

## **CT-Router LTE**



## Copyright © CAT Dorfer Consulting GmbH

Die in dieser Publikation veröffentlichten Beiträge sind urheberrechtlich geschützt. Übersetzungen, Nachdruck, Vervielfältigung sowie Speicherung in Datenverarbeitungsanlagen bedürfen der ausdrücklichen Genehmigung der CAT Dorfer Consulting GmbH.  
Alle Rechte vorbehalten.

CAT Dorfer Consulting GmbH  
Kampstrasse 7a  
D-24616 Hardebek  
Tel: +49 4324-88634  
Fax: +49 4324-88635  
Internet: <http://www.cat-t.de>  
email: [info@ccat-t.de](mailto:info@ccat-t.de)

Technische Änderungen vorbehalten.

Alle Warenzeichen und Produktbezeichnungen sind Warenzeichen, eingetragene Warenzeichen oder Produktbezeichnungen der jeweiligen Inhaber.

Alle Lieferungen und Leistungen erbringt die CAT Dorfer Consulting GmbH auf der Grundlage der Allgemeinen Geschäftsbedingungen der CAT Dorfer Consulting GmbH in der jeweils aktuellen Fassung. Alle Angaben basieren auf Herstellerangaben. Keine Gewähr oder Haftung bei fehlerhaften und unterbliebenen Eintragungen. Die Beschreibungen der Spezifikationen in diesem Handbuch stellen keinen Vertrag da.

Produkt-Nr.: LTE 230-00

# Inhalt

<b>Technische Daten</b> .....	<b>5</b>
<b>Hardware Installation</b> .....	<b>7</b>
Anschlussbelegung.....	7
LED Anzeigen.....	8
<b>Konfiguration WBM</b> .....	<b>9</b>
Start der Konfiguration.....	9
<b>Device Information</b> .....	<b>10</b>
Hardware.....	10
Software.....	11
<b>Status</b> .....	<b>12</b>
Radio.....	12
Network Connections.....	14
I/O Status.....	15
ComSERVER – Status (optional).....	16
Routing Table.....	17
DHCP Leases.....	18
<b>Local Network</b> .....	<b>19</b>
IP Configuration.....	19
DHCP Server.....	20
Static Routes.....	21
<b>Wireless Network</b> .....	<b>22</b>
Radio Setup.....	22
SIM.....	23
Backup SIM.....	25
SMS Configuration.....	26
Packet Data Setup.....	28
Static Routes.....	29
DynDNS.....	30
Connection Check.....	31
<b>Network Security</b> .....	<b>32</b>
General Setup.....	32
Firewall.....	33
NAT Table.....	34
<b>VPN</b> .....	<b>35</b>
IPSec.....	35
Connections.....	35
Connections Settings.....	36
Connection IKE.....	38
Certificates.....	40
Status.....	41

# Inhalt

OpenVPN.....	42
Tunnel .....	42
Port Forwarding.....	44
Certificates .....	45
Static Keys .....	46
Status .....	47
<b>I/O.....</b>	<b>48</b>
Inputs .....	48
Outputs .....	49
Phonebook.....	50
Socket Server .....	51
<b>System.....</b>	<b>52</b>
Web Configuration .....	52
User .....	53
Log Configuration .....	54
Log-File.....	55
ComSERVER - Serielle Schnittstelle konfigurieren (optional).....	56
SMTP Configuration .....	57
Configuration Up-/Download .....	58
RTC.....	59
Reboot .....	60
Firmware Update .....	61
<b>Abfrage und Steuerung über XML Dateien.....</b>	<b>62</b>
Format der XML Dateien .....	62
Beispiele zu den Basis-Einträgen:.....	62
a) E/A System .....	62
b) Allgemeine Informationen abfragen.....	63
c) SMS versenden.....	63
d) eMail versenden.....	63
Daten senden und empfangen .....	64
<b>Funktions-Test.....</b>	<b>65</b>
<b>Applikationsbeispiele .....</b>	<b>66</b>

## Technische Daten

Versorgung	
Versorgungsspannung	10V DC ... 30V DC über steckbare Schraubklemme
Nennstromaufnahme	< 250mA bei 24V, < 620mA bei 10V
Standby-Stromaufnahme	< 90mA bei 24V
LED-Anzeige	Power (LED grün), Dauerlicht: Betrieb

Schnittstelle	
<b>Netzschnittstelle</b>	
LTE Frequenzen	800, 850, 900, 1800, 1900, 2100, 2600 MHz (LTE)
Sendeleistung	23 dB
UMTS Frequenzen	850 MHz, 1900 MHz, 2100 MHz (UMTS/HSPA)
Sendeleistung	23 dB
GSM Frequenzen	850 MHz, 900 MHz, 1800 MHz, 1900 MHz (GPRS/EDGS)
Sendeleistung	max. 32,5 dB
SIM-Schnittstelle	2 Schnittstellen, 1,8 Volt und 3-Volt-SIM-Karte
Antennenanschluss	50 Ω Impedanz SMA-Antennenbuchse
LED	SIM (LED grün), NET (LED Bargraph)
<b>Ethernet-Schnittstelle</b>	
Anschlussart	RJ45-Buchse, geschirmt
Übertragungsrate	10/100 MBit/s
Unterstützte Protokolle	TCP/IP, UDP/IP, FTP, HTTP
Hilfsprotokolle	ARP, DHCP, PING( ICMP), SNMP V1, SMTP
LED-Anzeige / Steuer- signalindikator	ACT (LED gelb), Ethernet-Datenübertragung
Unterstützte Protokolle	LINK (LED grün), Ethernet-Link hergestellt
<b>I/O's</b>	4 Eingänge, 4 Ausgänge

## Technische Daten

Physikalische Merkmale	
Größe (HxBxT)	101 mm x 116 mm x 23 mm
Umgebungstemperatur	Betrieb -25°C...+70°C, Lagerung -40°C ...+85°C
Luftfeuchtigkeit	0...95% (nicht kondensierend)
Schutzart	IP30

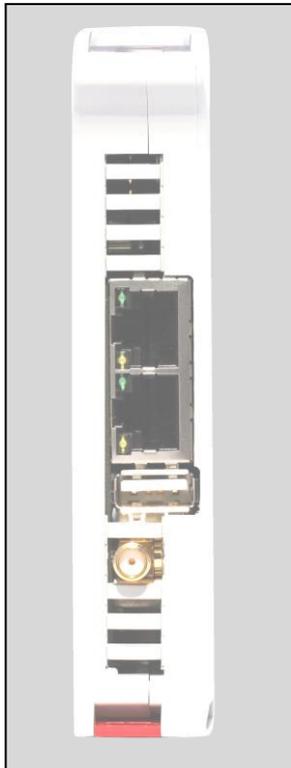
CE-Konformität gemäß R&TTE-Richtlinie 1999/5/EG	
EMV	EN 61000-6-2, EN55022 Class B
Sicherheit	EN 60950
Funk	EN 301511

Zulassungen	
UL, USA / Kanada	in Bearbeitung

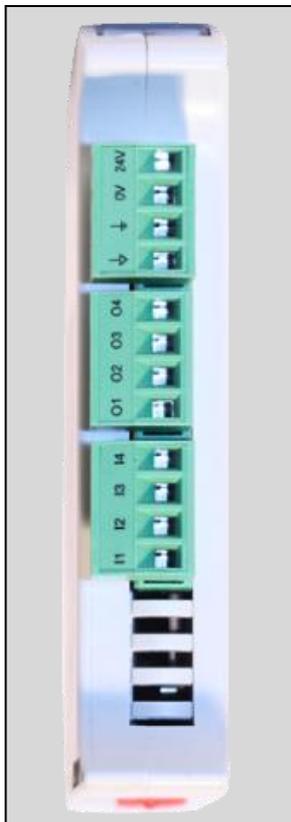
Technische Änderungen vorbehalten!

# Hardware Installation

## Anschlussbelegung



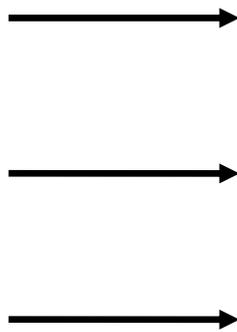
- ← Ethernet 1
- ← Ethernet 2
- ← USB
- ← SMA diversity Antenne



Stromversorgung
10V - 30V DC
0V
NC
NC

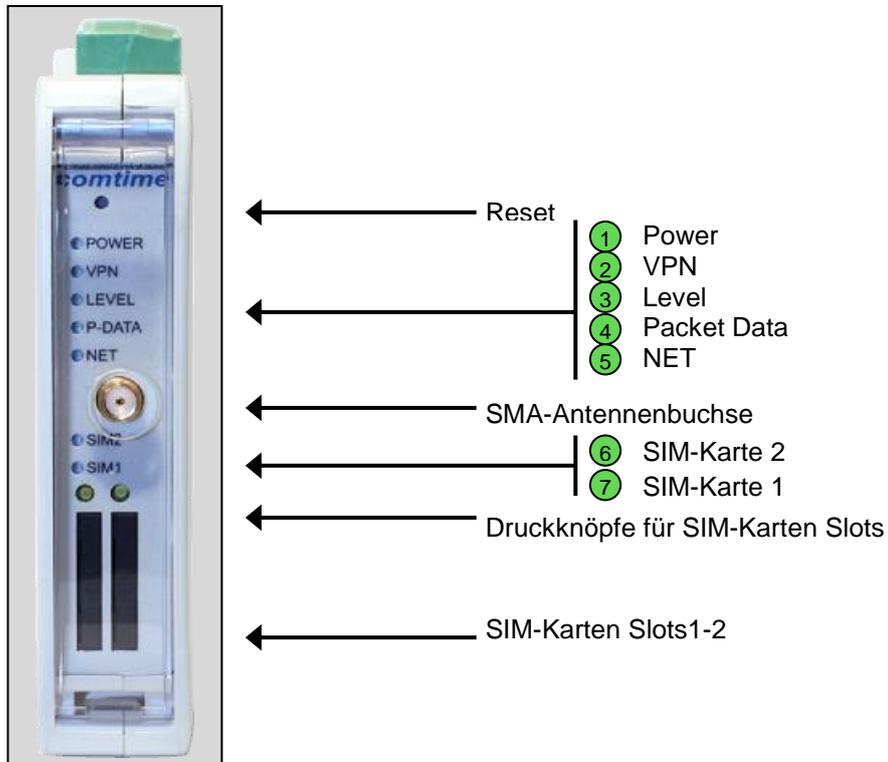
Digitaler Ausgang
O4
O3
O2
O1

Digitaler Eingang
I4
I3
I2
I1



## Hardware Installation

### LED Anzeigen



LED Router LTE	
LED	Erklärung
SIM-Karte 1/2	Aus = keine SIM-Karte Ein = SIM / PIN ok schnelles Blinken = falsche PIN langsam Blinken = keine PIN
NET	Aus = nicht eingebucht Blinken = GPRS/EDGE/UMTS/HSDPA/HSUPA Ein = LTE
Packet Data	Aus = keine Verbindung Blinken = Modem Verbindung Ein = Paketdaten-Verbindung
Level	Aus = nicht eingebucht Blinken: kurz Ein - lang Aus = -109dBm ... -89dBm Blinken: lang Ein - kurz Aus = -87dBm ... -67dBm Ein = -65dBm ... -51dBm oder besser
VPN	Aus = keine VPN-Verbindung Ein = VPN-Verbindung aktiv
Power	Aus = keine Stromversorgung Ein = Stromversorgung aktiv

## Konfiguration WBM

Die Konfiguration des CT-Router LTE erfolgt über eine Webbrowser basierende Funktion. Hierfür müssen zunächst folgende Bedingungen erfüllt sein:

- Der Computer, der zur Konfiguration des Routers verwendet wird, verfügt über eine LAN-Schnittstelle.
- Auf dem Computer ist ein Webbrowser installiert (z.B. Google Chrome, Mozilla Firefox, Microsoft Internet Explorer).
- Der Router ist mit einer Spannungsquelle verbunden.

### Start der Konfiguration

1. Ethernet-Verbindung zwischen Computer und Router herstellen.
2. IP-Adresse der LAN-Schnittstelle auf das Netz des Routers abstimmen.
3. Webbrowser öffnen.
4. Die IP-Adresse des Routers (192.168.0.1) in das Adressfeld des Browsers eingeben und mit Eingabe bestätigen. Anschließend wird eine Benutzername/Passwort-Abfrage erfolgen.

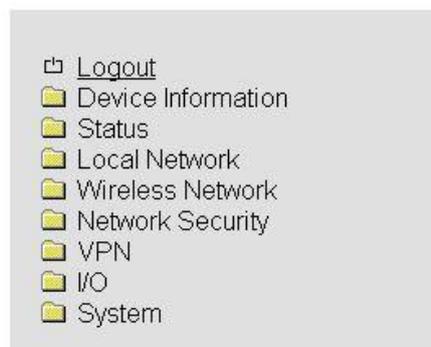


Im Auslieferungszustand lautet der Benutzername „admin“ und das Passwort „admin“ (das Ändern des Passwortes wird im späteren Verlauf beschrieben).

Des Weiteren gibt es zwei User-Level:

- User: Lesezugriff auf „Device Information“
- Admin: Lese- und Schreibzugriff auf alle Bereiche

Nach der Eingabe des Benutzernamens und des Passwortes öffnet sich das Hauptmenü zur Konfiguration des CT-Router HSPA.



## Device Information

In diesem Bereich können Sie genauere Informationen zur eingebauten Hardware, sowie der installierten Software einsehen.

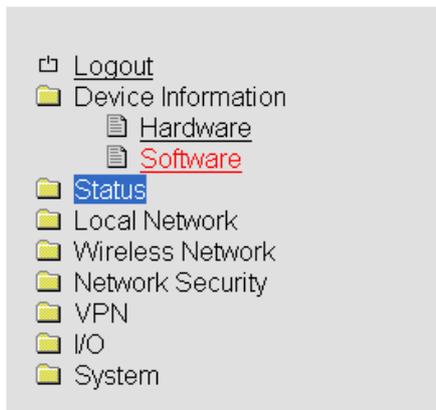
### Hardware

CT-Router HSPA	
Hardware Information	
Address	comtime GmbH 22848 Norderstedt Germany
Internet	<a href="http://www.comtime-com.de">www.comtime-com.de</a>
Type	CT-Router HSPA
Order-No.	229-01
Serial Number	2000010001
Hardware	Rev. A virtual
Release Version	1.01.2
Operating System	Linux 3.2.0-4-amd64
Web Based Management	1.36.10
MAC Address LAN1	8C-89-A5-61-93-E4
MAC Address LAN2	
Radio-Engine	PH8-P
Radio-Firmware	REVISION 02.002
IMEI	112233445566778

Tabellarische Übersicht der eingebauten Hardware.

## Device Information

### Software



#### CT-Router HSPA

Software Information	
alertsd	0.71.3
busybox	1.18.5-1.6
conchkd	0.30.2
dnsmasq	2.57-1.2
dropbear	0.53.1-1.6
ez-ipupdate	3.0.11b8-1.0
gsmCtrlD	3.5.8
inputsd	0.13.3
iproute2	2.6.38-1.3
ipsec	2.8.11-2.0
iptables	1.4.10-1.1
liboping	0.5.1-1.1
msmtp	1.4.27-1.0
netplug	1.2.9-1.2
openntpd	3.10p2-1.1
openssl	1.0.0k
openvpn	2.2.2-1.1
portmap	6.0-1.2
pppd	2.4.5-1.6
watchdog	0.16.3

Tabellarische Übersicht der auf dem CT-Router LTE installierten Software.

## Status

In diesem Menü werden Ihnen aktuelle Status-Informationen zum GSM-Netz und Netzwerkverbindungen angezeigt.

### Radio

- Logout
- Device Information
- Status
  - Radio**
  - Network Connections
  - I/O Status
  - Routing Table
  - DHCP Leases
  - System Info
- Local Network
- Wireless Network
- Network Security
- VPN
- I/O
- System

#### CT-Router HSPA

Radio Status	
Provider	Beispielprovider
Networkstatus	busy
Signal Level	<div style="display: inline-block; width: 50px; height: 10px; background-color: green; border: 1px solid black;"></div> -83 dBm
Packet Data	offline
Local Area Code	579
Cell ID	2606587

Status → Radio	
Radio Status	Erklärung
Provider	Providername
Networkstatus	<p><b>Registered home:</b> Einwahl im heimatlichen Mobilfunknetz</p> <p><b>Roaming:</b> Einwahl in das Mobilfunknetz über einen fremden Provider</p> <p><b>Waiting for PIN:</b> es ist noch keine PIN-Eingabe erfolgt</p> <p><b>Waiting for PUK:</b> PIN wurde drei Mal falsch eingegeben, PUK erforderlich</p> <p><b>Wrong PIN:</b> falsche PIN-Eingabe</p> <p><b>No SIM Card:</b> es ist keine SIM-Karte vorhanden</p> <p><b>Power off:</b> LTE-Modul nicht bereit</p>
Signal Level	Signalstärke des Netzes (dBm-Wert)

## Status

Packet Data	<b>offline:</b> Paketdaten-Verbindung nicht aufgebaut <b>GPRS online:</b> Aktive Paketdaten-Verbindung, GPRS-Signal <b>EDGE online:</b> Aktive Paketdaten-Verbindung, EDGE-Signal <b>UMTS online:</b> Aktive Paketdaten-Verbindung, UMTS-Signal <b>HSDPA/UPA online:</b> Aktive Paketdaten-Verbindung, HSDPA/UPA-Signal <b>LTE online:</b> Aktive Paketdaten-Verbindung, LTE-Signal
Local Area Code	Gebietskennzahl des Mobilfunknetzes
Cell ID	ID der Mobilfunkzelle

# Status

## Network Connections

Logout
Device Information
Status
Radio
Network Connections
I/O Status
Routing Table
DHCP Leases
System Info
Local Network
Wireless Network
Network Security
VPN
I/O
System

### CT-Router HSPA

Network Connections	
Wireless Network	
Link	not connected
Local Network	
Link	connected
IP Address	85.214.27.44
Netmask	255.255.255.255
IP Address Alias(1)	85.214.242.129
Netmask Alias(1)	255.255.255.255

Status → Network Connections	
Network Connections	Erklärung
<b>Wireless Network</b>	
Link	<b>TCP/IP connected:</b> TCP/IP Verbindung im Mobilfunknetz aufgebaut. <b>VPN connected:</b> VPN Verbindung im Mobilfunknetz aufgebaut. <b>not connected:</b> Es besteht keine aktive Verbindung im Mobilfunknetz.
IP Address	zugewiesene IP-Adresse (Providervorgabe)
Netmask	zugewiesene Netzmaske (Providervorgabe)
DNS Server	DNS-Server IP-Adresse
Sec. DNS Server	alternative DNS-Server IP-Adresse
RX Bytes	Anzahl der empfangenen Daten seit Login in das Mobilfunknetz in Bytes.
TX Bytes	Anzahl der gesendeten Daten seit Login in das Mobilfunknetz in Bytes.
<b>Local Network</b>	
Link	<b>connected:</b> Lokale Ethernet-Verbindung aufgebaut <b>not connected:</b> keine lokale Ethernet-Verbindung aufgebaut
IP Address	Ethernet IP-Adresse
Netmask	Ethernet Netzmaske

## I/O Status

Logout
Device Information
Status
Radio
Network Connections
I/O Status
Routing Table
DHCP Leases
System Info
Local Network
Wireless Network
Network Security
VPN
I/O
System

## CT-Router HSPA

I/O Status		
Input		
#1	Low	SMS,E-Mail
#2	High	E-Mail
#3	Low	None
#4	Low	None
Output		
#1	Off	Manual
#2	On	Remote Controlled
#3	Off	Packet Service
#4	On	Incoming Call

Tabellarische Übersicht aller aktuellen Input- und Outputeinstellungen.

# Status

## ComSERVER – Status (optional)

- Logout
- Device Information
- Status
  - Radio
  - Network Connections
  - I/O Status
  - ComSERVER**
  - Routing Table
  - DHCP Leases
  - System Info
- Local Network
- Wireless Network
- Network Security
- VPN
- I/O
- System

**CR-230 UR**

ComSERVER Status	
Link	Enabled
TCP Remote	192.168.0.3
Baud rate	115200
Data bits	8
Parity	None
Stop bits	1
Flow control	RTS/CTS

*oder*

- Logout
- Device Information
- Status
  - Radio
  - Network Connections
  - I/O Status
  - ComSERVER**
  - Routing Table
  - DHCP Leases
  - System Info
- Local Network
- Wireless Network
- Network Security
- VPN
- I/O
- System

**CR-230 UR**

ComSERVER Status	
Link	Enabled
TCP Remote	waiting

Status → ComSERVER	
ComSERVER	Erklärung
Link	Hier wird der Status der ComSERVER (seriellen) Verbindung angezeigt:
TCP Remote	
Baud Rate	
Data bits	
Parity	
Stop bits	
Flow control	

## Routing Table

- ☐ Logout
- 📁 Device Information
- 📁 Status
  - 📄 Radio
  - 📄 Network Connections
  - 📄 I/O Status
  - 📄 **Routing Table**
  - 📄 DHCP Leases
  - 📄 System Info
- 📁 Local Network
- 📁 Wireless Network
- 📁 Network Security
- 📁 VPN
- 📁 I/O
- 📁 System

### CT-Router HSPA

Kernel IP routing table							
Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
0.0.0.0	85.214.26.1	0.0.0.0	UG	0	0	0	eth0
10.8.0.0	10.8.0.2	255.255.255.0	UG	0	0	0	tun2
10.8.0.2	0.0.0.0	255.255.255.255	UH	0	0	0	tun2
10.11.0.0	10.11.0.2	255.255.255.0	UG	0	0	0	tun1
10.11.0.2	0.0.0.0	255.255.255.255	UH	0	0	0	tun1
10.142.0.0	10.142.0.2	255.255.255.0	UG	0	0	0	tun0
10.142.0.2	0.0.0.0	255.255.255.255	UH	0	0	0	tun0
85.214.26.1	0.0.0.0	255.255.255.255	UH	0	0	0	eth0

### Status → Routing Table

Routing Table	Erklärung
---------------	-----------

Enthält unter anderen Informationen zum Ziel, Gateway, zur Subnetzmaske und Metrik.

# Status

## DHCP Leases

Logout
Device Information
Status
Radio
Network Connections
I/O Status
Routing Table
DHCP Leases
System Info
Local Network
Wireless Network
Network Security
VPN
I/O
System

### CT-Router HSPA

DHCP Leases		
Host Name	Client MAC Address	Client IP Address
raspberrypi	B8-27-EB-75-F1-CE	192.168.2.102
thinkpad	00-16-6F-81-47-B2	192.168.2.105
DMP117	00-05-CD-13-9E-2F	192.168.2.117
Vbox8	08-00-27-48-75-8D	192.168.2.127
S685-IP	7C-2F-80-15-62-D5	192.168.2.129

Status → DHCP Leases	
DHCP Leases	Erklärung
Tabellarische Übersicht aller vom CT-Router HSPA vergebenen DHCP-Daten.	
Host Name	Hostname des im Netzwerk befindlichen Endgerätes
Client MAC Address	MAC-Adresse des im Netzwerk befindlichen Endgerätes
Client IP Address	IP-Adresse des im Netzwerk befindlichen Endgerätes

# Local Network

Im Menü „Local Network“ können Sie die lokale Netzwerkeinstellung für den CT-Router HSPA vornehmen.

## IP Configuration

- Logout
- Device Information
- Status
- Local Network
  - IP Configuration
  - DHCP Server
  - Static Routes
- Wireless Network
- Network Security
- VPN
- I/O
- System

**CT-Router HSPA**

**IP Configuration**

Current Address

IP Address

Subnet Mask

Type of the IP address assignment Static Address ▾

Alias Addresses

IP Address	Subnet Mask	<input type="button" value="New"/>
------------	-------------	------------------------------------

Local Network → IP Configuration	
IP Configuration	Erklärung
Current Address	
IP Address	aktuelle IP-Adresse des Routers
Subnet Mask	Subnetzmaske der aktuellen IP-Adresse
Type of the IP address assignment	<b>Static:</b> Statische IP-Adresse (Standardeinstellung) <b>DHCP:</b> Dynamische IP-Adresse, wird beim Start des Routers von einem DHCP-Server bezogen
Alias Addresses	Max. 8 zusätzliche IP-Adressen sowie Subnetzmasken zuweisbar.
IP Address	alternative IP-Adresse des Routers
Subnet Mask	alternative Subnetzmaske des Routers

## Local Network

### DHCP Server

- Logout
- Device Information
- Status
- Local Network
  - IP Configuration
  - DHCP Server**
  - Static Routes
- Wireless Network
- Network Security
- VPN
- I/O
- System

**CT-Router HSPA**

**DHCP Server**

DHCP Server Disabled ▾

Domain Name example.net

Lease Time (d,h,m,s) 24h

Dynamic IP address allocation Disabled ▾

Begin IP Range 192.168.0.10

End IP Range 192.168.0.30

Static IP address allocation

Host Name	Client MAC Address	Client IP Address	
			New

Apply

Local Network → DHCP Server	
DHCP Server	Erklärung
DHCP Server	Deaktiviert / Aktiviert
Domain Name	Domain-Namen eintragen, der über DHCP verteilt wird.
Lease Time (d,h,m,s)	Zeitraum, in dem die Netzwerkkonfigurationen gültig sind.
Dynamic IP address allocation	Dynamische IP-Adressen-Zuweisung: Bei Aktivierung können Sie die entsprechenden Netzwerkparameter eintragen / Der DHCP-Server vergibt IP-Adressen aus dem angegebenen IP-Bereich.
Begin IP Range	IP-Bereichsanfang
End IP Range	IP-Bereichsende
Static IP address allocation	IP-Adressen werden MAC-Adressen eindeutig zugeordnet.
Client MAC Address	MAC-Adresse des verbundenen Endgerätes
Client IP Address	IP-Adresse des verbundenen Endgerätes  IP-Adressen dürfen nicht aus den dynamischen IP-Adressen Zuweisungen stammen.  Eine IP-Adresse darf nicht mehrfach zugeordnet werden, da sonst einer IP-Adresse mehreren MAC-Adressen zugewiesen wird.

# Local Network

## Static Routes

The screenshot shows the configuration interface for a CT-Router HSPA. On the left is a navigation tree with the following items: Logout, Device Information, Status (highlighted), Local Network (expanded), IP Configuration, DHCP Server, Static Routes (highlighted), Wireless Network, Network Security, VPN, I/O, and System. The main panel is titled 'Local Static Routes' and contains a table with the following data:

Network	Gateway	
0.0.0.0/0	0.0.0.0	<input type="button" value="New"/> <input type="button" value="Delete"/> <input type="button" value="Cancel"/>

Below the table is an  button.

Local Network → Static Routes	
Static Routes	Erklärung
Network	Netzwerk in CIDR-Form
Gateway	Gateway-Adresse des Netzwerkes
Max. 8 Netzwerke eintragbar.	

## Wireless Network

Im "Wireless Network"-Menü legen Sie Einstellungen für die Nutzung des Mobilfunknetzwerkes des Router HSPA fest.

### Radio Setup

- Logout
- Device Information
- Status
- Local Network
- Wireless Network
  - Radio Setup**
  - SIM
  - Backup SIM
  - SMS Configuration
  - Packet Data Setup
  - Static Routes
  - DynDNS
  - Connection Check
- Network Security
- VPN
- I/O
- System

**CT-Router HSPA**

**Radio Setup**

Frequency	Europe/Asia (900/1800 MHz) ▾
UMTS Freq.	Europe/Asia 2100 MHz ▾
Backup SIM	Disabled ▾
Provider Timeout	10 min.
Backup Runtime	23 hrs.
Daily relogin	Disabled ▾
Time	01:00

Wireless Network → Radio Setup	
Radio Setup	Erklärung
Frequency	Frequenzbereich des Routers mithilfe einer Dropdown-Liste auswählen.
UMTS Freq.	Frequenzbereich für UMTS mithilfe einer Dropdown-Liste auswählen / UMTS kann auch deaktiviert werden.
Backup SIM	Zweite SIM-Karte kann für eine Backup-Mobilfunkverbindung genutzt werden.
Provider Timeout	Zeit in Minuten für Aktivierung der Backup-SIM-Karte nach Ausfall der Primären.
Backup Runtime	Laufzeit in Stunden der zweiten SIM-Karte
Daily relogin	<b>Disable:</b> Deaktivierung des täglichen Logins <b>Enable:</b> Aktivierung des täglichen Logins (Primär vor Sekundär SIM)
Time	Zeitpunkt der Neuansmeldung des Routers in das Mobilfunknetz (Es erfolgt zunächst eine Abmeldung. Bei Neuansmeldung Primär vor Sekundär SIM).

# Wireless Network

## SIM

- Logout
- Device Information
- Status
- Local Network
- Wireless Network
  - Radio Setup
  - SIM**
  - Backup SIM
  - SMS Configuration
  - Packet Data Setup
  - Static Routes
  - DynDNS
  - Connection Check
- Network Security
- VPN
- I/O
- System

### CT-Router HSPA

**SIM**

Country	Germany	Set
PIN	<input type="text"/>	
Roaming	Enabled	
Provider	Auto	
Username	<input type="text"/>	
Password	<input type="text"/>	
APN	web.vodafone.de	
Authentication	All Protocols	
Apply		

Wireless Network → SIM	
SIM	Erklärung
Country	Auswahl des Landes, in dem der Router in das GSM-Netz eingewählt wird. (Schränkt die Auswahl unter dem Punkt "Provider" ein.)
PIN	PIN-Eingabe der SIM-Karte
Roaming	<b>Enable:</b> Es besteht die Möglichkeit, dass der Router sich über ein fremdes Netz einwählen kann. Hierbei können je nach Vertrag zusätzliche Kosten entstehen.
	<b>Disable:</b> Deaktivierung des Roamings. Es wird automatisch das Heimatnetz des Providers genutzt. Sollte dies nicht möglich sein, kommt keine Verbindung zustande.
Provider	Nur wenn das Roaming aktiviert ist, ist eine Auswahl möglich. <b>Auto:</b> Automatische Auswahl des Providers
Username	Benutzernamen für Paketdaten-Zugang (Providervorgabe)
Password	Passwort für Paketdaten-Zugang (Providervorgabe)
Benutzername und Passwort immer angeben, da sonst keine Paketdaten-Verbindung zustande kommt.	
APN	Name des Anschlusspunktes im Paketdaten-Netzwerk (Providervorgabe)

## Wireless Network

Authentication	<p>Authentifizierung wird durch Protokolle geschützt.</p> <p><b>All Protocols:</b> Alle Protokolle sind erlaubt</p> <p><b>refuse MSCHAP:</b> Ablehnung des Microsoft Challenge-Handshake Authentication Protocol.</p> <p><b>CHAP only:</b> Nur Challenge-Handshake Authentication Protocol</p> <p><b>PAP only:</b> Nur Password Authentication Protocol</p>
----------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## Wireless Network

### Backup SIM

- Logout
- Device Information
- Status
- Local Network
- Wireless Network
  - Radio Setup
  - SIM
  - Backup SIM
  - SMS Configuration
  - Packet Data Setup
  - Static Routes
  - DynDNS
  - Connection Check
- Network Security
- VPN
- I/O
- System

**CT-Router HSPA**

**Backup SIM**

Country	Germany	Set
PIN	<input type="text"/>	
Roaming	Enabled	
Provider	Auto	
Username	<input type="text"/>	
Password	<input type="text"/>	
APN	<input type="text"/>	
Authentication	All Protocols	
Apply		

Wireless Network → Backup SIM	
Backup SIM	Erklärung
Country	Auswahl des Landes, in dem der Router in das GSM-Netz eingewählt wird (Schränkt die Auswahl unter dem Punkt "Provider" ein.)
PIN	PIN-Eingabe der SIM-Karte
Roaming	<p><b>Enable:</b> Es besteht die Möglichkeit, dass der Router sich über ein fremdes Netz einwählen kann. Hierbei können je nach Vertrag zusätzliche Kosten entstehen.</p> <p><b>Disable:</b> Deaktivierung des Roamings. Es wird automatisch das Heimatnetz des Providers genutzt. Sollte dies nicht möglich sein, kommt keine Verbindung zustande.</p>
Provider	<p>Nur wenn das Roaming aktiviert ist, ist eine Auswahl möglich.</p> <p><b>Auto:</b> Automatische Auswahl des Providers</p>
Username	Benutzernamen für Paketdaten-Zugang (Providervorgabe)
Password	Passwort für Paketdaten-Zugang (Providervorgabe)
Benutzername und Passwort nicht leer lassen, da sonst keine Paketdaten-Verbindung zustande kommt.	
APN	Name des Anschlusspunktes im Paketdaten-Netzwerk (Providervorgabe)
Authentication	Authentifizierung wird durch Protokolle geschützt.
	<b>All Protocols:</b> Alle Protokolle sind erlaubt
	<b>refuse MSCHAP:</b> Ablehnung des Microsoft Challenge-Handshake Authentication Protocol.
	<b>CHAP only:</b> Nur Challenge-Handshake Authentication Protocol
	<b>PAP only:</b> Nur Password Authentication Protocol

## Wireless Network

### SMS Configuration

#### Steuerung des Mobilfunkrouters per SMS

Klicken unter „SMS Control“ auf Enable. Definieren Sie zum Schutz ein SMS-Passwort. Das Passwort kann bis zu 7 alphanumerische Zeichen enthalten.

#### SMS-Syntax

Die Steuerung erfolgt nach folgender SMS Syntax:

```
#<password>:<command>
<password> = ('A'-'Z', '0'-'9') // bis zu 7 alphanumerische Zeichen

<command> = SET:<sub_cmd> // set command (ON)
<command> = CLR:<sub_cmd> // clear command (OFF)
<sub_cmd> = OUTPUT // output set to ON/OFF
<sub_cmd> = IPSEC // IPsec VPN 1 ON/OFF
<sub_cmd> = IPSEC:n // IPsec VPN n ON/OFF, n={1..x}

<command> = SEND:STATUS // send a status SMS to the caller
<command> = RESET // reset all alarms
<command> = REBOOT // Reboot des Routers
```

#### Beispiel:

Einschalten des Outputs der I/O-Schnittstelle. Das (Beispiel-)Passwort lautet: „ct12345“. Die SMS an die Rufnummer des Routers muss dann folgenden Inhalt haben: #ct12345:SET:OUTPUT

#### Weiterleitung einer SMS an einen Socket Server

Der Router kann empfangene SMS Nachrichten an ein Endgerät über die Ethernet Schnittstelle weiterleiten. Auf dem Endgerät muss dafür ein Socket Server zum Empfang von XML-Dateien installiert sein.

Klicken Sie Enable unter „SMS forward“. Tragen Sie die Empfänger-IP-Adresse und den Port des Endgerätes ein, zu dem Sie kommunizieren möchten. Default-Wert für den Server ist Port 1432. Die empfangene SMS wird im folgenden Formatbeispiel weitergeleitet:

**Wichtiger Hinweis!!** Die Rufnummer muss dem Router zur Identifizierung als Eintragung im Telefonbuch bekannt sein.

#### Beispiel:

```
<?xml version="1.0"?>
<cmgr origaddr="+49172123456789" timestamp="10/05/21,11:27:14+08">
SMS message</cmgr>
origaddr = Rufnummer des Absenders
timestamp = Zeitstempel des Service Center im GSM 03.40 Format
```

## Wireless Network

### SMS Configuration

- Logout
- Device Information
- Status
- Local Network
- Wireless Network
  - Radio Setup
  - SIM
  - Backup SIM
  - SMS Configuration
  - Packet Data Setup
  - Static Routes
  - DynDNS
  - Connection Check
- Network Security
- VPN
- I/O
- System

CT-Router HSPA

SMS Configuration

SMS control	Enabled <input type="button" value="v"/>
SMS Password	<input type="text"/>
SMS forward	Disabled <input type="button" value="v"/>
Server IP Address	192.168.0.200
Server Port (default 1432)	1432
<input type="button" value="Apply"/>	

Wireless Network → SMS Configuration	
SMS Configuration	Erklärung
SMS control	<b>Disable:</b> den Router per SMS steuern - deaktiviert <b>Enable:</b> den Router per SMS steuern - aktiviert
SMS Password	SMS-Passwort zum Steuern per SMS
SMS forward	<b>Disable:</b> SMS-Nachrichten über Ethernet weiterleiten - deaktiviert. <b>Enable:</b> SMS-Nachrichten über Ethernet weiterleiten - aktiviert.
Server IP Address	Weiterleitung der SMS erfolgt an diese IP-Adresse
Server Port (default 1432)	Weiterleitung der SMS erfolgt an diesen Port.

## Wireless Network

### Packet Data Setup

- Logout
- Device Information
- Status
- Local Network
- Wireless Network
  - Radio Setup
  - SIM
  - Backup SIM
  - SMS Configuration
  - Packet Data Setup
  - Static Routes
  - DynDNS
  - Connection Check
- Network Security
- VPN
- I/O
- System

#### CT-Router HSPA

#### Packet Data Setup

Packet Data	Disabled ▾
Debug Mode	Disabled ▾
Allow Compression	Disabled ▾
MTU (default 1500)	1500
Event	Initiate ▾
Manual DNS	Disabled ▾
DNS Server	0.0.0.0
Sec. DNS Server	0.0.0.0
<input type="button" value="Apply"/>	

Wireless Network → Packet Data Setup	
Packet Data Setup	Erklärung
Packet Data	<b>Disable:</b> Deaktivierung der Paketdaten-Verbindung <b>Enable:</b> Aktivierung der Paketdaten-Verbindung / virtuelle dauerhafte Verbindung, erst bei tatsächlicher Datenübertragung entsteht Traffic.
Debug Mode	Zu Diagnosezwecken zur Paketdaten-Verbindung können Informationen im Log-File gespeichert werden. Diese Option kann aktiviert oder deaktiviert werden.
Allow Compression	<b>Disable:</b> Daten-Kompression aktiviert <b>Enable:</b> Daten Kompression deaktiviert
MTU (default 1500)	Maximale Paketgröße in Bytes
Event	<b>Initiate:</b> automatischer Start der Paketdaten-Verbindung <b>Initiate on Input #1... #4:</b> manueller Start über Schalteingang
Manual DNS	<b>Disable:</b> Deaktivierung der manuellen DNS-Einstellung (DNS wird vom Provider empfangen). <b>Enable:</b> Aktivierung der manuellen DNS-Einstellung
DNS Server	IP-Adresse, primärer DNS-Server im Mobilfunknetz
Sec. DNS Server	IP-Adresse, sekundärer DNS-Server im Mobilfunknetz

## Wireless Network

### Static Routes

- Logout
- Device Information
- Status
- Local Network
- Wireless Network
  - Radio Setup
  - SIM
  - Backup SIM
  - SMS Configuration
  - Packet Data Setup
  - Static Routes
  - DynDNS
  - Connection Check
- Network Security
- VPN
- I/O
- System

**CT-Router HSPA**

**Wireless Static Routes**

Network	Gateway	
0.0.0.0/0	0.0.0.0	New
		Delete
		Cancel
Apply		

Wireless Network → Static Routes	
Static Routes	Erklärung
Network	Netzwerk in CIDR-Form
Gateway	Gateway-Adresse des Netzwerkes
Max. 8 Netzwerke eintragbar	

## Wireless Network

### DynDNS

- Logout
- Device Information
- Status
- Local Network
- Wireless Network
  - Radio Setup
  - SIM
  - Backup SIM
  - SMS Configuration
  - Packet Data Setup
  - Static Routes
  - DynDNS
  - Connection Check
- Network Security
- VPN
- I/O
- System

**CT-Router HSPA**

**DynDNS Setup**

Status	Enabled <input type="button" value="v"/>
DynDNS Provider	DynDNS.org <input type="button" value="v"/>
DynDNS Username	<input type="text"/>
DynDNS Password	<input type="text"/>
DynDNS Hostname	<input type="text"/>
<input type="button" value="Apply"/>	

Wireless Network → DynDNS	
DynDNS	Erklärung
DynDNS	<b>Disable:</b> Deaktivierung der DynDNS <b>Enable:</b> Aktivierung der DynDNS
DynDNS Provider	Auswahl des DynDNS-Anbieters
DynDNS Username	Benutzername des DynDNS-Accounts
DynDNS Password	Passwort des DynDNS-Accounts
DynDNS Hostname	Hostname des Routers beim DynDNS-Service

# Wireless Network

## Connection Check

- Logout
- Device Information
- Status
- Local Network
- Wireless Network
  - Radio Setup
  - SIM
  - Backup SIM
  - SMS Configuration
  - Packet Data Setup
  - Static Routes
  - DynDNS
  - Connection Check
- Network Security
- VPN
- I/O
- System

**CT-Router HSPA**

Connection Check

Status Disabled

---

Host #1  Local

Host #2  Local

Host #3  Local

---

Check every  min.

Max retry

Activity None

Wireless Network → Connection Check	
Connection Check	Eklärung
Connection Check	<b>Disable:</b> Deaktivierung der Verbindungsprüfung der Paketdaten-Verbindung <b>Enable:</b> Aktivierung der Verbindungsprüfung der Paketdaten-Verbindung
Host #1...#3	IP-Adresse oder Hostnamen als Referenzpunkt zur Verbindungsprüfung <b>Local:</b> Aktivierung bei Adressen, die über einen VPN-Tunnel erreichbar sind
Check every	Es wird alle x Minuten die Verbindung geprüft.
Max. retry	Maximale Anzahl der Verbindungsversuche
Activity	Bei Verbindungsabbruch eine der folgenden Aktionen ausführen: <b>Reboot:</b> Router Neustart <b>Reconnect:</b> Verbindung wird versucht neu aufzubauen <b>Relogin:</b> Mobilfunkinterface wird heruntergefahren und erneuter Versuch eines Verbindungsaufbaus mit Login. <b>None:</b> keine Aktion wird ausgeführt

## Network Security

In diesem „Network Security“-Menü nehmen Sie Einstellungen zu Netzwerksicherheit vor.

### General Setup

- Logout
- Device Information
- Status
- Local Network
- Wireless Network
- Network Security
  - General Setup
  - Firewall
  - NAT table
- VPN
- I/O
- System

CT-Router HSPA

#### Network Security Setup

Firewall	Enabled <input type="button" value="v"/>
Block outgoing Netbios	Enabled <input type="button" value="v"/>
Ping (ICMP) external	Disabled <input type="button" value="v"/>
Web based Management external	Disabled <input type="button" value="v"/>
NAT table	Enabled <input type="button" value="v"/>
NAT (Masquerade) external	Enabled <input type="button" value="v"/>

Network Security → General Setup	
General Setup	Erklärung
Firewall	<p><b>Disable:</b> Deaktivierung der integrierten Stateful Packet Inspection Firewall</p> <p><b>Enable:</b> Aktivierung der integrierten Stateful Packet Inspection Firewall</p>
Block outgoing Netbios	<p>Netbios-Anfragen gehen von Windows-Systemen im lokalen Netzwerk aus und verursachen einen erhöhten Datenverkehr.</p> <p><b>Disable:</b> Netbios-Anfragen werden erlaubt</p> <p><b>Enable:</b> Netbios-Anfragen werden geblockt</p>
Ping (ICMP) external	<p>Ping-Anfragen prüfen, ob ein Gerät im Netzwerk erreichbar ist. Dadurch erhöht sich der Datenverkehr.</p> <p><b>Disable:</b> Ping-Anfragen aus dem externen IP-Netz werden nicht beantwortet</p> <p><b>Enable:</b> Ping-Anfragen aus dem externen IP-Netz werden beantwortet</p>
Web based Management external	<p><b>Disable:</b> Externe WBM Konfiguration ist deaktiviert</p> <p><b>Enable:</b> Externe WBM Konfiguration ist aktiviert</p>
NAT (Masquerade) external	<p><b>Disable:</b> IP-Masquerading deaktiviert</p> <p><b>Enable:</b> IP-Masquerading aktiviert</p>

# Network Security

## Firewall

Network Security → Firewall	
Firewall	Erklärung
Incoming Traffic	
Protocol	Protokollauswahl: TCP, UDP, ICMP, all
From IP / To IP	IP-Adressenbereich in CIDR-Form (0.0.0.0/0 bedeutet alle IP-Adressen)
From Port / To Port	Portbereich ("any" bezeichnet alle Ports)
Action	<p><b>Accept:</b> Datenpakete werden angenommen.</p> <p><b>Reject:</b> Datenpakete werden abgelehnt. Benachrichtigung an den Absender, dass die Daten abgelehnt werden.</p> <p><b>Drop:</b> Datenpakete werden "fallen gelassen" d.h. sie werden abgewiesen und der Absender erhält keine Benachrichtigung.</p>
Log	<p><b>Yes:</b> Aktivierung der Regel wird protokolliert</p> <p><b>No:</b> Aktivierung der Regel wird nicht protokolliert.</p>
New / Delete	Neue Regel aufstellen / bestehende Regel löschen
	Mit den Pfeilen können Regeln nach oben oder unten verschoben werden.
Outgoing Traffic	<p>Verhält sich ähnlich zum „Incoming Traffic“, jedoch beziehen sich diese Regeln auf den ausgehenden Datenverkehr.</p> <p>Ist keine Regel vorhanden, so sind alle ausgehenden Verbindungen verboten (mit Ausnahme von VPN-Verbindungen)</p>

# Network Security

## NAT Table

- Logout
- Device Information
- Status
- Local Network
- Wireless Network
- Network Security
  - General Setup
  - Firewall
  - NAT table
- VPN
- I/O
- System

**CT-Router HSPA**

---

**NAT table**

Forwarding Incoming Traffic

Protocol	In Port	To IP	To Port	Masq	Comment	Log	
<input type="button" value="Apply"/>							

Network Security → NAT table	
Firewall	Erklärung
Protocol	Protokollauswahl: TCP, UDP, ICMP, all
In Port / To Port	Portbereich ("any" bezeichnet alle Ports)
To IP	IP-Adressenbereich in CIDR-Form (0.0.0.0/0 bedeutet alle IP-Adressen)
Masq	<b>Yes:</b> IP-Masquerading aktiviert / Antwort in Mobilfunknetze möglich <b>No:</b> IP-Masquerading deaktiviert / Antwort in Mobilfunknetze nicht möglich
Log	<b>Yes:</b> Aktivierung der Regel wird protokolliert <b>No:</b> Aktivierung der Regel wird nicht protokolliert
New / Delete	Neue Regel aufstellen / bestehende Regel löschen
	Mit den Pfeilen können Regeln nach oben oder unten verschoben werden.

## VPN

Im Menü VPN können Sie einerseits Einstellungen zur Internet Protocol Security (IPsec) andererseits zum virtuellen privaten Netzwerk (OpenVPN) vornehmen.

Für eine VPN-Verbindung müssen die IP-Adressen der VPN-Gegenstellen bekannt und adressierbar sein.

### IPSec

Die VPN-Gegenstelle muss IPsec mit folgender Konfiguration unterstützen:

- Authentifizierung über X.509-Zertifikate oder Preshared Secret Key (PSK)
- ESP
- Diffie-Hellman Gruppe 2 oder 5
- 3DES oder AES encryption
- MD5 oder SHA-1 Hash Algorithmen
- Tunnel-Modus
- Quick Mode
- Main Mode
- SA Lifetime (1 Sekunde bis 24 Stunden)

### Connections

- Logout
- Device Information
- Status
- Local Network
- Wireless Network
- Network Security
- VPN
  - IPsec
    - Connections**
    - Certificates
    - Status
  - OpenVPN
- I/O
- System

**CT-Router HSPA**

**IPsec Connections**

Monitor DynDNS No

Check interval 600 sec.

Enabled	Name	Settings	IKE
No <input type="button" value="v"/>	vpn1	<input type="button" value="Edit"/>	<input type="button" value="Edit"/>
No <input type="button" value="v"/>	vpn2	<input type="button" value="Edit"/>	<input type="button" value="Edit"/>
No <input type="button" value="v"/>	vpn3	<input type="button" value="Edit"/>	<input type="button" value="Edit"/>
No <input type="button" value="v"/>	vpn4	<input type="button" value="Edit"/>	<input type="button" value="Edit"/>
No <input type="button" value="v"/>	vpn5	<input type="button" value="Edit"/>	<input type="button" value="Edit"/>

VPN → IPsec → Connections	
IPsec Connections	Erklärung
Monitor DynDNS	VPN-Gegenstelle hat keine feste IP und als Remote Host wird ein DynDNS-Name genutzt, so kann diese Funktion aktiviert werden, um die Verbindung zu überprüfen.
Check Interval	Prüfintervall in Sekunden
Enable	VPN-Verbindung aktivieren (=Yes) oder deaktivieren (=No)
Name	Name der VPN-Verbindung festlegen
Settings	Einstellungen für IPsec
IKE	Einstellungen für das Internet-Key-Exchange-Protokoll

# VPN-IPsec

## Connections Settings

- Logout
- Device Information
- Status
- Local Network
- Wireless Network
- Network Security
- VPN
  - IPsec
    - Connections
    - Certificates
    - Status
  - OpenVPN
- I/O
- System

**CT-Router HSPA**

---

**IPsec Connection Settings**

Name: vpn1

VPN: Disabled

Authentication: X.509 Remote Certificate

Remote Certificate: None

Local Certificate: None

Remote ID:

Local ID:

Address Remote Network: 192.168.9.0/24

Address Local Network: 192.168.0.0/24

Connection NAT: None

Remote Connection: Accept

Autoreset: 60 min.

VPN → IPsec → Connections → Settings → Edit	
Settings	Erklärung
Name	Name der VPN-Verbindung
VPN	Aktivieren (=Enable) oder Deaktivieren (=Disable) der VPN-Verbindung
Remote Host	IP-Adresse / URL der Gegenstelle  Kann nur eingestellt werden, wenn unter Remote Connection "Initiate" ausgewählt wurde. Wurde unter Remote Connection "Accept" ausgewählt, so wird der Wert für Remote Host auf "%any" gesetzt, und es wird auf eine Verbindung gewartet.
Authentication	X.509 Remote Certificate - VPN-Teilnehmer haben einen privaten und einen öffentlichen Schlüssel (X.509-Zertifikat).  Preshared Secret Key - VPN-Teilnehmer besitzen einen privaten Schlüssel (ein gemeinsames Passwort).
Remote Certificate	VPN-Gegenstellen Authentifizierung erfolgt über ein Zertifikat, das in dem Menü "IPsec Certificates" hochgeladen werden muss.
Local Certificate	Router Authentifizierung bei der VPN-Gegenstelle erfolgt über ein Zertifikat, das in dem Menü "IPsec Certificates" hochgeladen werden muss.

## VPN-IPsec

Remote ID	<p><b>Leer:</b> Kein Eintrag in der Zeile bedeutet, dass die Angaben aus dem Zertifikat gewählt werden.</p> <p><b>Subject:</b> Eine IP-Adresse, E-Mail-Adresse oder ein Hostname bedeutet, dass diese Einträge auch im Zertifikat vorhanden sein sollten, damit sich der Router authentifizieren kann.</p>
Local ID	Siehe Remote ID
Address Remote Network	IP-Adresse/Subnetzmaske des Netzwerkes, zu dem eine VPN-Verbindung aufgebaut wird.
Address Local Network	IP-Adresse/Subnetzmaske vom lokalen Netzwerk.
Local 1:1 NAT	IP-Adresse vom lokalen Netzwerk, unter der das Netzwerk per 1:1 NAT aus dem Remote-Netz erreicht werden kann/soll.
Remote Connection	<p><b>Accept:</b> VPN-Verbindung wird von einer Gegenstelle aufgebaut und vom Router akzeptiert.</p> <p><b>Initiate:</b> VPN-Verbindung geht vom Router aus.</p> <p><b>Initiate on Input:</b> Startet / Stoppt den VPN-Tunnel durch digitalen Eingang.</p> <p><b>Initiate on SMS:</b> VPN-Verbindung wird durch eine SMS gestartet</p> <p><b>Initiate on Call:</b> VPN-Verbindung wird durch einen Anruf gestartet</p>
Autoreset	Kann bei "Initiate on SMS" und muss bei "Initiate on Call" festgelegt werden. Es wird ein Zeitraum festgelegt, nach wieviel Minuten die VPN-Verbindung per Autoreset gestoppt wird.

# VPN-IPsec

## Connection IKE

- Logout
- Device Information
- Status
- Local Network
- Wireless Network
- Network Security
- VPN
  - IPsec
    - Connections
    - Certificates
    - Status
  - OpenVPN
- I/O
- System

**CT-Router HSPA**

**IPsec - Internet Key Exchange Settings**

Name	vpn1
------	------

**Phase 1 ISAKMP SA**

ISAKMP SA Encryption	AES-128
ISAKMP SA Hash	all
ISAKMP SA Lifetime	3600 sec.

**Phase 2 IPsec SA**

IPsec SA Encryption	AES-128
IPsec SA Hash	all
IPsec SA Lifetime	28800 sec.

Perfect Forward Secrecy (PFS)	Yes
DH/PFS Group	2/modp1024
Rekey	Yes
Dead Peer Detection	Yes
DPD Delay	30 sec.
DPD Timeout	120 sec.

Settings
Apply

VPN → IPsec → Connections → IKE → Edit	
IKE	Erklärung
Name	Name der VPN-Verbindung.
<b>Phase 1 ISAKMP SA</b>	Schlüsselaustausch
ISAKMP SA Encryption	Verschlüsselungsalgorithmus-Auswahl
ISAKMP SA Hash	Hash-Algorithmus-Auswahl
ISAKMP SA Lifetime	Lebensdauer des ISAKMP SA Schlüssels. Standardeinstellung 3600 Sekunden (1 Stunde) max. Einstellwert 86400 Sekunden (24 Stunden)
<b>Phase 2 IPsec SA</b>	Datenaustausch
Ipsec SA Encryption	siehe ISAKMP SA Encryption
Ipsec SA Hash	siehe ISAKMP SA Hash
Ipsec Lifetime	Lebensdauer des Ipsec SA Schlüssels. Standardeinstellung 28800 Sekunden (8 Stunden) max. Einstellwert 86400 Sekunden (24 Stunden)

## VPN-IPsec

Perfect Forward Secrecy (PFS)	Aktivieren (=Yes) oder Deaktivieren (=No) der PFS Funktion.
DH/PFS Group	Im Ipsec werden beim Datenaustausch in bestimmten Intervallen die Schlüssel erneuert. Mit PFS werden hierbei mit der Gegenstelle im Schlüsselaustauschverfahren neue Zufallszahlen ausgehandelt. Auswahl des Verfahrens.
Dead Peer Detection	Unterstützt die Gegenstelle ein solches Protokoll, so kann überprüft werden, ob die Verbindung "tot" ist oder nicht. Die Verbindung wird versucht neu aufzubauen.  <b>No:</b> Keine Dead Peer Detection <b>Yes:</b> Bei VPN Initiate wird versucht, neuzustarten "Restart. Bei VPN Accept wird die Verbindung geschlossen "Clear".
DPD Delay (sec.)	Zeitintervall in Sekunden, in dem die Peer-Verbindung überprüft wird.
DPD Timeout (sec.)	Zeitspanne in Sekunden nach der ein Timeout erfolgen soll.

# VPN-IPsec

## Certificates

- Logout
- Device Information
- Status
- Local Network
- Wireless Network
- Network Security
- VPN
  - IPsec
    - Connections
    - Certificates**
    - Status
  - OpenVPN
- I/O
- System

**CT-Router HSPA**

---

**IPsec Certificates**

**Load Remote Certificate (.cer .crt)**

Upload  Keine Datei ausgewählt.

**Load Own PKCS#12 Certificate (.p12)**

Upload  Keine Datei ausgewählt.

Password

**Remote Certificates**

Name

**Own Certificates**

Name

VPN → IPsec → Certificates	
Certificates	Erklärung
Load Remote Certificate	Hochladen von Zertifikaten, mit denen eine Authentifizierung für den Router bei der VPN-Gegenstelle erfolgen kann.
Load Own PKCS#12 Certificate	Hochladen eines Zertifikats (Providervorgabe)
Password	Passwort für das PKCS#12 Zertifikat / das Passwort wird beim Export vergeben
Remote Certificates	Tabellarische Übersicht aller "Remote Certificates" / mit "Delete" wird ein Zertifikat gelöscht
Own Certificates	Tabellarische Übersicht aller "Own Certificates" / mit "Delete" wird ein Zertifikate gelöscht

# VPN-IPsec

## Status

- Logout
- Device Information
- Status
- Local Network
- Wireless Network
- Network Security
- VPN
  - IPsec
    - Connections
    - Certificates
    - Status
  - OpenVPN
- I/O
- System

### CT-Router HSPA

IPsec Status			
Active IPsec Connections			
Name	Remote Host	ISAKMP SA	IPsec SA

VPN → IPsec → Status	
Status	Erklärung
Name	Name der VPN-Verbindung
Remote Host	IP-Adresse oder URL der Gegenstelle
ISAKMP SA	Aktiv (grünes Feld)
IPSec SA	Aktiv (grünes Feld)

# VPN - OpenVPN

## OpenVPN

### Tunnel

- Logout
- Device Information
- Status
- Local Network
- Wireless Network
- Network Security
- VPN
  - IPsec
  - OpenVPN
    - Tunnel 1
    - Tunnel 2
    - Port Forwarding
    - Certificates
    - Static Keys
    - Status
- I/O
- System

CT-Router HSPA

OpenVPN Tunnel 1

VPN	Enabled <input type="button" value="v"/>
Name	tunnel1
Remote Host	<input type="text"/>
Remote Port	1194
Protocol	UDP <input type="button" value="v"/>
LZO Compression	Disabled <input type="button" value="v"/>
Allow Remote Float	<input type="checkbox"/>
Redirect Default Gateway	<input type="checkbox"/>
<input type="checkbox"/> Local Port	1194

Authentication	X.509 Certificate <input type="button" value="v"/>
Local Certificate	None <input type="button" value="v"/>
Check Remote Certificate Type	<input type="checkbox"/>
Connection NAT	None <input type="button" value="v"/>
Encryption	BLOWFISH 128 Bit <input type="button" value="v"/>

<input checked="" type="checkbox"/> Keep Alive	30 sec.
Restart	120 sec.

VPN → OpenVPN → Tunnel	
OpenVPN Tunnel	Erklärung
VPN	OpenVPN Tunnel aktiv (=Enable) oder inaktiv (=Disable)
Name	Name der OpenVPN-Verbindung
Remote Host	IP-Adresse oder URL der Gegenstelle
Remote Port	Port der Gegenstelle (Standard: 1194)
Protocol	UDP- oder TCP-Protokoll für die OpenVPN-Verbindung festlegen!
LZO Compression	<b>Disabled:</b> Keine Kompression <b>Adaptive:</b> Adaptive Kompression <b>Yes:</b> Kompression aktiviert
Allow Remote Float	Option: Bei der Kommunikation mit dynamischen IP-Adressen akzeptiert die OpenVPN-Verbindung authentifizierte Pakete von jeder IP-Adresse.
Local Port	Lokaler Port
Authentication	Authentifizierungsart der OpenVPN-Verbindung festlegen (X.509, PSK oder Username/Password)!

## VPN - OpenVPN

Local Certifacation	Zertifikat vom Router für die Authentifizierung bei der Gegenstelle
Check Remote Certificate Type	Option: Zertifikate der OpenVPN-Verbindung überprüfen
Address Local Network	IP-Adresse/Subnetzmaske des lokalen Netzwerks
Local 1:1 NAT	Option: IP-Adresse vom lokalen Netzwerk, unter der das Netzwerk per 1:1 NAT aus dem Remote-Netz erreicht werden kann/soll.
Encryption	Verschlüsselungsalgorithmus der OpenVPN-Verbindung
Keep Alive	Zeitintervall in Sekunden von Keep Alive-Anfragen an die Gegenstelle
Restart	Zeitspanne in Sekunden nach der die Verbindung neu gestartet werden soll, falls keine Antwort auf die Keep Alive-Anfragen erfolgt.

# VPN - OpenVPN

## Port Forwarding

**comtime**

- Logout
- Device Information
- Status
- Local Network
- Wide Area Network
- Network Security
- VPN
  - IPsec
  - OpenVPN
    - Tunnel 1
    - Tunnel 2
    - Port Forwarding**
    - Certificates
    - Static Keys
    - Status
- I/O
- System

**CT-Router LAN**

Port Forwarding						
Protocol	In Port	To IP	To Port	Masq	Comment	
TCP	80	192.168.0.6	1025	No		New
						Delete
Apply						

VPN → OpenVPN → Port Forwarding	
Port Forwarding	Erklärung
Protocol	Auswahl: TCP / UDP / ICMP
In Port	Port Nr. eingehende Verbindung
To IP	IP Adresse von Ziel
To Port	Port Nr. Vom Ziel

# VPN - OpenVPN

## Certificates

- Logout
- Device Information
- Status
- Local Network
- Wireless Network
- Network Security
- VPN
  - IPsec
  - OpenVPN
    - Tunnel 1
    - Tunnel 2
    - Port Forwarding
    - Certificates
    - Static Keys
    - Status
- I/O
- System

**CT-Router HSPA**

**OpenVPN Certificates**

**Load Own PKCS#12 Certificate (.p12)**

Upload  Keine Datei ausgewählt.

Password

**Load CA Certificate (.crt)**

Upload  Keine Datei ausgewählt.

**Own Certificates**

Name

**CA Certificates**

Name

VPN → OpenVPN → Certificates	
OpenVPN Certificates	Erklärung
Load Own PKCS#12 Certificate	Hochladen eines Zertifikats, das von Ihrem Provider stammt.
Password	Passwort für das PKCS#12 Zertifikat. Das Passwort wird beim Export vergeben.
Own Certificates	Tabellarische Übersicht aller "Own Certificates" / mit "Delete" werden die Zertifikate gelöscht

## VPN - OpenVPN

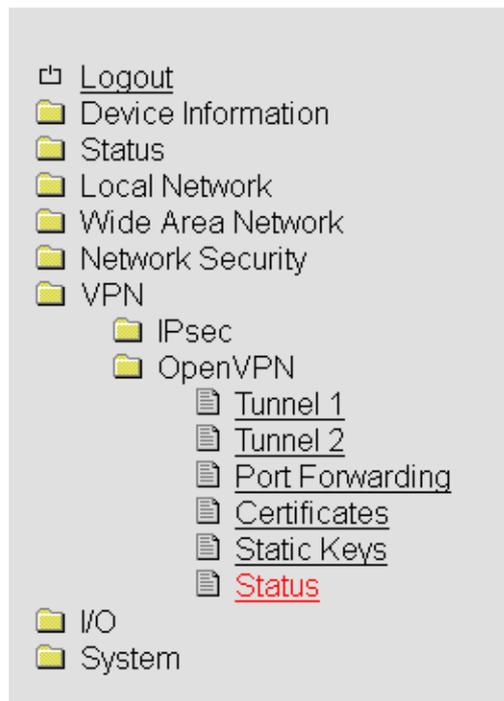
### Static Keys

The screenshot shows the web interface for configuring OpenVPN static keys on a CT-Router HSPA. On the left is a navigation menu with categories like Logout, Device Information, Status, Local Network, Wireless Network, Network Security, VPN, IPsec, OpenVPN, Tunnel 1, Tunnel 2, Port Forwarding, Certificates, Static Keys (highlighted), and Status. Below these are I/O and System sections. The main content area is titled 'CT-Router HSPA' and contains three sections: 'OpenVPN static Keys' with a 'Generate static Key' button and a 'Save' button; 'Load static Key' with an 'Upload' button, a file selection field showing 'Keine Datei ausgewählt', and an 'Apply' button; and 'Static Keys' with a 'Name' label.

VPN → OpenVPN → Static Keys	
Static Keys	Erklärung
Generate static Key	Einen statischen Schlüssel generieren und speichern.
Load static Key	Statischen Schlüssel in den Router laden (den gleichen statischen Schlüssel muss auch die Gegenstelle besitzen).
Static Keys	Tabellarische Übersicht aller geladenen statischen Schlüssel.

## VPN - OpenVPN

### Status



#### CT-Router LAN

OpenVPN Status		
Active OpenVPN Connections		
Name	Remote Host	Status
tunnel1	83.169.36.106:1194	

VPN → OpenVPN → Status	
OpenVPN Status	Erklärung
Name	Name der VPN-Verbindung
Remote Host	IP-Adresse oder URL der Gegenstelle
Status	Aktiv (=grünes Feld)

## I/O

Der CT-Router HSPA verfügt über vier digitale Ein- und Ausgänge, die in dem „I/O“-Menü von Ihnen konfiguriert werden können.

### Inputs

I/O → Inputs	
Inputs	Erklärung
High	Option: Bei einem High-Pegel kann eine Nachricht per SMS oder E-Mail verschickt werden.
Low	Option: Bei einem Low-Pegel kann eine Nachricht per SMS oder E-Mail verschickt werden.

Stellt man nun eine der oben dargestellten Optionen ein, so muss man diese mit "apply" bestätigen. Erst dann können die Einstellungen für die Benachrichtigung editiert werden.

SMS: Eine oder mehrere Rufnummern werden aus dem eingespeicherten Telefonbuch selektiert, und Sie können einen individuellen Nachrichtentext festlegen.

E-Mail: Sie können einen Empfänger, einen Kopie-Empfänger, einen Betreff und einen Nachrichtentext festlegen.

### Schalteingänge anschließen

- Schließen Sie die Schalteingänge an den jeweiligen steckbaren Schraubklemmen an.
- An die Schalteingänge (I1 ... I4) können Sie 10 ... 30 V DC anschließen.
- Das 0-V-Potential der Schalteingänge müssen Sie an die "0 V" Klemme des Spannungs-Anschlusses anschließen.

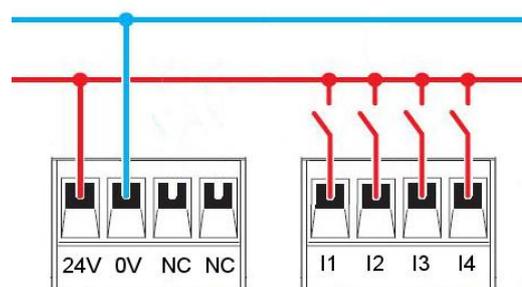


Bild Verdrahtung der Eingänge

## Outputs

- Logout
- Device Information
- Status
- Local Network
- Wireless Network
- Network Security
- VPN
- I/O
  - Inputs
  - Outputs
  - Phonebook
  - Socket Server
- System

### CT-Router HSPA

**Outputs**

#1	<input type="button" value="On"/>		Manual	▼
off	<input type="checkbox"/> Autoreset		10	min.
#2	<input type="button" value="Off"/>		Remote Controlled	▼
on	<input checked="" type="checkbox"/> Autoreset		10	min.
#3	<input type="button" value="On"/>		Packet Service	▼
off	<input type="checkbox"/> Autoreset		10	min.
#4	<input type="button" value="Off"/>		Incoming Call	▼
on	<input type="checkbox"/> Autoreset		10	min.

I/O → Outputs	
Outputs	Erklärung
Optionen	<p><b>Manual:</b> An- / Ausschalten erfolgt manuell über das WBM</p> <p><b>Remote Controlled:</b> An- / Ausschalten per SMS oder Socket Server. Zusätzlich kann die Funktion Autoreset genutzt werden, bei der eine Zeitspanne in Minuten festgesetzt wird.</p> <p><b>Radio Network:</b> Ausgang wird geschaltet, falls der Router sich in ein Mobilfunknetz einklinkt.</p> <p><b>Paket Service:</b> Ausgang wird geschaltet, falls der Router eine Paket-Verbindung aufbaut und eine IP-Adresse vom Provider zugewiesen bekommen hat.</p> <p><b>VPN Service:</b> Ausgang wird geschaltet, falls eine VPN-Verbindung besteht.</p> <p><b>Incoming Call:</b> Ausgang wird geschaltet, falls der Router angerufen wird und die Rufnummer im Telefonbuch steht.</p> <p><b>Connection Lost:</b> Der Ausgang wird geschaltet, falls eine Verbindung abbricht.</p>
Autoreset	Zeitraum in Minuten festlegen, nachdem der Ausgang zurückgesetzt wird.

Die kurzschlussfesten Schaltausgänge (O1 ... O4) sind für maximal 150 mA bei 10 ... 30 V DC ausgelegt.

Das 0-V-Potential der Schaltausgänge müssen Sie an die "0 V" Klemme des Spg-Anschlusses anschließen

## I/O

## Phonebook

- ☐ Logout
- 📁 Device Information
- 📁 Status
- 📁 Local Network
- 📁 Wireless Network
- 📁 Network Security
- 📁 VPN
- 📁 I/O
  - 📄 Inputs
  - 📄 Outputs
  - 📄 **Phonebook**
  - 📄 Socket Server
- 📁 System

**CT-Router HSPA**

**SMS Phonebook**

#1	<input type="text" value="1234567890"/>	#11	<input type="text"/>
#2	<input type="text"/>	#12	<input type="text"/>
#3	<input type="text"/>	#13	<input type="text"/>
#4	<input type="text"/>	#14	<input type="text"/>
#5	<input type="text"/>	#15	<input type="text"/>
#6	<input type="text"/>	#16	<input type="text"/>
#7	<input type="text"/>	#17	<input type="text"/>
#8	<input type="text"/>	#18	<input type="text"/>
#9	<input type="text"/>	#19	<input type="text"/>
#10	<input type="text"/>	#20	<input type="text"/>

I/O → Phonebook	
Phonebook	Erklärung
#1 ... #20	Rufnummern für I/O Input und I/O Output

## Socket Server

- ☐ Logout
- 📁 Device Information
- 📁 Status
- 📁 Local Network
- 📁 Wireless Network
- 📁 Network Security
- 📁 VPN
- 📁 I/O
  - 📄 Inputs
  - 📄 Outputs
  - 📄 Phonebook
  - 📄 Socket Server
- 📁 System

**CT-Router HSPA**

**Socket Configuration**

Socket Server	Enabled ▾
Server Port (default 1432)	1432

I/O → Socket Server	
Socket Server	Erklärung
Socket Server	<p><b>Disable:</b> Ansteuern des Routers über Ethernet deaktiviert</p> <p><b>Enable:</b> Ansteuern des Routers über Ethernet aktiviert</p>
Server Port (default 1432)	<p>Socket Server Port festlegen (Port 80 kann nicht genutzt werden). Daten, die an den Router geschickt werden, müssen XML Version 1.0 konform sein.</p> <p>Beispiel:</p> <pre>&lt;?xml version="1.0"?&gt; &lt;io&gt; &lt;input no="1" value="on"&gt; &lt;output no="2" value="off"&gt; &lt;output no="3" /&gt; &lt;/io&gt;</pre>

# System

Im Systemmenü können allgemeine Einstellungen für den CT-Router HSPA getroffen werden.

## Web Configuration

The screenshot shows the CT-Router HSPA web interface. On the left is a navigation menu with the following items: Logout, Device Information, Status, Local Network, Wireless Network, Network Security, VPN, I/O, and System. Under the System menu, several sub-items are listed: Web Configuration (highlighted in red), User, Log Configuration, Log-File, SMTP Configuration, Configuration, Up-/Download, RTC, Reboot, and Firmware Update. On the right, the 'Web Configuration' settings page is displayed, featuring a 'Server Port (default 80)' input field with the value '80' and an 'Apply' button below it.

System → Web Configuration	
Web Configuration	Erklärung
Server Port (default 80)	Porteinstellung für WBM über Internetbrowser.

# System

## User

- Logout
- Device Information
- Status
- Local Network
- Wireless Network
- Network Security
- VPN
- I/O
- System
  - Web Configuration
  - User**
  - Log Configuration
  - Log-File
  - SMTP Configuration
  - Configuration
  - Up-/Download
  - RTC
  - Reboot
  - Firmware Update

**CT-Router HSPA**

**User Setup**

**admin**

Old password

New password

Retype new password

---

**user**

Old password

New password

Retype new password

System → User	
User	Erklärung
admin	Uneingeschränkter Zugriff (Schreiben und Lesen) Neues Passwort festlegen
user	Eingeschränkter Zugriff (nur Lesen / nicht alle Bereiche) Neues Passwort festlegen

# System

## Log Configuration

- Logout
- Device Information
- Status
- Local Network
- Wireless Network
- Network Security
- VPN
- I/O
- System
  - Web Configuration
  - User
  - Log Configuration
  - Log-File
  - SMTP Configuration
  - Configuration
  - Up-/Download
  - RTC
  - Reboot
  - Firmware Update

**CT-Router HSPA**

**Log Configuration**

Remote UDP Logging	Disabled ▾
Server IP Address	192.168.0.200
Server Port (default 514)	514
Non volatile Log	Disabled ▾

System → Log Configuration	
Log Configuration	Erklärung
Remote UPD Logging	<b>Disabled:</b> Externes Logging deaktiviert <b>Enabled:</b> Externes Logging aktiviert
Server IP Address	IP-Adresse vom externen Log-Server
Server Port (default 514)	Port vom externen Log-Server
Non volatile Log	<b>Disable:</b> Speichert das Log intern auf einem vorher festgelegten Server. <b>USB-Stick:</b> Speichert das Log auf einem USB-Stick. Der USB-Stick muss am Router angeschlossen werden! <b>SD-Card:</b> Speichert das Log auf einer SD-Karte.

## Log-File

- ▢ Logout
- ▢ Device Information
- ▢ Status
- ▢ Local Network
- ▢ Wireless Network
- ▢ Network Security
- ▢ VPN
- ▢ I/O
- ▢ System
  - ▢ Web Configuration
  - ▢ User
  - ▢ Log Configuration
  - ▢ Log-File
  - ▢ SMTP Configuration
  - ▢ Configuration
  - ▢ Up-/Download
  - ▢ RTC
  - ▢ Reboot
  - ▢ Firmware Update

**CT-Router HSPA**

**Log-File**

Clear
View
Save

```

Aug 27 10:00:33 atomlab kernel: imklog 5.8.3, log source = /proc/kmsg stc
Aug 27 10:00:33 atomlab rsyslogd: [origin software="rsyslogd" swVersion="
Aug 27 10:00:33 atomlab kernel: [ 0.000000] Initializing cgroup subsys
Aug 27 10:00:33 atomlab kernel: [ 0.000000] Initializing cgroup subsys
Aug 27 10:00:33 atomlab kernel: [ 0.000000] Linux version 3.0.0-1-686-
Aug 27 10:00:33 atomlab kernel: [ 0.000000] Disabled fast string opere
Aug 27 10:00:33 atomlab kernel: [ 0.000000] BIOS-provided physical RAM
Aug 27 10:00:33 atomlab kernel: [ 0.000000] BIOS-e820: 00000000000000C
Aug 27 10:00:33 atomlab kernel: [ 0.000000] BIOS-e820: 0000000000008fC
Aug 27 10:00:33 atomlab kernel: [ 0.000000] BIOS-e820: 000000000000e0C
Aug 27 10:00:33 atomlab kernel: [ 0.000000] BIOS-e820: 00000000000100C
Aug 27 10:00:33 atomlab kernel: [ 0.000000] BIOS-e820: 0000000003f534C
Aug 27 10:00:33 atomlab kernel: [ 0.000000] BIOS-e820: 0000000003f53cC
Aug 27 10:00:33 atomlab kernel: [ 0.000000] BIOS-e820: 0000000003f5cdC
Aug 27 10:00:33 atomlab kernel: [ 0.000000] BIOS-e820: 0000000003f5d1C
Aug 27 10:00:33 atomlab kernel: [ 0.000000] BIOS-e820: 0000000003f660C
Aug 27 10:00:33 atomlab kernel: [ 0.000000] BIOS-e820: 0000000003f6f0C
Aug 27 10:00:33 atomlab kernel: [ 0.000000] BIOS-e820: 0000000003f6f2C

```

System → Log-File	
Log-File	Erklärung
Clear	Einträge im internen Log-File werden gelöscht
View	Log-File Einträge werden im Browser-Fenster angezeigt
Save	Log-File wird gespeichert

# System

## ComSERVER - Serielle Schnittstelle konfigurieren (optional)

The screenshot shows the configuration page for the ComSERVER serial interface on a CR-230 UR router. The left-hand navigation pane lists various system settings, with 'System' expanded to show 'ComSERVER' in red. The main configuration area contains the following settings:

- Status: Enabled
- Connection Type: Server RAW
- Server Port (default 3001): 3001
- Baud rate: 115200
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: RTS/CTS

An 'Apply' button is located at the bottom of the configuration form.

System → ComSERVER	
ComSERVER	Erklärung
Status	Schnittstelle: Disabled / Enabled
Connection Type	Einstellen der seriellen Verbindung – RAW oder RFC2217
Server Port (default 3001)	Auswahl des Ports für die Netzkommunikation
Baud Rate	300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 Baud
Data bits	Datenformat einstellen: Wählen Sie die Einstellungen für Datenbits, Parität und Stopbits
Parity	
Stop bits	
Flow control	Art der Flusskontrolle auswählen

### Zusammenfassung der Übertragungsparameter:

Baudrate:	110, 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200
Anzahl der Datenbits:	7 oder 8
Anzahl der Stopbits:	1 oder 2
Parität:	none, even, odd,
Flusssteuerung:	RTS/CTS, XON/XOF, RS485 RTS oder keine

## SMTP Configuration

- ☐ Logout
- 📁 Device Information
- 📁 Status
- 📁 Local Network
- 📁 Wireless Network
- 📁 Network Security
- 📁 VPN
- 📁 I/O
- 📁 System
  - 📄 Web Configuration
  - 📄 User
  - 📄 Log Configuration
  - 📄 Log-File
  - 📄 **SMTP Configuration**
  - 📄 Configuration
  - 📄 Up-/Download
  - 📄 RTC
  - 📄 Reboot
  - 📄 Firmware Update

**CT-Router HSPA**

**SMTP Configuration**

SMTP Server	<input style="width: 90%;" type="text"/>
Server Port (default 25)	<input style="width: 80%;" type="text" value="25"/>
Transport Layer Security	<input style="width: 80%;" type="text" value="None"/>
Authentication	<input style="width: 80%;" type="text" value="Plain Password"/>
<input style="width: 90%;" type="text" value="Username"/>	
<input style="width: 90%;" type="text" value="Password"/>	
<input style="width: 90%;" type="text" value="From"/>	
<input type="button" value="Apply"/>	

System → SMTP Configuration	
SMTP Configuration	Erklärung
SMTP Server	IP-Adresse / Hostname des SMTP Servers
SMTP Port (default 25)	Port des SMTP Servers
Transport Layer Security	Verschlüsselung: Keine, STARTTLS, SSL/TLS
Authentication	No authentication: Keine Authentifizierung Plain Password: Authentifizierung Benutzername und Passwort (unverschlüsselte Übertragung der Authentifizierungsdaten). Encrypted Password: Authentifizierung mit Benutzername und Passwort (verschlüsselte Übertragung der Authentifizierungsdaten)
Username	Benutzername
Password	Passwort
From	Absender der Mail

# System

## Configuration Up-/Download

- Logout
- Device Information
- Status
- Local Network
- Wireless Network
- Network Security
- VPN
- I/O
- System
  - Web Configuration
  - User
  - Log Configuration
  - Log-File
  - SMTP Configuration
  - Configuration Up-/Download
  - RTC
  - Reboot
  - Firmware Update

**CT-Router HSPA**

**Configuration Up-/Download**

Download  XML-Format Save

Upload  Keine Datei ausgewählt. Apply

Reset to Factory Defaults Apply

System → Configuration Up-/Download	
Up-/Download	Erklärung
Download	Aktuelle Konfigurationen herunterladen
Upload	Gesicherte oder veränderte Konfigurationen hochladen und mit "apply" bestätigen.
Reset to Factory Defaults	Konfigurationen und IP-Einstellungen auf Werkeinstellung zurücksetzen. Hochgeladene Zertifikate bleiben erhalten.

# System

## RTC

- Logout
- Device Information
- Status
- Local Network
- Wireless Network
- Network Security
- VPN
- I/O
- System
  - Web Configuration
  - User
  - Log Configuration
  - Log-File
  - SMTP Configuration
  - Configuration
  - Up-/Download
  - RTC
  - Reboot
  - Firmware Update

**CT-Router HSPA**

---

**Real Time Clock (RTC)**

---

New Time

---

Timezone

Daylight saving time

---

NTP Synchronisation

NTP Server  Local

**Time Server for Local Network**

Time Server

System → RTC	
RTC	Erklärung
New Time	Manuelle Zeitkonfiguration, falls kein NTP-Server vorhanden ist.
Timezone	Zeitzonenauswahl
Daylight saving time	<b>Disable:</b> Sommerzeitberücksichtigung deaktiviert <b>Enable:</b> Sommerzeitberücksichtigung aktiviert
NTP Synchronisation	Datum und Uhrzeit können mit einem NTP-Server synchronisiert werden. Bei Erstverwendung dieser Funktion kann die erste Synchronisation bis zu 15 Minuten dauern.
NTP Server	Im LAN-Netzwerk kann der Router als NTP-Server eingestellt werden. Es wird hierzu eine Adresse von einem NTP-Server benötigt. Die NTP Synchronisation muss auf Enable gestellt werden.
Time Server	<b>Disable:</b> Zeitserverfunktion für das lokale Netzwerk deaktiviert <b>Enable:</b> Zeitserverfunktion für das lokale Netzwerk aktiviert

# System

## Reboot

- Logout
- Device Information
- Status
- Local Network
- Wireless Network
- Network Security
- VPN
- I/O
- System
  - Web Configuration
  - User
  - Log Configuration
  - Log-File
  - SMTP Configuration
  - Configuration
  - Up-/Download
  - RTC
  - Reboot
  - Firmware Update

**CT-Router HSPA**

---

**Reboot**

Daily reboot	Sun	Mon	Tue	Wed	Thu	Fri	Sat
	<input type="checkbox"/>						

Time

Event

System → Reboot	
Reboot	Erklärung
Reboot NOW!	Sofortigen Neustart des Routers erzwingen!
Daily reboot	Den Router an bestimmten Wochentagen zum bestimmten Zeitpunkt neustarten. Mit Klicken auf die Kontrollkästchen legen Sie die Wochentage für den Neustart fest.
Time	Uhrzeit des Neustarts (Stunde:Minute)
Event	Router kann mit digitalem Eingang neugestartet werden. Signal sollte nach einem Neustart wieder "Low" sein.

# System

## Firmware Update

- Logout
- Device Information
- Status
- Local Network
- Wireless Network
- Network Security
- VPN
- I/O
- System
  - Web Configuration
  - User
  - Log Configuration
  - Log-File
  - SMTP Configuration
  - Configuration
  - Up-/Download
  - RTC
  - Reboot
  - Firmware Update

**CT-Router HSPA**

**Firmware Update Modem**

Upload  Keine Datei ausgewählt.

**Update Web Based Management**

Upload  Keine Datei ausgewählt.

System → Firmware Update	
Reboot	Erklärung
Firmware Update Modem	Diese Updates sorgen für Funktionserweiterungen und Produktaktualisierungen.
Update Web Based Management	Diese Updates beziehen sich auf die Konfiguration über einen Internetbrowser.

## Abfrage und Steuerung über XML Dateien

### Format der XML Dateien

Jede Datei beginnt mit dem Header:

```
<?xml version="1.0"?>
```

oder

```
<?xml version="1.0" encoding="UTF-8"?>
```

Gefolgt von dem Basis-Eintrag. Folgende Basis-Einträge stehen zur Auswahl:

<code>&lt;io&gt;</code>	<code>&lt;/io&gt;</code>	# E/A-System
<code>&lt;info&gt;</code>	<code>&lt;/info&gt;</code>	# Allgemeine Informationen abfragen
<code>&lt;cmgr ...&gt;</code>	<code>&lt;/cmgr&gt;</code>	# SMS versenden (nur Mobilfunkgeräte)
<code>&lt;email ...&gt;</code>	<code>&lt;/email&gt;</code>	# eMail versenden

Alle Daten werden in UTF-8 kodiert. Folgende Zeichen müssen als Sequenzen übertragen werden:

& - `&amp;`;

< - `&lt;`;

> - `&gt;`;

" - `&quot;`;

' - `&apos;`;

### Beispiele zu den Basis-Einträgen:

#### a) E/A System

```
<?xml version="1.0"?>
```

```
<io>
```

```
<output no="1"/> # Zustand von Ausgang 1 abfragen
```

```
<output no="2" value="on"/> # Ausgang 2 einschalten
```

```
<input no="1"/> # Zustand von Eingang 1 abfragen
```

```
</io>
```

Hinweis: Als "value" kann sowohl on/off als auch 0/1 angegeben werden.

Zurückgegeben wird immer on oder off.

Zurückgeliefert wird etwa folgendes:

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<result>
```

```
<io>
```

```
<output no="1" value="off"/> # Zustand von Ausgang 1; hier eingeschaltet
```

```
<output no="2" value="on"/> # Zustand von Ausgang 2; wurde eingeschaltet
```

```
<input no="1" value="off"/> # Zustand von Eingang 1; hier ausgeschaltet
```

```
</io>
```

```
</result>
```

Zu beachten ist, dass Ausgänge, welche ferngesteuert werden sollen, als "Remote Controlled" konfiguriert sein müssen

## Abfrage und Steuerung über XML Dateien

### b) Allgemeine Informationen abfragen

```
<?xml version="1.0"?>
<info>
<device />          # Gerätedaten abfragen
<radio />          # Daten zur Funkverbindung abfragen (nur Mobilfunkgeräte)
</info>
```

Zurückgeliefert wird etwa folgendes:

```
<?xml version="1.0" encoding="UTF-8"?>
<result>
<info>
<device>
<serialno>13120004</serialno>
<hardware>A</hardware>
<firmware>1.00.4-beta</firmware>
<wbm>1.34.8</wbm>
<imei>359628040604790</imei>
</device>
<radio>
<provider>Vodafone.de</provider>
<rssi>15</rssi>
<creg>1</creg>
<lac>0579</lac>
<ci>26330CD</ci>
<packet>0</packet>
</radio>
</info>
</result>
```

### c) SMS versenden

```
<?xml version="1.0"?>
<cmgs destaddr="0123456789">Dies ist der SMS-Text</cmgs>
```

Zurückgeliefert wird etwa folgendes:

```
<?xml version="1.0" encoding="UTF-8"?>
<result>
<cmgs length="98">SMS accepted</cmgs>
</result>
```

### d) eMail versenden

```
<?xml version="1.0"?>
<email to="x.yz@diesunddas.de" cc="info@andere.de">
<subject>Test Mail</subject>
<body>
  Dies ist ein mehrzeiliger eMail-Text.
  mfg. ihr Router
</body>
</email>
```

## Abfrage und Steuerung über XML Dateien

Zurückgeliefert wird etwa folgendes:

```
<?xml version="1.0" encoding="UTF-8"?>
<result>
<email>done</email>
</result>
```

oder im Fehlerfall:

```
<?xml version="1.0" encoding="UTF-8"?>
<result>
<email error="3">transmisson failed</email>
</result>
```

Hinweis zur Darstellung: die Einrückungen und Zeilenumbrüche dienen nur der Verständlichkeit und müssen so nicht gesendet werden, noch werden sie so gesendet. Alle empfangenen Daten sollten mit einem XML-Parser wie z.B. Expat interpretiert werden.

### Daten senden und empfangen

Der Kommunikationsablauf ist folgender:

- Verbindung zum Socket-Server aufbauen
- Daten senden
- Zurückgegebene Daten mit XML-Parser interpretieren
- Verbindung schließen

## Funktions-Test

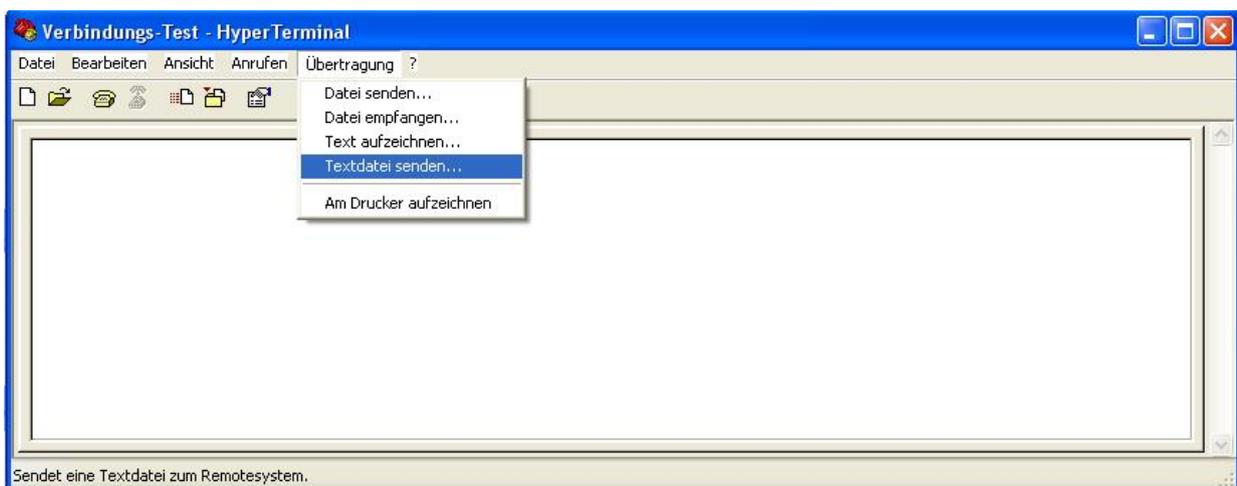
### Funktions-Test mittels Windows Hyperterminal

Für einen Test kann unter Windows das bekannte Programm „Hyperterminal“ verwendet werden. Über Hyperterminal können XML-Dateien an den Socket Server des Routers gesendet werden. Die entsprechenden XML-Dateien (siehe Kapitel „Abfrage und Steuerung über XML Dateien“) müssen dafür vorab auf Ihren Bediener-PC gespeichert worden sein. Öffnen Sie Hyperterminal und konfigurieren Sie die gewünschte Verbindung (Hier ein Beispiel unter der Verwendung von Default-Einstellungen):

**Hostadresse:** 192.168.0.1 (IP-Adresse des Routers / Socket Servers)  
**Anschlussnummer:** 1432 (Port des Socket Servers)  
**Verbindung herstellen über:** TCP/IP (Winsock)



Öffnen Sie die Verbindung und wählen Sie im Menü von Hyperterminal „Übertragung / Textdatei senden....“ die zu übertragende XML-Datei aus.



Nach der erfolgreichen Übertragung erhalten Sie die Antwort auf Ihre Anfrage.

## Applikationsbeispiele

### Eine Verbindung zum Internet herstellen

Mit dem IKOM-ROUTER haben Sie via Mobilfunknetz den Zugang zum Internet. Es wird eine SIM-Karte eines Mobilfunknetzbieners benötigt, die für Paketdaten-Dienste, zum Beispiel GPRS/EDGE oder UMTS/HSPDA, freigeschaltet ist.

Der IKOM-ROUTER ist bei dieser Applikation:

- Router
- Default Gateway
- DNS-Server
- Firewall

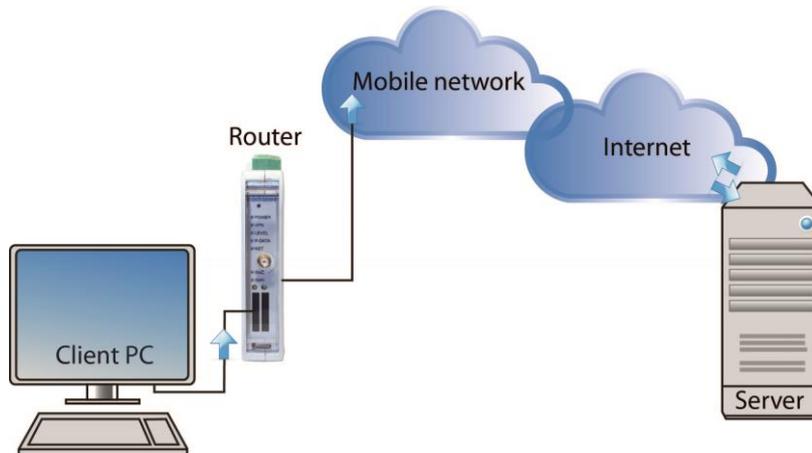


Bild: Zugang zum Internet

Vor dem Start prüfen Sie ob ausreichende Netzabdeckung durch Ihren Provider zur Verfügung steht, nur dann können Datenverbindungen aufgebaut werden.

### ROUTER konfigurieren:

- Öffnen Sie auf dem PC einen Browser.
- IP-Adresse im Adressfeld des Browsers eingeben (default 192.168.0.1)
- Benutzername und Kennwort eingeben (Default: Benutzername „admin“ und Kennwort „admin“)
- Öffnen Sie „Wireless Network“ und „SIM“ und tragen Sie in das Feld „PIN“ die PIN-Nummer der SIM-Karte ein. Tragen Sie zusätzlich die Zugangsdaten, APN, Username und Password für die Paketdatenübertragung in Ihrem Mobilfunknetz ein. Die Zugangsdaten erhalten Sie von Ihrem Mobilfunkanbieter.

Das Bild zeigt die Web-Oberfläche des comtime CT-Router HSPA. Die linke Seite zeigt ein Navigationsmenü mit den folgenden Optionen: Logout, Device Information, Status, Local Network, Wireless Network (Radio Setup, SIM, Backup SIM, SMS Configuration, Packet Data Setup, Static Routes, DynDNS, Connection Check), Network Security, VPN, I/O, System. Die rechte Seite zeigt die Konfiguration der SIM-Karte mit folgenden Feldern:

SIM	
Country	Germany [Set]
PIN	[ ]
Roaming	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Provider	Auto [ ]
Username	[ ]
Password	[ ]
APN	web.vodafone.de
Authentication	All Protocols [ ]
[ Apply ]	

## Applikationsbeispiel

- Wechseln Sie zu „Wireless Network“ und „Packed Data Setup“ und aktivieren Sie die Paketdatenübertragung im Mobilfunknetz.  
Setzen Sie dazu „Packet Data“ auf „Enable“.

**comtime**

**CT-Router HSPA**

**Packet Data Setup**

Packet Data	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Debug Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Allow Compression	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
MTU (default 1500)	1500
Event	Initiate
Manual DNS	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
DNS Server	0.0.0.0
Sec. DNS Server	0.0.0.0

Apply

- Damit Sie von Ihrem PC ins Internet gelangen, müssen Sie in den Netzwerkeinstellungen die IP-Adresse des Routers als Default-Gateway und als DNS-Server eintragen.  
Die Einstellungen für Ihr Betriebssystem finden Sie in der entsprechenden Dokumentation

**Eigenschaften von Internetprotokoll (TCP/IP)**

Allgemein

IP-Einstellungen können automatisch zugewiesen werden, wenn das Netzwerk diese Funktion unterstützt. Wenden Sie sich andernfalls an den Netzwerkadministrator, um die geeigneten IP-Einstellungen zu beziehen.

IP-Adresse automatisch beziehen

Folgende IP-Adresse verwenden:

IP-Adresse: 192 . 168 . 0 . 5

Subnetzmaske: 255 . 255 . 255 . 0

Standardgateway: 192 . 168 . 0 . 1

DNS-Serveradresse automatisch beziehen

Folgende DNS-Serveradressen verwenden:

Bevorzugter DNS-Server: 192 . 168 . 0 . 1

Alternativer DNS-Server: . . .

Erweitert...

OK Abbrechen