comtime

CT-Router LAN

user manual

Copyright © comtime GmbH

Copyright Statement
The contents of this publication are protected by copyright. Translations, reprints, reproduction and storage in data processing systems require the express permission of comtime GmbH.

comtime GmbH
Gutenbergring 22
22848 Norderstedt
Germany

Tel: +49 (0)40 55 44 89 40
Fax: +49 (0)40 55 44 89 45

Internet: http://www.comtime-com.de
email: support@comtime-com.de

Subject to technical alterations.

All trademarks and product designations are trademarks, registered trademarks or product designations of their respective owners.
comtime GmbH provides all goods and services on the basis of the General Terms and Conditions of comtime GmbH currently valid. All information is based on information provided by the manufacturer(s). No responsibility or liability will be assumed for incorrect or missing entries. The descriptions of the specifications in this manual do not constitute an agreement.

Product no: 266-000

Content

Content

Technical data

Supply	
Supply voltage	10 V DC ... 30 V DC via plugable screw terminals
Nominal current consumption	< 90mA at 24V
LED display	Power (LED green) Continuous light: Operation

Protocols / Interfaces	
Protocols / services	DHCP-Server, HTTP-Server, FTP, NAT, Firewall, SMS, OpenVPN, IPSec, DynDNS, NTP
VPN	Secure data encryption with IPSec and Open VPN (including X.509 support)
Ethernet interface	
Connection	2 x RJ45 socket, shielded
Transmission rate	10/100 MBit/s
Supported protocols	TCP/IP, UDP/IP, FTP, HTTP
Auxiliary protocols	ARP, DHCP, PING(ICMP), SNMP V1, SMTP
LED display / control signal	ACT (LED yellow), Ethernet data transmission
	LINK (LED green), Ethernet link established
Serial interface	optional
I/O	4 inputs, 4 outputs via plugable screw terminals

Physical features	
Size (HxWxD)	101x116 x22,5 mm
Environmental temperature	Operation -25...+70°C, Storage -40 …+85°C
Humidity	0...95% (not condensing)
Protection class	IP30

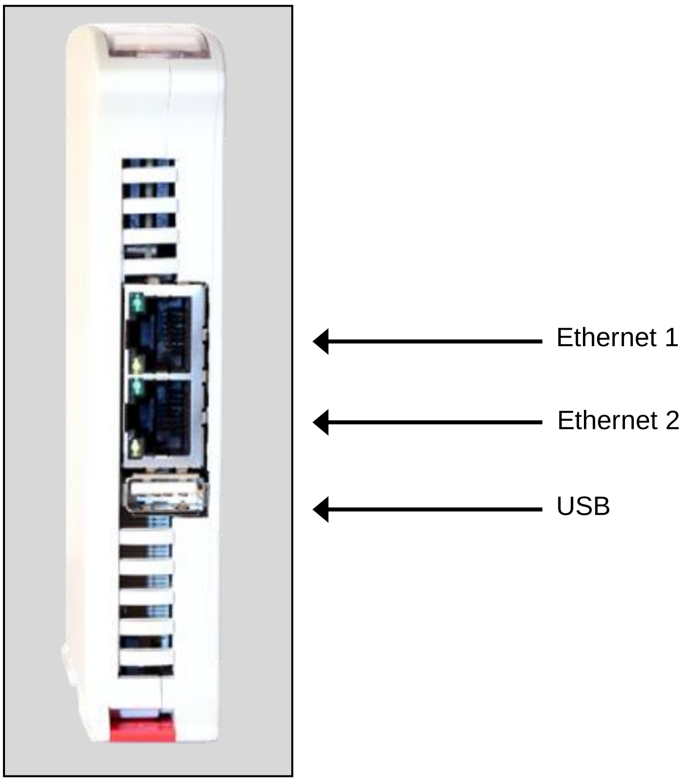
CE conformity according to R&TTE directive 1999/5/EC	
EMV	EN 61000-6-2, EN55022 Class A
Safety	EN 60950
Radio	EN 301511

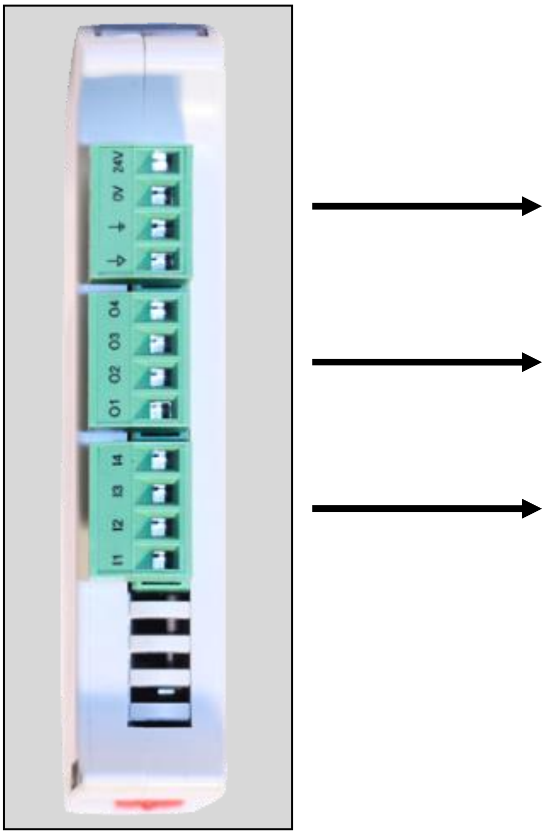
Certifications	
UL, USA / Kanada	in processing

Technical changes reserved

Hardware installation

Terminal assignment





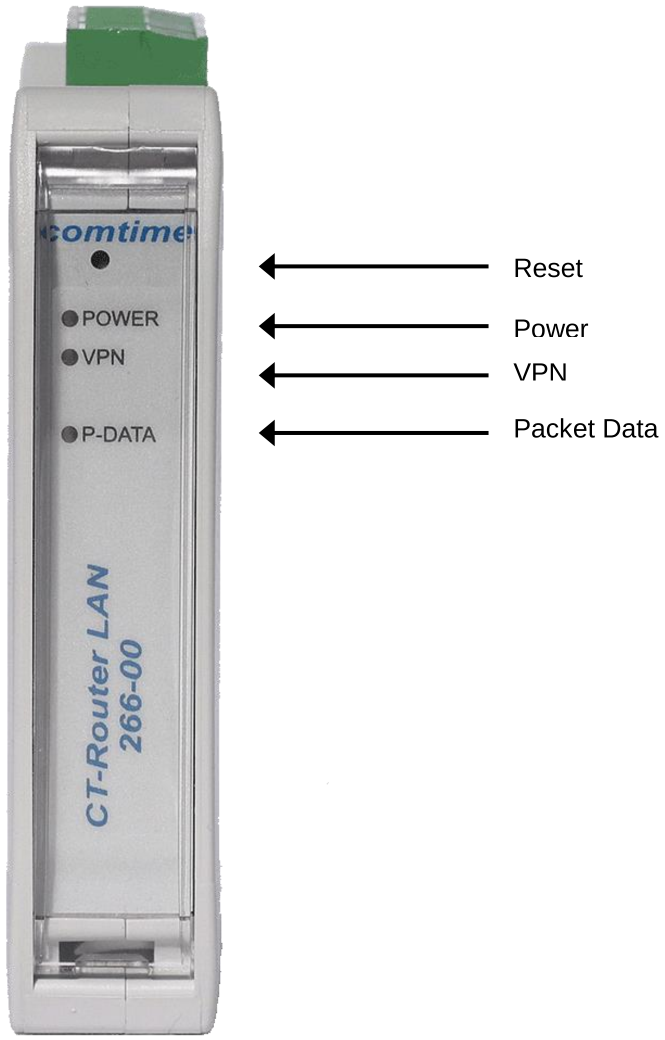
Supply voltage
10V - 30V DC
0V
NC
NC

Digital output
O4
O3
O2
O1

Digital input
I4
I3
I2
I1

Hardware installation

LED indicators



LED Router HSPA	
LED	Explanation

Package Data	Off = no connection
	Flashing = modem connection
	On = package data connection

VPN	Off = no VPN connection
	On = VPN connection activated

Power	Off = no power supply
	On = power supply activated

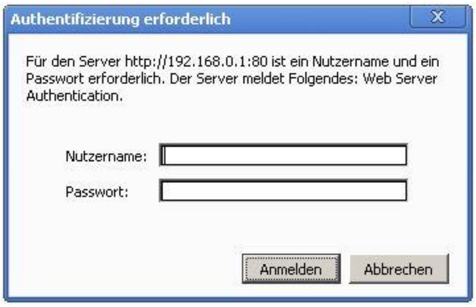
Configuration WBM

The configuration of the CT-Router is performed via a Web browser based function. To do so, first fulfil the following conditions:

- The PC which is used for the configuration of the router is equipped with a LAN interface.
- A Web browser (e.g. Google Chrome, Mozilla Firefox, Microsoft IE) is installed on the PC.
- The router is connected to a voltage source.

Starting the configuration

1. Establish an Ethernet connection between the PC and the router.
2. Adjust the IP address of the LAN interface to the network of the router.
3. Open Web browser.
4. Enter the IP address of the router (192.168.0.1) into the address field of the browser and confirm by pressing the Enter key. Then user name/password request is performed.


Authentifizierung erforderlich

Für den Server http://192.168.0.1:80 ist ein Nutzername und ein Passwort erforderlich. Der Server meldet Folgendes: Web Server Authentication.

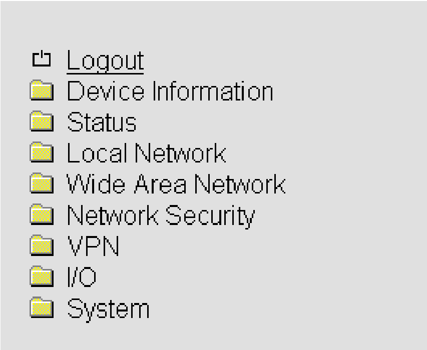
Upon delivery the user name is "admin" and the password is "admin" (it is described later on how to change the password).

Furthermore, there are two user levels:

- User: Read access on "Device information".
- Admin: Read and write access to all areas.

After having entered the user name and the password the main menu will open up to configure the CT-Router.

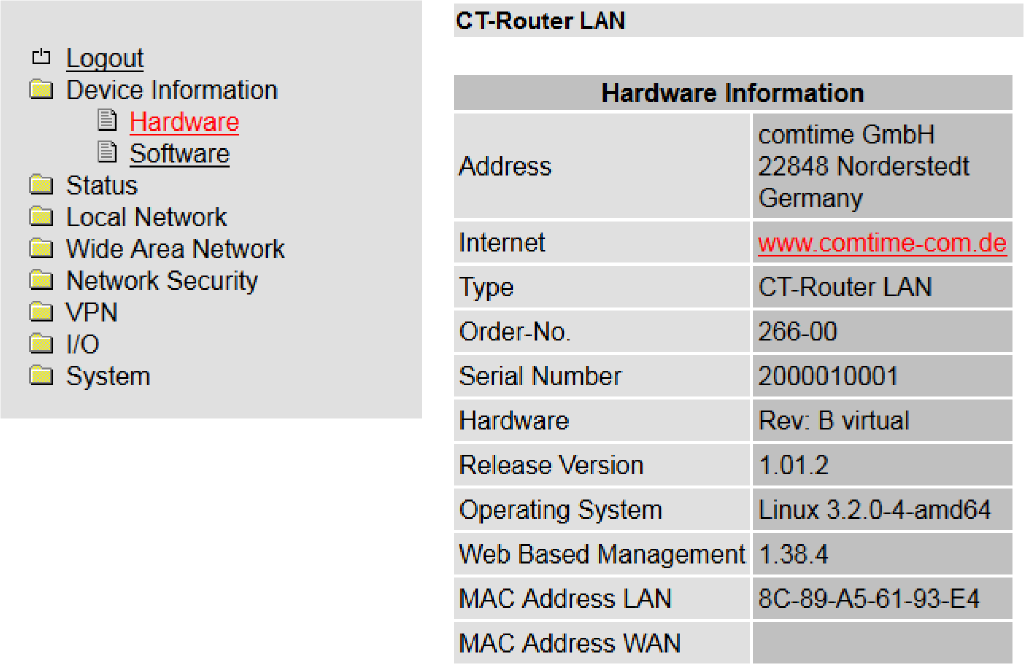
.



Device information

In this area you can see more detailed information about the built-in hardware as well as about the installed software.

Hardware



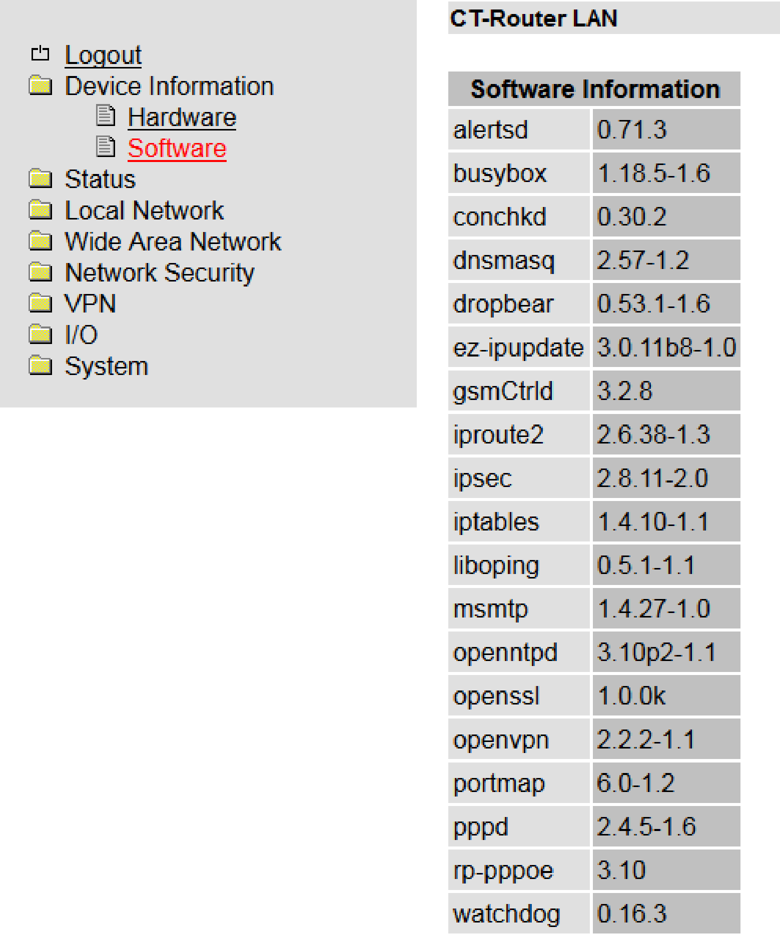
CT-Router LAN

Hardware Information	
Address	comtime GmbH 22848 Norderstedt Germany
Internet	www.comtime-com.de
Type	CT-Router LAN
Order-No.	266-00
Serial Number	2000010001
Hardware	Rev: B virtual
Release Version	1.01.2
Operating System	Linux 3.2.0-4-amd64
Web Based Management	1.38.4
MAC Address LAN	8C-89-A5-61-93-E4
MAC Address WAN	

Here you will find a tabular overview of the built-in hardware.

Device information

Software



CT-Router LAN

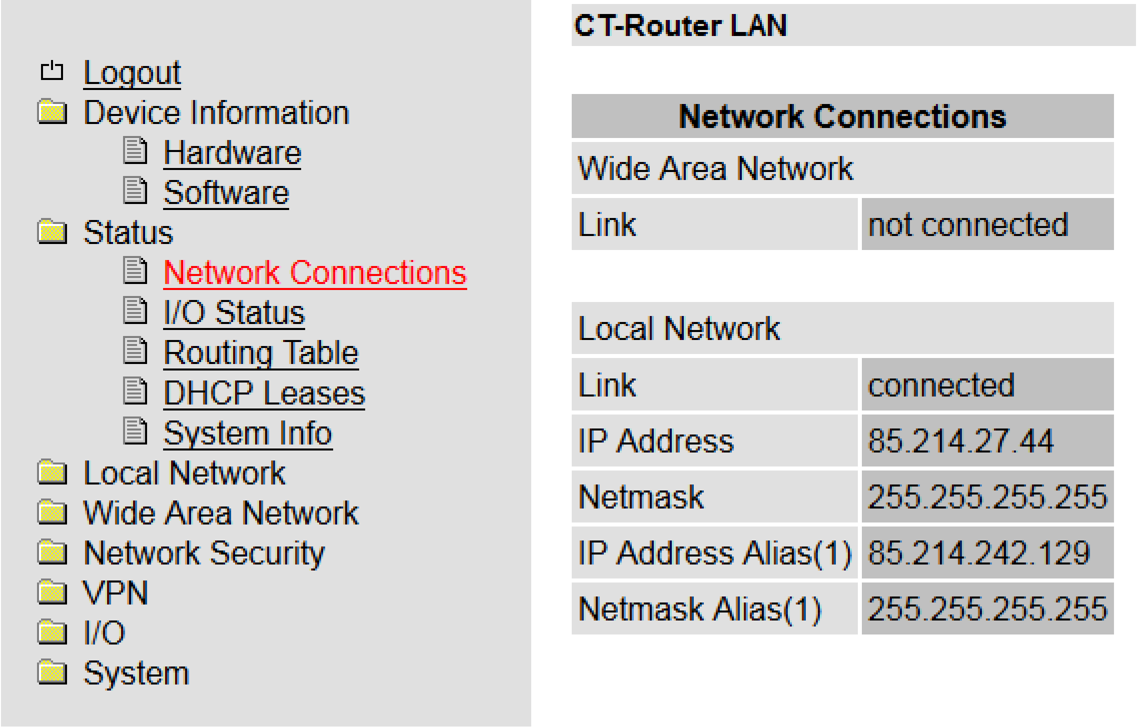
Software Information	
alertsd	0.71.3
busybox	1.18.5-1.6
conchkd	0.30.2
dnsmasq	2.57-1.2
dropbear	0.53.1-1.6
ez-ipupdate	3.0.11b8-1.0
gsmCtrld	3.2.8
iproute2	2.6.38-1.3
ipsec	2.8.11-2.0
iptables	1.4.10-1.1
liboping	0.5.1-1.1
msmtp	1.4.27-1.0
openntpd	3.10p2-1.1
openssl	1.0.0k
openvpn	2.2.2-1.1
portmap	6.0-1.2
pppd	2.4.5-1.6
rp-pppoe	3.10
watchdog	0.16.3

Here you will find a tabular overview of the software installed on the CT-Router.

Status

In this menu all current status information about the the network connections are displayed.

Network Connections



CT-Router LAN

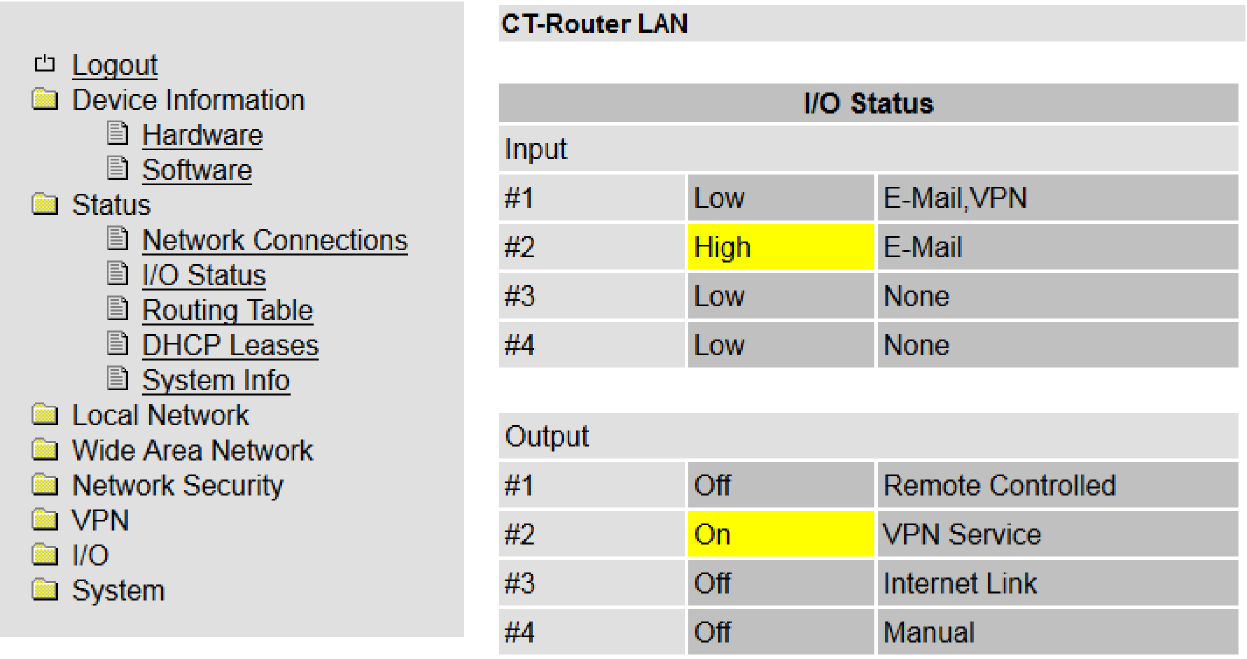
Network Connections	
Wide Area Network	
Link	not connected

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 conncetions	Explanation
Wireless Network	
Link	**TCP/IP connected:** TCP/IP connection established in the mobile phone network. **VPN connected:** VPN connection established in the mobile phone network **Not connected:** There is no active connection in the mobile phone network
IP Address	Assigned IP address (pre-setting of the provider)
Netmask	Assigned netmask (pre-setting of the provider)
DNS Server	DNS server IP-address
Sec. DNS Server	alternative DNS-Server IP-address
RX Bytes	Number of the received data since login into the mobile phone network in bytes.
TX Bytes	Number of the sent data since login into the mobile phone network in bytes.
Local Network	
Link	**connected:** Local Ethernet connection established. **not connected:** No local Ethernet connection established.
IP Address	Ethernet IP-address
Netmask	Ethernet netmask

Status

I/O status



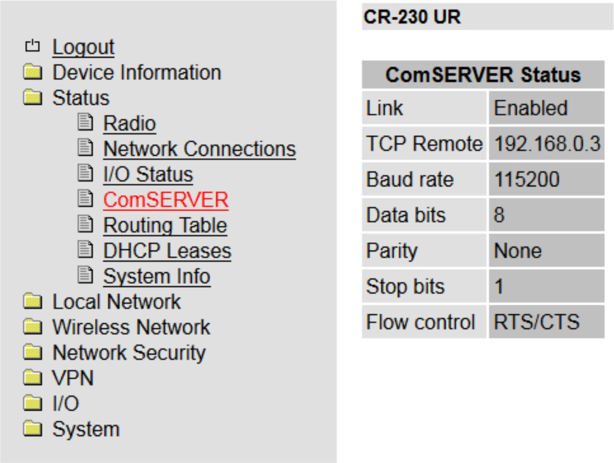
CT-Router LAN

I/O Status		
Input		
#1	Low	E-Mail,VPN
#2	High	E-Mail
#3	Low	None
#4	Low	None
Output		
#1	Off	Remote Controlled
#2	On	VPN Service
#3	Off	Internet Link
#4	Off	Manual

Here you will find an overview in tabular form of all current input and output settings.

Status

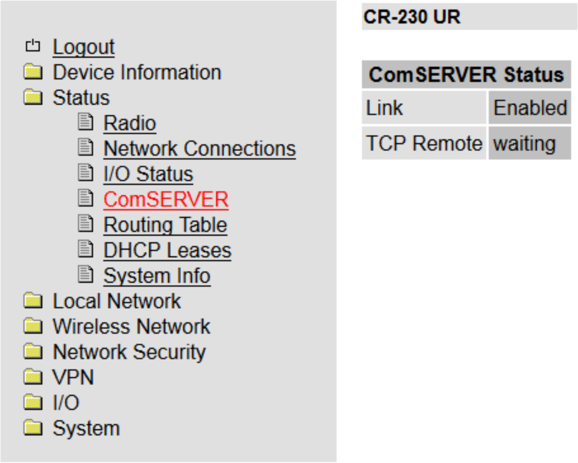
ComSERVER – status (optional)



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

or



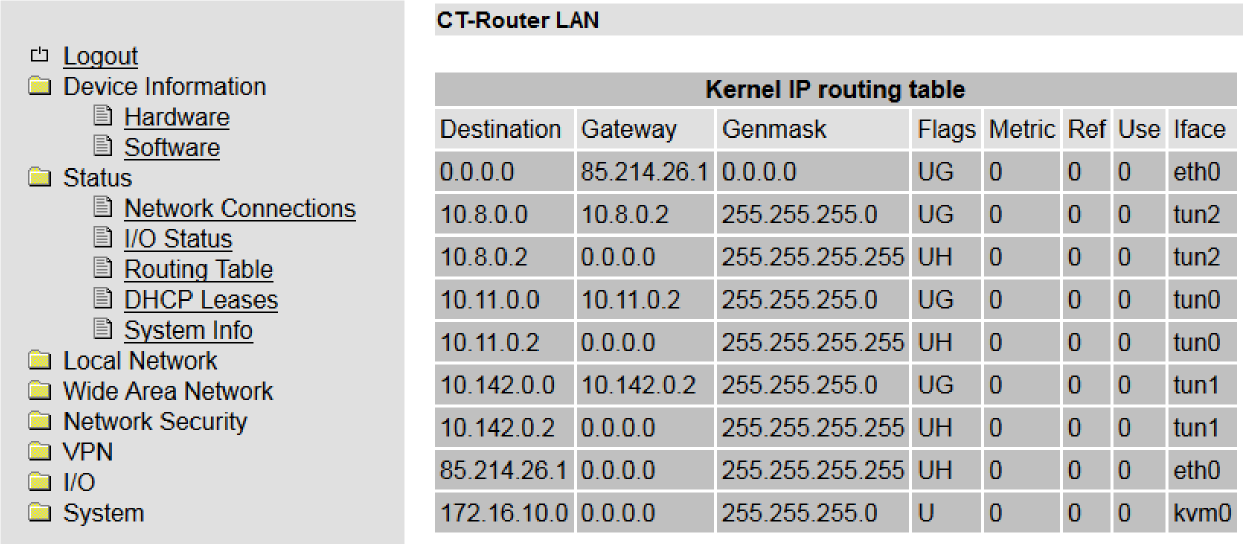
CR-230 UR

ComSERVER Status	
Link	Enabled
TCP Remote	waiting

Status →ComSERVER	
ComSERVER	Explanation
Link	The status of the ComServer connection (serial) is displayed:
TCP Remote	
Baud Rate	
Data bits	
Parity	
Stop bits	
Flow control	

Status

Routing table



CT-Router LAN

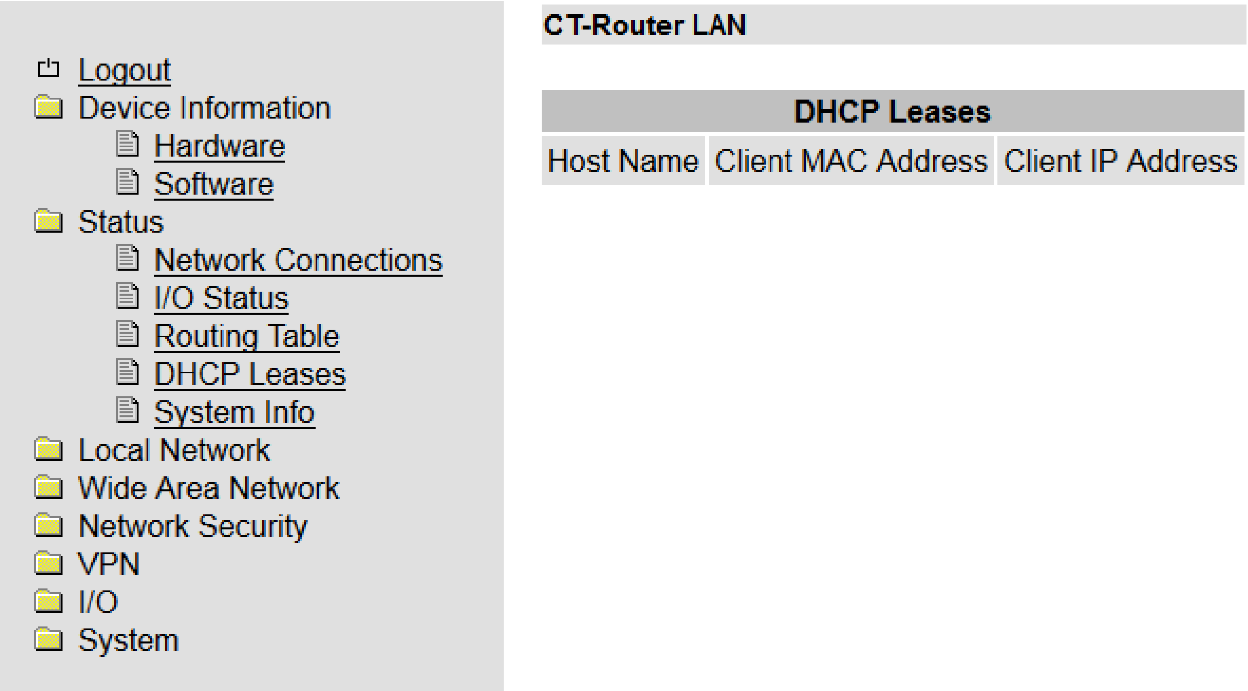
Kernel IP routing table

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	tun0
10.11.0.2	0.0.0.0	255.255.255.255	UH	0	0	0	tun0
10.142.0.0	10.142.0.2	255.255.255.0	UG	0	0	0	tun1
10.142.0.2	0.0.0.0	255.255.255.255	UH	0	0	0	tun1
85.214.26.1	0.0.0.0	255.255.255.255	UH	0	0	0	eth0
172.16.10.0	0.0.0.0	255.255.255.0	U	0	0	0	kvm0

Status →Routing table	
Routing Table	Explanation
Includes among others information about the target gateway to the subnet mask and metrics.	

Status

DHCP Leases



- Logout
- Device Information
  - Hardware
  - Software
- Status
  - Network Connections
  - I/O Status
  - Routing Table
  - DHCP Leases
  - System Info
- Local Network
- Wide Area Network
- Network Security
- VPN
- I/O
- System

CT-Router LAN

DHCP Leases

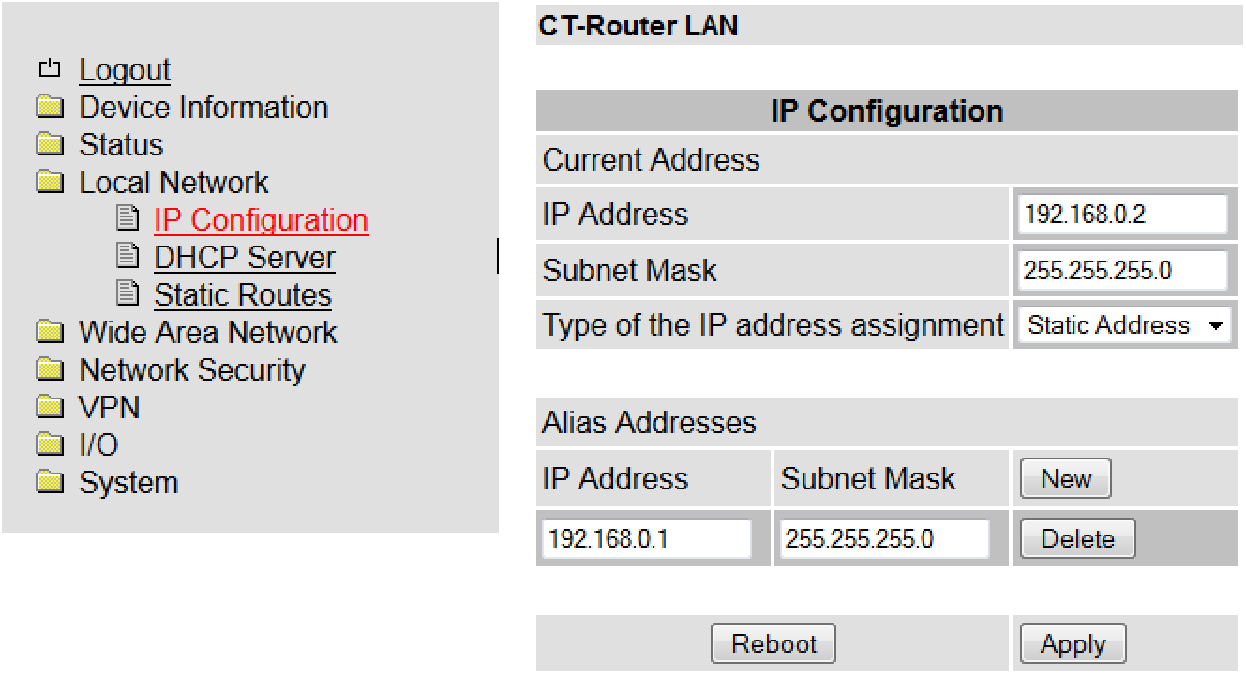
Host Name	Client MAC Address	Client IP Address

Status →DHCP leases	
DHCP Leases	Explanation
Here you will find an overview in tabular form of all DHCP data assigned by the AK-DinRail-3G-Router.	
Host name	Host name of the terminal in the network.
Client MAC address	MAC address of the terminal in the network.
Client IP address	IP address of the terminal in the network.

Local network

In the menu "Local network" you can set the local network settings for the CT-Router.

IP configuration



CT-Router LAN

IP Configuration

Current Address

IP Address	192.168.0.2
Subnet Mask	255.255.255.0
Type of the IP address assignment	Static Address

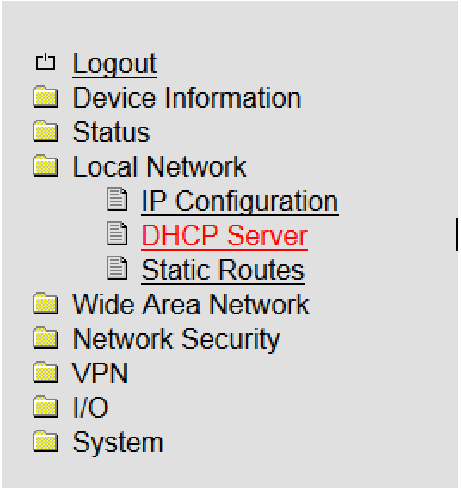
Alias Addresses

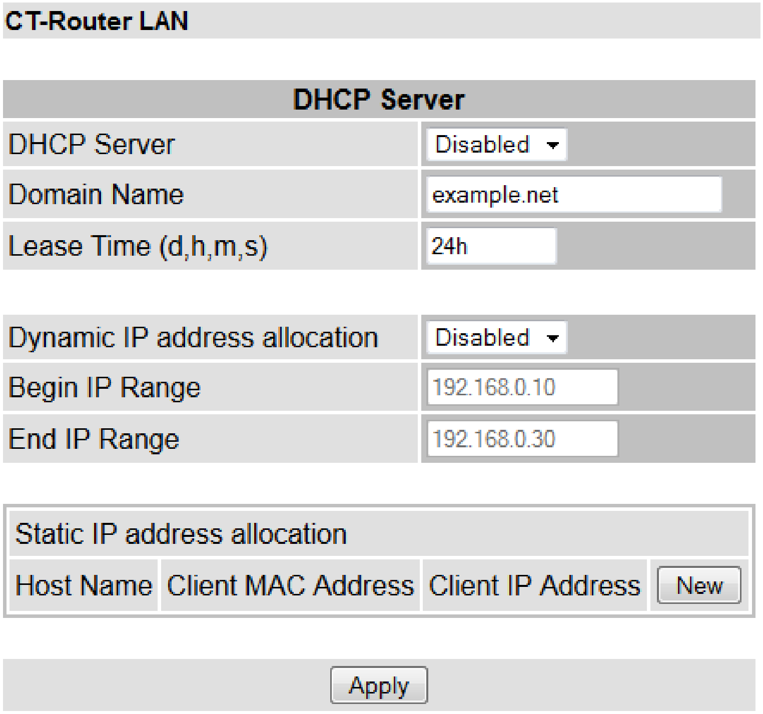
IP Address	Subnet Mask
192.168.0.1	255.255.255.0

Local network → IP configuration	
IP configuration	Explanation
Current address	
IP Address	Current IP address of the router
Subnet mask	Subnet mask of the current IP address
Type of the IP address assignment	**Static:** Static IP address (Standard setting) **DHCP:** Dynamic IP address is referred to when starting up the router from a DHCP server
Alias addresses	Max. 8 additional IP addresses as well as subnet masks can be assigned.
IP address	Alternative IP address of the router
Subnet mask	Alternative subnet mask of the router

Local network

DHCP server




CT-Router LAN

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

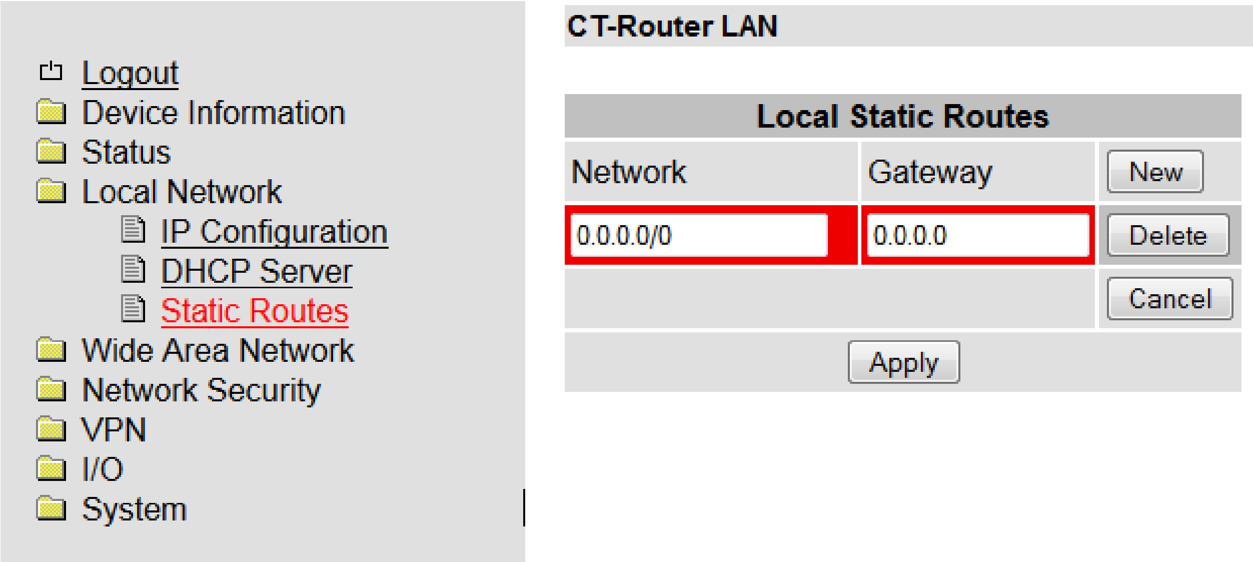
Static IP address allocation

Host Name	Client MAC Address	Client IP Address	New

Local network → DHCP server	
DHCP server	**Explanation**
DHCP server	Deactivated / Activated
Domain name	Enter Domain name which is distributed via DHCP.
Lease time (d,h,m,s)	Period of time during which the network configurations are valid.
Dynamic IP address allocation	Dynamic IP address assignment: When activating you can enter the corresponding network parameters / The DHCP server assigns IP addresses of the indicated IP range.
Begin IP range	Beginning of the IP range
End IP range	End of the IP range
Static IP address allocation	IP addresses are clearly assigned to MAC addresses.
Client MAC address	MAC address of the connected terminal
Client IP address	IP address of the connected terminal IP addresses must not originate from the dynamic IP address assignments. An IP address must not be assigned several times otherwise an IP

Local network

Static routes



CT-Router LAN

Local Static Routes

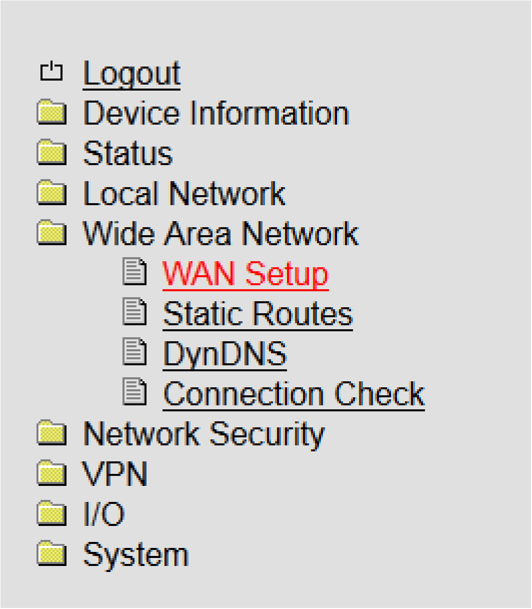
Network	Gateway
0.0.0.0/0	0.0.0.0

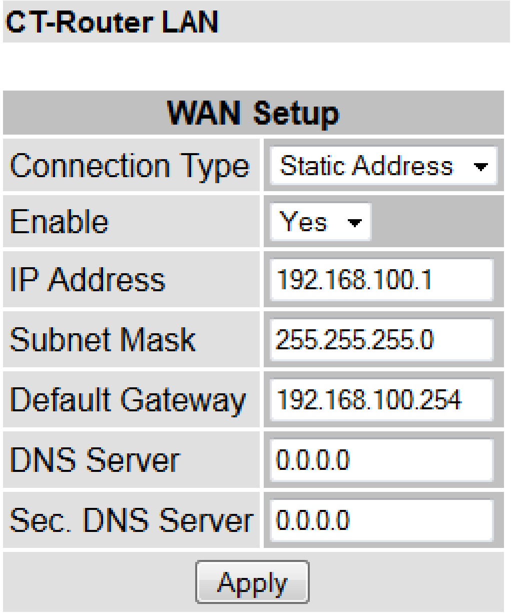
Local network → Static routes	
Static routes	**Explanation**
Network	Network in CIDR form
Gateway	Gateway address of the network
Max. 8 networks can be entered.	

Wide Area Network

Determine the settings for the use of CT-Router in the “Wide Area Network ” menu.

WAN Setup




CT-Router LAN

WAN Setup	
Connection Type	Static Address
Enable	Yes
IP Address	192.168.100.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.100.254
DNS Server	0.0.0.0
Sec. DNS Server	0.0.0.0

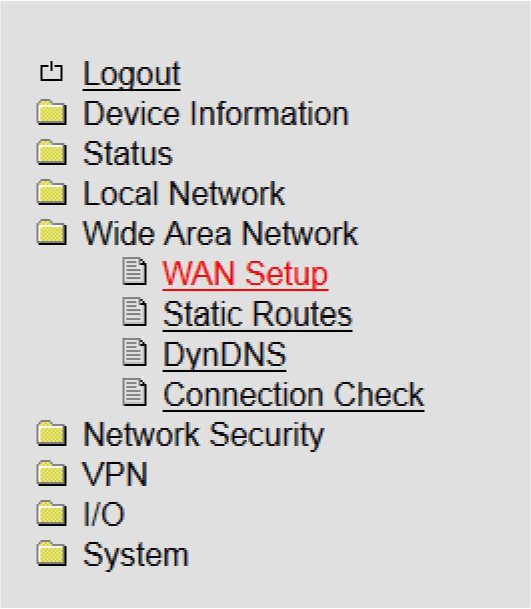
Wide Area Networks	
WAN Setup	Explanation
Connection Type	Select the connection in the "Connection Type" menu and set it to Enable "Yes". Then click "Apply"

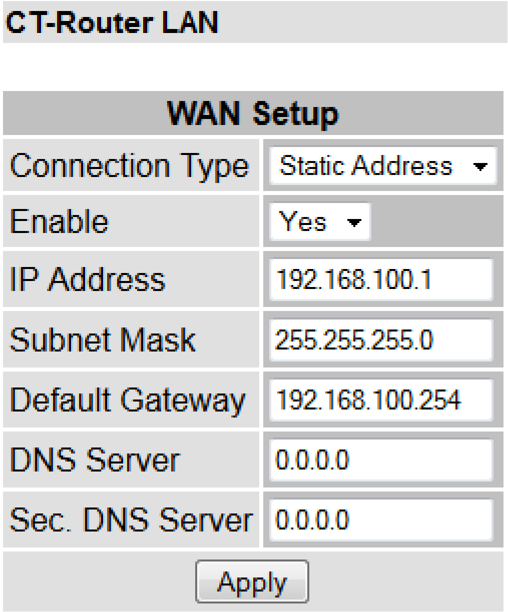
- Possible types of connection in the "Connection Type" menuStatic Address
- DHCP Client
- PPOE

Wide Area Network

Static Address

Setting for use in local area networks




CT-Router LAN

WAN Setup

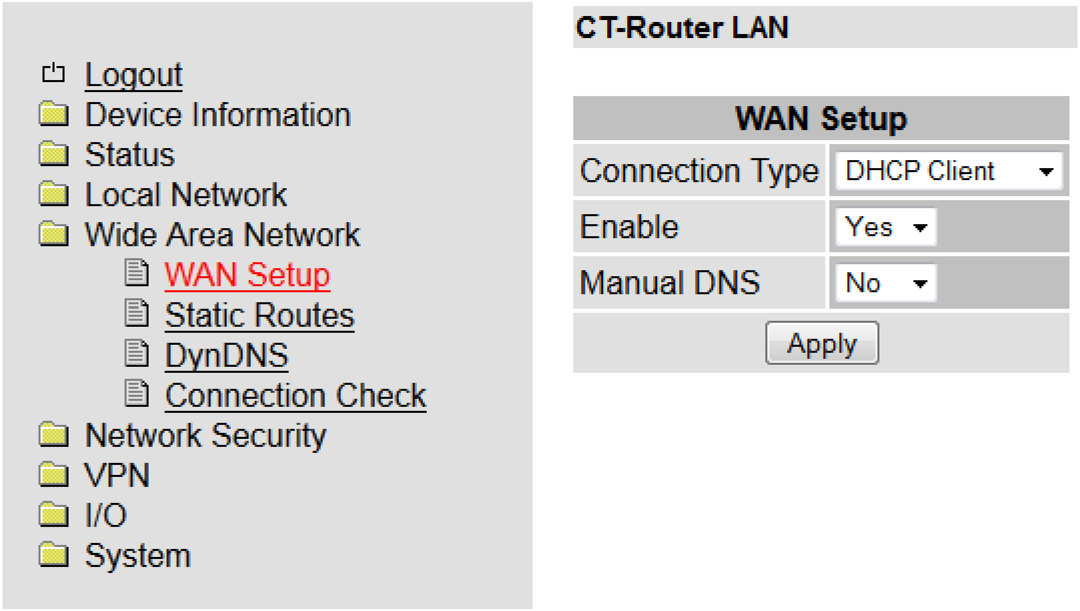
Connection Type	Static Address
Enable	Yes
IP Address	192.168.100.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.100.254
DNS Server	0.0.0.0
Sec. DNS Server	0.0.0.0

Wide Area Networks	
WAN Setup	Explanation
IP Address	IP address of the router on the WAN interface
Subnet Mask	subnet mask
Default Gateway	IP address of the gateway to the Internet
DNS Server	IP address of the DNS server
Sec. DNS Server	IP address of a second DNS server

Wide Area Network

DHCP Client

Einstellung für den Betrieb mit Kabelmodems



Connection Type: DHCP Client

Enable: Yes

Manual DNS: No

Soll dem Router aus dem Netzwerk automatisch eine IP-Adresse zugewiesen werden setzen Sie den „Connection Type“ auf „DHCP Client“ und bestätigen mit „Apply“.

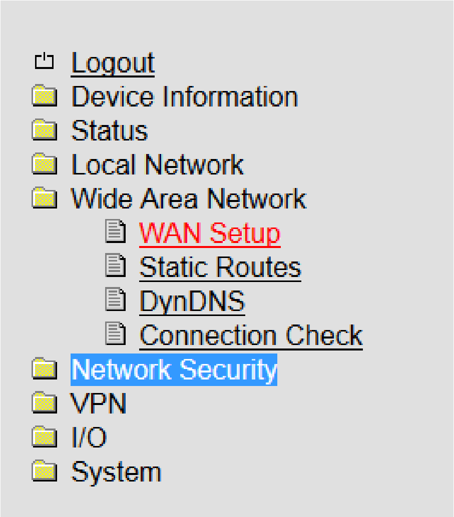
Wenn Sie die IP-Adressen des DNS-Servers manuell einstellen wollen setzen Sie unter „Manual DNS“ die Einstellung „Yes“ und geben die IP-Adressen ein und klicken abschließend auf „Apply“.

Wide Area Networks	
WAN Setup	Erklärung
DNS Server	IP-Adresse des DNS Servers
Sec. DNS Server	IP-Adresse eines zweiten DNS Servers

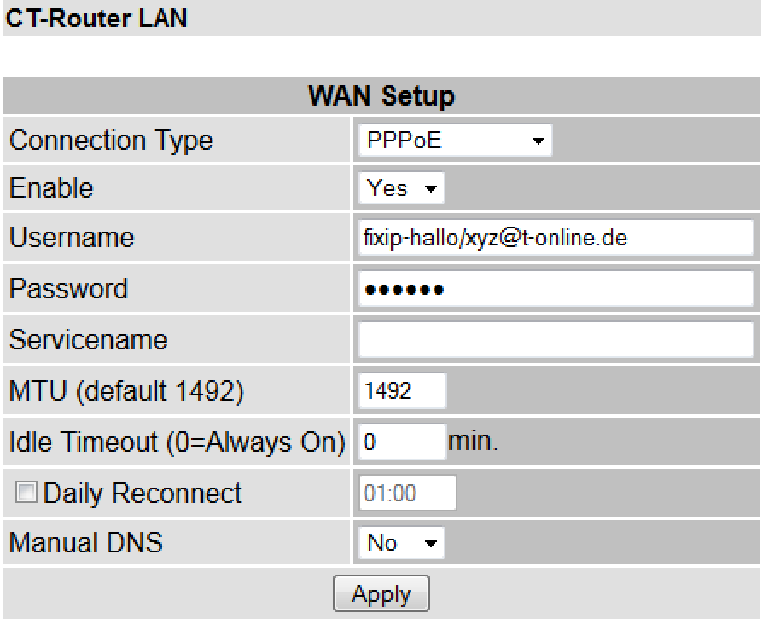
Wide Area Network

PPPoE

Einstellung für den Betrieb mit DSL-Modems
Bei einen Betrieb an einem (DSL-)Modem wählen Sie unter „Connection Type‟ die Einstellung „PPPoE‟ und mit „Apply‟ bestätigen



- Logout
- Device Information
- Status
- Local Network
- Wide Area Network
  - WAN Setup
  - Static Routes
  - DynDNS
  - Connection Check
- Network Security
- VPN
- I/O
- System



CT-Router LAN

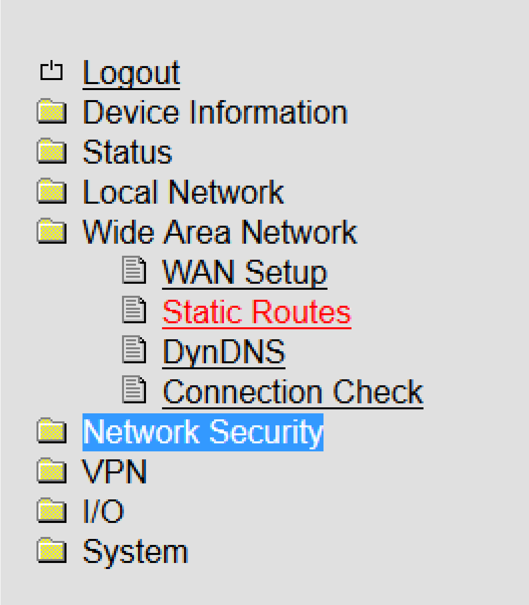
WAN Setup	
Connection Type	PPPoE
Enable	Yes
Username	fixip-hallo/xyz@t-online.de
Password	••••••
Servicename	
MTU (default 1492)	1492
Idle Timeout (0=Always On)	0 min.
□ Daily Reconnect	01:00
Manual DNS	No

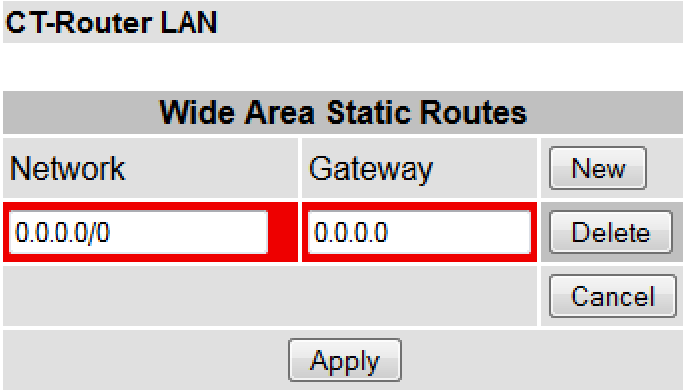
Apply

Wide Area Networks	
WAN Setup	**Erklärung**
Username	Username für den Zugang zum Netz
Password	Password für den Zugang zum Netz
Servername	Service-Name für den Zugang (DSL-) Netz
MTU (default 1492)	Maximale Größe der unfragmentierten Datenpakets
Idle Timeout (0=Always On)	Der Router trennt die Verbindung nach der eingestellten Zeit. Der Timer startet wenn keine Daten übertragen mehr werden.
Daily Reconnect	Wiederholtes Einbuchen in das (DSL-)Netz zu einer definierten Uhrzeit
Manual DNS	Yes: Manuelle Einstellung No: Keine manuelle Einstellung

Wide Area Network

Static routes



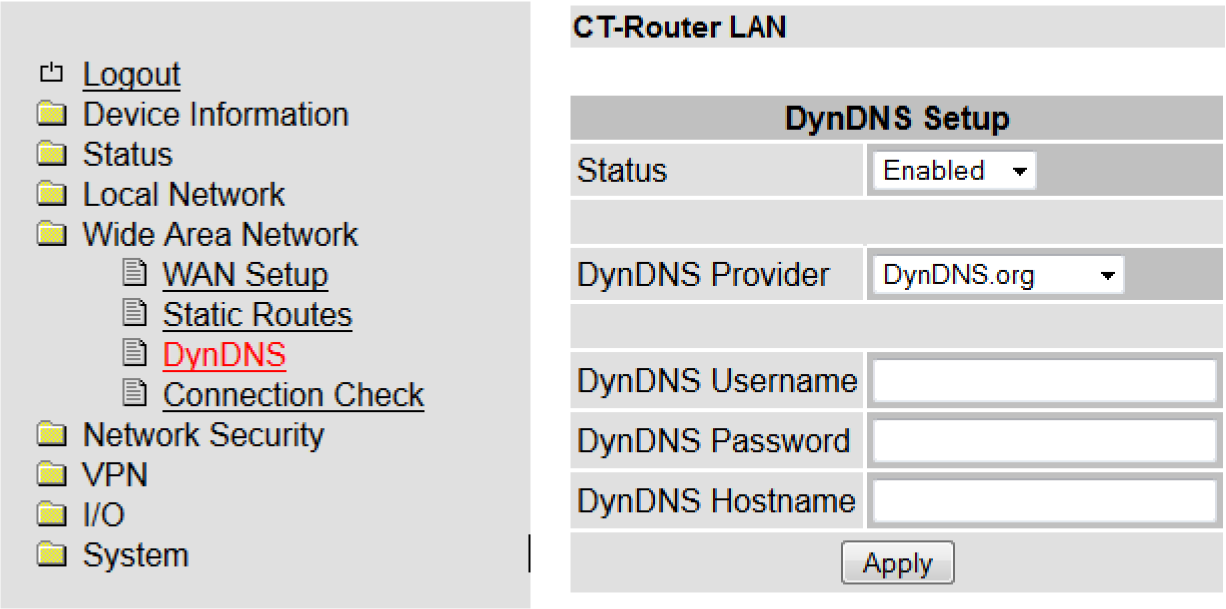


Network	Gateway
0.0.0.0/0	0.0.0.0

Wireless network → Static routes	
Static routes	Explanation
Network	Network in CIDR form
Gateway	Gateway address of the network
Max. 8 networks can be entered.	

Wide Area Network

DynDNS



Logout
Device Information
Status
Local Network
Wide Area Network
WAN Setup
Static Routes
DynDNS
Connection Check
Network Security
VPN
I/O
System

CT-Router LAN

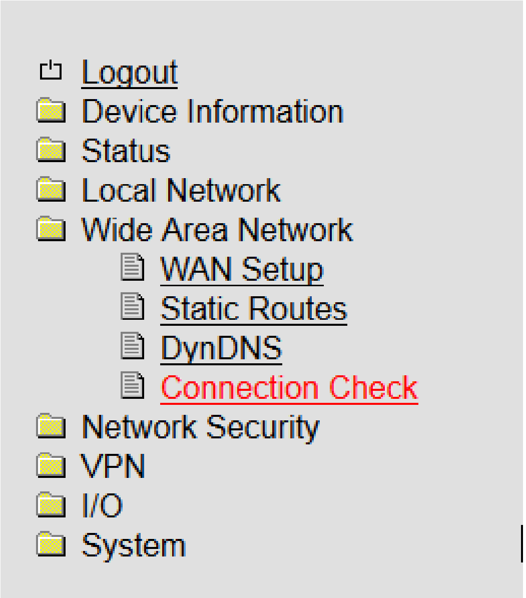
DynDNS Setup

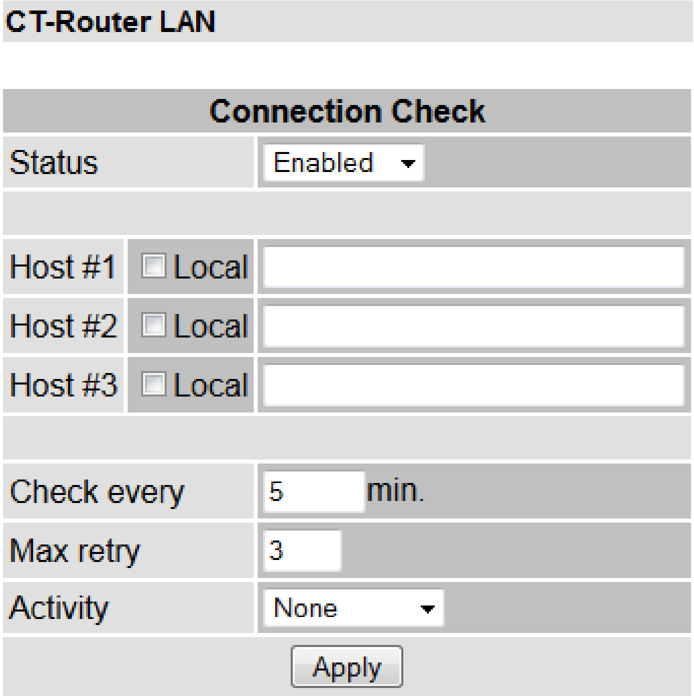
Status	Enabled
DynDNS Provider	DynDNS.org
DynDNS Username	
DynDNS Password	
DynDNS Hostname	

Wireless network → DynDNS	
DynDNS	Explanation
DynDNS	**Disable:** Deactivating the DynDNS **Enable:** Activating the DynDNS
DynDNS provider	Selection of the DynDNS provider
DynDNS username	User name of the DynDNS account
DynDNS password	Password of the DynDNS account
DynDNS host name	Host name of the router in the DynDNS service

Wide Area Network

Connection Check





CT-Router LAN

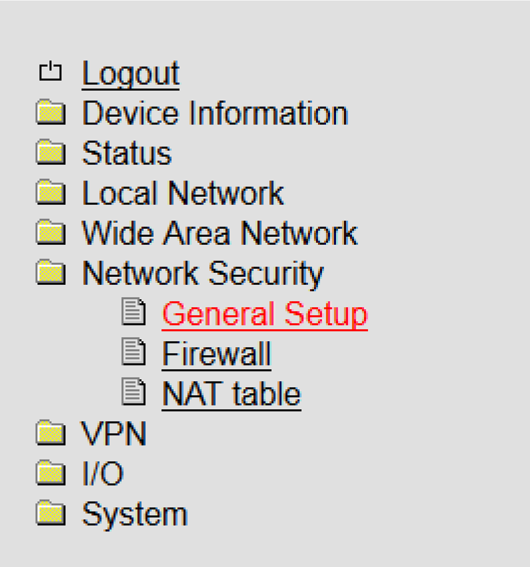
Connection Check		
Status	Enabled ▾	
Host #1	□ Local	
Host #2	□ Local	
Host #3	□ Local	
Check every	5 min.	
Max retry	3	
Activity	None ▾	

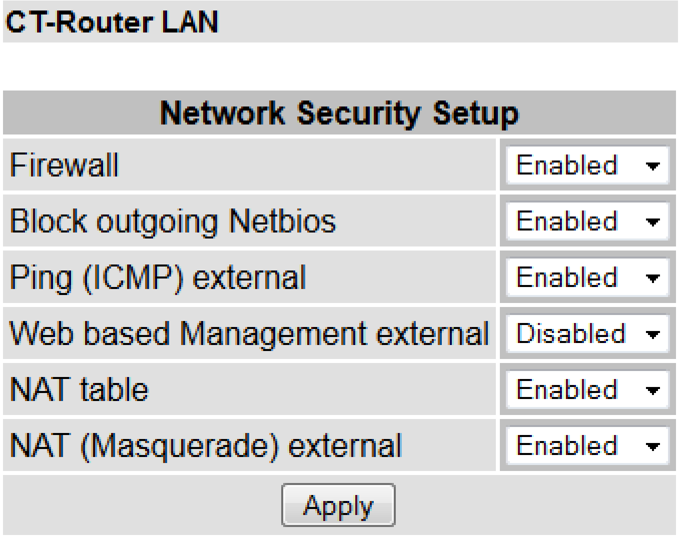
Wireless network → Connection check	
Connection check	Explanation
Connection check	**Disable:** Deactivating the connection check of the package data connection **Enable:** Activating the connection check of the package data connection
Host #1…#3	IP address or host name as reference point for the connection check **Local:** Activating for addresses which are available via a VPN tunnel.
Check every	Checking the connection every x minutes.
Max. retry	Maximum number of connection trials
Activity	Perform one of the following actions in case of a loss of connection: **Reboot:** Restarting the router **Reconnect:** The system tries to re-establish the connection **Re-login:** Mobile phone interface is shut down and the system tries to establish a connection with login. **None:** No action is being performed

Network security

Perform the settings for network security in the menu "Network security".

General setup



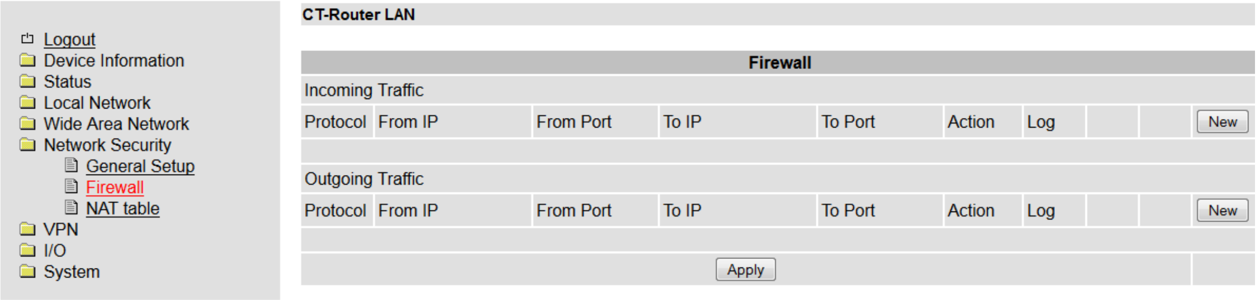

CT-Router LAN

Network Security Setup	
Firewall	Enabled
Block outgoing Netbios	Enabled
Ping (ICMP) external	Enabled
Web based Management external	Disabled
NAT table	Enabled
NAT (Masquerade) external	Enabled

Network security → General setup	
General setup	Explanation
Firewall	**Disable** Deactivating the integrated stateful package inspection Firewall **Enable:** Activating the integrated stateful package inspection Firewall
Block outgoing Netbios	Netbios inquiries are originated by Windows systems in the local network and are causing an increased data traffic. **Disable:** Netbios inquiries are allowed. **Enable:** Netbios inquiries are blocked.
Ping (ICMP) external	Check if a device in the network can be accessed by means of ping requests. Thus the data traffic is being increased. **Disable:** Ping requests from an external IP network are not answered. **Enable:** Ping requests from an external IP network are answered.
Web based management external	**Disable:** External WBM configuration is deactivated. **Enable:** External WBM configuration is activated.
NAT (Masquerade) external	**Disable:** IP masquerading deactivated. **Enable:** IP masquerading activated.

Network security

Firewall



Firewall

Incoming Traffic

Protocol	From IP	From Port	To IP	To Port	Action	Log

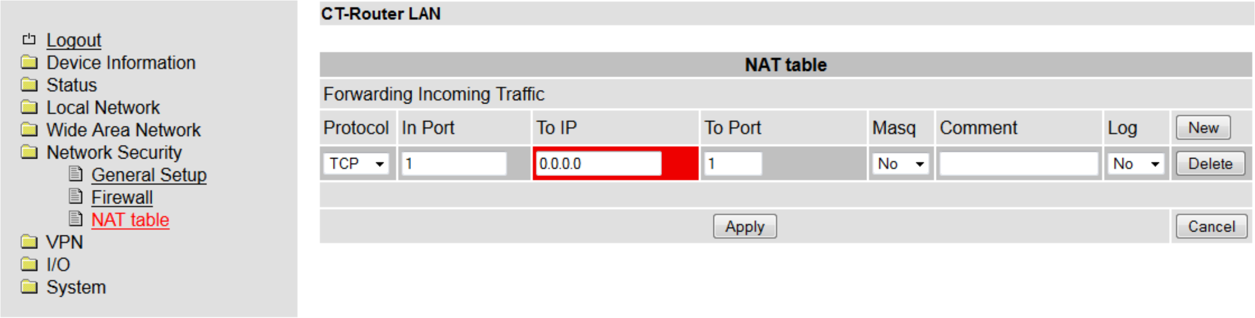
Outgoing Traffic

Protocol	From IP	From Port	To IP	To Port	Action	Log

Network security → Firewall	
Firewall	Explanation
Incoming traffic	
Protocol	Protocol selection: TCP, UDP, ICMP, all
From IP / To IP	IP address range in CIDR form (0.0.0.0/0 means all IP addresses)
From Port / To Port	Port range ("any" means all ports)
Action	**Accept:** Data packages are accepted. **Reject:** Data packages are rejected. Message to the sender that the data are rejected. **Drop:** Data packages are "dropped", i.e. they are rejected and the sender is not informed about the
Log	**Yes:** Activation of the rule is logged. **No:** Activation of the rule is not logged.
New / Delete	Establish new rules / delete existing rules
	It is possible to move the rules up or down using the arrows.
Outgoing Traffic	Behaves similar as "Incoming traffic" but these rules refer to the outgoing data traffic. If no rule is available all outgoing connections are forbidden (except for VPN connections)

Network security

NAT Table



CT-Router LAN

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

NAT table

Forwarding Incoming Traffic

Protocol	In Port	To IP	To Port	Masq	Comment	Log	New
TCP	1	0.0.0.0	1	No		No	Delete

Apply

Cancel

Network scurity →NAT table	
Firewall	Explanation
Protocol	Protocol selection: TCP, UDP, ICMP, all
In Port / To Port	Port range ("any" means all ports)
To IP	IP address range in CIDR form (0.0.0.0/0 means all IP addresses)
Masq	**Yes:** IP masquerading activated / Answering in mobile phone networks is possible **No:** IP masquerading deactivated / Answering in mobile phone networks is not possible
Log	**Yes:** Activation of the rule is logged. **No:** Activation of the rule is not logged.
New / Delete	Establish new rules / delete existing rules
	It is possible to move the rules up or down using the arrows.

VPN

In the menu OpenVPN you can perform on the one hand settings for the Internet protocol security (IPsec) on the other hand for virtual private network (VPN).

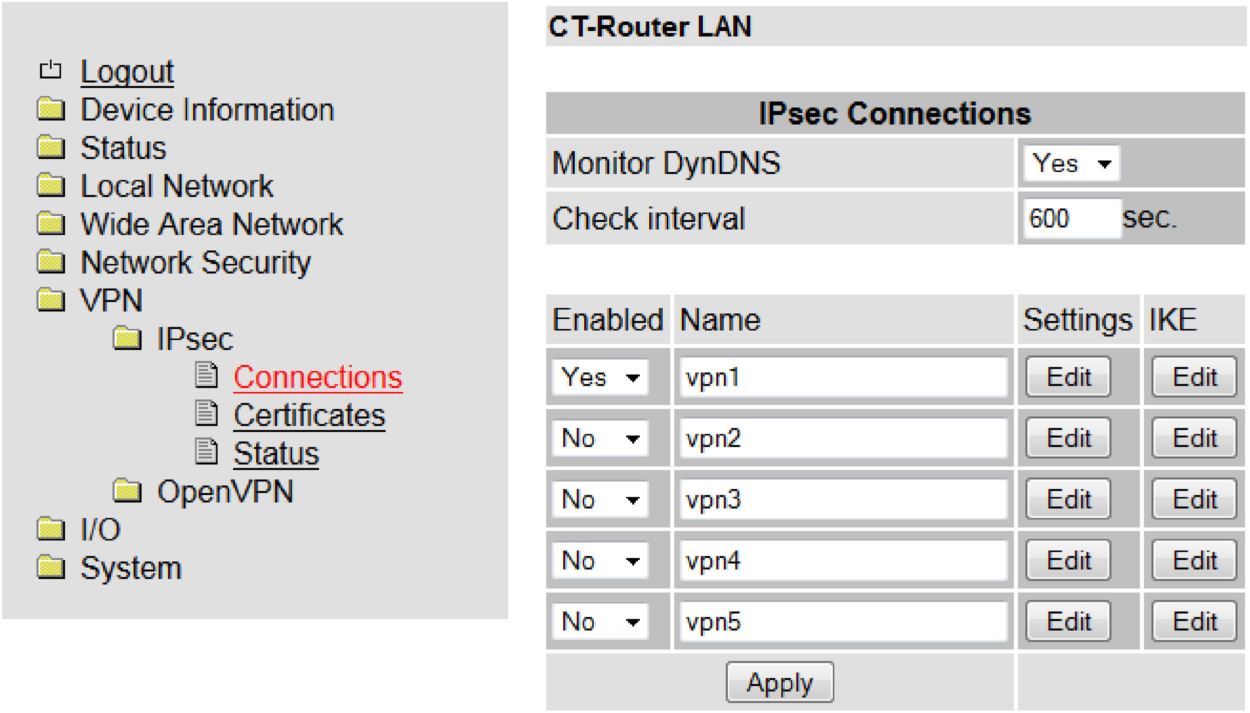
For a VPN connection, the IP addresses of the VPN remote sites must be known and addressable.

IPSec

The VPN remote sites peer must support IPsec with the following configuration:

- authentication using X.509 certificates or preshared secret key (PSK)
- ESP
- Diffie Hellman groups 2 or 5
- 3DES or AES encryption
- MD5 or SHA-1 Hash algorithms
- Tunnel modus
- Quick mode
- Main mode
- SA Lifetime (1 second to 24 hours)

Connections



CT-Router LAN

IPsec Connections

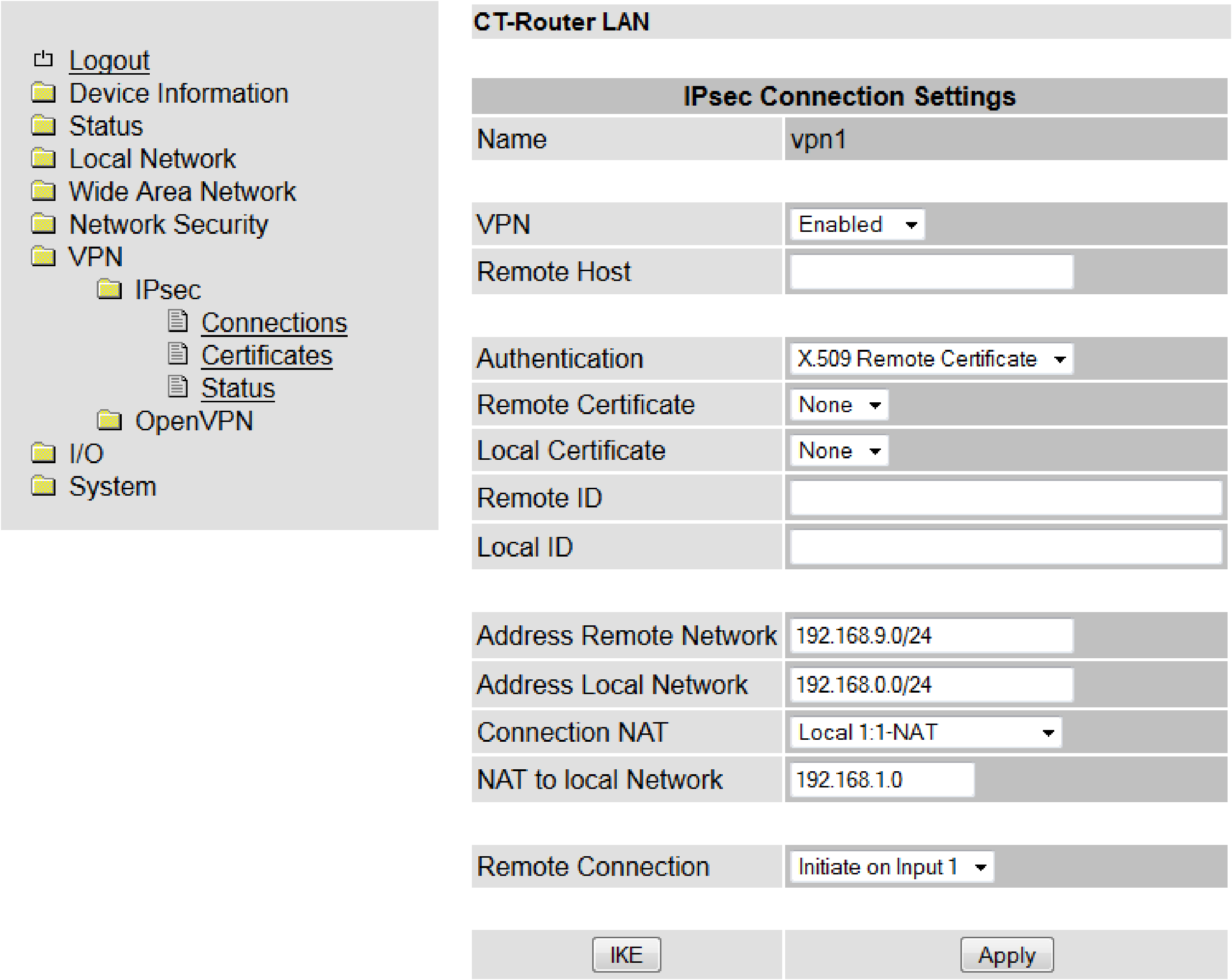
Monitor DynDNS	Yes
Check interval	600 sec.

Enabled	Name	Settings	IKE
Yes	vpn1	Edit	Edit
No	vpn2	Edit	Edit
No	vpn3	Edit	Edit
No	vpn4	Edit	Edit
No	vpn5	Edit	Edit

VPN → IPsec → Connections	
IPsec connections	**Explanation**
Monitor DynDNS	The VPN remote station does not have a firm IP and a DynDNS name is used as remote host so that this function can be activated in order to check the connection.
Check Interval	Check interval in seconds
Enable	Activate VPN connection (=Yes) or deactivate VPN connection (=No)
Name	Determine name of the VPN connection
Settings	Settings for IPsec
IKE	Settings for the Internet key exchange log

VPN-IPsec

Connections settings



CT-Router LAN

IPsec Connection Settings	
Name	vpn1
VPN	Enabled
Remote Host	
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	Local 1:1-NAT
NAT to local Network	192.168.1.0
Remote Connection	Initiate on Input 1

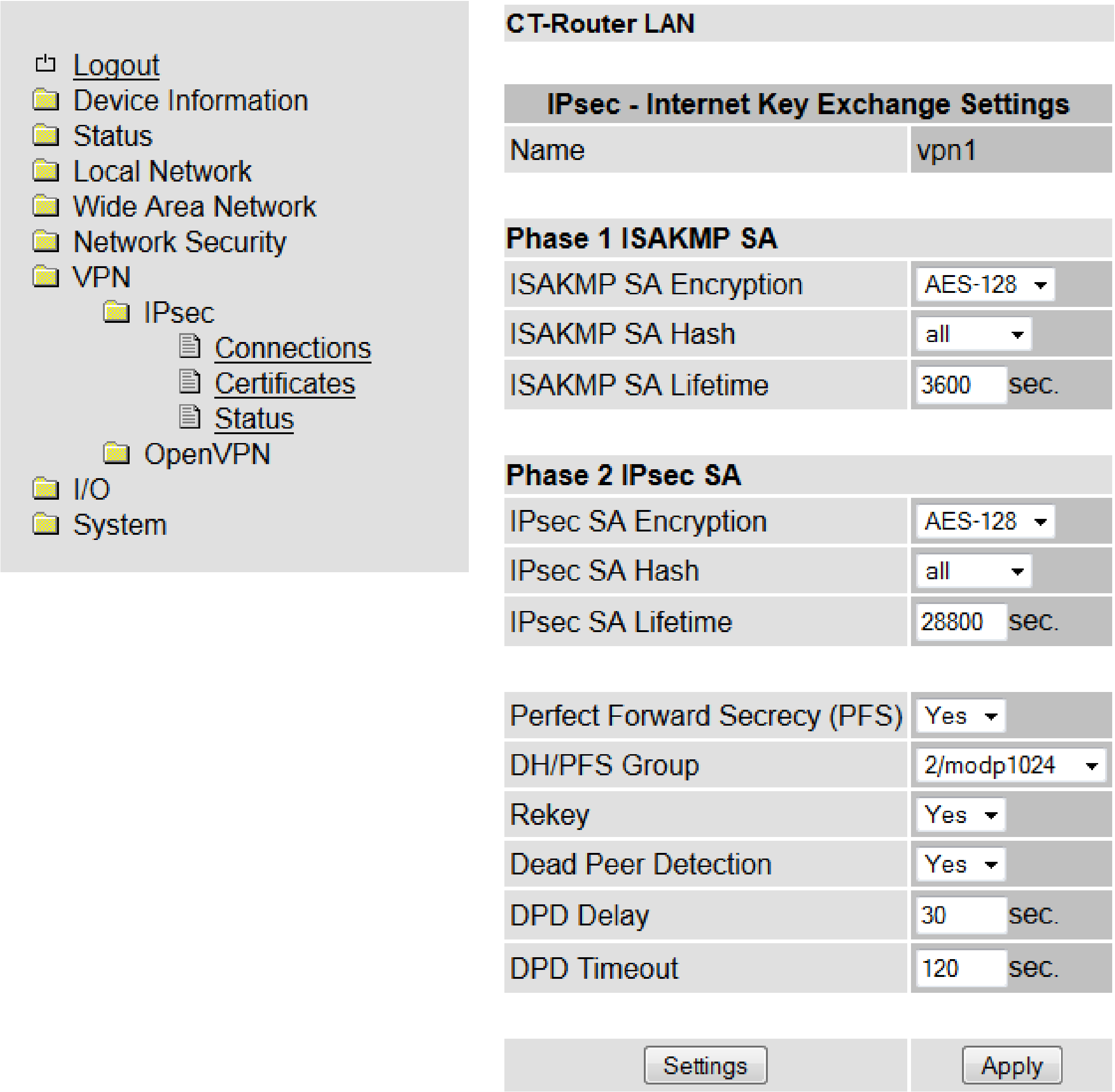
VPN → IPsec → Connections → Settings → Edit	
Settings	**Explanation**
Name	Name of the VPN connection
VPN	Activating (=Enable) or deactivating (=Disable) of the VPN connection
Remote host	IP address / URL of the remote station Can only be set if "Initiate" was selected under remote connection. If "Accept" was selected under remote connection the value for the remote host will be set to "%any" and the system is waiting for connection.
Authentication	X.509 remote certificate - VPN subscribers have a private and a public key (X.509 certificate). Preshared secret key - VPN subscribers have a private key (a mutual password).
Remote certificate	VPN remote station authentication is performed via a certificate which needs to be uploaded in the menu "IPsec certificates".
Local certificate	Router authentication at the VPN remote station is performed via a certificate which needs to be uploaded in the menu "IPsec certificates".

VPN-IPsec

Remote ID	**Empty:** No entry in this row means that the indications are selected from the certificate. **Subject:** IP address, E-mail address or host name mean that these entries should also be available in the certificate in order that it is possible to authenticate the router.
Local ID	See remote ID
Address remote network	IP address/subnet mask of the network for which a VPN connection is established.
Address local network	IP address/subnet mask of the local network.
Local 1:1 NAT	IP address of the local network under which the network can/shall be accessed by 1:1 NAT from the remote network.
Remotec	**Accept:** VPN connection is established from a remote station and accepted by the router. **Initiate:** VPN connection is starting from the router. **Initiate on input:** Starts / stops the VPN tunnel by digital input. **Initiate on SMS:** VPN connection is started by an SMS. **Initiate on call:** VPN connection is started by a call.
Autoreset	Can be determined by "Initiate on SMS" and must be determined by "Initiate on Call". A period of time is determined after how many minutes the VPN connection is stopped by autoreset.

VPN-IPsec

Connection IKE



CT-Router LAN

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.

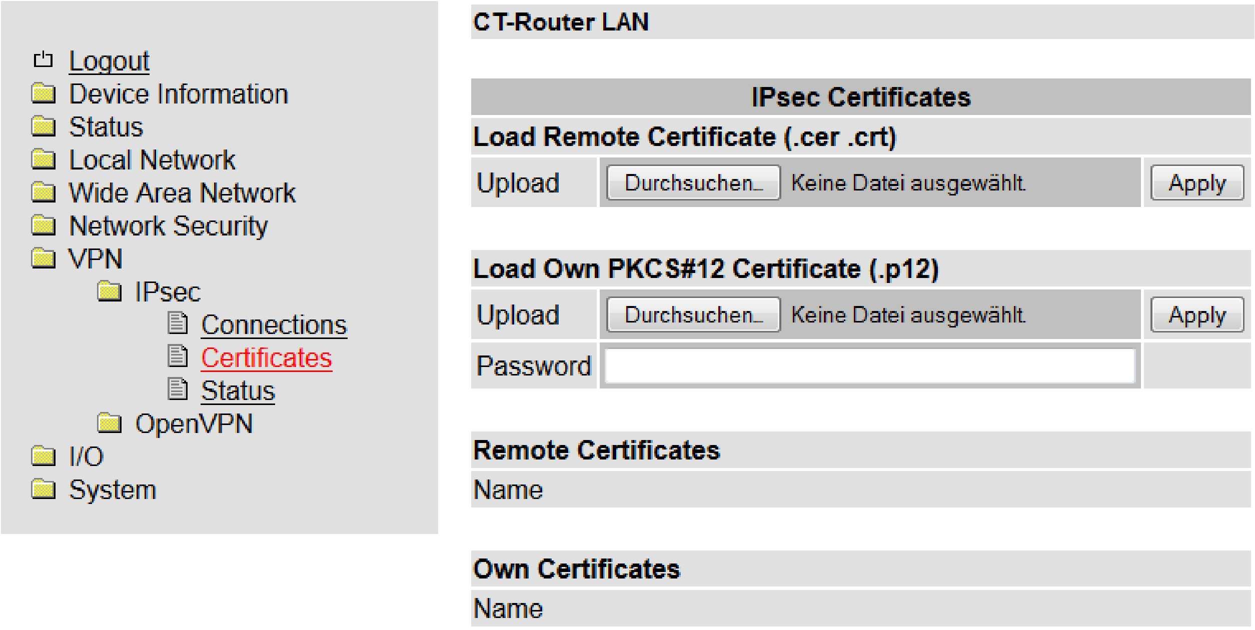
VPN → IPsec → Connections → IKE → Edit	
IKE	Explanation
Name	Name of the VPN connection.
Phase 1 ISAKMP SA	Key exchange
ISAKMP SA Encryption	Choice of encryption algorithm
ISAKMP SA Hash	Choice of hash algorithm
ISAKMP SA Lifetime	Lifetime of the ISAKMP SA key. Standard setting 3600 seconds (1 hour) max. setting value 86400 seconds (24 hours)
Phase 2 IPsec SA	Data exchange

VPN-IPsec

Ipsec SA Encryption	see ISAKMP SA Encryption
Ipsec SA Hash	see ISAKMP SA Hash
Ipsec Lifetime	Lifetime of the Ipsec SA key. Standard setting 28800 seconds (8 hours) max. setting value 86400 seconds (24 hours)
Perfect Forward Secrecy (PFS)	Activating (=Yes) or deactivating (=No) the PFS function.
DH/PFS Group	In the Ipsec the keys are renewed in certain intervals during data exchange. At this new random numbers are negotiated with the remote station in the key exchange process. Selection of the process.
Dead Peer Detection	If the remote station supports such a protocol it is possible to check if the connection is "dead" or not. The system tries to re-establish the connection. **No:** No dead peer detection **Yes:** If VPN initiate is enabled the system tries to restart "Restart". In the function VPN accept the connection will be closed "Clear".
DPD Delay (sec.)	Time interval in seconds during which the peer connection is being checked.
DPD Timeout (sec.)	Time period in seconds after which a timeout is being performed.

VPN-IPsec

Certificates



CT-Router LAN

IPsec Certificates

Load Remote Certificate (.cer .crt)

Upload	Durchsuchen... Keine Datei ausgewählt.	Apply

Load Own PKCS#12 Certificate (.p12)

Upload	Durchsuchen... Keine Datei ausgewählt.	Apply
Password		

Remote Certificates

Name

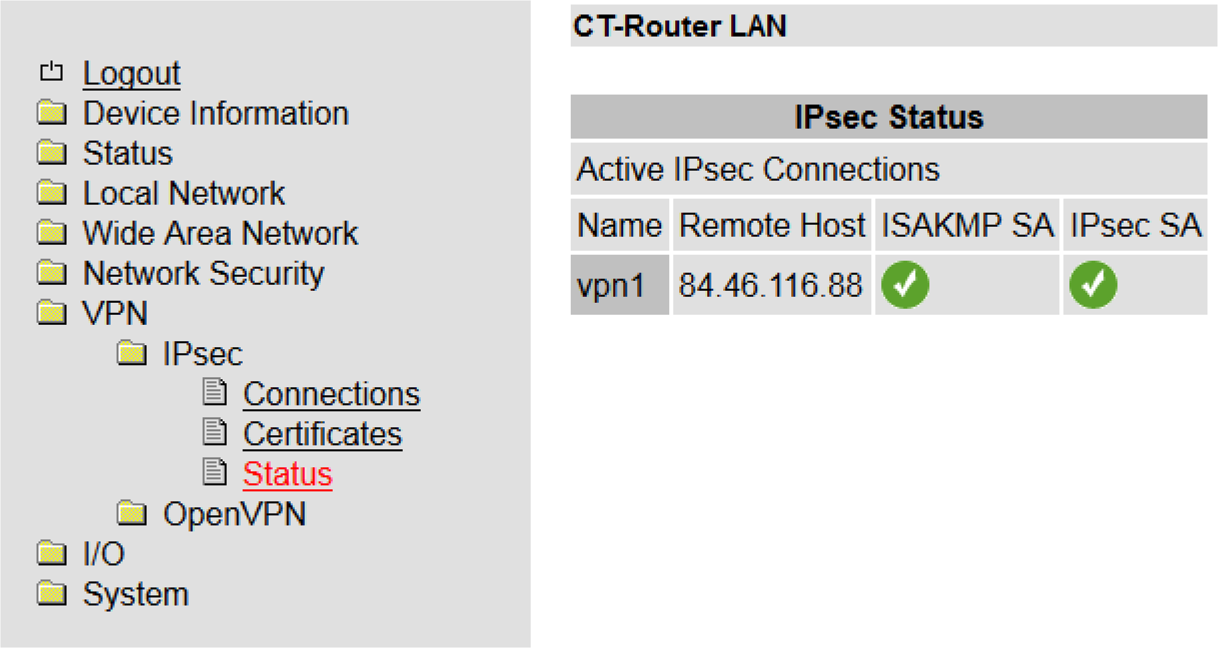
Own Certificates

Name

VPN → IPsec → Certificates	
Certificates	Explanation
Load remote certificate	Uploading of certificates which allow to perform an authentication for the router at the VPN remote station.
Load Own PKCS#12 Certificate	Uploading a certificate (pre-setting of the provider)
Password	Password for the PKCS#12 certificate / The password is assigned for export
Remote certificates	Here you will find an overview in tabular form of all "Remote certificates" / a certificate is deleted using the function "Delete"
Own certificates	Here you will find an overview in tabular form of all "Own certificates" / a certificate is deleted using the function "Delete"

VPN-IPsec

Status



IPsec Status

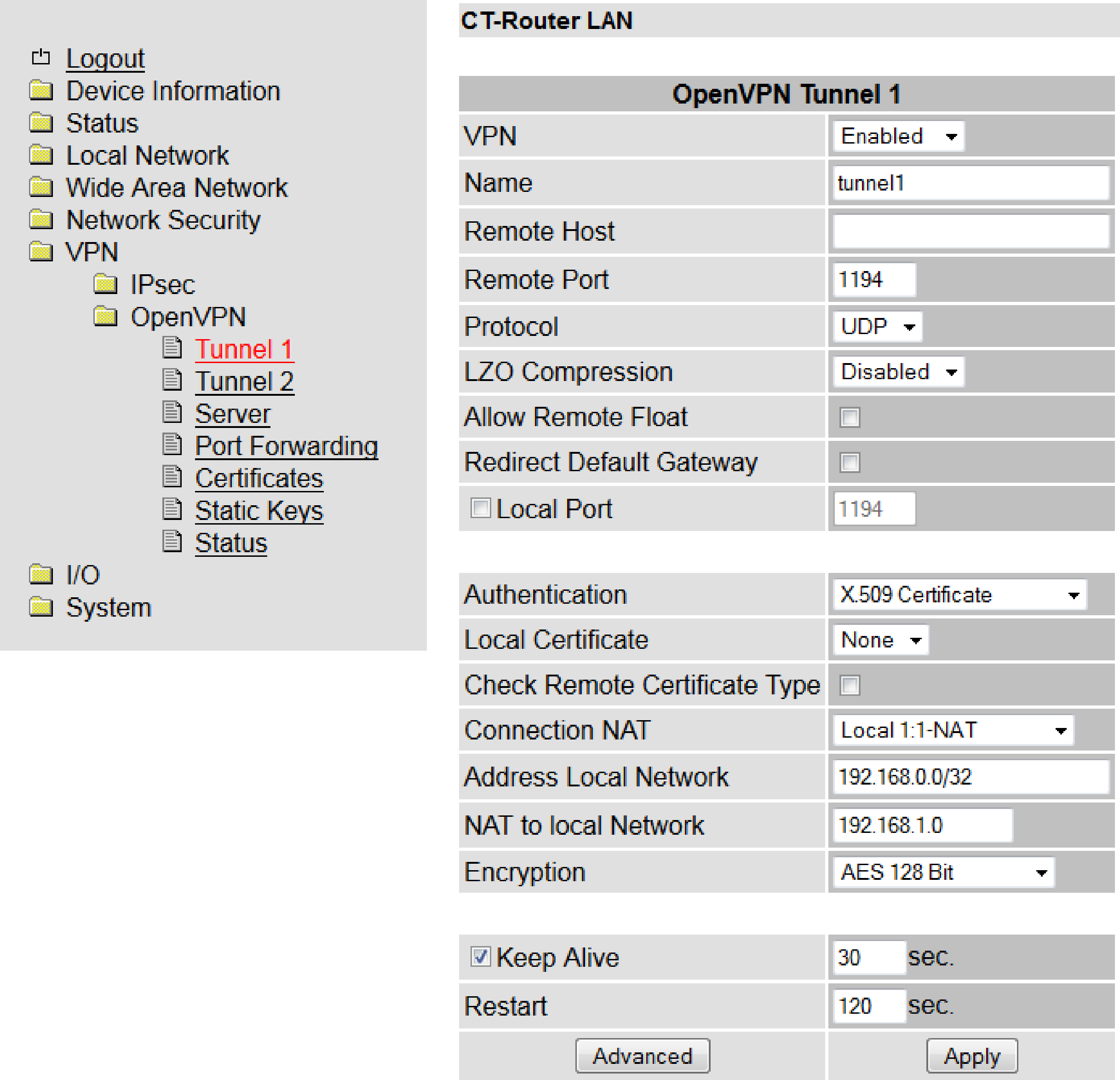
Active IPsec Connections

Name	Remote Host	ISAKMP SA	IPsec SA
vpn1	84.46.116.88	✓	✓

VPN → IPsec → Status	
Status	Explanation
Name	Name of the VPN connection
Remote host	IP address or URL of the remote station
ISAKMP SA	Activated (green field)
IPSec SA	Activated (green field)

VPN - OpenVPN

Tunnel



OpenVPN Tunnel 1	
VPN	Enabled
Name	tunnel1
Remote Host	
Remote Port	1194
Protocol	UDP
LZO Compression	Disabled
Allow Remote Float	□
Redirect Default Gateway	□
□ Local Port	1194
Authentication	X.509 Certificate
Local Certificate	None
Check Remote Certificate Type	□
Connection NAT	Local 1:1-NAT
Address Local Network	192.168.0.0/32
NAT to local Network	192.168.1.0
Encryption	AES 128 Bit
☑ Keep Alive	30 sec.
Restart	120 sec.

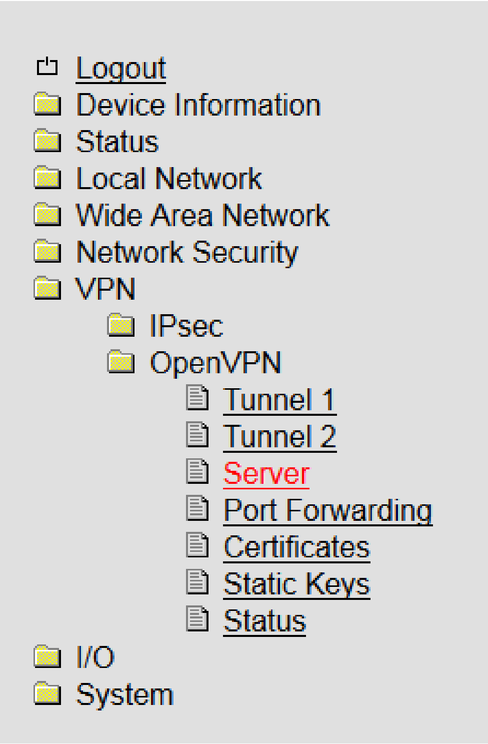
VPN → OpenVPN → Tunnel	
OpenVPN tunnel	Explanation
VPN	OpenVPN Tunnel activated (=Enable) or inactivated (=Disable)
Name	Name of the OpenVPN connection
Remote host	IP address or URL of the remote station
Remote pPort	Port of the remote station (Standard: 1194)
Protocol	Determine UDP or TCP protocol for the OpenVPN connection!
LZO compression	**Disabled:** No compression **Adaptive:** Adaptive compression **Yes:** Compression activated

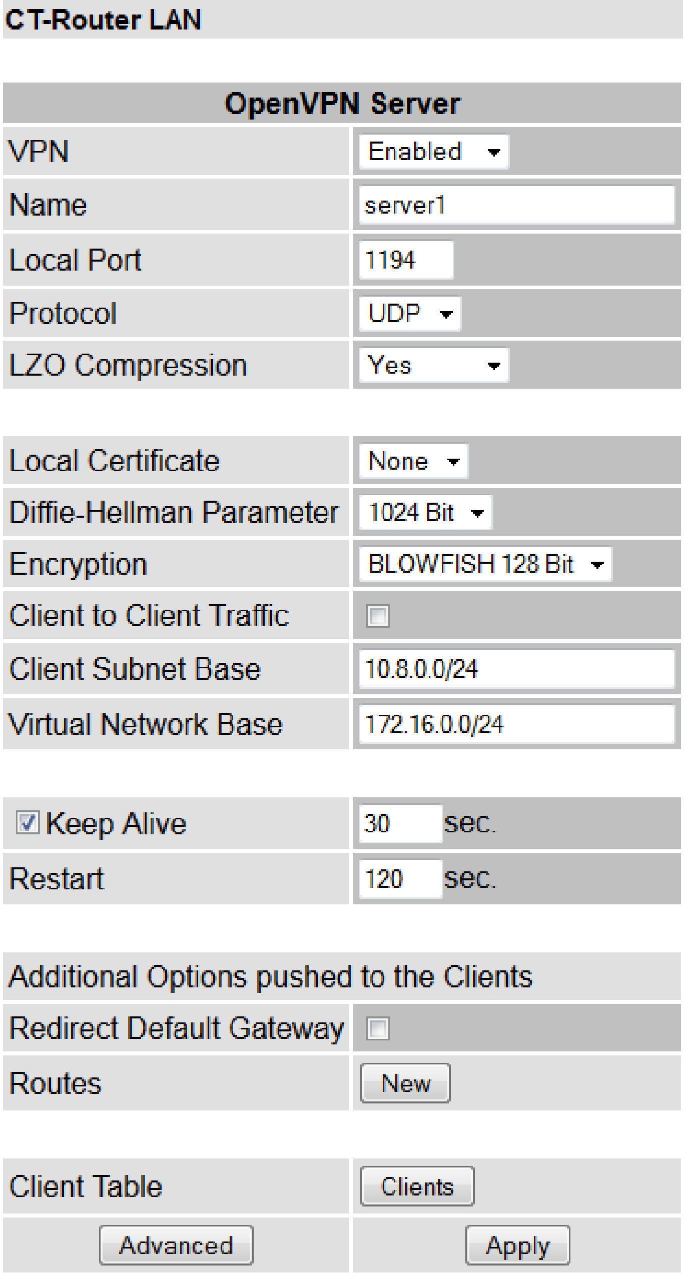
VPN - OpenVPN

Allow remote float	Option: For the communication with dynamic IP addresses the OpenVPN connection accepts authenticated packages of any IP address.
Local port	Local port
Authentication	Determine type of authentication of the OpenVPN connection (X.509 or PSK)!
Local certifacation	Certificate of the router for the authentication at the remote station.
Check remote certificate type	Option: Check certificates of the OpenVPN connection.
Address local network	IP address/subnet mask of the local network
Local 1:1 NAT	Option: IP address of the local network under which the network can/shallbe accessed by 1:1 NAT from the remote network.
Encryption	Encryption algorithm of the OpenVPN connection
Keep alive	Time interval in seconds of keep alive inquiries to the remote station
Restart	Time period in seconds after which the connection shall be restarted if there is no answer to the keep alive requests.

VPN - OpenVPN

Server




CT-Router LAN

OpenVPN Server	
VPN	Enabled
Name	server1
Local Port	1194
Protocol	UDP
LZO Compression	Yes
Local Certificate	None
Diffie-Hellman Parameter	1024 Bit
Encryption	BLOWFISH 128 Bit
Client to Client Traffic	□
Client Subnet Base	10.8.0.0/24
Virtual Network Base	172.16.0.0/24
☑ Keep Alive	30 sec.
Restart	120 sec.

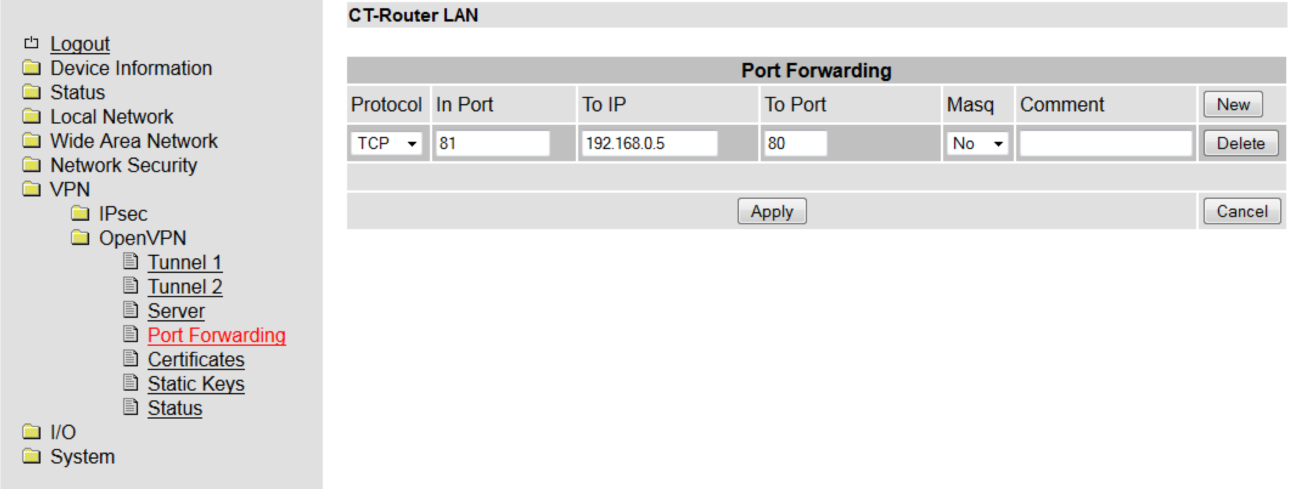
Additional Options pushed to the Clients	
Redirect Default Gateway	□
Routes	New
Client Table	Clients

VPN → OpenVPN → Tunnel	
OpenVPN tunnel	**Explanation**
VPN	OpenVPN Tunnel activated (=Enable) or inactivated (=Disable)
Name	Name of the OpenVPN connection
Local Port	Port of the local station (Standard: 1194)
Protocol	Determine UDP or TCP protocol for the OpenVPN connection!
LZO compression	**Disabled:** No compression **Adaptive:** Adaptive compression **Yes:** Compression activated

VPN - OpenVPN

Local certifacation	Certificate of the router for the authentication at the remote station.
Diffie-Hellman Parameter	
Encryption	Encryption algorithm of the OpenVPN connection
Client to Client Traffic	
Client Subnet Base	IP address/subnet mask of the local network
Virtual Network Base	Option: IP address of the local network under which the network can/shallbe accessed by 1:1 NAT from the remote network.
Keep alive	Time interval in seconds of keep alive inquiries to the remote station
Restart	Time period in seconds after which the connection shall be restarted if there is no answer to the keep alive requests.
Additional Options pushed to the Clients	
Redirect Default Gateway	
Routes	
Client Table	

Port Forwarding



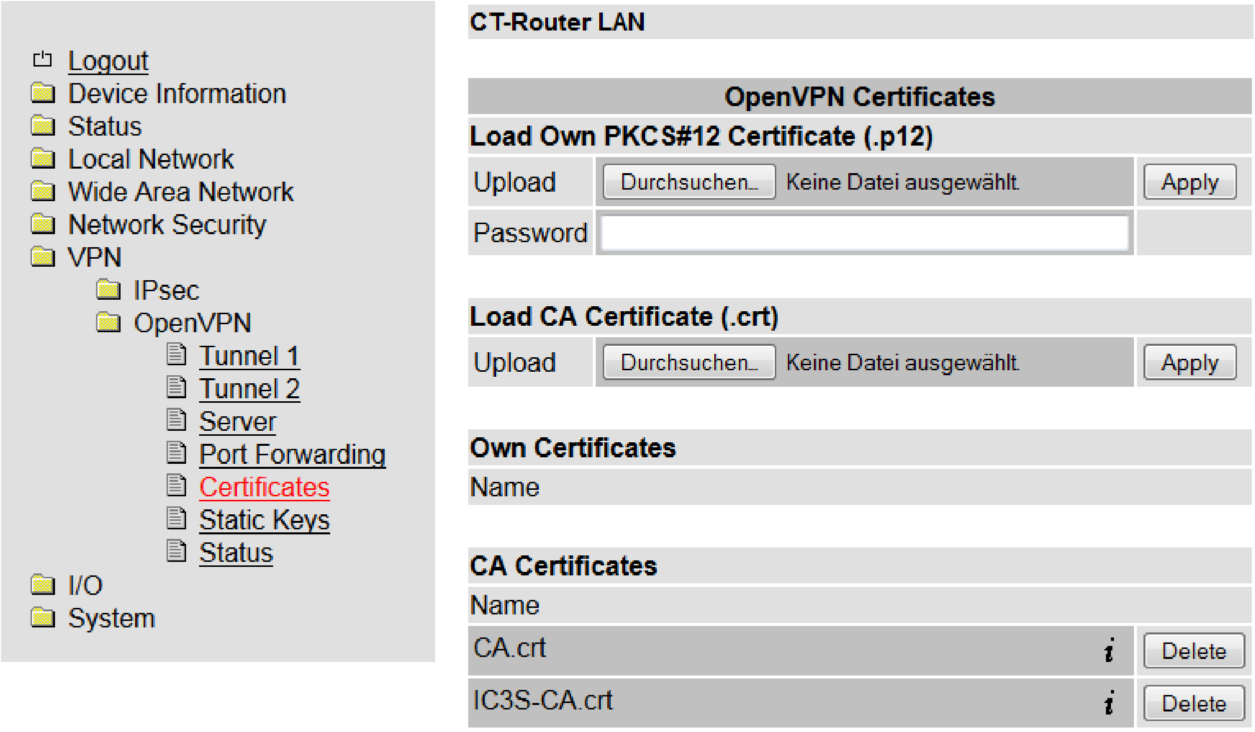
Port Forwarding

Protocol	In Port	To IP	To Port	Masq	Comment
TCP	81	192.168.0.5	80	No	

VPN → OpenVPN → Port Forwarding	
Port forwarding	**Explanation**
Protocol	Selection:TCP / UDP / ICMP
In port	Port no. incoming connection
To IP	IP address of target
To port	Port no. from target

VPN - OpenVPN

Certificates



CT-Router LAN

OpenVPN Certificates

Load Own PKCS#12 Certificate (.p12)

Upload: Keine Datei ausgewählt.

Password:

Load CA Certificate (.crt)

Upload: Keine Datei ausgewählt.

Own Certificates

Name

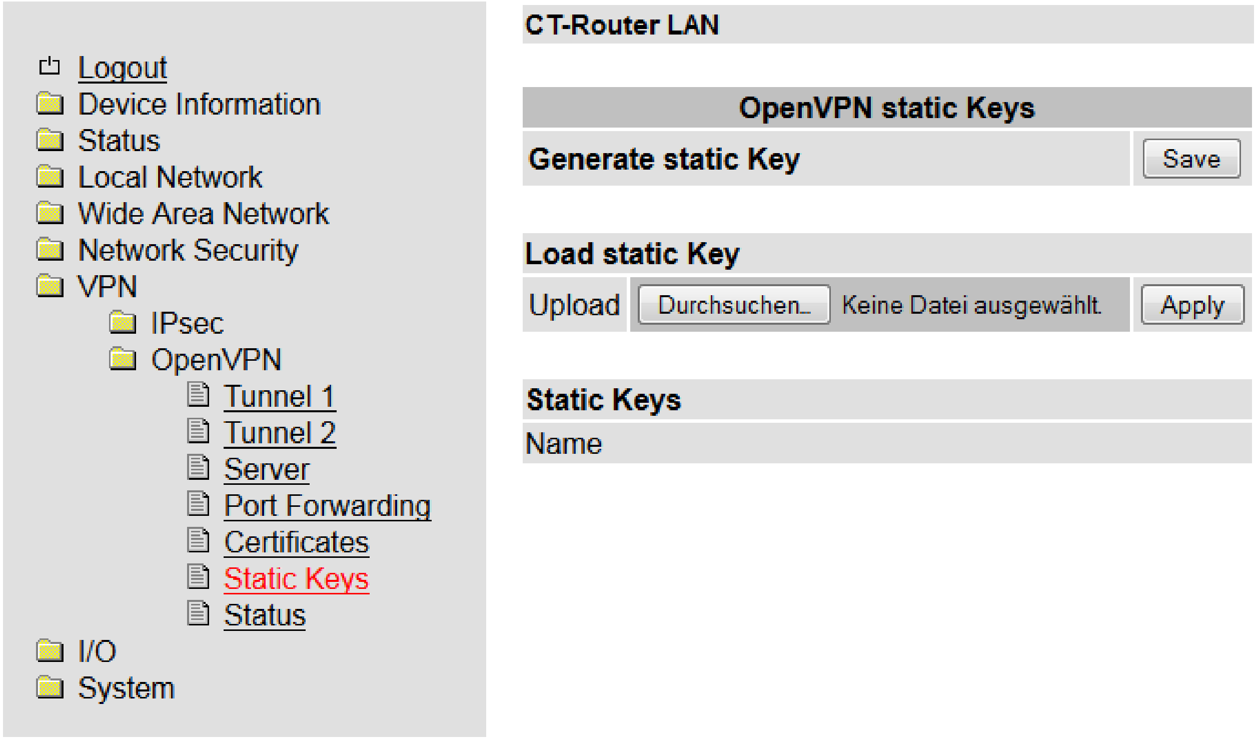
CA Certificates

Name
CA.crt
IC3S-CA.crt

VPN → OpenVPN → Certificates	
OpenVPN certificates	Explanation
Load Own PKCS#12 certificate	Uploading a certificate which is originated from your provider.
Password	Password for the PKCS#12 certificate. The password is assigned during export.
Own certificates	Here you will find an overview in tabular form of all "Own certificates" / the certificates are deleted using the function "Delete"

VPN - OpenVPN

Static keys



CT-Router LAN

OpenVPN static Keys

Generate static Key

Load static Key

Upload Keine Datei ausgewählt.

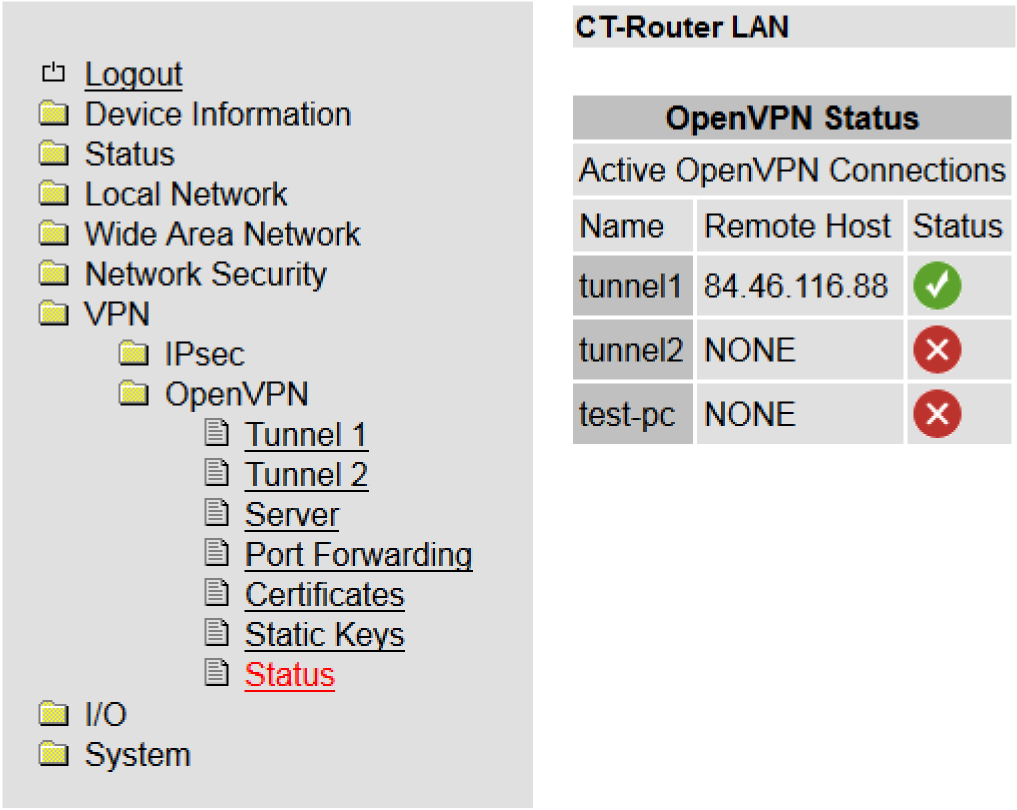
Static Keys

Name

VPN → OpenVPN → Static keys	
Static keys	**Explanation**
Generate static key	Generating and saving a static key.
Load static key	Load static key in the router (the remote station must have the same static key).
Static keys	Here you will find an overview in tabular form of all loaded static keys.

VPN - OpenVPN

Status



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

CT-Router LAN

OpenVPN Status

Active OpenVPN Connections

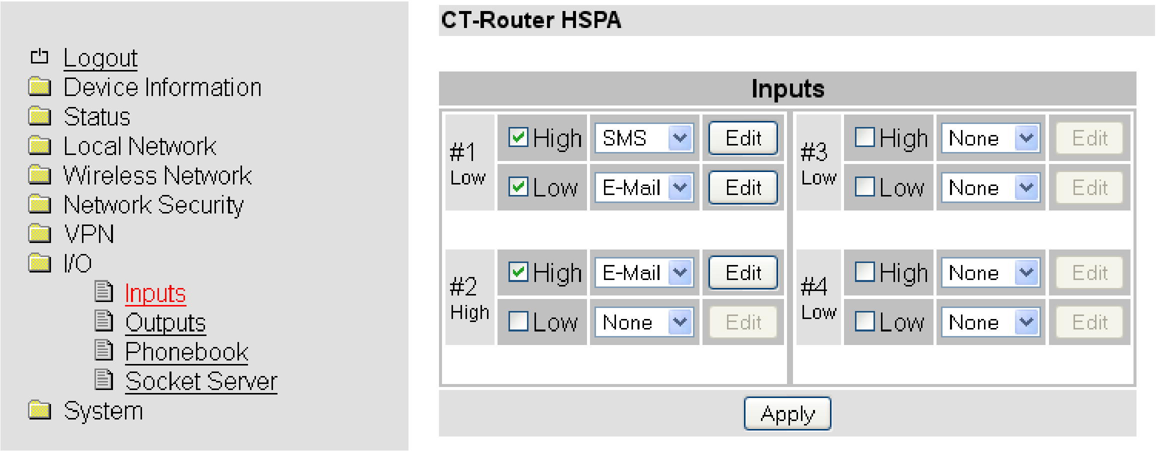
Name	Remote Host	Status
tunnel1	84.46.116.88	✓
tunnel2	NONE	✗
test-pc	NONE	✗

VPN → OpenVPN → Status	
OpenVPN status	Explanation
Name	Name of the VPN connection
Remote host	IP address or URL of the remote station
Status	Activated (=green field)

I/O

The CT-Router HSPA is equipped with four digital inputs and outputs which can be configured by you in the "I/O" menu.

Inputs

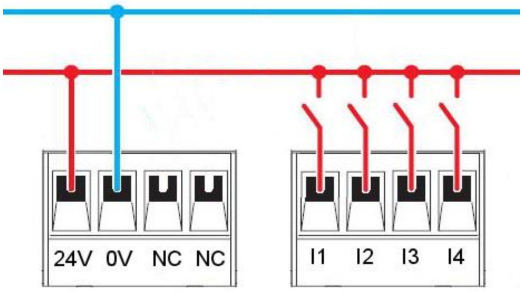


#1 Low	☑ High	SMS	Edit	#3 Low	□ High	None	Edit
	☑ Low	E-Mail	Edit		□ Low	None	Edit
#2 High	☑ High	E-Mail	Edit	#4 Low	□ High	None	Edit
	□ Low	None	Edit		□ Low	None	Edit

I/O →Inputs	
Inputs	**Explanation**
High	Option: In a high level it is possible to send a message via SMS or E-mail.
Low	Option: In a low level it is possible to send a message via SMS or E-mail.
If you only set one of the above described options it is necessary to confirm it by pressing the button "apply". Only then it is possible to edit the settings for the message. SMS: One or several phone numbers are selected from the stored phone book and you can determine an individual message text. E-mail: You can determine a recipient, a copy recipient, a subject and a message text.	

Connect switch inputs

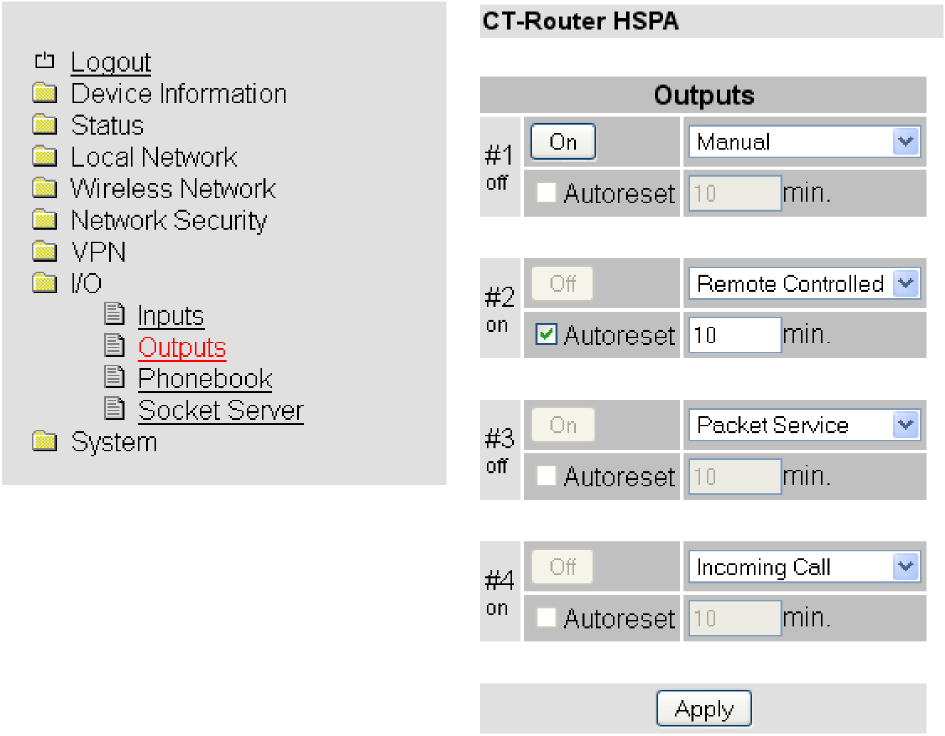
- Connect the switch inputs to the respective clamp
- Connect the switching inputs (I1 ... I4) to the 10 ... 30 V DC connection.
- The 0 V potential of the switch inputs must be connected to the "0V" clamp of the voltage connection.



Wiring the Inputs

I/O

Outputs



CT-Router HSPA

Outputs

#1 off: On · Manual · □ Autoreset 10 min.

#2 on: Off · Remote Controlled · ☑ Autoreset 10 min.

#3 off: On · Packet Service · □ Autoreset 10 min.

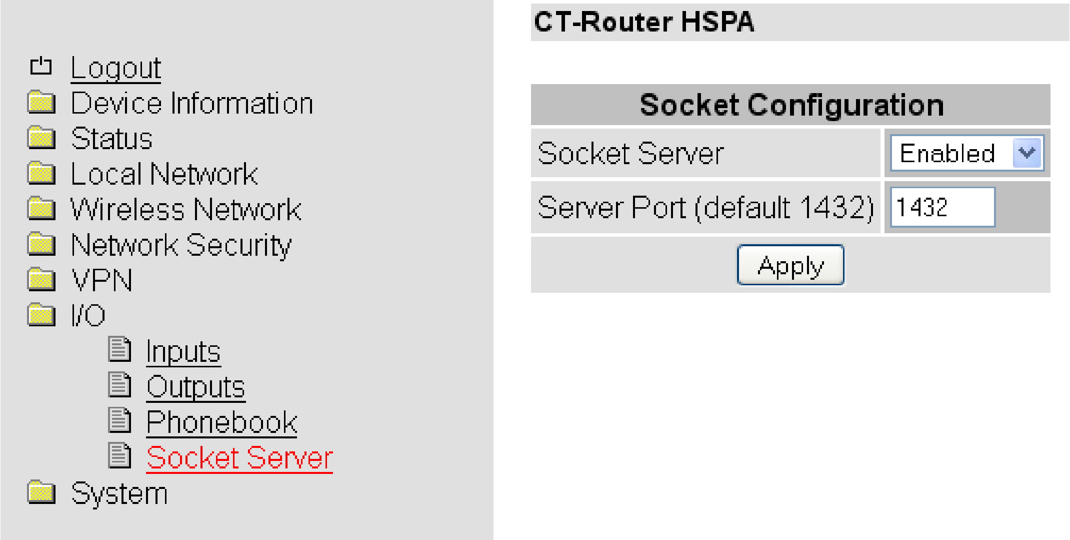
#4 on: Off · Incoming Call · □ Autoreset 10 min.

I/O →Outputs	
Outputs	**Explanation**
Optionen	Manual: The device is switched ON / OFF manually via the WBM. **Remote controlled:** Switching on / off by SMS or socket server. Additionally it is possible to use the function "autoreset" for which a time period in minutes is being determined. **Radio network:** Output is switched if the router engages in a mobile phone network. Package service: Output is switched if the router establishes a package connection and if an IP address has been assigned by the provider. **VPN service**: Output is switched if a VPN connection is existing. **Incoming call:** Output is switched if the router is called and if the phone number is in the phone book. **Connection lost:** The output is switched if a connection is interrupted.
Autoreset	Determine time period in minutes after which the output is reset.

The switching outputs (O1 ... O4) are for a maximum of 150 mA at 30 V DC 10 ... designed.
The 0 V potential of the switching outputs must be connected to the "0V" clampof the voltage connection

I/O

Socket Server



CT-Router HSPA

Socket Configuration

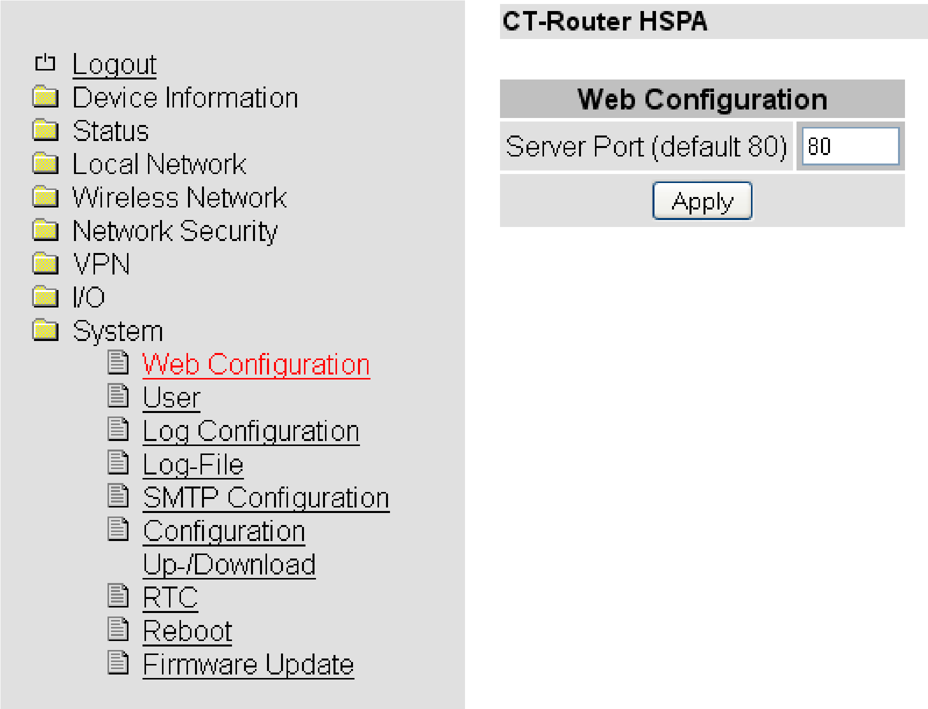
Socket Server	Enabled
Server Port (default 1432)	1432

I/O → Socket Server	
Socket server	**Explanation**
Socket server	**Disable:** Triggering of the router via Ethernet is deactivated. **Enable:** Triggering of the router via Ethernet is activated.
Server port (default 1432)	Determine socket server port (Port 80 cannot be used). Data which are send to the router have to be compliant with XML version 1.0. Example: <?xml version="1.0"?> <io> <input no="1" value="on"> <output no="2" value="off"> <output no="3" /> </io>

System

It is possible to make general settings for the AK-DinRail-3G-Router in the system menu.

Web configuration



CT-Router HSPA

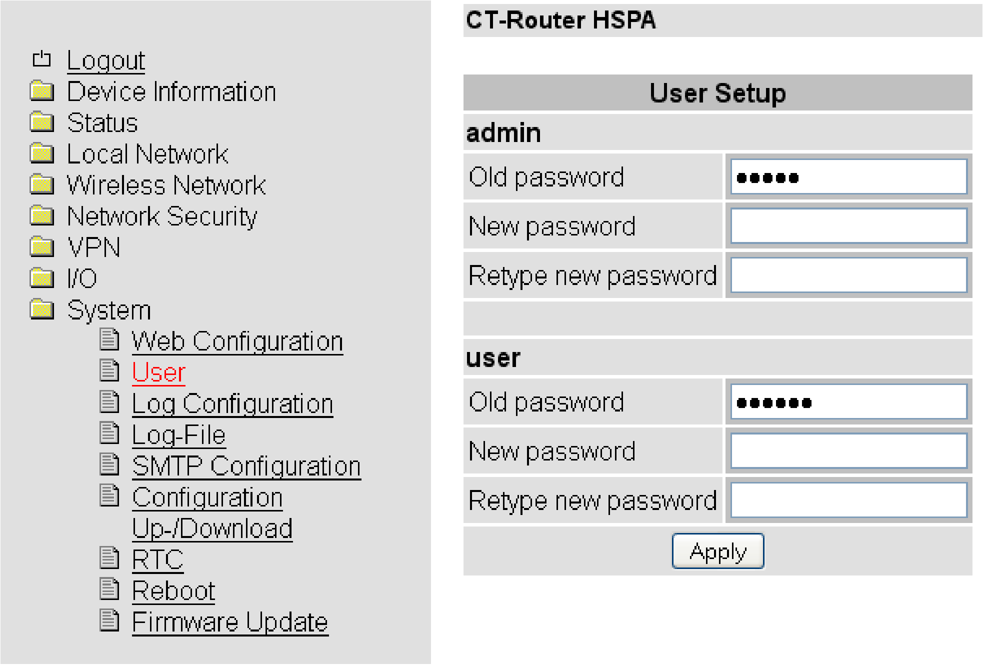
Web Configuration

Server Port (default 80): 80

System → Web configuration	
Web configuration	**Explanation**
Server Port (default 80)	Port setting for WBM via Internet browser.

System

User



CT-Router HSPA

User Setup

admin

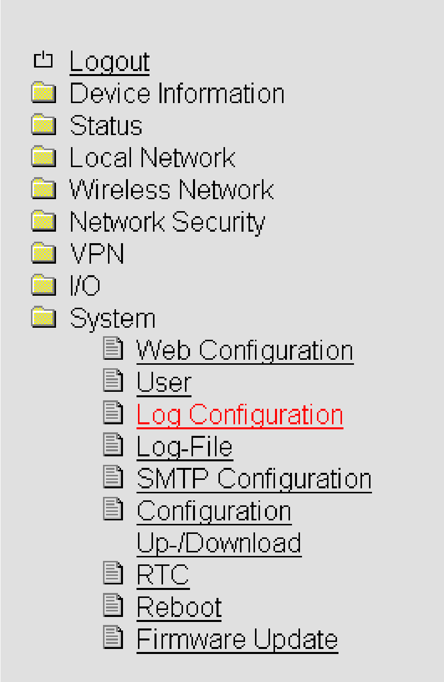
Old password	•••••
New password	
Retype new password	

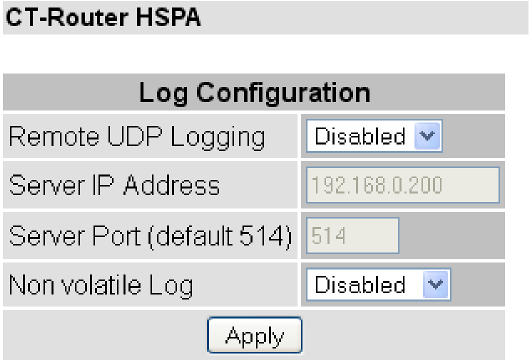
user

Old password	••••••
New password	
Retype new password	

System → User	
User	Explanation
admin	Unlimited access (writing and reading) Determine new password.
user	Limited access (only reading / not all areas) Determine new password.

Log configuration





CT-Router HSPA

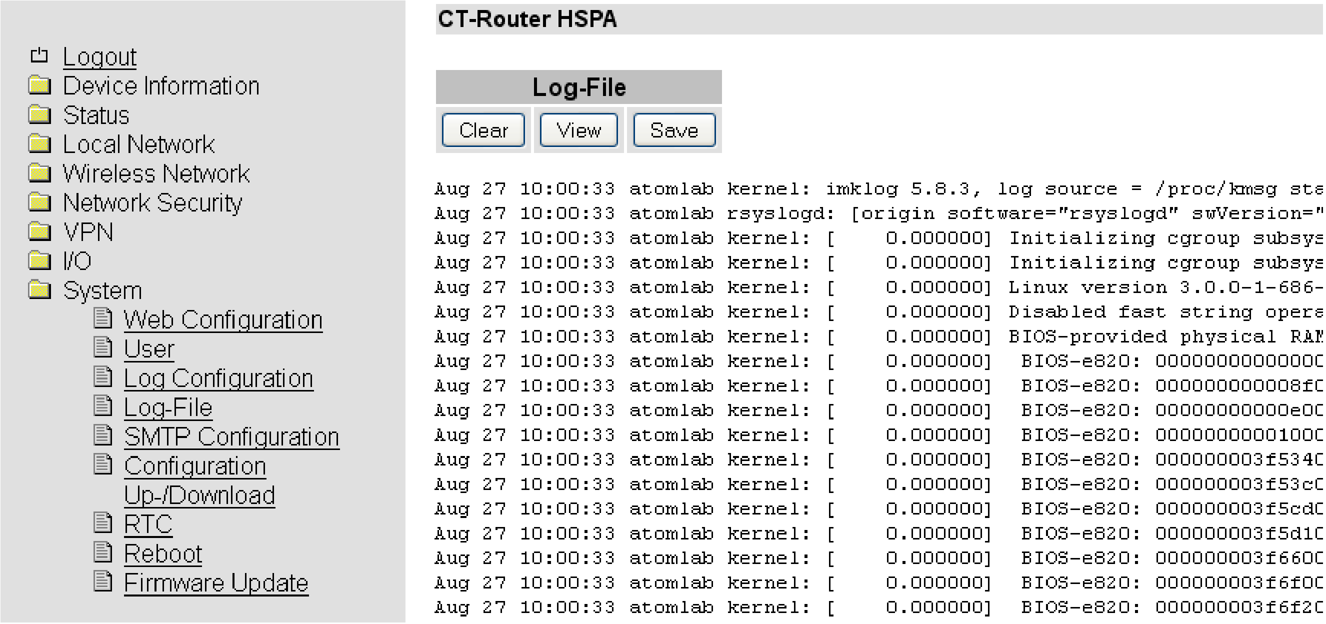
Log Configuration

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	**Explanation**
Remote UPD logging	**Disabled:** External logging deactivated. **Enabled:** External logging activated.
Server IP Address	IP address of the external log server.
Server port (default 514)	Port of the external log server.
Non volatile log	**Disable:** Saves the log internal / on a previously determined server. **USB stick:** Saves the log on a USB stick. The USB stick has to be connected to the router! **SD card:** Saves the log on an SD card. The SD card holder is available upon customer request an SD card will be optionally installed

System

Log file

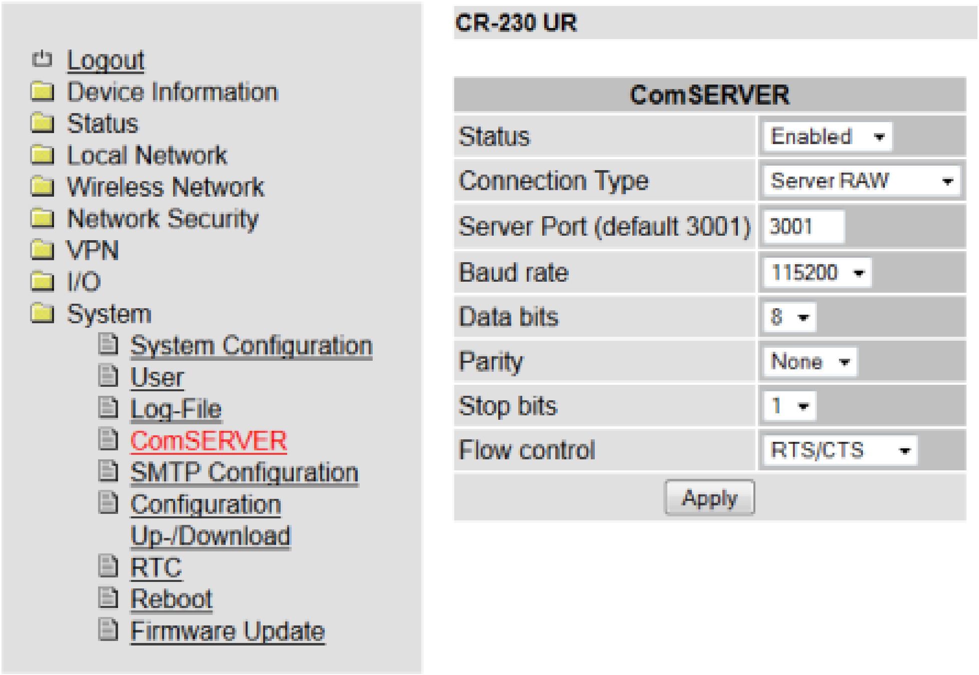


```
Aug 27 10:00:33 atomlab kernel: imklog 5.8.3, log source = /proc/kmsg sta
Aug 27 10:00:33 atomlab rsyslogd: [origin software="rsyslogd" swVersion="
Aug 27 10:00:33 atomlab kernel: [    0.000000] Initializing cgroup subsys
Aug 27 10:00:33 atomlab kernel: [    0.000000] Initializing cgroup subsys
Aug 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 opera
Aug 27 10:00:33 atomlab kernel: [    0.000000] BIOS-provided physical RAM
Aug 27 10:00:33 atomlab kernel: [    0.000000]  BIOS-e820: 00000000000000
Aug 27 10:00:33 atomlab kernel: [    0.000000]  BIOS-e820: 000000000008f0
Aug 27 10:00:33 atomlab kernel: [    0.000000]  BIOS-e820: 00000000000e00
Aug 27 10:00:33 atomlab kernel: [    0.000000]  BIOS-e820: 00000000001000
Aug 27 10:00:33 atomlab kernel: [    0.000000]  BIOS-e820: 000000003f5340
Aug 27 10:00:33 atomlab kernel: [    0.000000]  BIOS-e820: 000000003f53c0
Aug 27 10:00:33 atomlab kernel: [    0.000000]  BIOS-e820: 000000003f5cd0
Aug 27 10:00:33 atomlab kernel: [    0.000000]  BIOS-e820: 000000003f5d10
Aug 27 10:00:33 atomlab kernel: [    0.000000]  BIOS-e820: 000000003f6600
Aug 27 10:00:33 atomlab kernel: [    0.000000]  BIOS-e820: 000000003f6f00
Aug 27 10:00:33 atomlab kernel: [    0.000000]  BIOS-e820: 000000003f6f20
```

System → Log-File	
Log-File	**Explanation**
Clear	Entries in the internal log file are deleted.
View	Log file entries are displayed in the browser window.
Save	Log file is saved.

System

ComSERVER - Serielle Schnittstelle konfigurieren (optional)



ComSERVER	
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

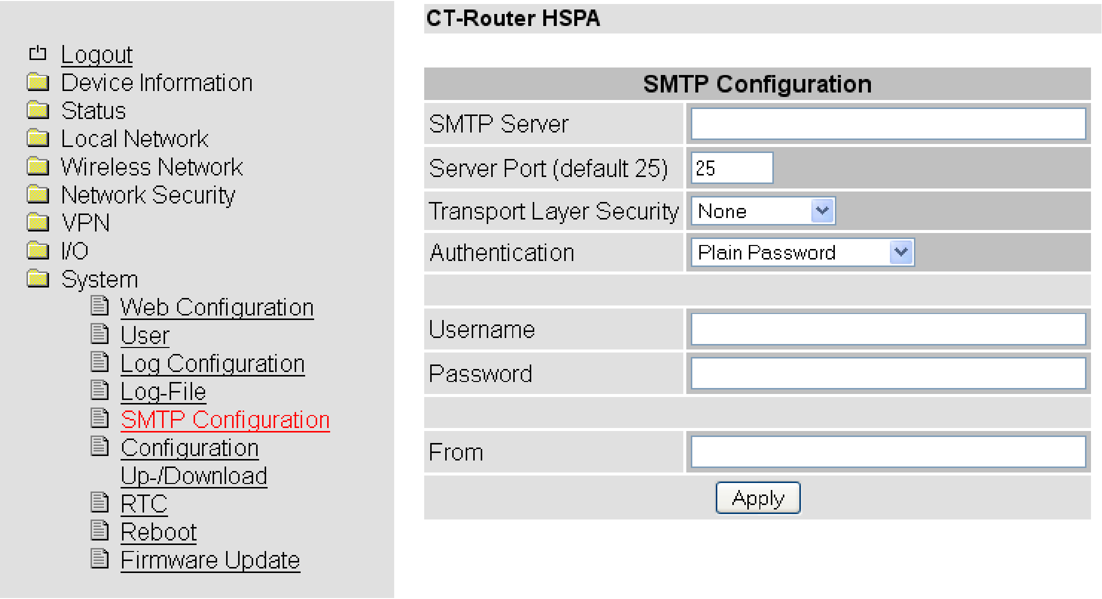
System →ComSERVER	
ComSERVER	**Explanation**
Satus	Schnittstelle: Disabled / Enabled
Connection Type	Einstellen der seriellen Verbindung – RAW oder RFC2217
Server Port (default 3001)	Auswahl des Ports für die Netzwerkkommunikation
Baud Rate	300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 Baud
Data bits	Datenformat einstellen: Wählen Sie die Einstellungen für Datenbits, Parität und Stoppbits
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

System

SMTP Configuration



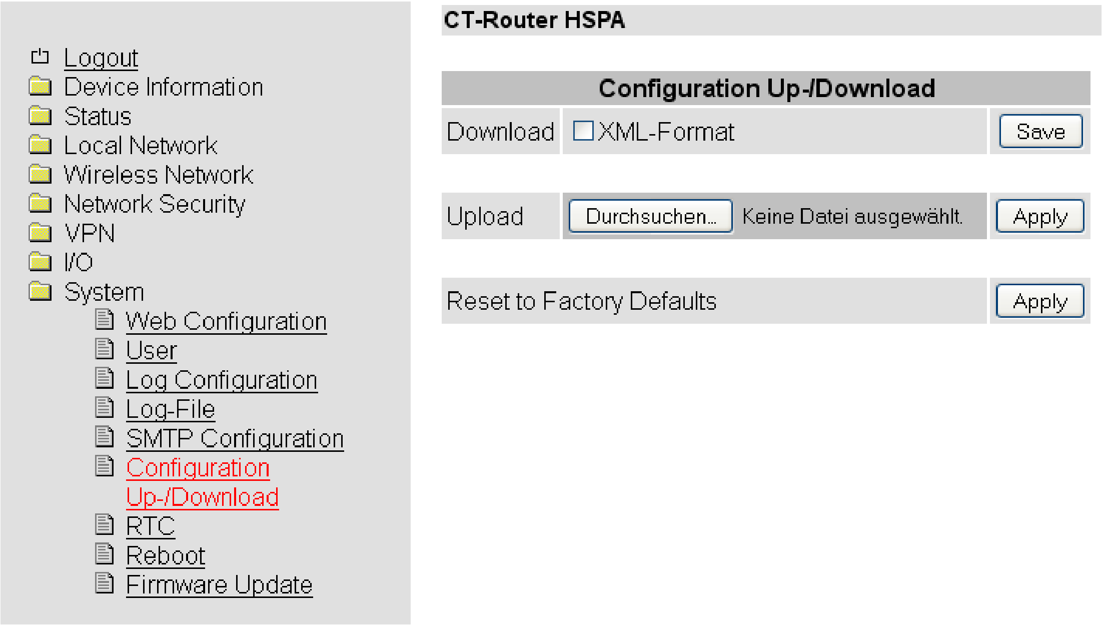
CT-Router HSPA

SMTP Configuration	
SMTP Server	
Server Port (default 25)	25
Transport Layer Security	None
Authentication	Plain Password
Username	
Password	
From	

System →SMTP Configuration	
SMTP configuration	**Explanation**
SMTP Server	IP address / host name of the SMTP server
SMTP Port (default 25)	Port of the SMTP server
Transport layer security	Encryption: None, STARTTLS, SSL/TLS
Authentication	No authentication: No authentication Plain password: Authentication user name and password (unencrypted transmission of the authentication data). Encrypted password: Authentication with user name and password (unencrypted transmission of the authentication data).
Username	User name
Password	Password
From	sender of the mail

System

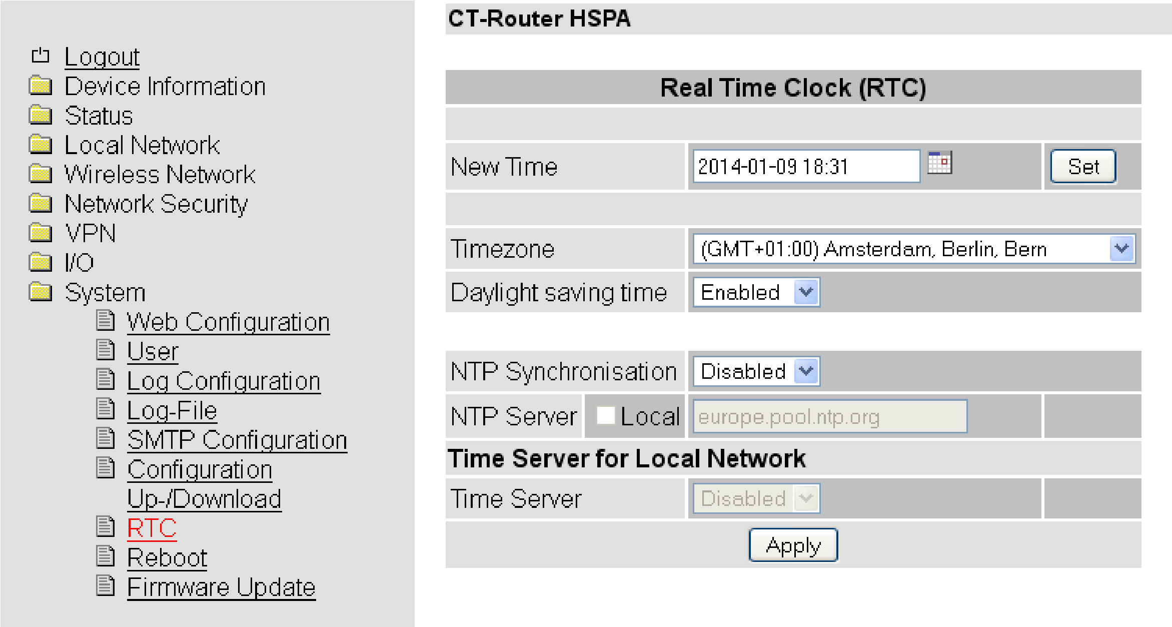
Configuration Up-/Download



System → Configuration Up-/Download	
Up-/Download	**Explanation**
Download	Download current configurations.
Upload	Upload secured or modified configuration and confirm by pressing the button "apply".
Reset to factory defaults	Reset the configuration and IP settings to factory settings. Uploaded certificates are maintained.

System

RTC



CT-Router HSPA

Real Time Clock (RTC)

New Time	2014-01-09 18:31
Timezone	(GMT+01:00) Amsterdam, Berlin, Bern
Daylight saving time	Enabled
NTP Synchronisation	Disabled
NTP Server □ Local	europe.pool.ntp.org

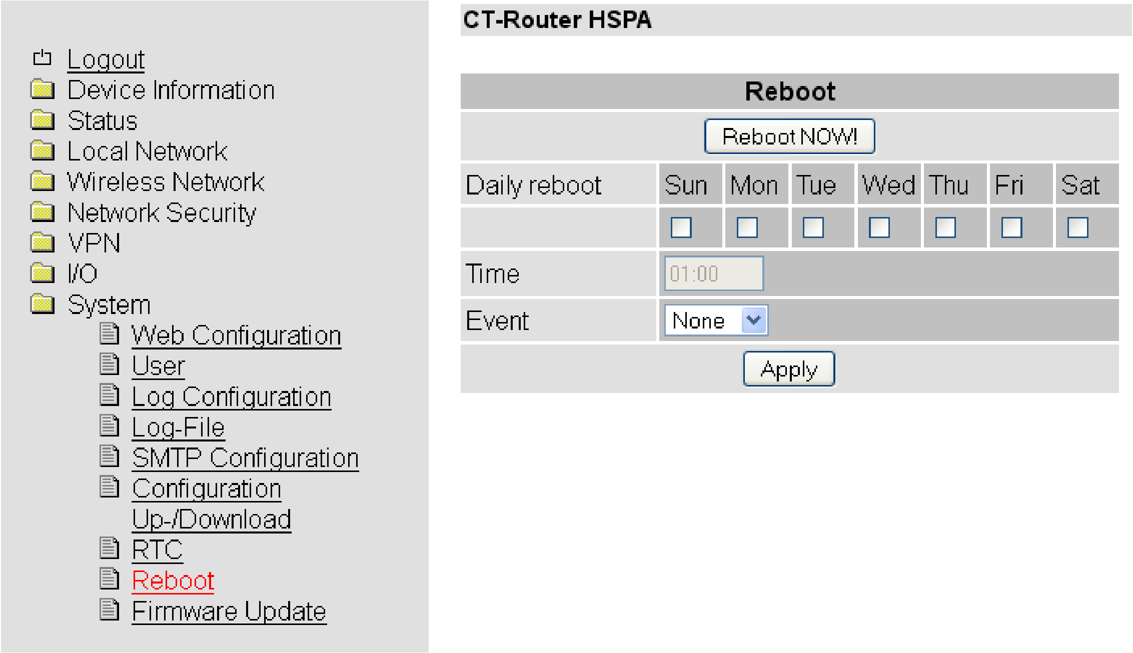
Time Server for Local Network

Time Server	Disabled

System → RTC	
RTC	**Explanation**
New Time	Manuelle Zeitkonfiguration, falls kein NTP-Server vorhanden ist.
Time zone	Selection of time zone.
Daylight saving time	**Disable:** Consideration of summertime deactivated. **Enable:** Consideration of summertime activated.
NTP Synchronisation	Date and time can be synchronized using an NTP server. If this function is used for the first time the first synchronisation may take up to 15 minutes.
NTP Server	The router can be set as NTP server in the LAN network. To do so an address of an NTP server is required. The NTP synchronisation must be set to enable.
Time Server	**Disable:** Time sever function for the local network is deactivated. **Enable:** Time sever function for the local network is activated.

System

Reboot

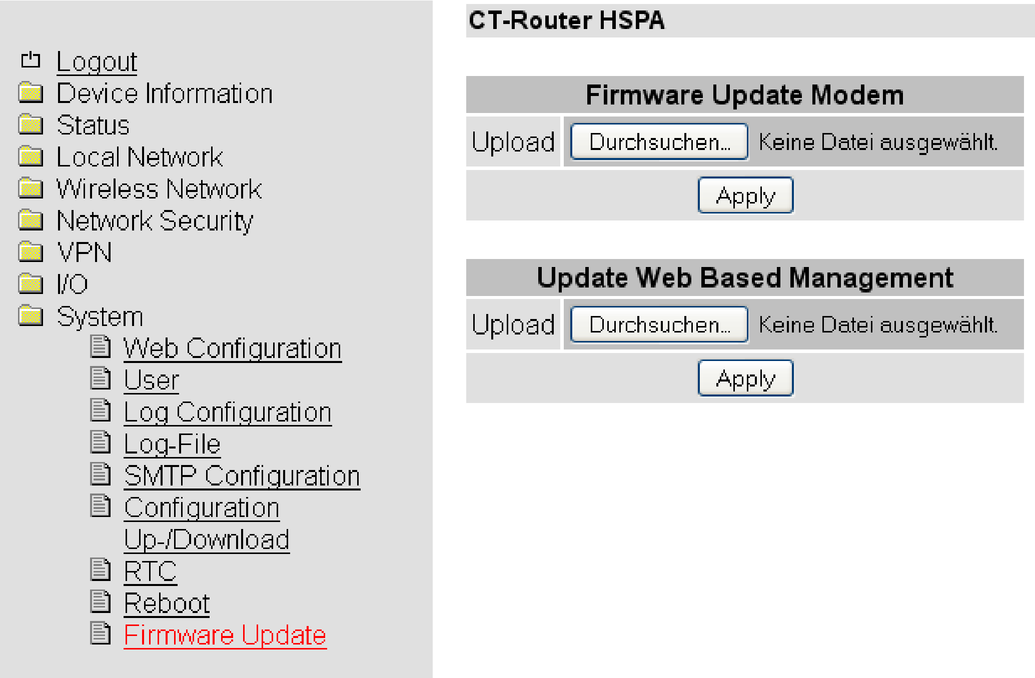


Daily reboot	Sun	Mon	Tue	Wed	Thu	Fri	Sat
	□	□	□	□	□	□	□
Time	01:00						
Event	None						

System → Reboot	
Reboot	**Explanation**
Reboot NOW!	Force immediate restart of the router!
Daily reboot	Restart the router on certain days of a week at a certain point in time. Determine the days of the week for the restart by clicking on the check box.
Time	Time of the restart (hour: minute).
Event	The router can be restarted with a digital input. The signal should be "Low" after a restart.

System

Firmware update



CT-Router HSPA

Firmware Update Modem

Upload Keine Datei ausgewählt.

Update Web Based Management

Upload Keine Datei ausgewählt.

System → Firmware update	
Reboot	Explanation
Firmware update modem	These updates provide for function extensions and product updates.
Update Web based management	These updates refer to the configuration via an Internet browser.

Inquiry and control via XML files

Format of the XML files

Each file starts with the header:

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

oder

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

Followed by the base entry.
The following basic entries are available:

```
<io>            </io>              # I/O system
<info>          </info>            # Query General Information
<cmgr ...>      </cmgr>            # send SMS (mobile phones only)
<email ...>     </email>           # send email
```

All data are encoded in UTF-8.
The following characters must be transmitted as sequences:

```
&  -  &amp;
<  - &lt;
>  -  &gt;
"  -  &quot;
'  -  &apos;
```

Examples of the basic entries:
a) I/O system

```
<?xml version="1.0"?>
<io>
<output no="1"/>                  # State of output 1 query
<output no="2" value="on"/>       # switch on output 2
<input no="1"/>                   # State of input 1 query
</io>
```

Note: As a "value" can be used both on / off and 0/1 are given. Is always returned on or off

The system returns something like this:

```
<?xml version="1.0" encoding="UTF-8"?>
<result>
<io>
<output no="1" value="off"/>      # State of output 1;
<output no="2" value="on"/>       # State of output 2;
<input no="1" value="off"/>       # State of input 1;
</io>
</result>
```

Note, outputs which should be remote controlled "remote controlled" must be configured

Inquiry and control via XML files

b) Query General Information

```
<?xml version="1.0"?>
<info>
<device />              # query device data
<radio />               # Query data for radio communication (mobile phones only)
</info>
```

The system returns something like this:

```
<?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) send SMS

```
<?xml version="1.0"?>
<cmgs destaddr="0123456789"> This is the SMS text </cmgs>
```

The system returns something like this:

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

d) send eMail

```
<?xml version="1.0"?>
<email to="x.yz@diesunddas.de" cc="info@andere.de">
<subject>Test Mail</subject>
<body>

        This is a multiline text email.
        Best regards, your router

</body>
</email>
```

The response is delivered as follows:

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

or in case of an error:

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

Notes regarding the presentation: The indentations and line breaks only serve for a better understanding and do not need to be sent nor are they sent. All received data shall be interpreted using an XML-Parser such as e.g. Expat.

3. Sending and receiving data

The communication is performed as follows:

- Establish a connection to the socket server
- Send data
- Interpret return data using the XML-Parser
- Close connection

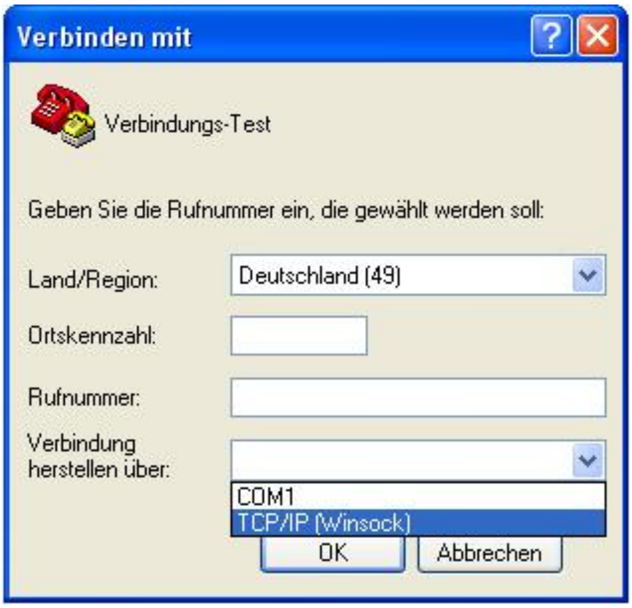
Functional test

Functional test by means of Windows Hyperterminal

In order to perform a test it is possible to use the known program "Hyperterminal" under Windows. Using Hyperterminal it is possible to send XML files to the socket server of the router. The corresponding XML files (see chapter "Inquiry and control via XML files") need to be saved on your user PC beforehand.
Open the Hyperterminal and configure the desired connection (Here an example using default settings):

Host address:	192.168.0.1 (IP address of the router / socket server)
Connection number:	1432 (Port of the socket server)
Establish connection via:	TCP/IP (Winsock)

Open



Verbinden mit

Verbindungs-Test

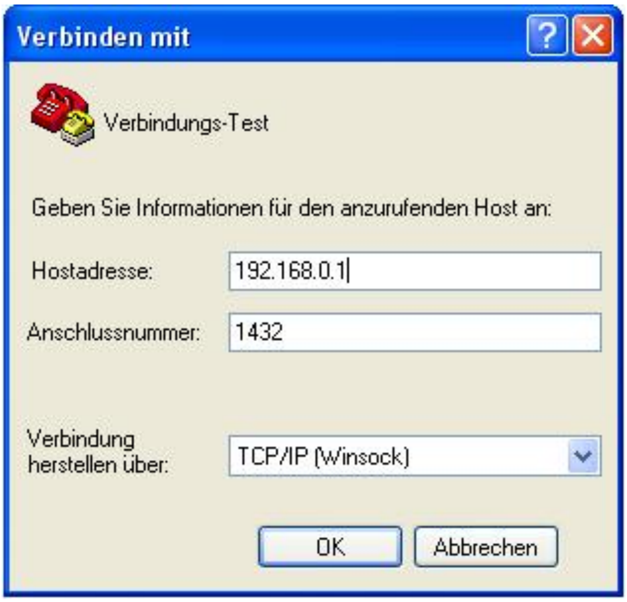
Geben Sie die Rufnummer ein, die gewählt werden soll:

Land/Region: Deutschland (49)

Ortskennzahl:

Rufnummer:

Verbindung herstellen über:



Verbinden mit

Verbindungs-Test

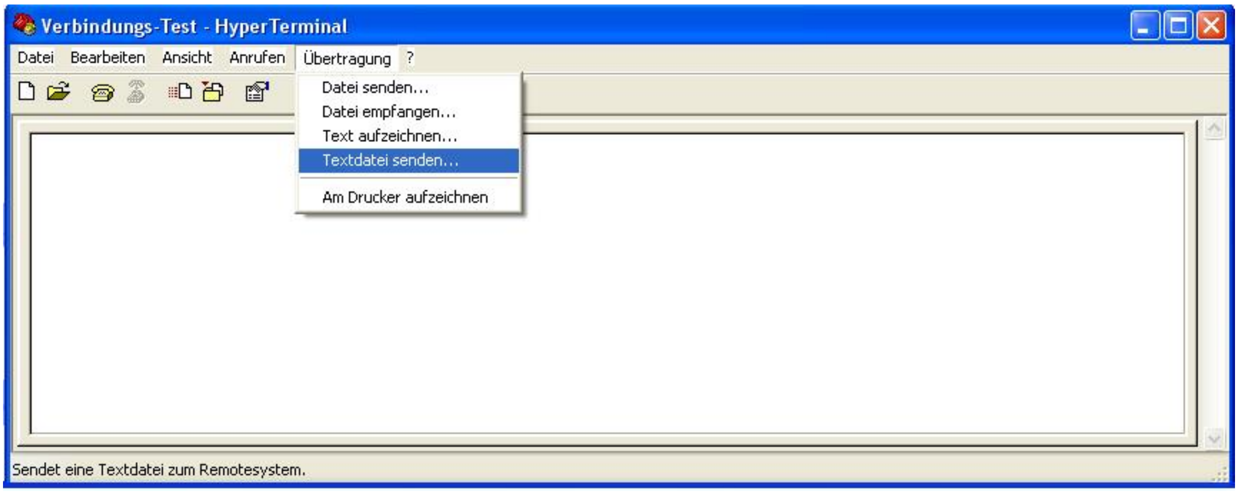
Geben Sie Informationen für den anzurufenden Host an:

Hostadresse: 192.168.0.1

Anschlussnummer: 1432

Verbindung herstellen über: TCP/IP (Winsock)

Open the connection and select the XML file which needs to be transferred in the menu of the Hyperterminal "Transfer / send text file...".



Verbindungs-Test - HyperTerminal

Sendet eine Textdatei zum Remotesystem.

After the successful transfer you will receive the answer to your inquiry.

Examples of an application

Establishing a connection to the Internet

Using the AK-DinRail-ROUTER you have access to the Internet via mobile phone networks.
A SIM card of your mobile phone provider which is released for package services
e.g. GPRS/EDGE or UMTS/HSPDA is required.
In this application the AK-DinRail-ROUTER is:

- Router
- Default gateway
- DNS server
- Firewall

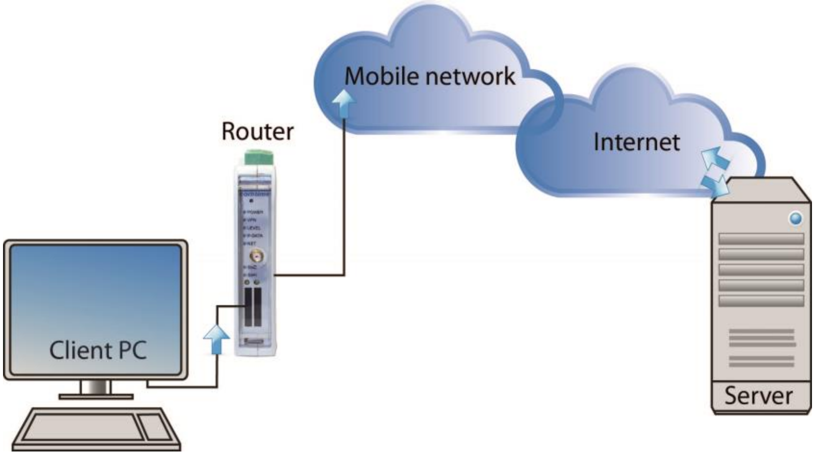
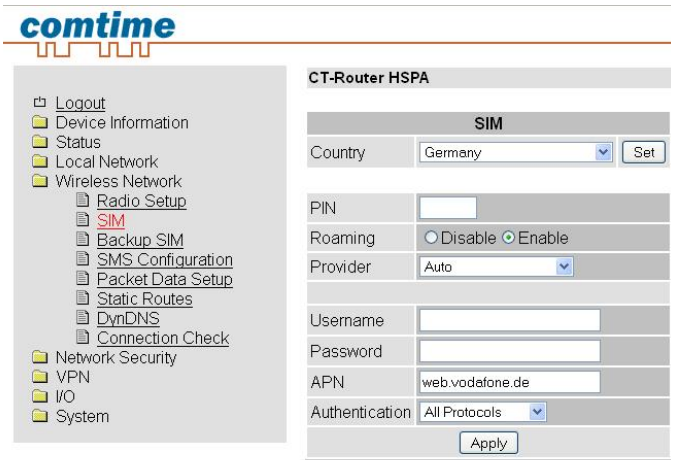


Illustration: Access to the Internet

Before start-up please check if your provider provides sufficient network coverage otherwise it is not possible to establish data connections

Configuring the ROUTER:

- Open a browser on the PC.
- Enter the IP address in the address field of the browser (default 192.168.0.1)
- Enter user name and password (Default: user name "admin" and password "admin")
- Open the "Wireless network" and "SIM" and enter the PIN number of the SIM card in the field "PIN". Additionally enter the access data, APN, user name and password for the package data transfer on your mobile phone network. You will receive the access data from your mobile phone provider.



CT-Router HSPA

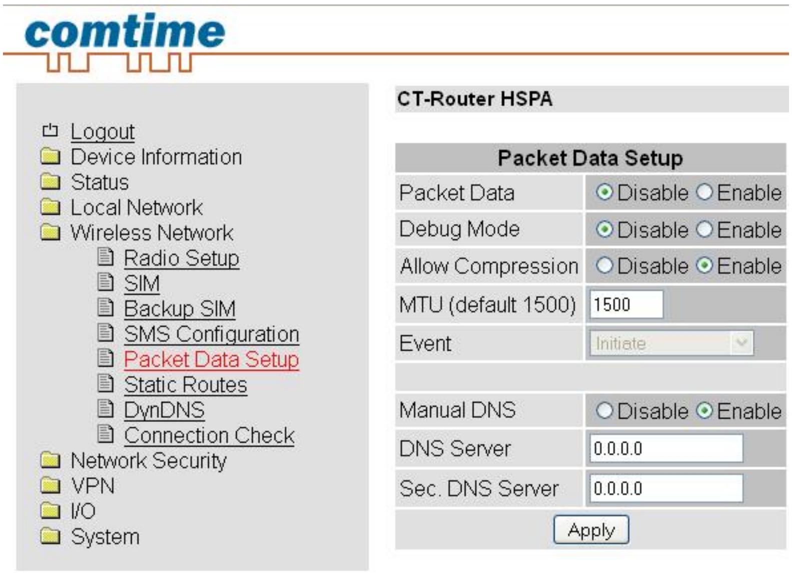
SIM

Country	Germany [Set]
PIN	
Roaming	○ Disable ● Enable
Provider	Auto
Username	
Password	
APN	web.vodafone.de
Authentication	All Protocols

Apply

Examples of an application

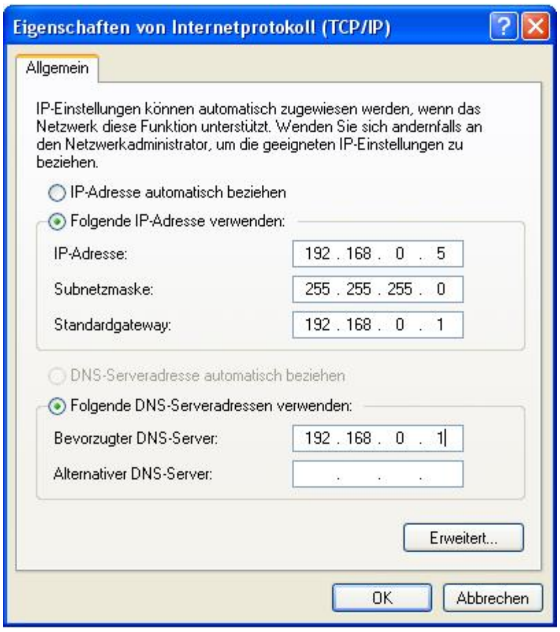
- Change over to a "Wireless network" and "Packed data setup" and activate the package data transfer in the mobile phone network.
  To do so, set "Package data" to "Enable".



CT-Router HSPA

Packet Data Setup	
Packet Data	● Disable ○ Enable
Debug Mode	● Disable ○ Enable
Allow Compression	○ Disable ● Enable
MTU (default 1500)	1500
Event	Initiate
Manual DNS	○ Disable ● Enable
DNS Server	0.0.0.0
Sec. DNS Server	0.0.0.0

- In order to access the Internet with your PC you have to enter the IP address of the router as default gateway and as DNS server in the network settings.
  Please find the settings for your operating system in the corresponding documentation.



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:	. . .