** im **status** gibt diese Angaben auch wieder.

### 6.4 IPsec VPN

Hier werden die Statusinformationen (Verbindungsname, ISAKMP SA Status und die Zeit bis zur Reauthentifizierung, IPsec SA Status und Zeit bis zum Rekeying, sowie Our und Peer IP) zu den aufgebauten IPsec Tunneln angezeigt.

Zudem können hier einzelne Tunnel getrennt werden.

Durch einen Klick auf den Verbindungsnamen erreicht man zudem weitere Informationen. So werden hier noch die ID's, die getunnelten Subnetze, die ausgehandelten IKE- und ESP-Algorithmen und die verwendete IKE Version ausgegeben. Ausserdem werden die aktiven SPI's (Security Parameters Index) angezeigt.

## 6.5 Load Balancer

### 6.5.1 Load Balancer Statistics

Hier finden Sie die Statistik des Load Balancers, wobei folgende Informationen angezeigt werden.

Kommando	Beschreibung
<b>Virtual Server</b>	Die IP-Adresse des Virtuellen Servers.
<b>Real Server</b>	Die IP-Adresse des Real Server.
<b>Forward</b>	Art der Verbindungsweiterleitung.
<b>Weight</b>	Die Gewichtung der Verbindung.
<b>Active Connections</b>	Anzahl der aktiv bestehenden Verbindungen.
<b>Inactive Connections</b>	Anzahl der inaktiv bestehenden Verbindungen z.B. Aufgrund eines noch nicht ausgelaufenen Persist.
<b>Statistic Details</b>	Unterhalb dieses Links werden die übertragenen Pakete der jeweiligen Verbindung angezeigt.

### 6.5.2 Load Balancer Connections

Die Übersicht über den Status der eingerichteten Load Balancer Verbindungen.

Kommando	Beschreibung
<b>Protocol</b>	Der Wert gibt das Protokoll der bestehenden Verbindung wieder
<b>Expire</b>	zeigt die Zeit in Minuten:Sekunden nach der die Session ausläuft
<b>State</b>	Anzeige des Verbindungsstatus
<b>Source</b>	IP-Adresse und Port des Clients
<b>Virtual</b>	IP-Adresse und Port des Virtuellen Servers
<b>Destination</b>	IP-Adresse und Port des Real Server

## 6.6 Log File Rotation

Mit Hilfe der Log File Rotation wird gewährleistet, dass der Speicher des Routers nicht vollgeschrieben wird. Dazu werden die Log Dateien zyklisch auf Ihre Größe geprüft und entsprechend rotiert, das heißt die Dateien werden umbenannt (z.B. messages nach messages.1). Nach Erreichen einer definierten Anzahl an rotierten Dateien werden die gelöscht.

## 6.7 PPP

Im Bereich PPP werden die aufgebauten Verbindungen mit den zugewiesenen IP-Adressen angezeigt.

## 6.8 Running Processes

In diesem Menü werden alle auf dem Router laufenden Prozesse aufgelistet. Dies kann zu Analyse Zwecken vorteilhaft sein.

Es stehen verschiedene Ansichten zur Verfügung:

Ansicht	Beschreibung
<b>PID</b>	<b>Nach Prozess ID geordnet</b> Zusätzlich werden noch der Owner (Start-User des Dienstes), das Start-Datum oder die Start-Zeit und das zugehörige Kommando angezeigt
<b>User</b>	<b>Prozesse nach User aufgelistet</b> sortiert nach CPU-Auslastung Hier werden noch die Prozess ID, die CPU-Auslastung, das Start-Datum oder die Start-Zeit und das zugehörige Kommando angezeigt
<b>Memory</b>	<b>Prozesse nach benutztem Speicherplatz sortiert</b> Angezeigt werden die Prozess ID, der Owner (Start-User des Dienstes), die Größe und das zugehörige Kommando
<b>CPU</b>	<b>Sortierung nach CPU-Auslastung</b> Hier werden die Prozess ID, der Owner (Start-User des Dienstes), die CPU-Auslastung und das zugehörige Kommando
<b>Search</b>	Hier können die Prozesse nach verschiedenen Parametern durchsucht werden
<b>Run..</b>	Unter »Command to run« können Kommandozeilenbefehle abgesetzt werden. So lässt sich hier z.B. ein <b>ping</b> ausführen  <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Hinweis</b></p> <ul style="list-style-type: none"> <li>➤ Der Router sendet die Ping Anfragen kontinuierlich, daher empfiehlt es sich den Parameter <b>-c</b> (count) zu verwenden, z.B. <b>-c 4</b> für vier Ping Echo Requests, wie bei Windows Geräten.</li> </ul> </div>

### CLI-Äquivalent:

Im Menü **status** der CLI lässt sich mit **processes** die Linux Kommandozeilenansicht der laufenden Prozesse aufrufen.

## 6.9 System Information

Diese Seite zeigt eine Vielzahl von Informationen zum System, zur verwendeten Hardware, über das Netzwerk, den Speicherverbrauch und zum Dateisystem an.

## 6.10 System Logs

Im Menü System Logs lassen sich bestehende Log-Dateien in der Weboberfläche ansehen, verwalten und neue Logs hinzufügen.

Um das Verhalten des Routers zu analysieren, oder Systemausgaben anzuzeigen kann hier das Routerlog angezeigt werden. Dazu ist nur ein Klick auf den **View...** Link in der Zeile **File /var/log/messages** nötig.

Auf der folgenden Seite kann man die Anzahl der ausgegebenen Zeilen anpassen und/oder einen Filter setzen.

**CLI-Äquivalent:**

Im **status** Menü kann das Logfile mit dem Befehl **view\_log** angesehen und mit **trace\_log** live wiedergegeben werden.

### 6.10.1 Logausgabe über eine SSH Verbindung

Nach erfolgter SSH-Anmeldung kann in neueren Firmware Versionen folgender Befehl abgesetzt werden:

**Beispiel**  
**log**

Es erscheint eine »live«-Ausgabe des Systemlogs, alle aktuellen Ereignisse werden direkt auf dem Bildschirm ausgegeben. Bei dem Befehl handelt es sich um einen Alias für **tail -F /var/log/messages**.

Optional kann durch Anfügen des **-n** Parameters noch die maximale Anzahl an ausgegebenen Zeilen definiert werden (z.B. 100 Zeilen):

**Beispiel**  
**log -n100**

Zusätzlich lässt sich das Live Log mittels **grep** oder **egrep** filtern, wobei grep nur einen Sentence suchen kann. Hierfür wird der grep Befehl mittels Pipe Operator (|) hinten angehängt.

**Beispiel**  
**log | egrep ': Connected \*\$|: Disconnected|: Starting Interface|Maximum Failed Ping-Requests reached!'**

Dieses Beispiel zeigt interessante Connection Manager Einträge an. Zudem lässt sich der Suchfilter auch auf Dateien anwenden:

**Beispiel**  
**egrep ': Connected \*\$|: Disconnected|: Starting Interface|Maximum Failed Ping-Requests reached!' /var/log/messages**

## 6.11 Webmin Actions Log

Unter diesem Menüpunkt lässt sich der Webmin Actions Log nach verschiedenen Parametern durchsuchen.

## 7 Das Permanent Save Menü

### 7.1 Save Config

Das Betriebssystem bei Geräten der C-, M- und G-Serie läuft nur im Arbeitsspeicher. Anpassungen die in den einzelnen Konfigurationsmodulen durchgeführt und dort mit Save oder Apply übernommen wurden, greifen nur zur Laufzeit.

Zum Abzuschließen einer Konfiguration ist es daher nötig die durchgeführten Änderungen dauerhaft zu speichern.

Dazu wechselt man auf die Seite **Permanent Save** und drückt auf **Save Config**.

#### **Achtung!**

- **Um die aktuelle Konfiguration inklusive aller Einstellungen und Anpassungen dauerhaft zu übernehmen ist es nötig *Permanent Save* > *Save Config* auszuführen, da die Änderungen sonst bei einem Neustart verloren gehen.**

#### **CLI-Äquivalent:**

Im Hauptmenü der CLI wird der Permanent Save mit **write** ausgeführt.

### 7.2 Save System to USB (nur bei M- und G-Serie)

Bei Geräten der M- und G-Serie ist es möglich das komplette System auf einen USB Stick zu sichern. Dazu wird ein TDT USB Init-Stick benötigt.

- ◊ Verbinden Sie den von TDT gelieferten USB Init-Stick mit einer **USB** Schnittstelle.
- ◊ Der Backup-Vorgang wird mit **Permanent Save** > **Save System to USB** gestartet, optional ist das mit dem Befehl **save\_system\_to\_usb** aus der Kommandozeile möglich.
- ◊ Der Vorgang kann mehrere Minuten dauern.
- ◊ **Achtung:** Entfernen Sie den USB Init-Stick nicht bevor die Meldung **System backup finished** erscheint.

Um ein So gesichertes System wiederherzustellen, wird wie in Kapitel [9.2](#) (Wiederherstellung des Auslieferungszustandes > [M3000 / G5000](#)) beschrieben verfahren.

#### **Achtung!**

- Es wird nur das **aktuell laufende System** auf den USB Stick gesichert.
- Bei der Wiederherstellung mit dem USB Stick wird das Backup auf **beide Systeme** geschrieben.

## 8 Konfiguration sichern und wiederherstellen

### Hinweis

- Es wird empfohlen die Konfiguration nach Abschluss aller Einstellungen lokal zu sichern.
- Die hier aufgeführten Sicherungsmöglichkeiten unterscheiden sich in Umfang und Routine.
- Eine Sicherung kann nur auf dem Weg zurückgespielt werden auf dem sie erstellt wurde.

### 8.1 Konfiguration sichern

#### 8.1.1 Webinterface

Zum Sichern der Konfiguration loggen Sie sich über den Browser auf das Webinterface des Routers ein und navigieren Sie zu **System > Configuration Handling**.

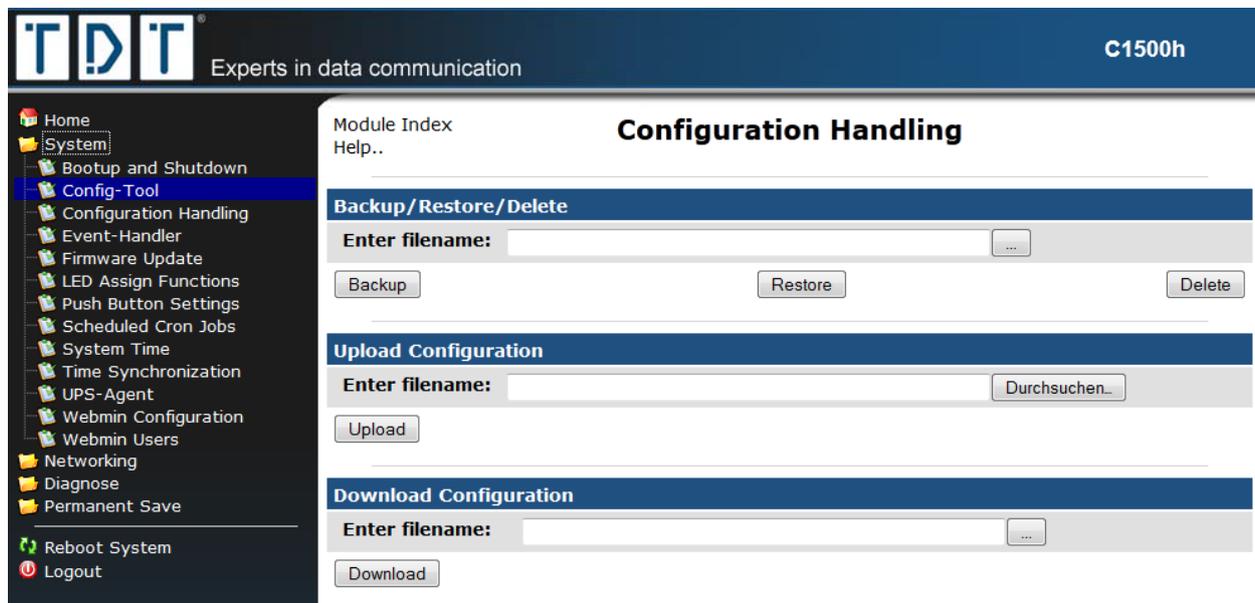


Abbildung 24: Konfiguration sichern und wiederherstellen

Hier vergeben Sie im oberen Feld (**Backup/Restore/Delete**) bei **Enter filename:** einen beliebigen Namen für die Konfiguration und speichern diese mit dem Button **Backup**.

Im zweiten Schritt wählen Sie im Bereich **Download Configuration** die gesicherte Konfiguration aus. Drücken Sie dazu den **...** Button um den Auswahldialog zu öffnen.

Über den **Download** Button kann jetzt die gewählte Konfiguration auf der lokalen Festplatte gespeichert werden. Nun können Sie diese Konfiguration als Email-Anhang verschicken (z.B. zur Fehleranalyse an den TDT Expert Support) oder um sie als Backup zu archivieren.

## 8.1.2 CLI

### Hinweis

- Zum lokalen Sichern der Konfiguration mittels CLI, wird ein SCP Programm, z.B. die Freeware »WinSCP« benötigt. Diese können Sie unter <http://winscp.net> kostenlos downloaden.

Loggen Sie sich zum Sichern der Konfiguration in der CLI ein. In der Hauptebene tippen Sie den Befehl **save <filename>** ein und bestätigen mit **[Enter]**. Die Konfigurations-Datei wird auf dem Router unter **/tmp/<filename>** gespeichert.

### Beispiel:

```
TDT(CLI): save test0
save_config to test0
OK
```

In unserem Beispiel wird die Datei unter **/tmp/test0** abgelegt.

Starten Sie nun »WinSCP« und loggen sich auf die IP des Routers ein. (User und Passwort wie für SSH).

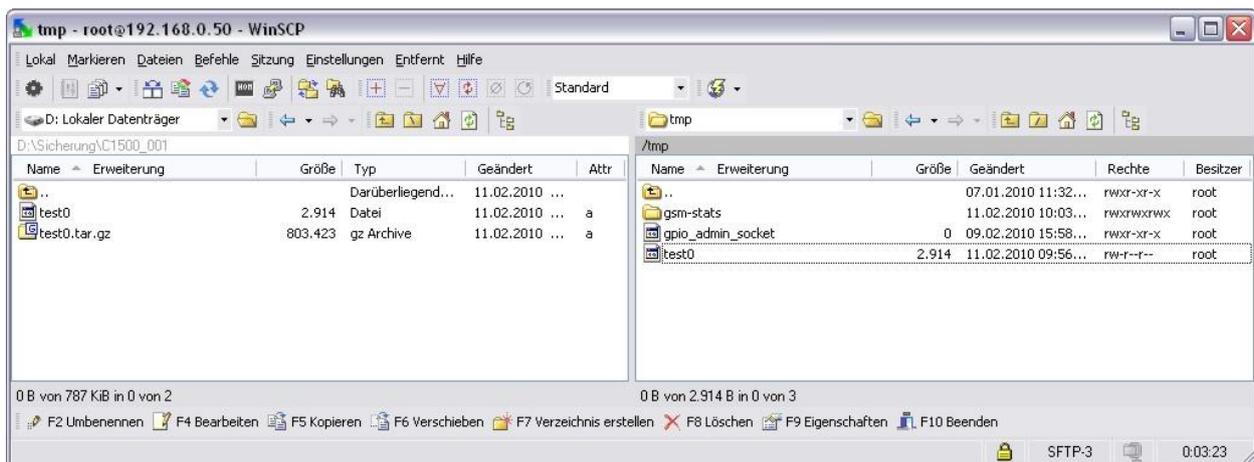


Abbildung 25: Sie sehen nun links im Fenster Ihre lokale Festplatte und rechts die Ordnerstruktur des Routers

Navigieren Sie auf dem Router in das Verzeichnis **/tmp** und kopieren Sie aus diesem Verzeichnis wahlweise per Kontextmenü oder Drag & Drop die entsprechende Datei auf Ihre lokale Festplatte. Nun können Sie diese Konfiguration als Email-Anhang verschicken oder archivieren.

### Hinweis

- Bei der Sicherung in der CLI werden nur die Parameter aus der Übersicht **TDT(CLI/status/show): running-config** gespeichert.

## 8.2 Konfiguration wiederherstellen

### 8.2.1 Webinterface

Zum Wiederherstellen einer bereits gesicherten Konfiguration Webinterface des Routers ein und navigieren Sie zu **System > Configuration Handling**.

Drücken Sie im Bereich **Upload Configuration** den **Durchsuchen...** Button um lokal die Datei auszuwählen die auf dem Router eingespielt werden soll.

Wählen Sie nun im oberen Feld bei **Backup/Restore/Delete** den **...** Button um die hochgeladene Konfiguration zu auszuwählen, oder geben Sie bei **Enter filename:** den Namen der bestehenden Konfiguration an und spielen diese mit dem **Restore** Button wieder ein.

**Achtung!**

- Alle existierenden Einstellungen gehen hierbei verloren.
- Um die Wiederherstellung abzuschließen muss der Router neu gestartet werden.

## 8.2.2 CLI

Zum Wiederherstellen einer bereits gesicherten Konfiguration loggen Sie sich bitte mit »WinSCP« auf den Router ein. Navigieren Sie auf Ihrer lokalen Festplatte der Konfigurations-Datei die wieder hergestellt werden soll, wechseln auf dem Router in das Verzeichnis **/tmp** und kopieren die gesicherte Konfiguration auf den Router.

Loggen Sie sich in der CLI ein, tippen in der Ebene Hauptmenü den Befehl **load <filename>** ein und bestätigen mit **[Enter]**. Die Konfigurations-Datei wird auf den Router zurückgespielt.

**Achtung!**

- Alle existierenden Einstellungen gehen hierbei verloren.
- Um die Wiederherstellung abzuschließen muss die Konfiguration mittels **write** übernommen, und der Router mit **reboot** neu gestartet werden.

**Beispiel:**

**TDT(CLI): load test0**

Load configuration... Done

In order to activate the changes, you need to permanently save the configuration

by executing "write" and performing a reboot!

OK

**TDT(CLI): write**

Saving /etc-RAMDISK to Flash... Done

OK

**TDT(CLI): reboot**

Broadcast message from root (pts/0) (Mon May 11 11:11:11 2009):

The system is going down for reboot NOW!

OK

## 9 Wiederherstellung des Auslieferungszustandes

Sollte sich der Router in einem Zustand befinden in dem keine Verbindung mehr möglich ist, kann ein Rücksetzen in den Auslieferungszustand nötig werden.

Zum Wiederherstellen wird nach den gerätespezifischen Anleitungen vorgegangen.

### Hinweis

- Mit dem »Configuration Handling« erstellte Konfigurationen bleiben dabei auf dem Router gespeichert.

### 9.1 C-Serie

- ◊ Drücken Sie den Reset-Button mit einem dünnen Gegenstand (z.B. Büroklammer) für mindestens 15 Sekunden.
- ◊ Während dieser 15 Sekunden beginnen nacheinander alle 3 LEDs zu leuchten.
- ◊ Jetzt erfolgt das wiederherstellen der Factory Settings, und ein automatischer Neustart.

Der Reset-Button bei der C-Serie kann aber auch verschiedene andere Funktionen ausführen.

Beim Drücken des Reset-Buttons leuchten die LEDs Power, L1 und L2 nacheinander auf. Je nach Kombination der LEDs führt das Loslassen den Buttons verschiedene Funktionen aus:

aktive LED	Zeit	Funktion
Power	0 - 3 Sekunden	Reboot des C1500
Power, L1	4 - 14 Sekunden	Der C1500 schaltet ab
Power, L1, L2	≥ 15 Sekunden	Wiederherstellung des Auslieferungszustandes (Factory Reset) und Reboot des Routers

### 9.2 M3000 / G5000 / L-Serie

- ◊ Fahren Sie das System möglichst geregelt herunter. Über das Webinterface wird dies unter **System > Bootup and Shutdown** mit dem Button **[Shutdown System]** ausgeführt, oder in der Komandozeile mit dem Befehl halt.
- ◊ Verbinden Sie den von TDT gelieferten USB Init-Stick mit einer **USB** Schnittstelle, und starten das Gerät neu.
- ◊ Das Gateway erkennt den USB Init-Stick beim Bootvorgang und stellt automatisch die originale Firmware oder das gesicherte System (siehe Kapitel [7.2](#)) wieder her.
- ◊ Der Vorgang kann mehrere Minuten dauern.
- ◊ Das Ende der Wiederherstellung wird durch 10 akustische Signale angezeigt und das Gerät schaltet sich ab.
- ◊ Nach dem Wiederherstellen entfernen Sie den USB Init-Stick und starten Ihr Gerät neu.

### Achtung!

- Bei einer Wiederherstellung mit dem USB Stick werden **beide Systeme** überschrieben.

## 10 Firmware Update

Die Router der C-, M-, G- und L-Serie arbeiten standardmäßig mit 2 Betriebssystemen.

Bei einem Update des Betriebssystems wird immer nur das momentan inaktive Betriebssystem aktualisiert.

### Hinweis

- Ab Firmwareversion xx.5.0, haben Sie die Möglichkeit ein differenzielles Update Version an den TDT Expert durchzuführen. Dazu wenden Sie sich bitte, unter Angabe Ihrer aktuellen Firmware Support.
- Zum Upload der neuen Firmware wird ein SCP Programm, z.B. die Freeware »WinSCP« benötigt. Diese können Sie unter <http://winscp.net> kostenlos downloaden.
- Das aktuelle System bleibt bei einem Update unverändert. Somit ist ein Wechsel zurück auf die vorherige Version ohne Probleme möglich.
- Während dem Updateprozess wird der Fortschritt angezeigt und die LEDs am Router blinken.

Laden Sie sich die aktuelle Firmware Version herunter und kopieren Sie diese anschließend mit einem SCP Programm in das **/tmp** Verzeichnis des Routers.

### 10.1 Webinterface

Über die Weboberfläche können Sie das Update einspielen indem Sie auf die Seite **System > Firmware Update** wechseln. Hier wird der aktuelle Firmware Stand so wie das aktive und das zu aktualisierende System angezeigt.



Abbildung 26: Das untere Ende der Distribuion Information: Update Firmware

Auf dieser Seite wählen Sie über den Button **...** die Firmware aus dem **/tmp** Verzeichnis aus und legen fest ob die bestehende Konfiguration übernommen werden soll.

**Hinweis**

- Die Option »Adopt configuration« ist standardmäßig gesetzt, damit die aktuelle Konfiguration des Routers auf das aktualisierte System übertragen wird.
- Um das System mit einer Grudkonfiguration zu erstellen, deaktivieren Sie diese Option.

Für ein differenzielles Update wählen Sie die entsprechende Datei aus und aktivieren die »Differential« Checkbox.

Um den Updateprozess zu starten klicken auf **Update**.

## 10.2 CLI

Das Firmware Update kann auch über die CLI durchgeführt werden. Dazu wechselt man in das Statusmenü (**TDT(CLI/status):**).

Der Kommandozeilen Befehl für die Aktualisierung setzt sich nach folgendem Schema zusammen.

**Schema**

```
Update_System -t <target> -f <file> [-diff]|[-server <server-url>] [-no-config]
```

Parameter	Beschreibung
<b>-t &lt;target&gt;</b>	<b>System1:</b> Update System auf hda1 <b>System2:</b> Update System auf hda2
<b>-f &lt;file&gt;</b>	Gibt den Namen der zu ladenden Firmware an. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Achtung</b></p> <ul style="list-style-type: none"> <li>➤ Die Datei muss mit absolutem Pfad angegeben werden!</li> </ul> </div>
<b>-diff</b>	Wird eine diff Datei verwendet, diesen Parameter setzen (optional)
<b>-server &lt;server-url&gt;</b>	Wenn mit einem diff Server synchronisiert werden soll (optional)
<b>-no-config</b>	Wird diese Option gesetzt, wird die Konfiguration des Routers verworfen (optional)

**Beispiel**

```
Update_System -t System1 -f /tmp/System_4_20121214_081025_Release-15.8.17-h.tar.bz2
```

Hiermit wird ein Update auf **System1** durchgeführt, welches die bestehende Konfiguration übernimmt.

**Hinweis**

- Soll bei dem Update das System mit einer Grundkonfiguration erstellt werden, muss der Parameter **-no-config** verwendet werden.

## 11 Das TDT\_SupportInfo Skript

In aktuellen Firmware Versionen ist standardmäßig das Skript **TDT\_SupportInfo** enthalten. Dieses wird aus der Kommandozeile (SSH) oder im Webinterface unter **Diagnose > Running Processes > Display: Run...** bei **Command to run** mit dem folgenden Befehl aufgerufen:

```
/etc/scripts/TDT_SupportInfo
```

Das Skript sammelt nun analyserlevante Daten und speichert diese gezippt unter:

```
/PermData/<yyyymmdd-hhmm>_SupportInfo.txt.bz2
```

Dadurch, dass das Skript die Daten packt und komprimiert, lassen sich diese auch gut über langsamere Verbindungen übertragen. Dazu wird zum Beispiel WinSCP verwendet.

Die Daten lassen sich aber auch direkt auf dem Gerät ansehen. Hierfür wird der folgende Befehl verwendet:

### **Beispiel**

```
bzcat /PermData/14921012-1012_SupportInfo.txt.bz2
```

### **Hinweis**

- Bitte senden Sie die erzeugte Datei bei Supportanfragen mithilfe des [Kontaktformulares](#) oder via Mail an [support@tdt.de](mailto:support@tdt.de) mit ein.

## 12 CLI Befehlsreferenz

Kommando	Beschreibung
<b>?</b>	durch die Eingabe eines Fragezeichens erhalten Sie eine Befehlsübersicht der aktuellen Ebene
<b>&lt;kommando&gt; ?</b>	gibt den(die) gesetzten Wert(e) aus
<b>quit</b>	mit diesem Befehl kann die CLI aus jeder Menü-Ebene direkt verlassen werden
<b>exit</b>	beendet die jeweils aktuelle Befehlsebene und kehrt zur übergeordneten Ebene zurück; im Hauptmenü wird mit <b>exit</b> die CLI verlassen

### Achtung!

- **Um die in der CLI durchgeführten Änderungen dauerhaft zu übernehmen ist es immer nötig im Hauptmenü einen Permanent Save mit dem Befehl *write* durchzuführen, da die Einstellungen sonst bei einem Router-Neustart verloren gehen.**

### 12.1 Hauptmenü - TDT(CLI)

Kommando	Beschreibung
<b>configuration</b>	öffnet das Konfigurationsmenü
<b>status</b>	öffnet das Statusmenü
<b>write</b>	speichert die aktuelle Konfiguration auf das Flash
<b>save &lt;filename&gt;</b>	speichert die Konfiguration in eine Datei im Verzeichnis <b>/tmp</b>
<b>load &lt;filename&gt;</b>	lädt eine im Verzeichnis <b>/tmp</b> gespeicherte Konfiguration <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Achtung!</b></p> <ul style="list-style-type: none"> <li>➤ Alle existierenden Einstellungen gehen hierbei verloren.</li> </ul> </div>
<b>include &lt;filename&gt;</b>	fügt den Inhalt einer Konfigurationsdatei der aktuellen Konfiguration an. Diese Datei muss im Verzeichnis <b>/tmp</b> liegen. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Achtung!</b></p> <ul style="list-style-type: none"> <li>➤ Existierenden Einstellungen werden bei Angabe abweichender Parameter überschrieben</li> </ul> </div>
<b>reboot</b>	führt einen Neustart des Systems durch
<b>shutdown</b>	fährt das System herunter und schaltet das Gerät aus
<b>halt</b>	fährt das Gerät sofort herunter

### 12.1.1 Konfigurationsmenü - TDT(CLI/configuration)

Kommando	Beschreibung
<b>network</b>	öffnet das Netzwerkmenü
<b>general</b>	öffnet das Menü für allgemeine Einstellungen

#### 12.1.1.1 Netzwerkmenü - TDT(CLI/configuration/network)

Kommando	Beschreibung
<b>interface</b>	öffnet das Interfacemenü
<b>dialup</b>	öffnet das Connection Manager Menü
<b>snmp</b>	öffnet das SNMP-Menü
<b>ntp</b>	öffnet das Zeitservermenü

##### 12.1.1.1.1 Interface-Menü - TDT(CLI/configuration/network/interface)

Kommando	Beschreibung
<b>ethernet &lt;instance&gt;</b>	<p>öffnet eine Ethernet Instanz</p> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p><b>Hinweis</b></p> <p>➤ immer unter Angabe der Instanz aufrufen</p> </div> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p><b>Beispiel</b></p> <p>TDT(CLI/configuration/network/interface): <b>ethernet eth1</b></p> </div>
<b>bridge &lt;instance&gt;</b>	<p>öffnet eine Bridge Instanz</p> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p><b>Hinweis</b></p> <p>➤ immer unter Angabe der Instanz aufrufen</p> </div>
<b>ppp &lt;instance&gt; &lt;type&gt;</b>	<p>öffnet eine PPP Instanz unter Angabe des Types <b>[umts,pppoe]</b></p> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p><b>Hinweis</b></p> <p>➤ immer unter Angabe von Instanz und Type aufrufen</p> </div> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p><b>Beispiel</b></p> <p>TDT(CLI/configuration/network/interface): <b>ppp ppp0 pppoe</b></p> </div>

12.1.1.1.1 Ethernet Instanz - TDT(CLI/configuration/network/interface/ethernet-#)

Kommando	Beschreibung
<b>ip</b>	<p>IP Adresse abfragen (mit dem Parameter [?]) oder angeben</p> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p><b>Abfragen</b> TDT(CLI/configuration/network/interface/ethernet-eth1): <b>ip ?</b> ip: 192.168.0.51</p> </div> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p><b>Angeben</b> TDT(CLI/configuration/network/interface/ethernet-eth1): <b>ip 192.168.0.100</b></p> </div>
<b>mask</b>	<p>Subnetzmaske abfragen (mit dem Parameter [?]) oder angeben</p> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p><b>Beispiel</b> TDT(CLI/configuration/network/interface/ethernet-eth1): <b>mask 255.255.255.0</b></p> </div>
<b>broadcast</b>	<p>Broadcastadresse abfragen (mit dem Parameter [?]) oder angeben</p> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p><b>Beispiel</b> TDT(CLI/configuration/network/interface/ethernet-eth1): <b>broadcast 192.168.0.255</b></p> </div>
<b>gateway</b>	<p>Standardgateway abfragen (mit dem Parameter [?]) oder angeben</p> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p><b>Beispiel</b> TDT(CLI/configuration/network/interface/ethernet-eth1): <b>gateway 192.168.0.1</b></p> </div>
<b>mtu</b>	<p>MTU abfragen (mit dem Parameter [?]) oder angeben</p> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p><b>Beispiel</b> TDT(CLI/configuration/network/interface/ethernet-eth1): <b>mtu 1500</b></p> </div>
<b>onboot</b>	Interface während des Bootvorgangs aktivieren [ <b>yes,no</b> ]
<b>onifplug</b>	Interface aktivieren wenn eine Verbindung besteht [ <b>yes,no</b> ]
<b>service</b>	gibt den Dienstyp an [ <b>ipv4,bridge-slave,dhcp-client</b> ]
<b>view</b>	gibt die gesetzten Einstellungen der aktuellen Instanz wieder
<b>apply</b>	Änderungen übernehmen
<b>delete</b>	aktuelle Instanz löschen

### 12.1.1.1.1.2 Bridge Instanz - TDT(CLI/configuration/network/interface/bridge-#)

Kommando	Beschreibung
<b>ip</b>	IP Adresse abfragen (mit dem Parameter [?]) oder angeben
<b>mask</b>	Subnetzmaske abfragen (mit dem Parameter [?]) oder angeben
<b>broadcast</b>	Broadcastadresse abfragen (mit dem Parameter [?]) oder angeben
<b>gateway</b>	Standardgateway abfragen (mit dem Parameter [?]) oder angeben
<b>mtu</b>	MTU abfragen (mit dem Parameter [?]) oder angeben
<b>onboot</b>	Interface während des Bootvorgangs aktivieren [ <b>yes,no</b> ]
<b>onifplug</b>	Interface erst aktivieren wenn eine Verbindung besteht [ <b>yes,no</b> ]
<b>service</b>	gibt den Dienstyp an [ <b>ipv4,dhcp-client</b> ]
<b>interfaces</b>	Mehrere Interfaces, mit Kommata getrennt zum Bridge Device hinzufügen  <div style="border: 1px solid black; padding: 5px; width: fit-content;"> <p><b>Beispiel</b>  TDT(CLI/configuration/network/interface/bridge-br0): interfaces <b>eth0,wlan0</b>  <b>OK</b></p> </div>
<b>addif</b>	Interface zum Bridge Device hinzufügen
<b>delif</b>	Interface vom Bridge Device löschen
<b>view</b>	gibt die gesetzten Einstellungen der aktuellen Instanz wieder
<b>apply</b>	Änderungen übernehmen
<b>delete</b>	aktuelle Instanz löschen

### 12.1.1.1.1.3 PPP Instanz - TDT(CLI/configuration/network/interface/ppp-#)

Kommando	Beschreibung
<b>device</b>	hier wird das Gerät für die Verbindung festgelegt
<b>type</b>	gibt den Typ der aktiven PPP-Instanz wieder (read only)
<b>conn-type</b>	<b>gprs:</b> nur GPRS wird für Verbindungen verwendet <b>umts:</b> nur UMTS wird für Verbindungen verwendet <b>auto:</b> der Verbindungstyp wird nach Verfügbarkeit ausgewählt
<b>sim</b>	legt fest welche SIM-Karte verwendet werden soll [ <b>1,2,external</b> ]
<b>apn</b>	Access Point Name des Mobilfunk Providers
<b>pin</b>	hier muss die PIN der SIM-Karte eingetragen werden
<b>plmn</b>	hier wird die Provider ID des Mobilfunk Anbieters eingetragen

} nur bei UMTS

Kommando	Beschreibung
<b>rp_pppoe_ac</b>	PPPoE Access Concentrator Name (optional)
<b>rp_pppoe_service</b>	PPPoE Service Name (optional)
	} nur bei PPPoE
<b>defaultroute</b>	nach dem Aushandeln/Aufbau der PPP-Verbindung eine Default Route für das PPP Interface setzen <b>[yes,no]</b>
<b>metric</b>	setzt die Routingmetrik des PPP Interfaces
<b>getip</b>	IP-Adresse wird von der Gegenstelle zugewiesen <b>[yes,no]</b>
<b>local</b>	Locale IP Adresse
<b>remote</b>	Remote IP Adresse
<b>refuse-eap</b>	EAP Authentifizierungsanforderung ablehnen <b>[yes,no]</b>
<b>refuse-mschap</b>	MS-CHAP Authentifizierungsanforderung ablehnen <b>[yes,no]</b>
<b>refuse-mschap-v2</b>	MS-CHAPv2 Authentifizierungsanforderung ablehnen <b>[yes,no]</b>
<b>user</b>	der vom Providers zugewiesene Username
<b>password</b>	das Passwort für den Account
<b>chap-max-challenge</b>	Es wird <b>n</b> -mal versucht eine CHAP Authentifizierung durchzuführen (Default: 10)
<b>chap-restart</b>	Zwischen den <i>CHAP challenge transmission</i> liegen <b>n</b> Sekunden (Default: 3 sec)
<b>mtu</b>	legt die maximale Größe eines gesendeten Datenpakets fest (Default: 1454)
<b>mru</b>	legt die maximale Größe eines zu empfangenden Datenpakets fest (Default: 1454)
<b>ipcp-accept-local</b>	Gegenstelle darf dem Router die lokale IP-Adresse zuweisen <b>[yes,no]</b>
<b>ipcp-accept-remote</b>	Gegenstelle darf dem Router die remote IP-Adresse zuweisen <b>[yes,no]</b>
<b>netmask</b>	legt die Netzmaske für das PPP Interface fest, wenn leer wird sie Remote zugewiesen
<b>usepeerdns</b>	Gegenstelle nach bekannten DNS Servern fragen die dann als DNS Server eingetragen werden <b>[yes,no]</b>
<b>demand</b>	Verbindung nur aufbauen wenn Daten gesendet werden <b>[yes,no]</b>
<b>idle</b>	Verbindung wird nach <b>n</b> Sekunden getrennt wenn keine Daten mehr gesendet oder empfangen werden
<b>persist</b>	im Fehlerfall 10 Mal versuchen die Verbindung erneut aufzubauen <b>[yes,no]</b>
<b>require-auth</b>	<b>[No]</b> erlaubt nur IP Adressen, zu denen noch keine Route besteht <b>[Never]</b> Benutzer müssen sich nicht authentifizieren <b>[Always]</b> eine Authentifikation ist immer erforderlich
<b>refuse-pap</b>	PAP Authentifizierungsanforderung ablehnen <b>[yes,no]</b>
<b>require-pap</b>	benötigt eine Authentifizierung über PAP <b>[yes,no]</b>
<b>refuse-chap</b>	CHAP Authentifizierungsanforderung ablehnen <b>[yes,no]</b>

Kommando	Beschreibung
<b>require-chap</b>	benötigt eine Authentifizierung über CHAP [ <b>yes, no</b> ]
<b>debug</b>	Connection Debugging [ <b>yes, no</b> ]
<b>vj</b>	VJ-Compression [ <b>yes, no</b> ]
<b>vjccomp</b>	VJ-Connection-ID Compression [ <b>yes, no</b> ]
<b>pcomp</b>	Protocol Field Compression [ <b>yes, no</b> ]
<b>accomp</b>	Address/Control Compression [ <b>yes, no</b> ]
<b>bsdcomp</b>	BSD Compression [auto,no,nr,nt] [ <b>yes, no</b> ]
<b>deflate</b>	Deflate Compression [auto,no,nr,nt] [ <b>yes, no</b> ]
<b>ccp</b>	Compression Control Protocol Übertragung [ <b>yes, no</b> ]
<b>magic</b>	Magic Number Übertragung [ <b>yes, no</b> ]
<b>predictor1</b>	Predictor-1 Compression [ <b>yes, no, auto</b> ]
<b>lcp-echo-failure</b>	Ist diese Option gewählt, nimmt pppd an, daß nachdem <b>n</b> LCP-echo-requests gesendet wurden und kein LCP-echo-reply als Antwort zurückgesendet wurde, die Gegenstelle nicht mehr erreichbar ist. Tritt dies auf, trennt pppd die Verbindung. Damit diese Option verwendet werden kann, muss eine Zahl größer 0 gegeben sein. Dies kann dazu verwendet werden, um die Verbindung automatisch zu beenden, wenn die Verbindung physikalisch getrennt worden ist.
<b>lcp-echo-interval</b>	Diese Option bewirkt, dass pppd alle <b>n</b> Sekunden einen LCP-echo-request an die Gegenstelle sendet. In der Regel antwortet die Gegenstelle darauf mit einem LCP-echo-reply. Die Option kann in Verbindung mit der Option LCP-ECHO-FAILURE benutzt werden, um zu erkennen, ob eine Gegenstelle nicht mehr erreichbar ist.
<b>domain</b>	Anzuhängender Domain Name
<b>logfile</b>	zusätzliches Logfile (/var/log/ppp/umts/ppp0.log) [ <b>yes, no</b> ]
<b>show-password</b>	PAP Passwort wird im Log angezeigt [ <b>yes, no</b> ]
<b>forceip</b>	nach dem Aushandeln/Aufbau der PPP Verbindung die eigene IP Adresse auf die angegebene Adresse ändern [ <b>yes, no</b> ]
<b>dyndns</b>	DynDNS-Update wenn das Interface in Betrieb geht [ <b>yes, no</b> ]
<b>dnsserverupdate</b>	DNS-Server-Update wenn das Interface in Betrieb geht [ <b>yes, no</b> ]
<b>passive</b>	LCP Passive Mode [ <b>yes, no</b> ]
<b>silent</b>	LCP Silent Mode [ <b>yes, no</b> ]
<b>holdoff</b>	Wartezeit in Sekunden bis eine beendete Verbindung neu initiiert wird
<b>load_default</b>	lädt die Default Einstellung [ <b>umts, pppe</b> ]
<b>view</b>	gibt die gesetzten Einstellungen der aktuellen Instanz wieder
<b>apply</b>	Änderungen übernehmen
<b>delete</b>	aktuelle Instanz löschen

### 12.1.1.1.2 Connection-Manager - TDT(CLI/configuration/network/dialup)

Kommando	Beschreibung
<b>static</b> < <i>interface</i> >	konfiguriert eine statische Einwahlverbindung <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Hinweis</b></p> <p>➤ immer unter Angabe des Interface aufrufen</p> </div>
<b>dynamic</b>	öffnet die Connection-Manager-Einstellungen

#### 12.1.1.1.2.1 Statische Verbindung - TDT(CLI/configuration/network/dialup/static-#)

Kommando	Beschreibung
<b>interface</b>	Gibt mit dem Parameter [ <i>?</i> ] das definierte Interface aus
<b>view</b>	gibt die gesetzten Einstellungen der aktuellen Instanz wieder
<b>apply</b>	Änderungen übernehmen
<b>delete</b>	aktuelle Instanz löschen

#### 12.1.1.1.2.2 Connection-Manager-Einstellungen - TDT(CLI/configuration/network/dialup/dynamic)

Kommando	Beschreibung
<b>activate</b>	aktiviert den Connection-Manager [ <i>yes, no</i> ]
<b>conn_entry</b> <#>	einen dynamischen Anwahl Eintrag konfigurieren
<b>view</b>	gibt die gesetzten Einstellungen der aktuellen Instanz wieder
<b>apply</b>	Änderungen übernehmen
<b>delete</b>	aktuelle Instanz löschen

##### 12.1.1.1.2.2.1 Anwahl Eintrag konfigurieren -

##### TDT(CLI/configuration/network/dialup/dynamic/conn\_entry-#)

Kommando	Beschreibung
<b>interface</b>	Auswahl der zu benutzenden Verbindung
<b>type</b>	Verbindungstyp
<b>iface_type</b>	Interface Typ
<b>max_neg_timeout</b>	legt die maximale Wartezeit für den Aufbau einer Verbindung in Sekunden fest (Default: 30 sec)
<b>power_up_delay</b>	wartet <i>n</i> Sekunden nach dem Start mit dem Aufbau der Verbindung; mit dieser Option lässt sich eine Startreihenfolge der Einträge festlegen
<b>dial_attempts</b>	legt die Anzahl der Wählversuche fest bevor der Status auf „disconnected“ geändert wird
<b>redial_delay</b>	definiert wie viele Sekunden das Gerät zwischen den einzelnen Wählversuchen wartet

Kommando	Beschreibung
<b>reset_umts_modem</b>	legt die Anzahl der Wählversuche fest bevor das UMTS-Modem zurückgesetzt wird
<b>reboot_failed</b>	nach <b>n</b> fehlgeschlagenen Verbindungsversuchen wird ein Router-Neustart durchgeführt (Zähler wird bei einer erfolgreichen Verbindung zurückgesetzt)
<b>reboot_deact</b>	nach <b>n</b> deaktivierten Verbindungsversuchen wird ein Router-Neustart durchgeführt (dieser Zähler wird jedes mal erhöht wenn eine Verbindung erfolgreich aufgebaut werden konnte, wird aber deaktiviert wenn Interface-Checker oder Ping-Checker einen Fehler melden)
<b>apply_oos</b>	dieser Verbindungseintrag soll außer Betrieb genommen werden (Out-of-Service) [ <b>yes, no</b> ]
<b>oos_time</b>	Zeit in Sekunden bis der Verbindungseintrag reaktiviert wird
<b>inhibit</b>	legt die Verbindungen fest, die die aktuelle unterbinden dürfen (mehrere Verbindungen kommagetrennt)
<b>inhibit_mode</b>	Inhibit Mode [ <b>active, connected, oos</b> ]
<b>debug</b>	legt den Level Debug-Modus für diese Verbindung fest [ <b>1, 2, 3</b> ]
<b>dyndns</b>	DynDNS Update wenn das Interface in Betrieb geht [ <b>yes, no</b> ]
<b>dnsserverupdate</b>	DNS Server Update wenn das Interface in Betrieb geht [ <b>yes, no</b> ]
<b>script_oosed</b>	Script das bei Statusänderung auf <b>Out-Of-Service</b> ausgeführt wird
<b>script_active</b>	Script das bei Statusänderung auf <b>Active</b> ausgeführt wird
<b>script_init</b>	Script das bei Statusänderung auf <b>Initialization</b> ausgeführt wird
<b>script_connected</b>	Script das bei Statusänderung auf <b>Connected</b> ausgeführt wird
<b>script_disconnecting</b>	Script das bei Statusänderung auf <b>Disconnecting</b> ausgeführt wird
<b>script_disconnected</b>	Script das bei Statusänderung auf <b>Disconnected</b> ausgeführt wird
<b>ping_target</b>	gibt die IP oder den Host an, der zum Testen gepingt wird
<b>ping_interface</b>	Interface to use for Ping
<b>ping_gateway</b>	legt den zu benutzenden Gateway fest
<b>ping_interval</b>	gibt das zu verwendende Ping Intervall an (Sekunden)
<b>ping_interval_2</b>	Zeit in Sekunden bis zum nächsten Ping nach einem unbeantworteten Ping
<b>ping_octets</b>	definiert die Größe des ICMP-Paketes (Bytes)
<b>ping_timeout</b>	legt fest wie lange auf eine ICMP-Antwort gewartet wird (Sekunden)
<b>ping_deact</b>	maximale Anzahl der unbeantworteten Ping-Anfragen bevor der zugehörige Eintrag deaktiviert wird
<b>ping_recovery</b>	aktiviert die Ping-Recovery [ <b>yes, no</b> ]

Kommando	Beschreibung
<b>ping_recovery_interval</b>	Zeit in Sekunden bis ein weiterer Ping durchgeführt wird
<b>ping_recovery_timeout</b>	legt fest wie lange auf eine ICMP-Antwort gewartet wird (Sekunden)
<b>ping_recovery_deact</b>	Anzahl der maximal erlaubten Ping Recovery-Anfragen die unbeantwortet bleiben dürfen bevor der zugehörige Eintrag deaktiviert wird
<b>conn_route &lt;#&gt;</b>	Konfigurationsmenü für eine Statische Route
<b>conn_def_route &lt;#&gt;</b>	Konfigurationsmenü für eine Default Route
<b>conn_log_entry &lt;#&gt;</b>	Konfigurationsmenü für einen Logical Connection-entry
<b>view</b>	gibt die gesetzten Einstellungen der aktuellen Instanz wieder
<b>apply</b>	Änderungen übernehmen
<b>delete</b>	aktuelle Instanz löschen

12.1.1.1.2.2.1.1 *Static Routing -TDT(CLI/configuration/network/dialup/dynamic/conn\_entry/conn\_route-#-#)*

Kommando	Beschreibung
<b>dst</b>	die zu verwendende Zieladresse (muss angegeben werden)
<b>via</b>	Gateway für die Statische Route
<b>dev</b>	das zu verwendende Interface (muss angegeben werden)
<b>metric</b>	legt die Routingmetrik fest
<b>view</b>	gibt die gesetzten Einstellungen der aktuellen Instanz wieder
<b>delete</b>	aktuelle Instanz löschen

12.1.1.1.2.2.1.2 *Default Routing -TDT(CLI/configuration/network/dialup/dynamic/conn\_entry/conn\_def\_route-#-#)*

Kommando	Beschreibung
<b>via</b>	Gateway für die Default Route
<b>dev</b>	das zu verwendende Interface (muss angegeben werden)
<b>metric</b>	legt die Routingmetrik fest
<b>view</b>	gibt die gesetzten Einstellungen der aktuellen Instanz wieder
<b>delete</b>	aktuelle Instanz löschen

12.1.1.1.2.2.1.3 *Logical Subordinated Connections - TDT(CLI/configuration/network/dialup/dynamic/conn\_entry/conn\_log\_entry-#-#)*

Kommando	Beschreibung
<b>type</b>	Verbindungstyp

Kommando	Beschreibung
<b>name</b>	Verbindungsname
<b>max_neg_timeout</b>	legt die maximale Wartezeit für den Aufbau einer Verbindung in Sekunden fest (Default: 30 sec)
<b>power_up_delay</b>	wartet <b>n</b> Sekunden nach dem Start mit dem Aufbau der Verbindung; mit dieser Option lässt sich eine Startreihenfolge der Einträge festlegen
<b>ping_target</b>	gibt die IP oder den Host an, der zum Testen gepingt wird
<b>ping_interface</b>	Interface to use for Ping
<b>ping_gateway</b>	legt den zu benutzenden Gateway fest
<b>ping_interval</b>	gibt das zu verwendende Ping Intervall an (Sekunden)
<b>ping_interval_2</b>	Zeit in Sekunden bis zum nächsten Ping nach einem unbeantworteten Ping
<b>ping_octets</b>	definiert die Größe des ICMP-Paketes (Bytes)
<b>ping_timeout</b>	legt fest wie lange auf eine ICMP-Antwort gewartet wird (Sekunden)
<b>ping_deact</b>	maximale Anzahl der unbeantworteten Ping-Anfragen bevor der zugehörige Eintrag deaktiviert wird
<b>ping_recovery</b>	aktiviert die Ping-Recovery [ <b>yes, no</b> ]
<b>ping_recovery_interval</b>	Zeit in Sekunden bis ein weiterer Ping durchgeführt wird
<b>ping_recovery_timeout</b>	legt fest wie lange auf eine ICMP-Antwort gewartet wird (Sekunden)
<b>ping_recovery_deact</b>	Anzahl der maximal erlaubten Ping Recovery-Anfragen die unbeantwortet bleiben dürfen bevor der zugehörige Eintrag deaktiviert wird
<b>dial_attempts</b>	legt die Anzahl der Wählversuche fest bevor der Status auf „disconnected“ geändert wird
<b>redial_delay</b>	definiert wie viele Sekunden das Gerät zwischen den einzelnen Wählversuchen wartet
<b>reboot_failed</b>	nach <b>n</b> fehlgeschlagenen Verbindungsversuchen wird ein Router-Neustart durchgeführt (Zähler wird bei einer erfolgreichen Verbindung zurückgesetzt)
<b>reboot_deact</b>	nach <b>n</b> deaktivierten Verbindungsversuchen wird ein Router-Neustart durchgeführt (dieser Zähler wird jedes mal erhöht wenn eine Verbindung erfolgreich aufgebaut werden konnte, wird aber deaktiviert wenn Interface-Checker oder Ping-Checker einen Fehler melden)
<b>apply_oos</b>	dieser Verbindungseintrag soll außer Betrieb genommen werden (Out-of-Service) [ <b>yes, no</b> ]
<b>oos_time</b>	Zeit in Sekunden bis der Verbindungseintrag reaktiviert wird
<b>deact_father</b>	legt fest ob die übergeordnete Verbindung deaktiviert werden soll [ <b>yes, no</b> ]
<b>inhibit</b>	legt die Verbindungen fest, die die aktuelle unterbinden dürfen (mehrere Verbindungen kommagetrennt)
<b>inhibit_mode</b>	Inhibit Mode [ <b>active, connected, oos</b> ]

Kommando	Beschreibung
<b>debug</b>	legt den Level Debug-Modus für diese Verbindung fest <b>[1,2,3]</b>
<b>change_log_pup_delay</b>	ändert das Power Up Delay für die ausgewählte Verbindung auf <b>n</b> Sekunden wenn die Verbindung getrennt wurde
<b>view</b>	gibt die gesetzten Einstellungen der aktuellen Instanz wieder
<b>delete</b>	aktuelle Instanz löschen

### 12.1.1.1.3 SNMP Einstellungen - TDT(CLI/configuration/network/snmp)

Kommando	Beschreibung
<b>syscontact</b>	eintragen des Systemkontakts  <div style="border: 1px solid black; padding: 5px;"> <p><b>Beispiel</b> TDT(CLI/configuration/network/snmp): <b>syscontact admin@tdt.de</b></p> </div>
<b>syslocation</b>	eintragen der System-Örtlichkeit  <div style="border: 1px solid black; padding: 5px;"> <p><b>Beispiel</b> TDT(CLI/configuration/network/snmp): <b>syslocation plant4-buildingNo7-floor3-room314</b></p> </div>
<b>snmpacces &lt;instance&gt;</b>	einrichten der Zugriffskontrolle  <div style="border: 1px solid black; padding: 5px;"> <p><b>Beispiel</b> TDT(CLI/configuration/network/snmp): <b>snmpaccess test0</b></p> </div>
<b>snmptrap &lt;instance&gt;</b>	einrichten der SNMP Traps  <div style="border: 1px solid black; padding: 5px;"> <p><b>Beispiel</b> TDT(CLI/configuration/network/snmp): <b>snmptrap test0</b></p> </div>
<b>snmpmon</b>	öffnet das SNMP-Monitoring Menü
<b>view</b>	gibt die gesetzten Einstellungen der aktuellen Instanz wieder
<b>apply</b>	Änderungen übernehmen
<b>start</b>	SNMP-Dienst starten
<b>stop</b>	SNMP-Dienst stoppen
<b>restart</b>	SNMP-Dienst neustarten

#### 12.1.1.1.3.1 SNMP Zugriffskontrolle - TDT(CLI/configuration/network/snmp/snmpacces-#)

Kommando	Beschreibung
<b>oid</b>	Restricted OID
<b>source</b>	Source Information <b>[Default,Hostname,Subnet]</b>

Kommando	Beschreibung
<b>hostname</b>	Source Hostname
<b>mode</b>	<b>[ro]</b> nur Lesezugriff <b>[rw]</b> Lese- und Schreibzugriffe werden erlaubt
<b>ip</b>	Source IP
<b>mask</b>	Source Maske (Bits)
<b>restrictoid</b>	Restrict OID-Access <b>[yes, no]</b>
<b>process</b>	Community aktivieren <b>[yes, no]</b>
<b>view</b>	gibt die gesetzten Einstellungen der aktuellen Instanz wieder
<b>apply</b>	Änderungen übernehmen
<b>delete</b>	aktuelle Instanz löschen

#### 12.1.1.1.3.2 SNMP Traps - TDT(CLI/configuration/network/snmp/snmptrap-#)

Kommando	Beschreibung
<b>hostname</b>	Host (wenn bei destination gewählt)
<b>process</b>	Trap-Destination aktivieren <b>[yes, no]</b>
<b>ip</b>	IP-Adresse (wenn bei destination gewählt)
<b>destination</b>	anfallende Traps werden an eine IP oder einen Host gesendet <b>[IP, Hostname]</b>
<b>type</b>	Destination-Type <b>[v1, v2trap, v2inform]</b>
<b>community</b>	Community-Name
<b>view</b>	gibt die gesetzten Einstellungen der aktuellen Instanz wieder
<b>apply</b>	Änderungen übernehmen
<b>delete</b>	aktuelle Instanz löschen

#### 12.1.1.1.3.3 SNMP Überwachung - TDT(CLI/configuration/network/snmp/snmpmon)

Kommando	Beschreibung
<b>authtrap</b>	Sendet Trap bei Authentifikationsfehler <b>[yes, no]</b>
<b>sysmon</b>	Systemmonitor aktivieren <b>[yes, no]</b>
<b>snmpproc &lt;instance&gt;</b>	Prozesse zur Überwachung angeben; es können die Anzahl der minimal und maximal laufenden Instanzen angegeben werden
<b>Snmpfile &lt;name&gt;</b>	legt Dateien zur Überwachung an
<b>disk_1</b>	Festplatte 1 Mount-Pfad
<b>disk_1_min</b>	Festplatte 1 minimaler Speicher in Bytes oder Prozent
<b>disk_1_value</b>	Festplatte 1 Wert/Name
<b>disk_2*</b>	analog zu Festplatte 1
<b>disk_3*</b>	analog zu Festplatte 1

Kommando	Beschreibung
<b>load_1_max</b>	Maximale Last im Schnitt der letzten Minute; bei Überschreiten der Last wird ein Trap gesendet
<b>load_5_max</b>	Maximale Last im Schnitt der letzten 5 Minuten; bei Überschreiten der Last wird ein Trap gesendet
<b>load_15_max</b>	Maximale Last im Schnitt der letzten 15 Minuten; bei Überschreiten der Last wird ein Trap gesendet
<b>view</b>	gibt die gesetzten Einstellungen der aktuellen Instanz wieder
<b>apply</b>	Änderungen übernehmen

#### 12.1.1.1.3.3.1 SNMP Prozessüberwachung - TDT(CLI/configuration/network/snmp/snmpmon/snmpproc-#)

Kommando	Beschreibung
<b>process</b>	aktiviert die Überwachung
<b>min</b>	Minimal laufende Instanzen
<b>max</b>	Maximal laufende Instanzen
<b>view</b>	gibt die gesetzten Einstellungen der aktuellen Instanz wieder
<b>apply</b>	Änderungen übernehmen
<b>delete</b>	aktuelle Instanz löschen

#### 12.1.1.1.3.3.2 SNMP-Datei-Einstellungen - TDT(CLI/configuration/network/snmp/snmpmon/snmpfile-#)

Kommando	Beschreibung
<b>process</b>	aktiviert die Überwachung
<b>size</b>	gibt die maximale Größe in Bytes an
<b>view</b>	gibt die gesetzten Einstellungen der aktuellen Instanz wieder
<b>apply</b>	Änderungen übernehmen
<b>delete</b>	aktuelle Instanz löschen

#### 12.1.1.1.4 NTP Einstellungen - TDT(CLI/configuration/network/ntp)

Kommando	Beschreibung
<b>ntpserver &lt;adress&gt;</b>	NTP-Server angeben oder abfragen
<b>broadcast</b>	Broadcast aktivieren/deaktivieren [ <b>yes, no</b> ]
<b>multicast</b>	MulticastEinstellung angeben oder abfragen [ <b>default, custom</b> ]
<b>custom</b>	Multicastadresse angeben oder abfragen
<b>driftfile</b>	Datei, welche die Abweichung (offset) aufzeichnet, angeben oder abfragen (Default: <b>/var/cache/ntp.drift</b> )

Kommando	Beschreibung
<b>keys</b>	Datei mit Authentifikationsschlüsseln angeben oder abfragen
<b>trustedkey</b>	Datei mit Liste der Trusted Keys angeben oder abfragen
<b>requestkey</b>	Authentifikations-Anfrage-Schlüssel angeben oder abfragen (xntpd)
<b>controlkey</b>	Authentifikations-Kontroll-Schlüssel angeben oder abfragen (ntpq)
<b>authdelay</b>	Authentifikations Delay (in sec) angeben oder abfragen
<b>offset_limit</b>	Maximal erlaubte Abweichung in Sekunden (0 erlaubt alle)
<b>view</b>	gibt die gesetzten Einstellungen der aktuellen Instanz wieder
<b>apply</b>	Änderungen übernehmen
<b>start</b>	NTP-Dienst starten
<b>stop</b>	NTP-Dienst stoppen
<b>restart</b>	NTP-Dienst neustarten

#### 12.1.1.1.4.1 NTP Server Einstellungen - TDT(CLI/configuration/network/ntp/ntpserver-#)

Kommando	Beschreibung
<b>version</b>	Protokoll-Version [ <b>Default, 1, 2, 3</b> ]
<b>key</b>	Authentifikationsschlüssel (optional)
<b>prefer</b>	Bevorzugter Server [ <b>yes, no</b> ]
<b>view</b>	gibt die gesetzten Einstellungen der aktuellen Instanz wieder
<b>delete</b>	aktuelle Instanz löschen

#### 12.1.1.2 Allgemeine Einstellungen - TDT(CLI/configuration/general)

Kommando	Beschreibung
<b>prompt</b>	ändert den Prompt der CLI  <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p><b>Beispiel</b>  TDT(CLI/configuration/general): <b>prompt</b>  <b>HalloWelt</b>  OK  HalloWelt(CLI/configuration/general):</p> </div>
<b>hostname</b>	System Hostname
<b>cli_port</b>	TCP-Port für die CLI (Default: <b>2000</b> )
<b>view</b>	gibt die gesetzten Einstellungen der aktuellen Instanz wieder
<b>apply</b>	Änderungen übernehmen

## 12.1.2 Statusmenü - TDT(CLI/status)

Kommando	Beschreibung
<b>modemstat</b>	zeigt den Status des integrierten GPRS-Moduls
<b>ppp_disc &lt;interface&gt;</b>	trennt eine aktive PPP-Verbindung
<b>connection_deact</b>	Deaktiviert einen Connection-Entry des Connection-Managers
<b>pppstat &lt;interface&gt;</b>	zeigt den Status einer PPP-Verbindung
<b>view_log</b>	gibt die Datei <b>/var/log/messages</b> am Bildschirm aus
<b>trace_log</b>	zeigt die aktuellen Einträge der Datei <b>/var/log/messages</b>
<b>trace &lt;options&gt;</b>	Trace auf die Schnittstelle des Routers mit den angegebenen Optionen, <b>trace --help</b> zeigt alle Optionen
<b>ifconfig</b>	gibt den Status der Netzwerkschnittstellen aus
<b>uptime</b>	zeigt die Laufzeit des Routers aus
<b>id</b>	zeigt die aktuelle Firmware-Version und die installierten Pakete an
<b>scan</b>	listet die gesamte Verzeichnisstruktur auf
<b>arp</b>	zeigt/löscht ARP-Einträge, mehr Informationen mit <b>arp --help</b>
<b>ping</b>	Sendet einen Ping Host mit angegebenen Optionen (Abbruch mit [ <b>STRG+C</b> ])
<b>traceroute</b>	Ermittelt den zurückgelegten Weg zu einem Host
<b>Update_System</b>	siehe Firmware-Update <a href="#">CLI</a>
<b>date</b>	gibt Systemzeit und -datum aus
<b>cpu</b>	gibt die Prozessor- und Arbeitsspeicherauslastung aus
<b>filesystem</b>	gibt Informationen über das Dateisystem aus
<b>processes</b>	gibt Informationen über laufende Prozesse, Prozessor und Arbeitsspeicher aus, hier erreichen Sie mit <b>h</b> die Hilfe und verlassen die Anzeige mit <b>q</b>
<b>show</b>	öffnet das Untermenü Show

### 12.1.2.1 Show-Menü - TDT(CLI/status/show)

Kommando	Beschreibung
<b>running-config</b>	gibt die aktuelle Konfiguration am Bildschirm aus

## 13 Hardware

### Konformitätserklärung:

TDT erklärt, dass die wesentlichen Anforderungen der R&TTE Richtlinie bei allen Produkten übereinstimmen.



Aktuelle Dokumente finden Sie unter [download.tdt.de](http://download.tdt.de).

### 13.1 C-Serie

#### 13.1.1 Technische Daten

##### 13.1.1.1 C1500xx

- ◊ 500Mhz Prozessor (lüfterlos)
- ◊ 256 MB RAM Arbeitsspeicher
- ◊ 4 GB Systemspeicher (Compact Flash, Dual Boot)
- ◊ 2 10/100 BaseT Ethernet Ports (Wake on LAN, passive Power over Ethernet)
- ◊ 1 Power LED
- ◊ 2 LEDs zur Anzeige von Statusinformationen (frei konfigurierbar)
- ◊ 2 USB 2.0 Ports (z.B. Backup, USV Verwaltung via USB to Seriell Adapter)
- ◊ 1 RS232 Konsolenport (zur Überwachung und Fehlersuche)
- ◊ Dual SIM (Einsatz von 2 SIM Karten für Backupszenarien)
- ◊ Echtzeit Uhr
- ◊ Robustes Metallgehäuse, optional mit Hutschieneclip
- ◊ Abmessungen: 158x28x157mm (BxHxT, ohne Antennen)
- ◊ Gewicht: ca. 870g
- ◊ Betriebstemperatur: -5°C (optional -25°C) - +60°C
- ◊ Luftfeuchtigkeit: 85% (nicht kondensierend)
- ◊ Eingangsspannung 7-18V DC / Netzteil 12V 2A / Leistungsaufnahme ~6W
- ◊ 3G+/4G Antennenanschluß: SMA female
- ◊ WLAN Antennenanschluß: Reverse SMA male
- ◊ GPS Antennenanschluß: SMA female (optional)
- ◊ CE konform und vibrationsgetestet

##### 13.1.1.2 C1550xxx

- ◊ 500Mhz Prozessor (lüfterlos)
- ◊ 256 MB RAM Arbeitsspeicher
- ◊ 4 GB Systemspeicher (Compact Flash, Dual Boot)
- ◊ 1 10/100 BaseT Ethernet Port (Wake on LAN, passive Power over Ethernet)
- ◊ 1 4Port 10/100 BaseT Ethernet Switch (bei DSL Modellen managed)
- ◊ 1 Power LED
- ◊ 10 LEDs zur Anzeige von Statusinformationen (frei konfigurierbar)
- ◊ 2 USB 2.0 Ports (z.B. Backup, USV Verwaltung via USB to Seriell Adapter)
- ◊ 1 RS232 Konsolenport (zur Überwachung und Fehlersuche)
- ◊ Dual SIM (Einsatz von 2 Mini-SIM Karten für Backupszenarien)
- ◊ Echtzeit Uhr
- ◊ Robustes Metallgehäuse, optional mit Hutschieneclip
- ◊ Abmessungen: 176x42x157mm (BxHxT, ohne Antennen)
- ◊ Gewicht: ca. 1000g

- ⦿ Betriebstemperatur: -5°C (optional -25°C) - +55°C
- ⦿ Luftfeuchtigkeit: 85% (nicht kondensierend)
- ⦿ Eingangsspannung 7-18V DC / Netzteil 12V 2A / Leistungsaufnahme ~9,5W
- ⦿ 3G+/4G Antennenanschluß: SMA female
- ⦿ WLAN Antennenanschluß: Reverse SMA male
- ⦿ GPS Antennenanschluß: SMA female (optional)
- ⦿ DSL Anschluß: RJ45 Buchse
- ⦿ CE konform und vibrationsgetestet

### 13.1.1.3 ELW Router C1550lw

- ⦿ 500Mhz Prozessor (lüfterlos)
- ⦿ 256 MB RAM Arbeitsspeicher
- ⦿ 4 GB Systemspeicher (Compact Flash, Dual Boot)
- ⦿ 1 10/100 BaseT Ethernet Port (Wake on LAN, passive Power over Ethernet)
- ⦿ 1 4Port 10/100 BaseT Ethernet Switch (bei DSL Modellen managed)
- ⦿ 1 Power LED
- ⦿ 10 LEDs zur Anzeige von Statusinformationen (frei konfigurierbar)
- ⦿ 2 USB 2.0 Ports (z.B. Backup, USV Verwaltung via USB to Seriell Adapter)
- ⦿ 1 RS232 Konsolenport (zur Überwachung und Fehlersuche)
- ⦿ Dual SIM (Einsatz von 2 Mini-SIM Karten für Backupszenarien)
- ⦿ Echtzeit Uhr
- ⦿ Robustes Metallgehäuse
- ⦿ Abmessungen: 176x42x157mm (BxHxT, ohne Antennen)
- ⦿ Gewicht: ca. 1000g
- ⦿ Betriebstemperatur: -5°C (optional -25°C) - +55°C
- ⦿ Luftfeuchtigkeit: 85% (nicht kondensierend)
- ⦿ Eingangsspannung 7-18V DC / Netzteil 12V 2A / Leistungsaufnahme ~9,5W
- ⦿ 2 3G+/4G Antennenanschlüsse: SMA Buchse
- ⦿ 2 WLAN Antennenanschlüsse: (reverse) RP-SMA Buchse
- ⦿ GPS Antennenanschluß: SMA Buchse
- ⦿ CE konform und vibrationsgetestet

### 13.1.2 Hardware Module

Der C-Serien Router kann mit folgenden Modulen ausgestattet werden.

	h	l	d	i	w	hd	hi	hw	hdi	hdw	ld	li	lw	ldi	ldw
2G/3G+	✓					✓	✓	✓	✓	✓					
LTE (4G)		✓									✓	✓	✓	✓	✓
DSL			✓			✓			✓	✓	✓			✓	✓
ISDN				✓			✓		✓			✓		✓	
WLAN					✓			✓		✓			✓		✓

### 13.1.3 DB9 / RS232 PIN- Belegung (DTE/V.24)

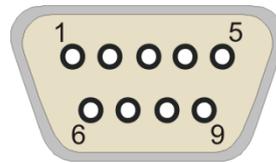


Abbildung 27

PIN	Name	Beschreibung
1	DCD	Carrier Detect
2	RxD	Receive Data
3	TxD	Transmitt Data
4	DTR	Data Term. Ready
5	GND	System Ground
6	DSR	Data Set Ready
7	RTS	Ready to Send
8	CTS	Clear to Send
9	RI	Ring Indicator

## 13.2 M3000

### 13.2.1 Unterstützte UMTS / GPRS Karten

Hersteller	Bezeichnung	Seriennummer
Option	GlobeTrotter 3G	CL?????????
Option	GlobeTrotter Fusion Quad Lite	QL?????????
Option	GlobeTrotter Express 7.2	FE?????????
Option	Globetrotter Fusion + HSDPA	NF?????????
Option	GlobeTrotter GT MAX	GA?????????
Novatel	Merlin XU870	
Novatel	Merlin U630	

### 13.2.2 Belegung des DSL/ISDN Y-Kabels

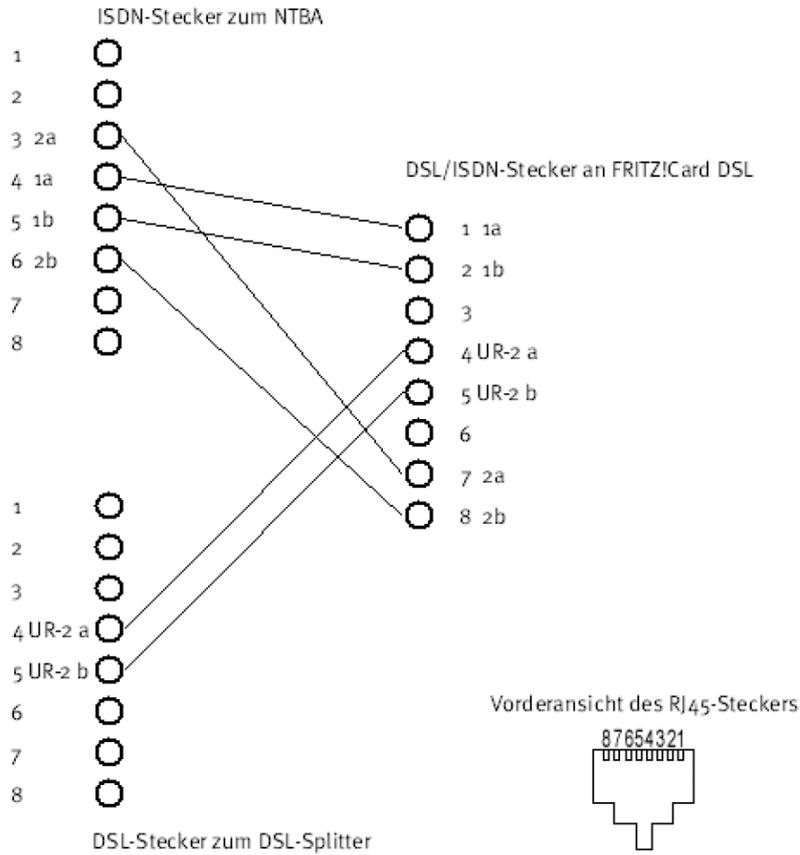


Abbildung 28

### 13.2.3 Ethernet 4 Port Karte

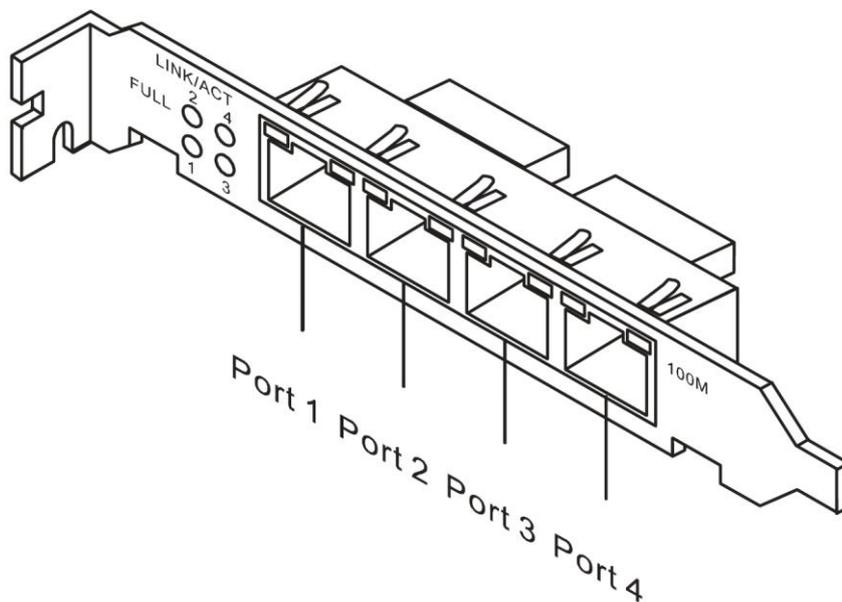


Abbildung 29

### 13.2.3.1 Pin Belegung der RJ45 PRI Stecker

Vorderansicht der RJ45 Steckers

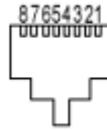


Abbildung 30

PIN 1	PIN 2	PIN 3	PIN 4	PIN 5	PIN 6	PIN 7	PIN 8
rx+	rx-	-	tx+	tx-	-	-	-

## 14 Wichtige Daten im Überblick

### 14.1 C-, M-, G-, und L-Serie Standard

Bei allen C-, M-, G- und L-Geräten sind die hier aufgeführten Daten standardmäßig voreingestellt.

<b>Voreingestelltes LAN Schnittstelle</b>	IP-Adresse eth1	192.168.0.50
	Subnetzmaske für eth1	255.255.255.0
<b>Voreingestellte WAN Schnittstelle</b>	IP-Adresse eth0	10.99.99.99
	Subnetzmaske für eth0	255.255.255.0
<b>Voreingestellte WLAN Konfiguration</b>  für Geräte mit WLAN Modul	IP-Adresse wlan0	172.16.0.50
	Subnetzmaske für wlan0	255.255.255.0
	SSID	TDT-AP
	Pre Shared Key (ASCII)	tdt-Router
	Kanal	1 (2412 MHz)
	Verschlüsselung	WPA+WPA2-PSK (AES/CCMP + TKIP)
<b>Webinterface</b>	Aufruf via SSL	<a href="https://&lt;Schnittstellen IP&gt;">https://&lt;Schnittstellen IP&gt;</a>
	Username	tdt
	Passwort	tdt
<b>SSH / CLI</b>	SSH Port	22
	CLI Port	2000
	Username	root
	Passwort	tdt
<b>Serial Port (RS232)</b>	Speed	38400 bit/s
	Datenbits	8
	Parität	keine
	Stopbits	1
<div style="border: 1px solid black; padding: 5px;"> <p><b>Hinweis</b></p> <p>➤ Zum Anschluss an einen PC ist ein Nullmodemkabel erforderlich.</p> </div>		

#### **ACHTUNG!**

- **Aus Sicherheitsgründen sollten die Passwörter für das Webintreface und den SSH-Zugriff geändert werden!**
- **Bei Modellen mit WLAN bitte unbedingt auch den *Pre Shared Key* ändern!**

<b>Firewall</b>	<p>Eingehende und ausgehende Verbindungen sind auf allen lokalen Netzwerkschnittstellen (eth0, eth1, wlan0) erlaubt.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Hinweis</b></p> <ul style="list-style-type: none"> <li>➤ eingehende PPP und WWAN Verbindungen werden standardmäßig geblockt</li> </ul> </div>
-----------------	---

<b>ppp2</b>	Schnittstelle für ISDN Dial-In Verbindung
<b>ppp3</b>	Schnittstelle für PPPoE/DSL Verbindung
<b>wwan0</b>	Schnittstelle für Funk Verbindung (z.B. C1500l): LTE/HSPA(+)/GPRS/EDGE/UMTS

## 14.1.1 Passwort ändern

### 14.1.1.1 Webinterface

Um das Passwort für Webinterface Benutzer zu ändern wird hier unter **System > Webmin Users > <USER>** der Parameter **Password** im Dropdown auf **Set to ..** und im nachfolgenden Textfeld das neue Passwort eingetragen und mit  gespeichert.

<p><b>Hinweis</b></p> <ul style="list-style-type: none"> <li>➤ Hiermit wird <b>nicht</b> der Kommandozeilenbenutzer root geändert. Dieses Passwort wird über die Kommandozeile geändert.</li> </ul>
---

### 14.1.1.2 Kommandozeilen-Benutzer *root*

Mit einem SSH Client (z.B. PuTTY) in der Kommandozeile einloggen und den Passwort Dialog mittels des Befehles **passwd** aufrufen.

<p><b>Beispiel:</b></p> <pre> root@hostname:~# passwd Changing password for root Enter the new password (minimum of 5 characters) Please use a combination of upper and lower case letters and numbers. New password: Re-enter new password: passwd: password changed. </pre>
---

Um das Passwort dauerhaft zu speichern wird in der Kommandozeile **save\_etc\_to\_flash** eingegeben, oder man wechselt im webinterface auf die Seite **Permanent Save** und drückt auf **Save Config**.

### 14.1.2 Arbeitsumgebung

Die C-, M-, G- und L-Geräte arbeiten innerhalb eines Temperaturbereichs von -5°C bis +60°C bei einer Luftfeuchtigkeit bis 85% (nicht kondensierend). Andere Temperaturbereiche auf Anfrage.

### 14.1.3 Konformitätserklärung

Hiermit erklärt TDT, dass alle Produkte mit Funkanlagen der Richtlinie 2014/53/EU entsprechen.

Der vollständige Text der EU-Konformitätserklärung ist unter der folgenden Internetadresse verfügbar: [download.tdt.de](http://download.tdt.de).



Hiermit erklärt TDT, dass alle Telekommunikationsendeinrichtungsprodukte der Richtlinie 2014/35/EU entsprechen.

Der vollständige Text der EU-Konformitätserklärung ist unter der folgenden Internetadresse verfügbar: [download.tdt.de](http://download.tdt.de).

Für ältere Produkte die das Lebensende erreicht haben:

TDT erklärt, dass die wesentlichen Anforderungen der R&TTE Richtlinie bei allen Produkten übereinstimmen.



Aktuelle Dokumente finden Sie unter [download.tdt.de](http://download.tdt.de).

## 14.2 Systemspezifische Daten

### 14.2.1 C-Router mit Mobilfunkmodul

<b>Mögliche Verbindungen</b>	GPRS, EDGE, UMTS, HSDPA, HSUPA, HSPA+, LTE		
<b>Speed Max Downlink</b>	Abhängig vom verwendeten Modem Type		
<b>Speed Max Uplink</b>	Abhängig vom verwendeten Modem Type		
<b>Simkarten</b>	Die Router sind DualSIM fähig (z.B. für Backup Verbindungen)		
	SIM1	auf der Vorderseite	
	SIM2	C1500/C1550 im Gehäuseinneren C2000 auf der Vorderseite	
<b>GPS (optional)</b>	Anschluss	SMA Buchse	
	Antenne	Cxxxx <b>h</b>	Erfordert eine passive GPS Antenne
		Cxxxx <b>l</b>	Erfordert eine aktive GPS Antenne
	GPS-Signal	1500MHz	

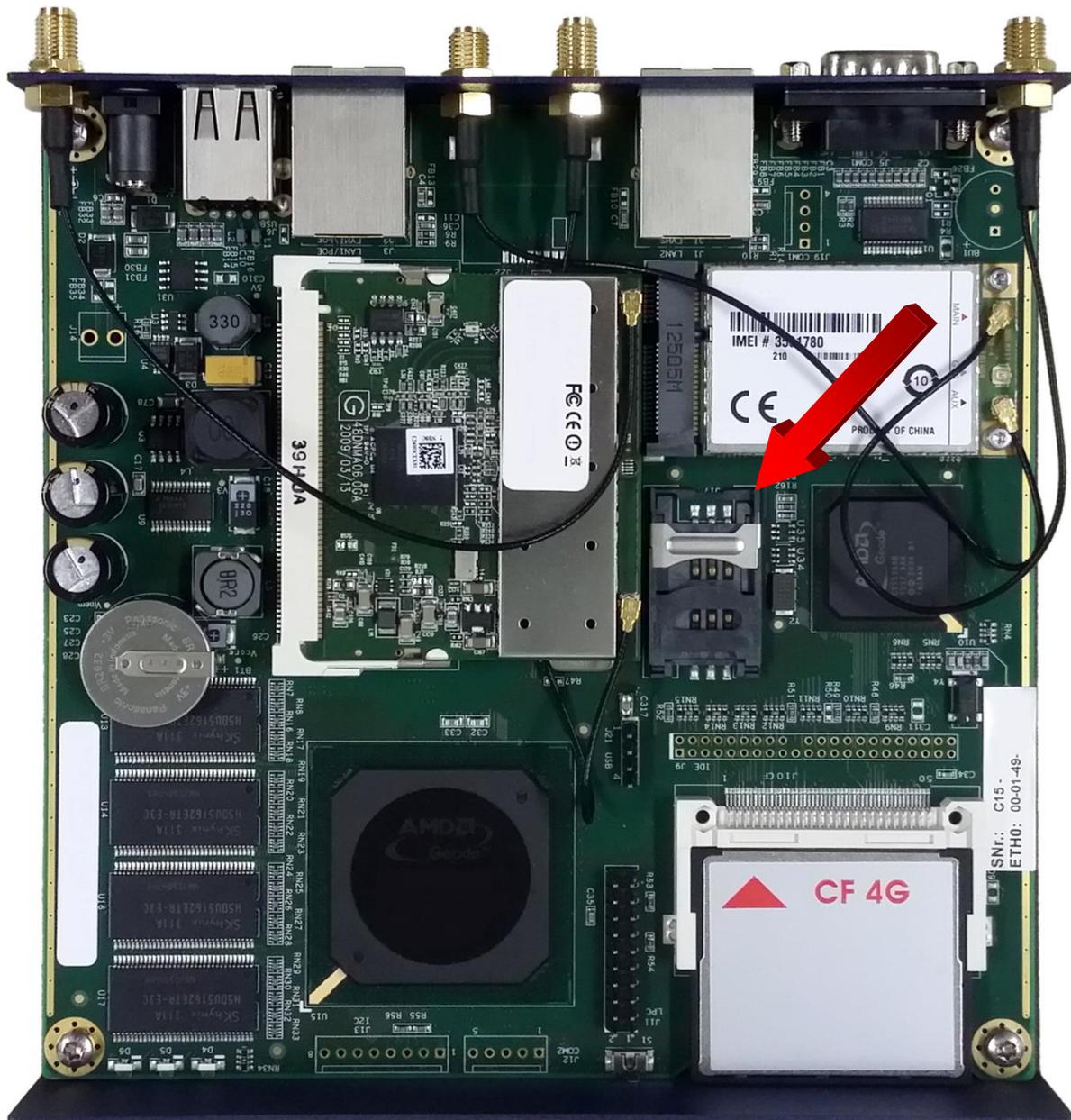


Abbildung 31: SIM 2 (exemplarisch in einem C1500w)

### 14.2.1.1 GPS

Um auf GPS Daten zugreifen zu können ist es nötig, dass ein GPS Anschluss vorhanden ist und eine für den Modemtyp passende GPS Antenne angeschlossen ist.

**Hinweis**

- GPS ist in der regulären Serie optional und wird nur bei ELW Ausprägungen serienmäßig bestückt.

### 14.2.1.1.1 GPS Daten auslesen

Mit dem Befehl **np /dev/gps0** können die aktuellen GPS-Daten in der Kommandozeile eines C-Serie Routers ausgelesen werden. Hierfür muss allerdings der Zeitserver deaktiviert werden, wenn bei **System > Time Synchronization** GPS als Zeitgeber für den NTP-Dienst verwendet wird.

### 14.2.1.1.2 GPS Daten senden

GPS-Daten (NMEA-Stream) können über das Netzwerk an einen Host (IP-Adresse Port Protokoll) gesendet werden. Ebenso können die Daten als UDP Broadcast oder TCP Server zur Verfügung gestellt werden.

Die Konfiguration wird direkt mittels Konfigurationsdatei durchgeführt. Hierfür befindet sich ein Konfigurationsmuster unter **/etc/kplex.conf.example**. Diese wird entsprechend den benötigten Anforderungen angepasst.

Um den Dienst zu starten wird die Konfigurationsdatei in **/etc/kplex.conf** umbenannt. Beim Systemstart wird der Dienst automatisch gestartet, ebenso nach einem Reset des Mobilfunkmodems. Zudem lässt sich der Dienst im laufenden Betrieb auf der Kommandozeile mittels des **kplex** starten.

Weiterführende Informationen können der Seite [www.stripdog.com/kplex](http://www.stripdog.com/kplex) entnommen werden.

## 14.2.2 C-Router mit WLAN

<b>Voreingestellte WLAN Konfiguration</b>	IP-Adresse wlan0	172.16.0.50
	Subnetzmaske für wlan0	255.255.255.0
	SSID	TDT-AP
	Pre Shared Key (ASCII)	tdt-Router
	Kanal	1 (2412 MHz)
	Verschlüsselung	WPA+WPA2-PSK (AES/CCMP + TKIP)
<div style="border: 1px solid black; padding: 5px; background-color: #f0f0f0;"> <p><b>Achtung!</b></p> <p>➤ <b>Bitte aus Sicherheitsgründen unbedingt den Pre Shared Key ändern!</b></p> </div>		

## 14.3 Software

Der vorliegende Router enthält Software, die unter verschiedenen Lizenzen verbreitet werden, insbesondere unter proprietärer Lizenz oder unter einer Open Source Lizenz (z.B. GNU General Public License, GNU Lesser General Public License oder FreeBSD License). TDT überlässt auf Verlangen den Quellcode relevanter Open Source Software, soweit die Nutzungsbedingungen solcher Open Source Software eine Herausgabe des Quellcodes vorsehen.

Einzelheiten zu verschiedenen Lizenzen, sowie der Source Code der als Open Source verbreiteten Dateien kann schriftlich, über [info@tdt.de](mailto:info@tdt.de) angefordert werden.

This product includes software developed by the Apache Group for use in the Apache HTTP server project (<http://www.apache.org>).

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org>).

## 15 Link Übersicht

### 15.1 Allgemeine Links

Beschreibung	Link
TDT - Experts in data communication	<a href="http://www.tdt.de">http://www.tdt.de</a>
TDT.de - Handbücher und HowTo's	<a href="http://download.tdt.de/">http://download.tdt.de/</a>
TDT mobileWatcher Demo	<a href="http://services.tdt.de">http://services.tdt.de</a>
TDT Helferlein	<a href="http://ip.tdt.de">http://ip.tdt.de</a> (z.B. IP, Ping Checker Calculator)

### 15.2 Wichtige Informationen

Beschreibung	Link
Public Land Mobile Network Numeric Provider ID	<a href="http://en.wikipedia.org/wiki/Mobile_Network_Code">http://en.wikipedia.org/wiki/Mobile_Network_Code</a>

### 15.3 Empfohlene Software

Beschreibung	Link
WinSCP – SCP Programm	<a href="http://winscp.net">http://winscp.net</a>
PuTTY – SSH Client	<a href="http://www.chiark.greenend.org.uk/~sgtatham/putty">http://www.chiark.greenend.org.uk/~sgtatham/putty</a>
OpenVPN – Client	<a href="http://openvpn.net/index.php/download/community-downloads.html">http://openvpn.net/index.php/download/community-downloads.html</a>
The GreenBow™ – IPsec Client	<a href="http://www.tdt.de/products/software/greenbow">http://www.tdt.de/products/software/greenbow</a>

### 15.4 Weiterführende Links

Description	Link
BIND DNS-Server	<a href="https://www.isc.org/software/bind">https://www.isc.org/software/bind</a>
DNSmasq	<a href="http://thekelleys.org.uk/dnsmasq/doc.html">http://thekelleys.org.uk/dnsmasq/doc.html</a>
DynDNS.com – Custom DNS Service	<a href="http://www.dyndns.com">http://www.dyndns.com</a>
GPS Multiplexer – kplex	<a href="http://www.stripdog.com/kplex">http://www.stripdog.com/kplex</a>
IPsec – strongSwan	<a href="https://wiki.strongswan.org">https://wiki.strongswan.org</a>
Linux Firewall – Iptables	<a href="http://www.netfilter.org/projects/iptables">http://www.netfilter.org/projects/iptables</a>
L2TP – openl2tp	<a href="http://www.openl2tp.org">http://www.openl2tp.org</a>
POSTFIX – Mail Transfer Agent	<a href="http://www.postfix.org">http://www.postfix.org</a>
Public Land Mobile Network Numeric Provider ID	<a href="http://en.wikipedia.org/wiki/Mobile_Network_Code">http://en.wikipedia.org/wiki/Mobile_Network_Code</a>