Manual

AK-DINRAIL-xG-Router

AK-DINRAIL-3G

AK-DINRAIL-4G

AK – Nord
EDV- Vertriebsges. mbH
Stormstrasse 8
D-25524 Itzehoe
Germany

Phone: +49 (0) 4821 8040350
Fax: +49 (0) 4821 4083024

Contents

Contents

Technical data

Supply	
Supply voltage	10V DC … 30V DC via pluggable screw terminals
Nominal current consumption	< 200mA at 24V, < 580mA at 10V
Standby current consumption	< 90mA at 24V
LED display	Power (LED green), Continuous light: Operation

Interface	
Network interface	
LTE frequencies (Only AK-DinRail-4G)	800 MHz, 850 MHz, 900 MHz,1800 MHz,1900 MHz,2100 MHz, 2600 MHz
Transmitting power	23 dB
LTE compatibility	LTE FDD: DL 100 Mbps/UL 50 Mbps @20M BW cat3
UMTS frequencies	850 MHz, 1900 MHz, 2100 MHz (UMTS/HSPA)
Transmitting power	0.25 W
UMTS compatibility	UMTS/HSPA 3GPP release 6 HSUPA max. 5.76Mbps HSDPA max. 7.2Mbps
SIM interface	2 interfaces, 1.8 volts and 3 volts SIM card
GSM frequencies	850 MHz, 900 MHz, 1800 MHz, 1900 MHz (GPRS/EDGS)
Transmitting power	Max. 2.0 W
GPRS compatibility	GPRS Class 12, Class B, Coding scheme: CS1 ... CS4
EDGE	EDGE (E-GRPS) Multislot Class 10
Antenna connection	50 Ω impedance SMA antenna socket
LED	SIM (LED green),NET (LED bargraph)
Ethernet interface	
Contact termination	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 indicator	ACT (LED yellow), Ethernet data transmission
	LINK (LED green), Ethernet link established
Serial interface	
Optional	
I/O	
4 inputs, 4 outputs via pluggable screw terminals	

Technical data

Physical features	
Size (HxWxD)	101mm x 116mm x 23 mm
Environmental temperature	Operation -25°C...+60°C, Storage -40°C …+75°C
Humidity	0...95% (not condensing)
Protection class	IP20

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

Certifications	
UL, USA / Canada	Under way

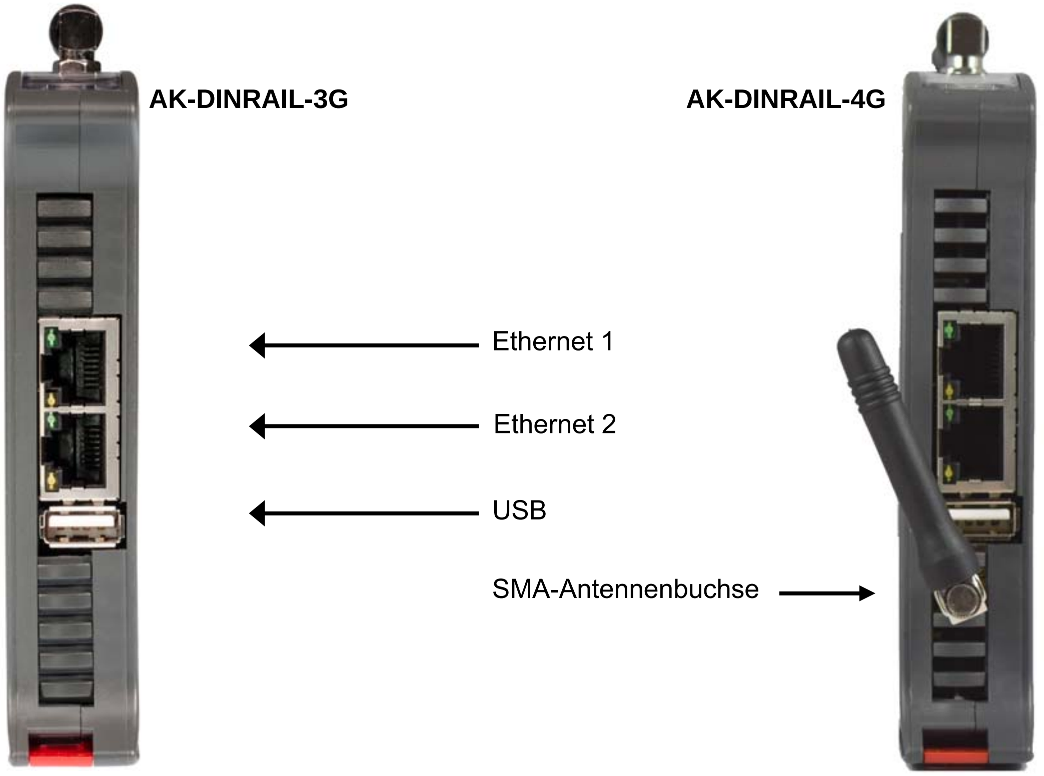
Technical changes reserved!

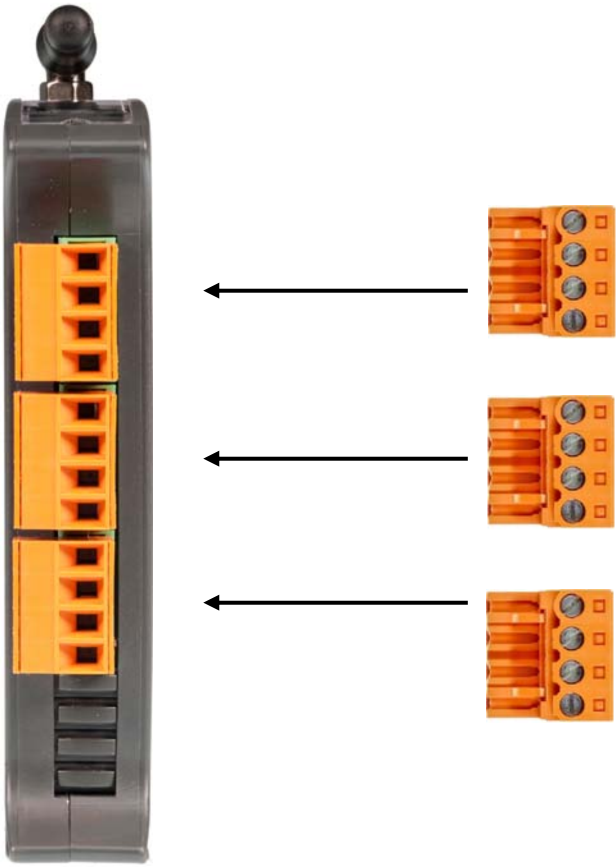
AK-DINRAIL-3G

AK-DINRAIL-4G

Hardware installation

Terminal assignment



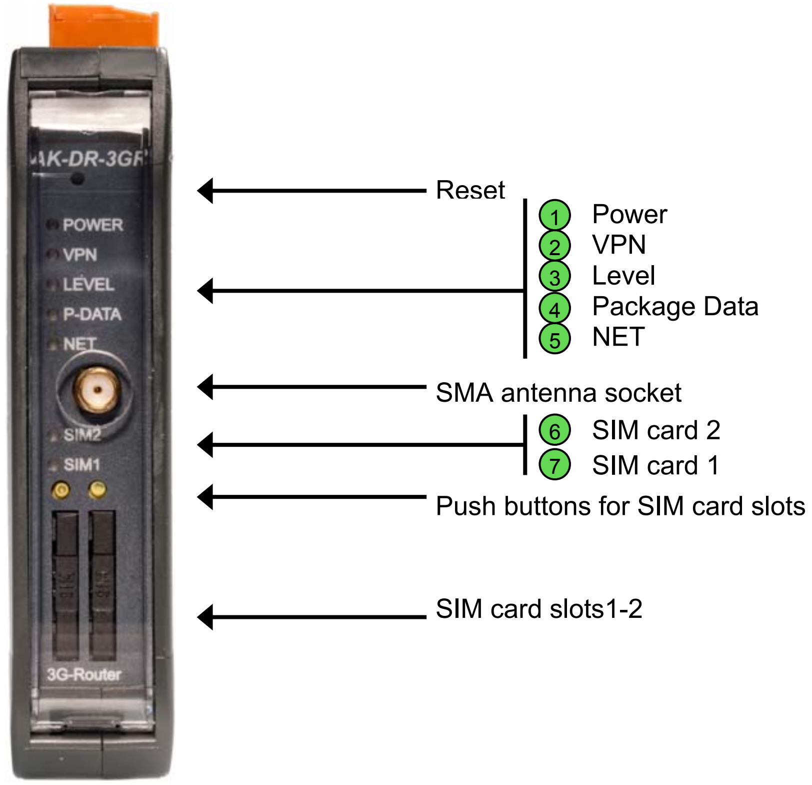


Supply voltage
10V - 30V DC
0V
NC
NC

Digital output
O4 (180mA,Vin)
O3 (180mA,Vin)
O2 (180mA,Vin)
O1 (180mA,Vin)

Digital input
I4
I3
I2
I1

Hardware installation



LED AK-DinRail-xG-Router	
LED	Explanation

SIM card 1/2	Off = no SIM card
	On = SIM / PIN ok
	Rapid flashing = wrong PIN
	Slow flashing = no PIN

NET	Off = not logged in
	Flashing = GPRS/EDGE
	On = UMTS/HSDPA/HSUPA

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

Level	Off = not logged in
	Flashing: short On - long Off = -109dBm … -89dBm
	Flashing: long On - short Off = -87dBm … -67dBm
	On = -65dBm … -51dBm or higher

VPN	Off = no VPN connection
	On = VPN connection activated

Power	Off = no power supply
	On = power supply activated

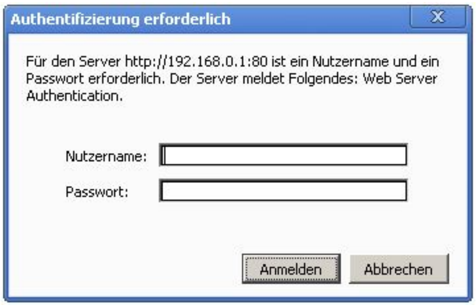
Configuration WBM

The configuration of the AK-DinRail-xG-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 Internet Explorer) 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.

Nutzername:

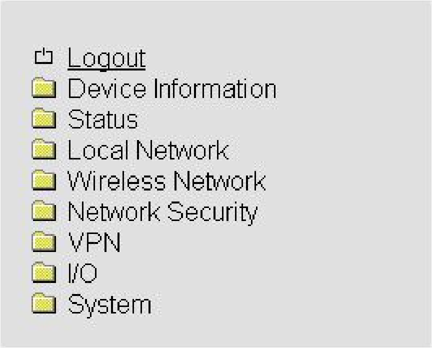
Passwort:

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.

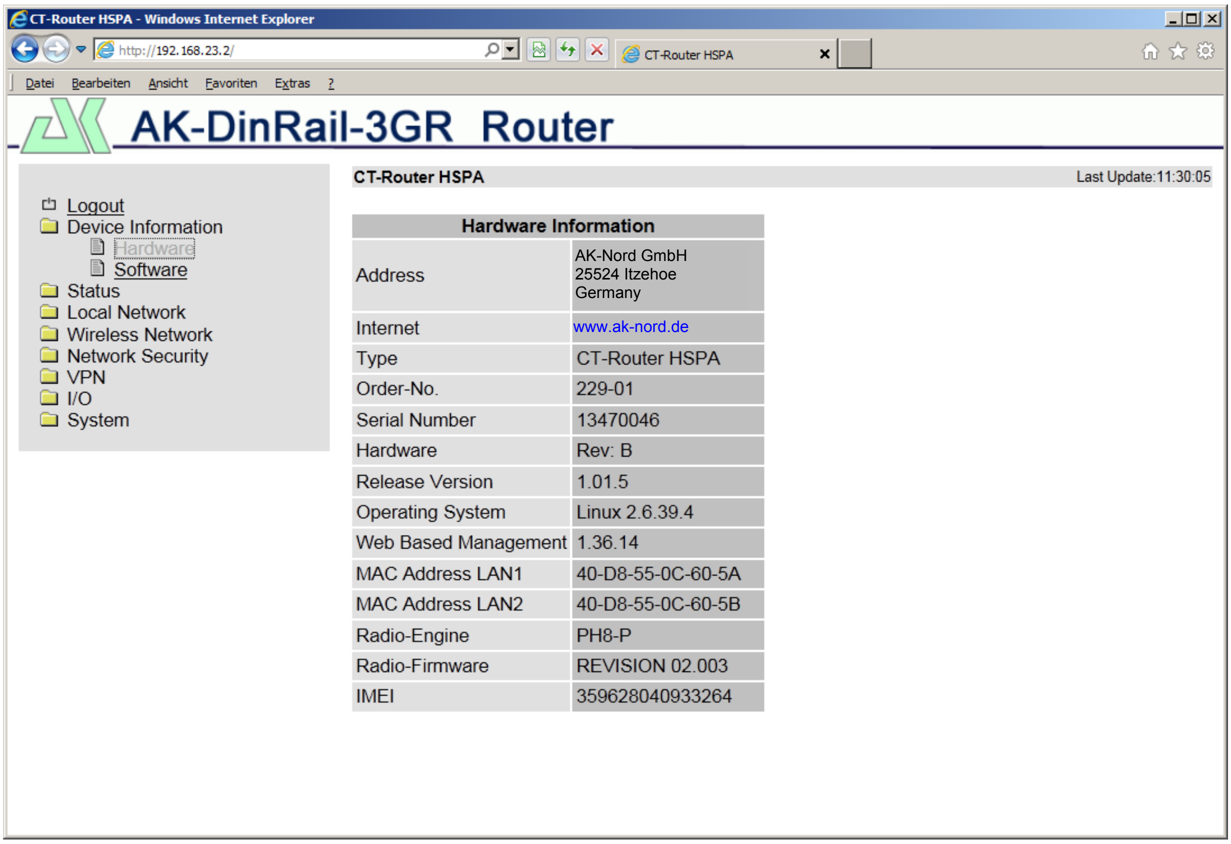
After having entered the user name and the password the main menu will open up to configure the AK-DinRail-xG-Router.



Device information

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

Hardware



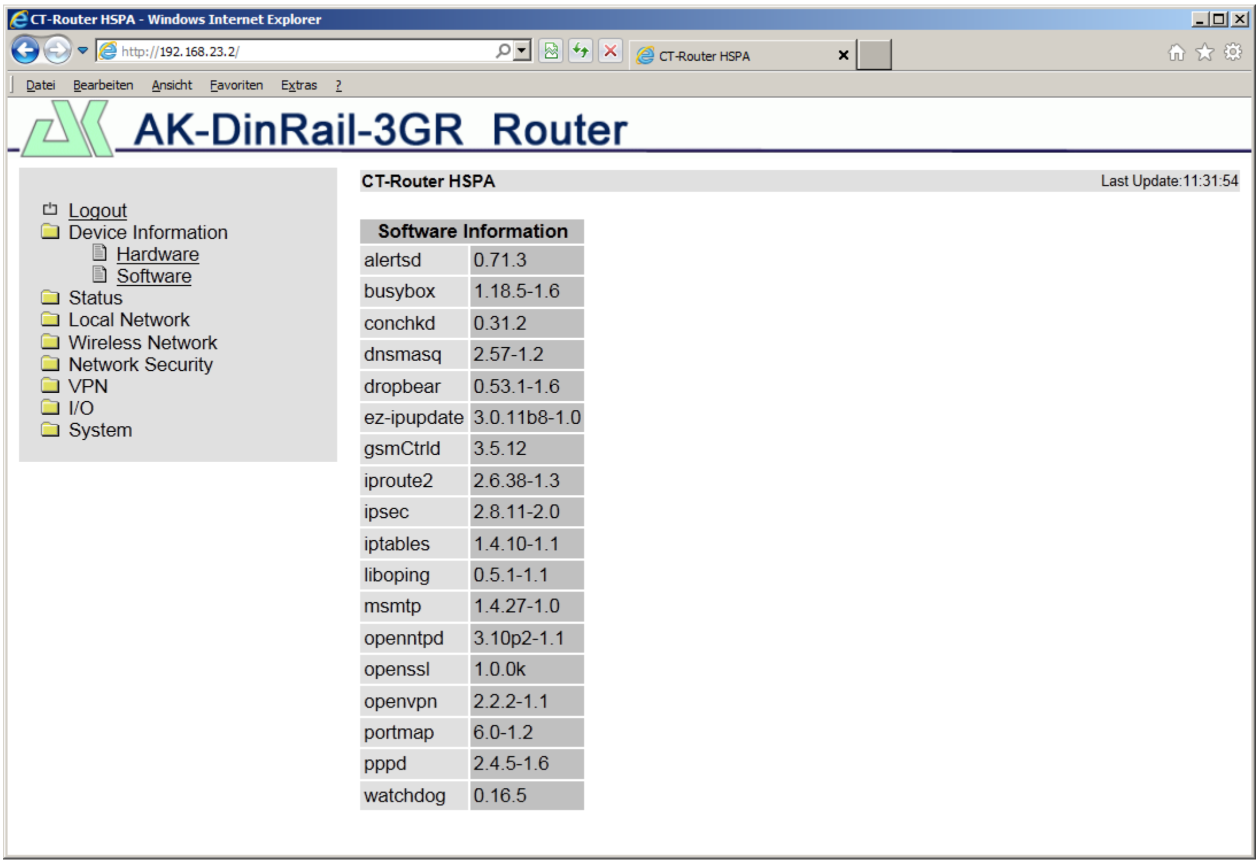
CT-Router HSPA Last Update:11:30:05

Hardware Information	
Address	AK-Nord GmbH 25524 Itzehoe Germany
Internet	www.ak-nord.de
Type	CT-Router HSPA
Order-No.	229-01
Serial Number	13470046
Hardware	Rev: B
Release Version	1.01.5
Operating System	Linux 2.6.39.4
Web Based Management	1.36.14
MAC Address LAN1	40-D8-55-0C-60-5A
MAC Address LAN2	40-D8-55-0C-60-5B
Radio-Engine	PH8-P
Radio-Firmware	REVISION 02.003
IMEI	359628040933264

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

Device information

Software



CT-Router HSPA Last Update:11:31:54

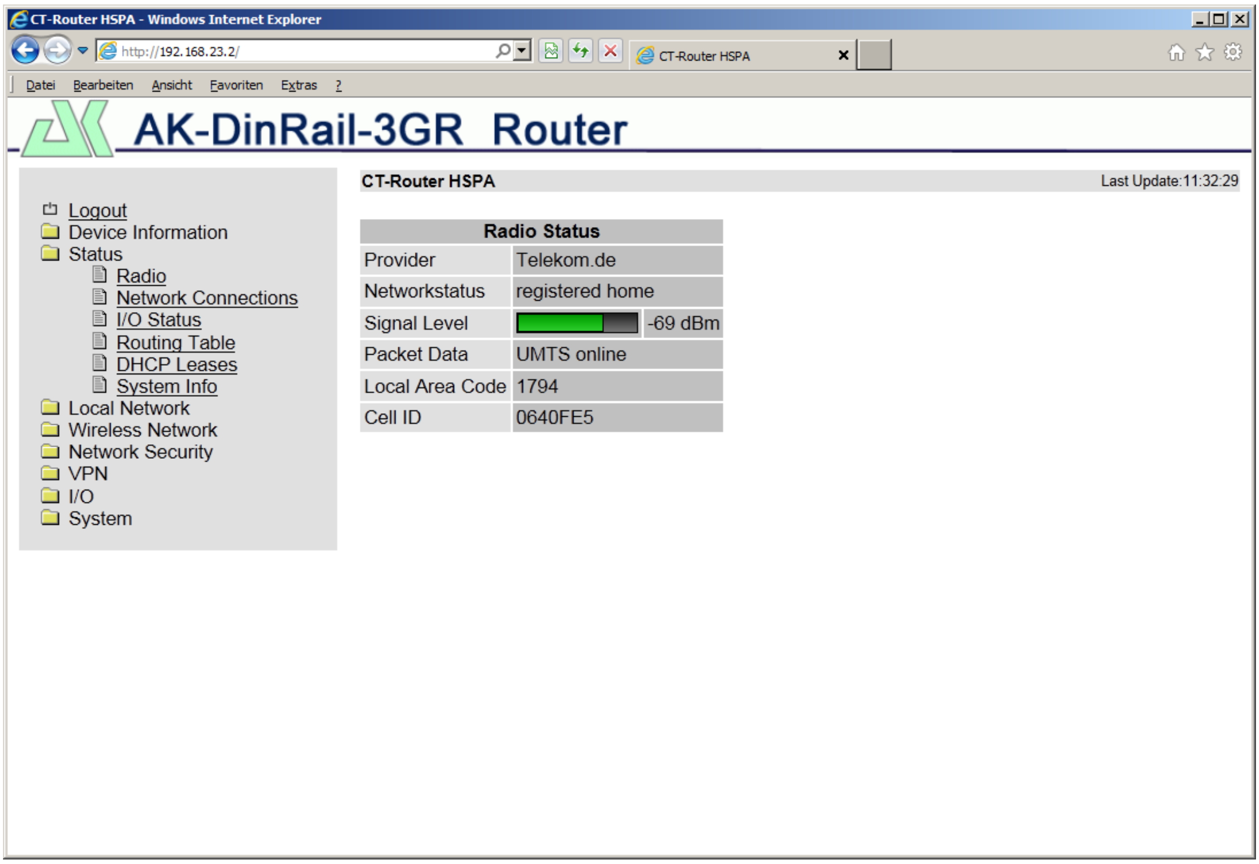
Software Information	
alertsd	0.71.3
busybox	1.18.5-1.6
conchkd	0.31.2
dnsmasq	2.57-1.2
dropbear	0.53.1-1.6
ez-ipupdate	3.0.11b8-1.0
gsmCtrld	3.5.12
iproute2	2.6.38-1.3
ipsec	2.8.11-2.0
iptables	1.4.10-1.1
liboping	0.5.1-1.1
msmtp	1.4.27-1.0
openntpd	3.10p2-1.1
openssl	1.0.0k
openvpn	2.2.2-1.1
portmap	6.0-1.2
pppd	2.4.5-1.6
watchdog	0.16.5

Here you will find a tabular overview of the software installed on the AK-DinRail-xG-Router.

Status

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

Radio



CT-Router HSPA Last Update:11:32:29

Radio Status	
Provider	Telekom.de
Networkstatus	registered home
Signal Level	-69 dBm
Packet Data	UMTS online
Local Area Code	1794
Cell ID	0640FE5

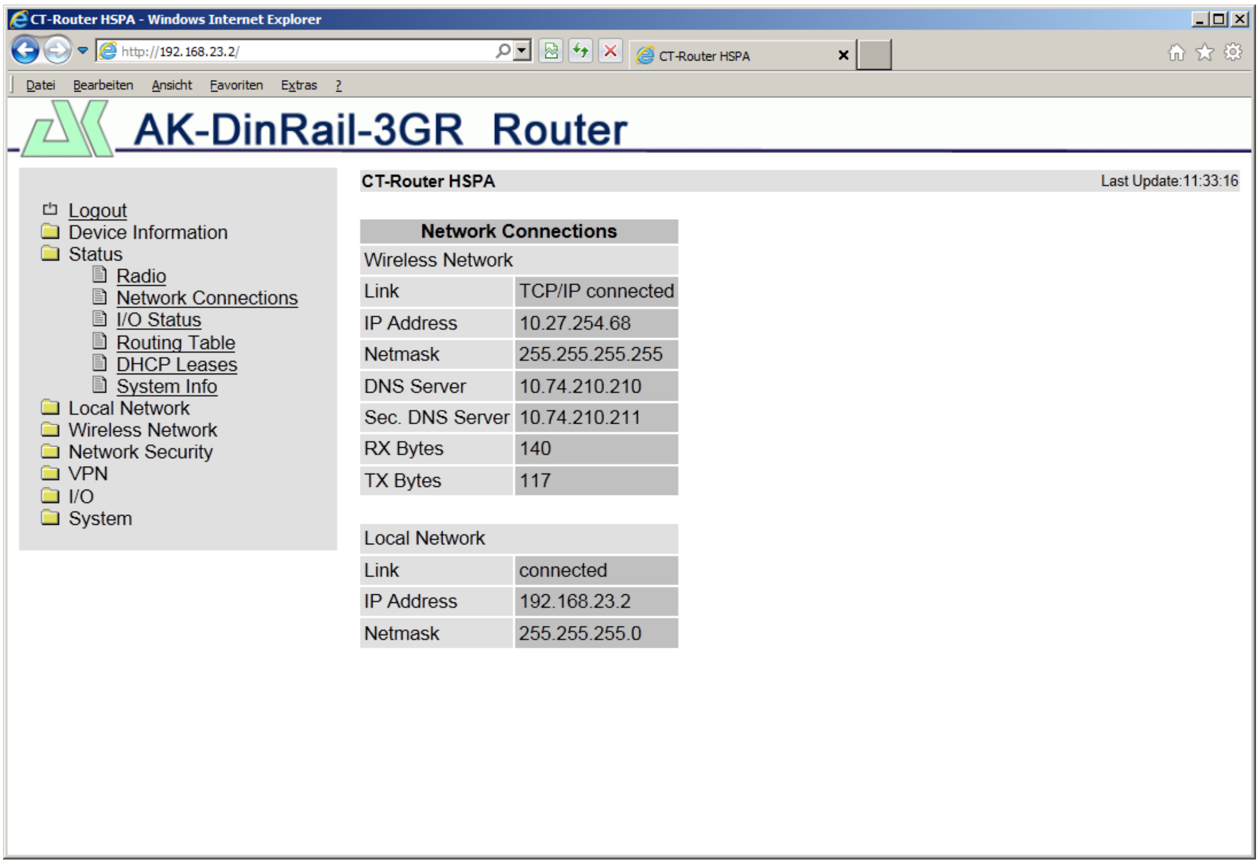
Status → Radio	
Radio status	**Explanation**
Provider	Provider name
Network status	**Registered home:** Dialling into the domestic mobile phone network. **Roaming:** Dialling into the mobile phone network via a foreign provider. **Waiting for PIN:** The PIN is not yet entered. **Waiting for PUK:** The incorrect PIN was entered three times, PUK is required. **Wrong PIN:** Wrong PIN entry. **No SIM card:** There is no SIM card available. **Power off:** GSM module not ready.
Signal level	Signal level of the network (dBm value)

Status

Package data	**Offline:** Package data connection not established. **GPRS online:** Active packet data connection, GPRS signal **EDGE online:** Active package data connection, EDGE signal **UMTS online:** Active package data connection, UMTS signal **HSDPA/UPA online:** Active package data connection, HSDPA/UPA signal **LTE online:** Active package data connection, LTE signal (Only AK-DinRail-4G)
Local Area Code	Local Area Code of the mobile phone network
Cell ID	ID of the mobile phone cell

Status

Network connections



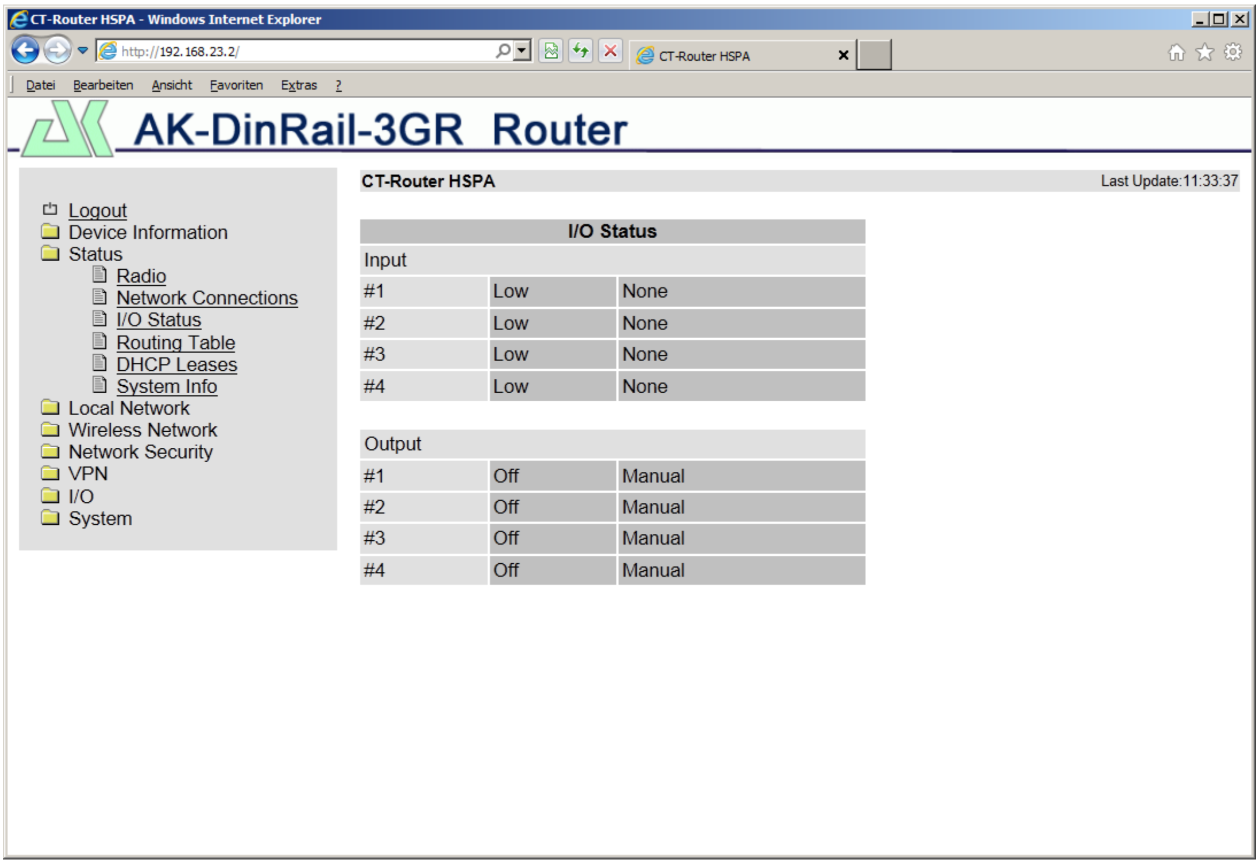
CT-Router HSPA Last Update:11:33:16

Network Connections	
Wireless Network	
Link	TCP/IP connected
IP Address	10.27.254.68
Netmask	255.255.255.255
DNS Server	10.74.210.210
Sec. DNS Server	10.74.210.211
RX Bytes	140
TX Bytes	117
Local Network	
Link	connected
IP Address	192.168.23.2
Netmask	255.255.255.0

Status → Network connections	
Network connections	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



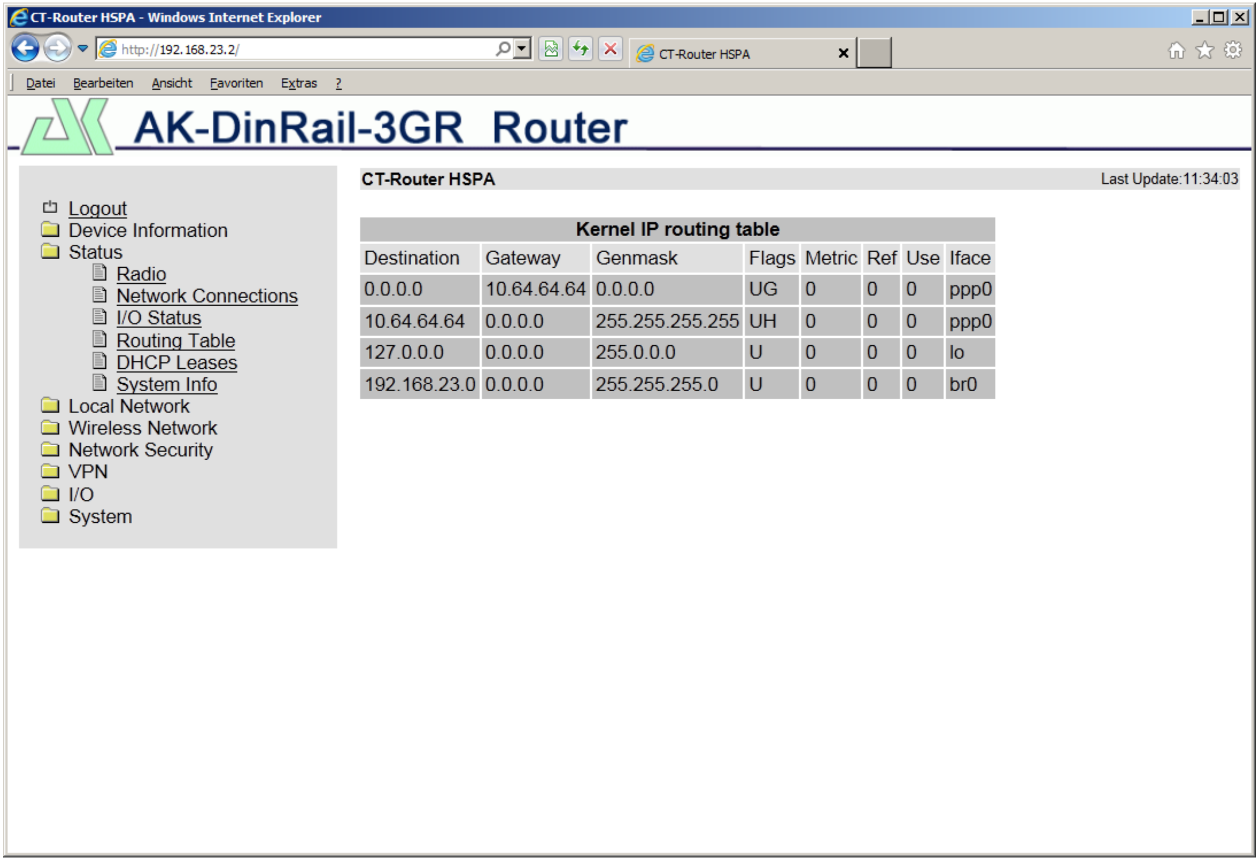
CT-Router HSPA Last Update:11:33:37

I/O Status		
Input		
#1	Low	None
#2	Low	None
#3	Low	None
#4	Low	None
Output		
#1	Off	Manual
#2	Off	Manual
#3	Off	Manual
#4	Off	Manual

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

Status

Routing table



CT-Router HSPA Last Update:11:34:03

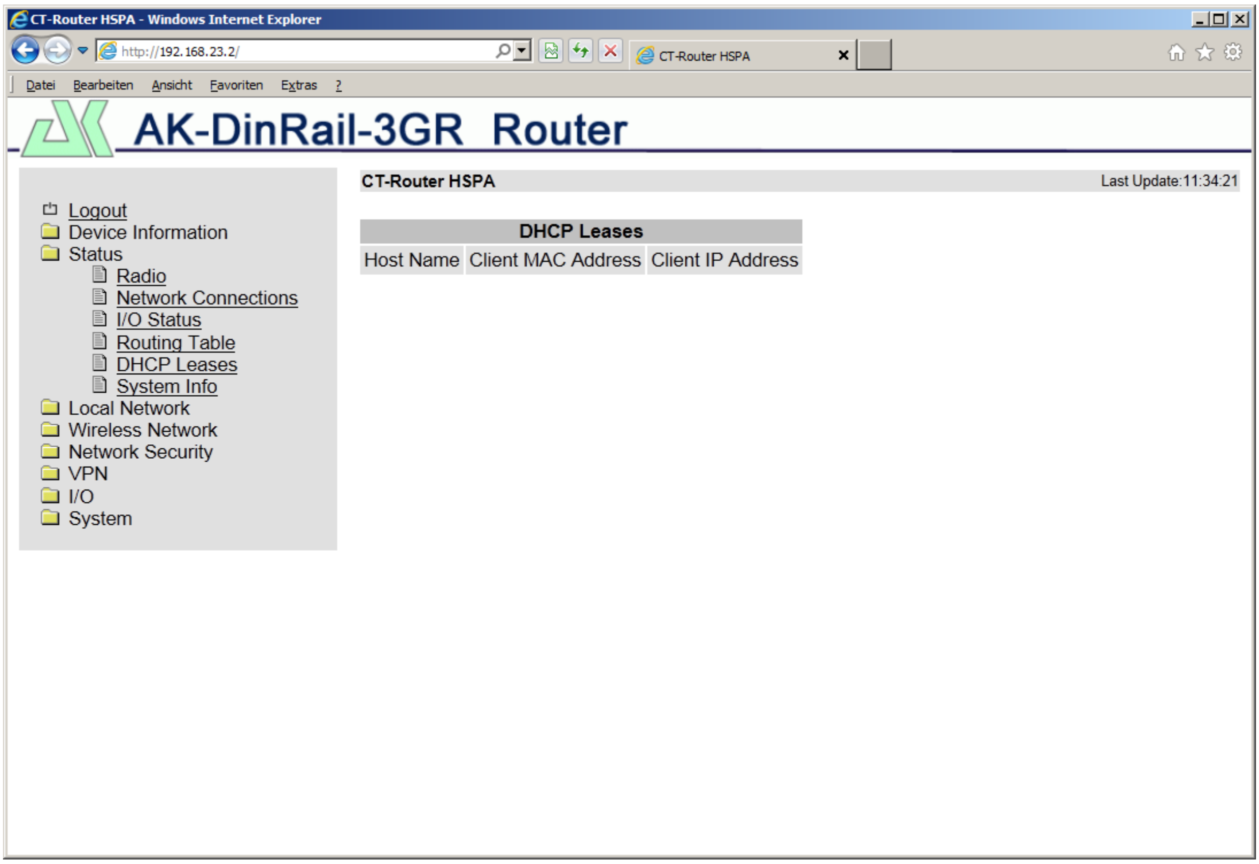
Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
0.0.0.0	10.64.64.64	0.0.0.0	UG	0	0	0	ppp0
10.64.64.64	0.0.0.0	255.255.255.255	UH	0	0	0	ppp0
127.0.0.0	0.0.0.0	255.0.0.0	U	0	0	0	lo
192.168.23.0	0.0.0.0	255.255.255.0	U	0	0	0	br0

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

Status

DHCP leases



CT-Router HSPA Last Update:11:34:21

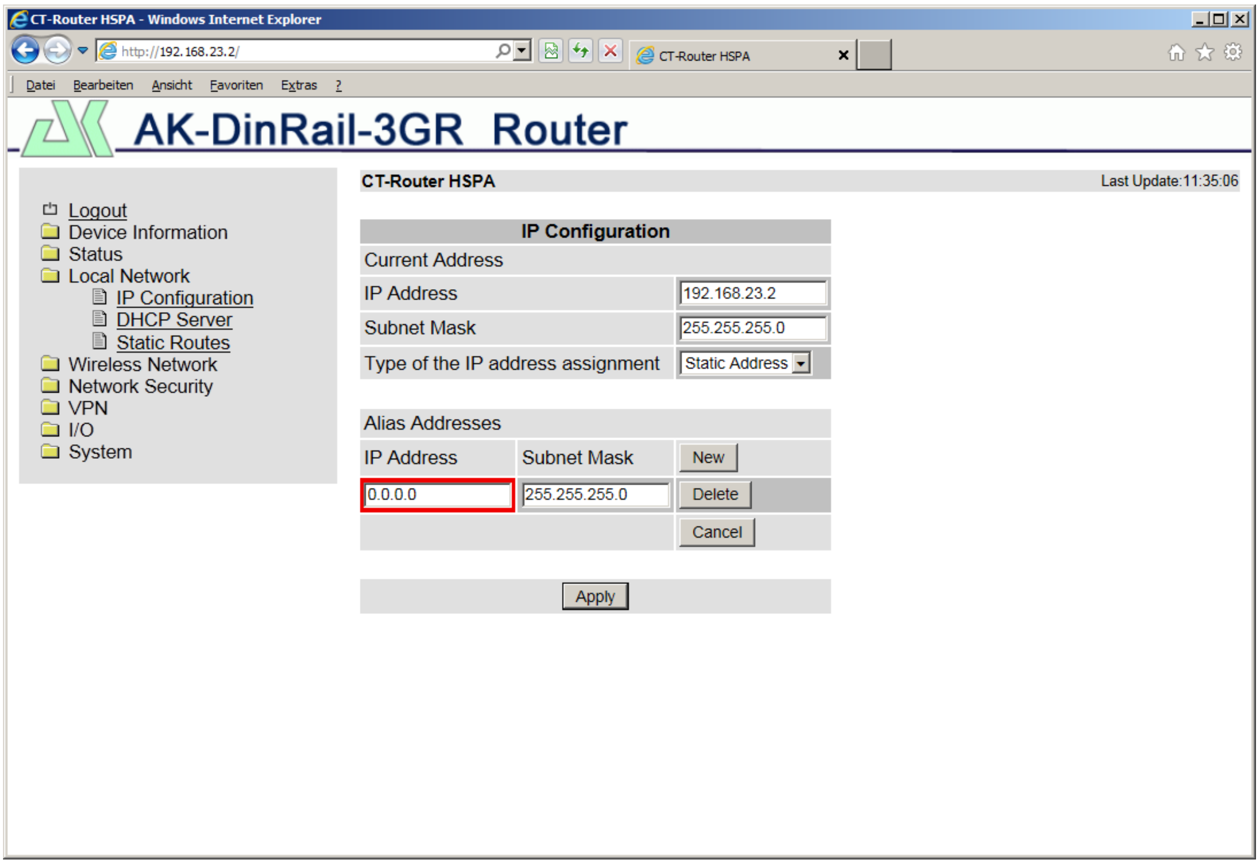
DHCP Leases		
Host Name	Client MAC Address	Client IP Address

Status →DHCP leases	
DHCP leases	Explanation
Here you will find an overview in tabular form of all DHCP data assigned by the AK-DinRail-xG-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 AK-DinRail-xG-Router.

IP configuration



CT-Router HSPA Last Update:11:35:06

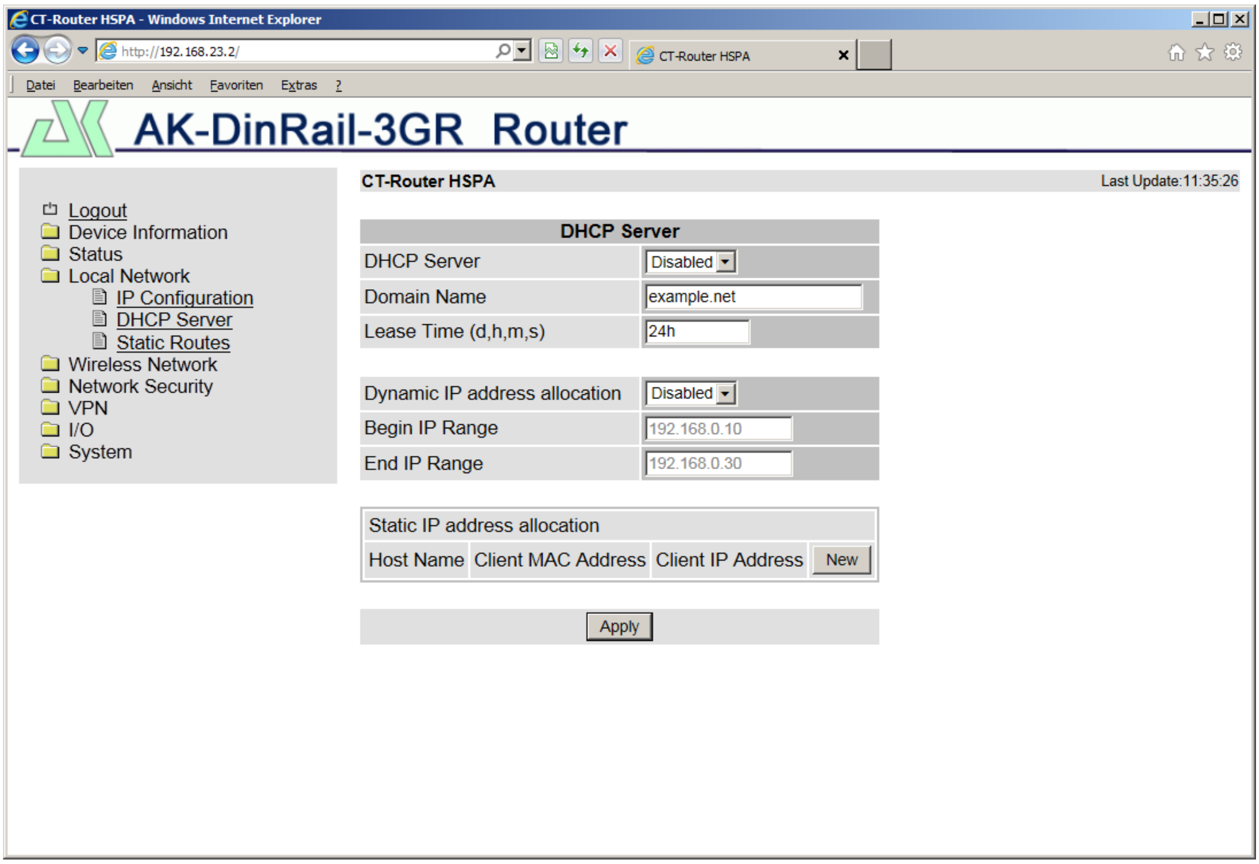
IP Configuration	
Current Address	
IP Address	192.168.23.2
Subnet Mask	255.255.255.0
Type of the IP address assignment	Static Address

Alias Addresses		
IP Address	Subnet Mask	New
0.0.0.0	255.255.255.0	Delete
		Cancel

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 HSPA Last Update:11:35:26

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

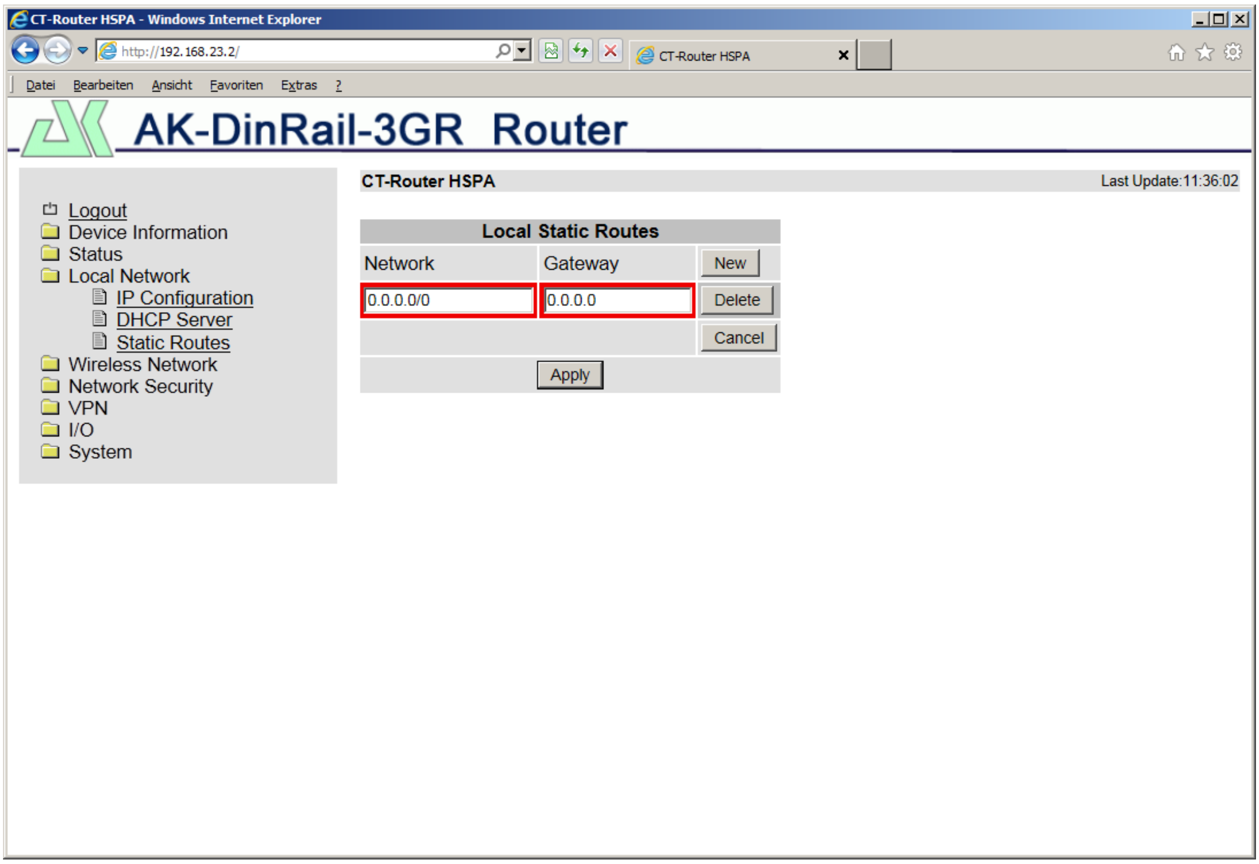
Host Name	Client MAC Address	Client IP Address	New

Apply

Local network → DHCP server	
DHCP server	**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 address is assigned to several MAC addresses.

Local network

Static routes



CT-Router HSPA

Last Update:11:36:02

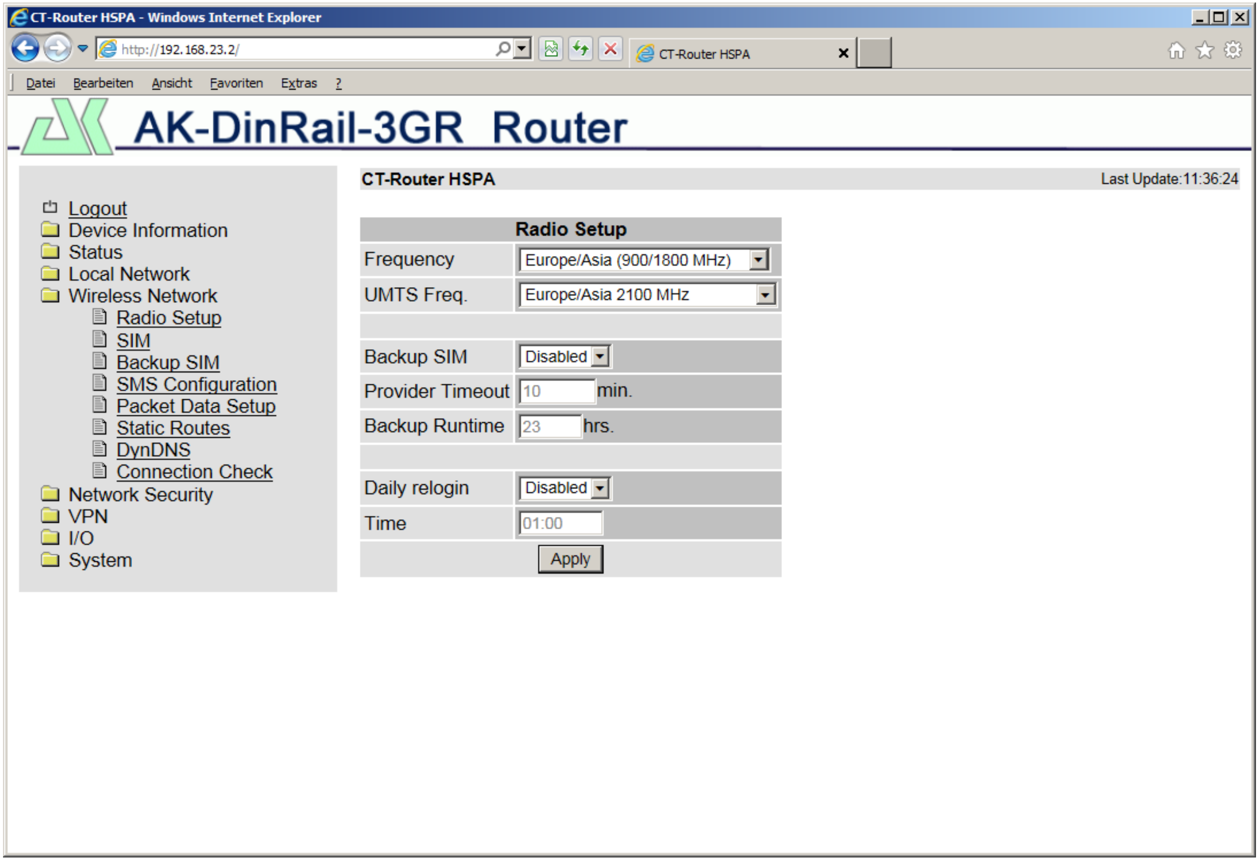
Local Static Routes		
Network	Gateway	New
0.0.0.0/0	0.0.0.0	Delete

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

Wireless network

Determine the settings for the use of the mobile phone network of the AK-DinRail-xG-Router in the “Wireless network” menu.

Radio setup



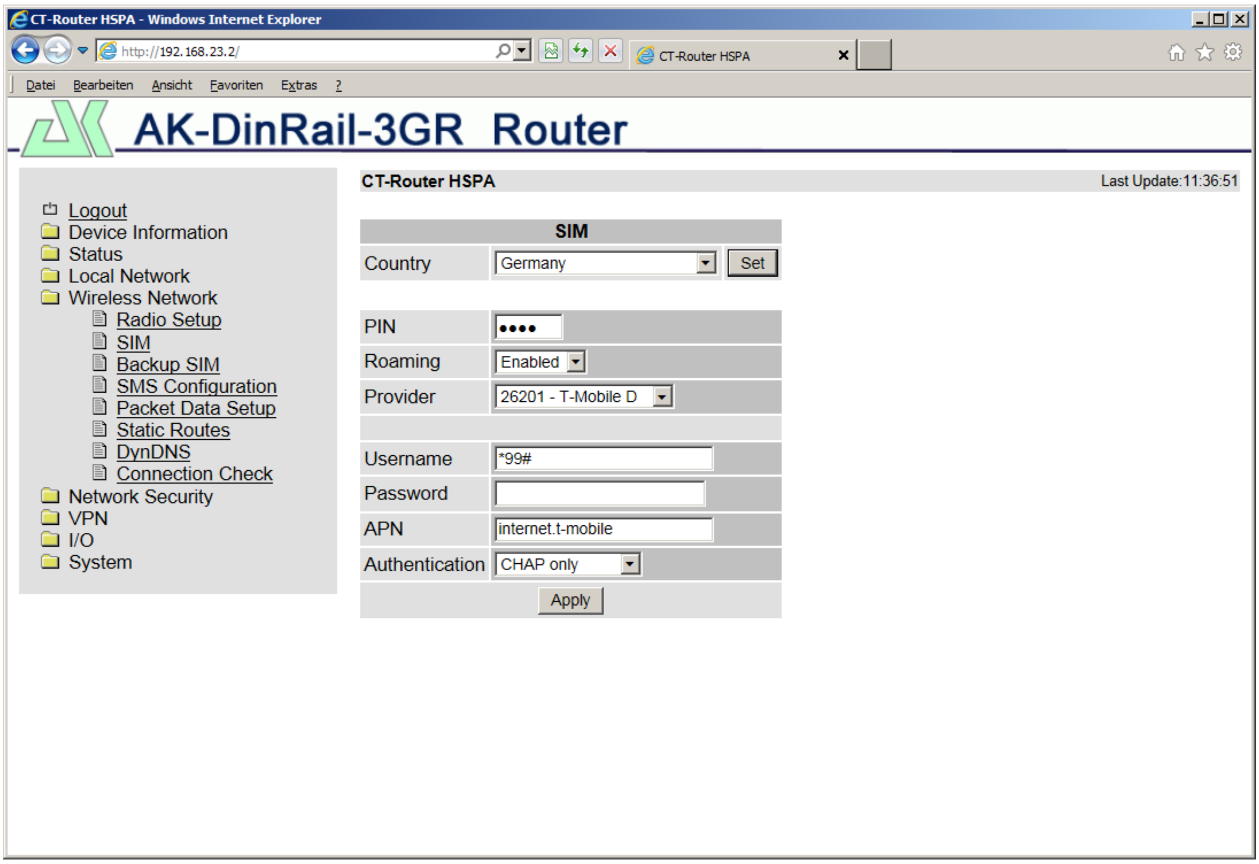
Radio Setup

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	**Explanation**
Frequency	Select a frequency range of the router by means of a drop-down list.
UMTS frequency	Select a frequency range for the UMTS/LTE by means of a drop-down list / it is also possible to deactivate the UMTS/LTE. (LTE only available at AK-DinRail-4G)
Backup SIM	Second SIM card can be used for a backup mobile phone connection.
Provider time-out	Time in minutes to activate the backup SIM card after failure of the primary.
Backup runtime	Runtime of the second SIM card in hours
Daily re-login	**Disable:** Deactivating the daily login **Enable:** Activating the daily login (Primary before secondary SIM)
Time	Point in time of the new registration of a router to the mobile phone network (First a logout is required. For login primary before secondary 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 Last Update:11:36:51

SIM	
Country	Germany [Set]
PIN	••••
Roaming	Enabled
Provider	26201 - T-Mobile D
Username	*99#
Password	
APN	internet.t-mobile
Authentication	CHAP only
	[Apply]

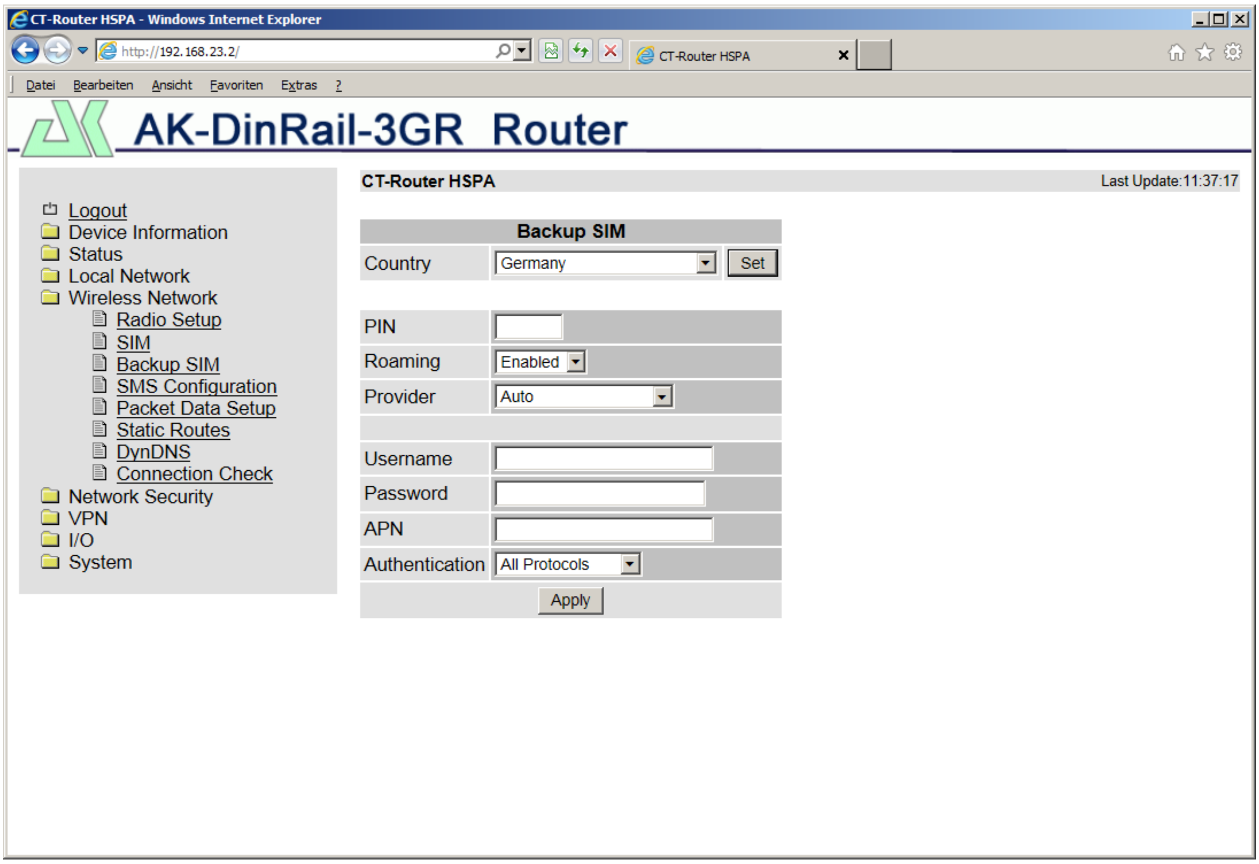
Wireless network → SIM	
SIM	Explanation
Country	Selection of the country in which the router is dialling into the GSM network. (Limits the selection under the item "Provider").
PIN	PIN entry of the SIM card
Roaming	**Enable:** There is the option that the router may dial into a foreign network. At this additional cost might accrue depending on the contract.
	Disable: Deactivating the roaming. The domain network of the provider is automatically used. If this is not possible no connection will be established.
Provider	Only the roaming is activated, a selection is possible. **Auto:** Automatic selection of the provider
User name	User name for package data access (pre-setting of the provider)
Password	Password for package data access (pre-setting of the provider)
Always indicate the user name and password otherwise no package data connections are established.	
APN	Name of the connection in the package data network (pre-setting of the provider)

Wireless network

Authentication	Authentication is protected by protocols. **All protocols:** All protocols are allowed **Refuse MSCHAP:** Refusal of the Microsoft Challenge-Handshake Authentication Protocol. **CHAP only:** Only Challenge-Handshake Authentication Protocol **PAP only:** Only Password Authentication Protocol

Wireless network

Backup SIM



CT-Router HSPA Last Update:11:37:17

Backup SIM	
Country	Germany
PIN	
Roaming	Enabled
Provider	Auto
Username	
Password	
APN	
Authentication	All Protocols

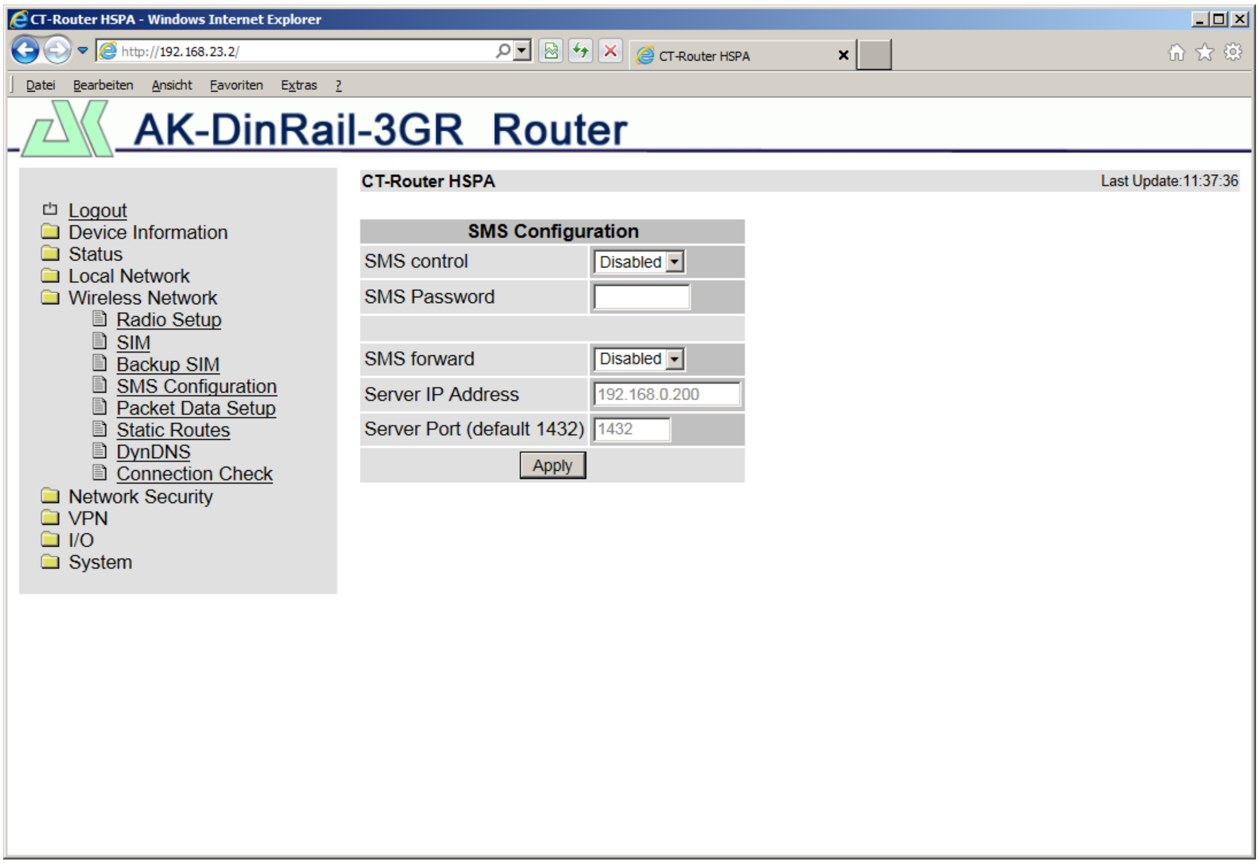
Wireless network → Backup SIM	
Backup SIM	**Explanation**
Country	Selection of the country in which the router is dialling into the GSM network. (Limits the selection under the item "Provider").
PIN	PIN entry of the SIM card
Roaming	**Enable:** There is the option that the router may dial into a foreign network. At this additional cost might accrue depending on the contract. **Disable:** Deactivating the roaming. The domain network of the provider is automatically used. If this is not possible no connection will be established.
Provider	Only the roaming is activated, a selection is possible. **Auto:** Automatic selection of the provider
User name	User name for package data access (pre-setting of the provider)
Password	Password for package data access (pre-setting of the provider)
Never leave user name and password empty otherwise no package data connections are established.	
APN	Name of the connection in the package data network (pre-setting of the provider)

Wireless network

Authentication	Authentication is protected by protocols. **All protocols:** All protocols are allowed **Refuse MSCHAP:** Refusal of the Microsoft Challenge-Handshake Authentication Protocol. **CHAP only:** Only Challenge-Handshake Authentication Protocol **PAP only:** Only Password Authentication Protocol

Wireless network

SMS configuration



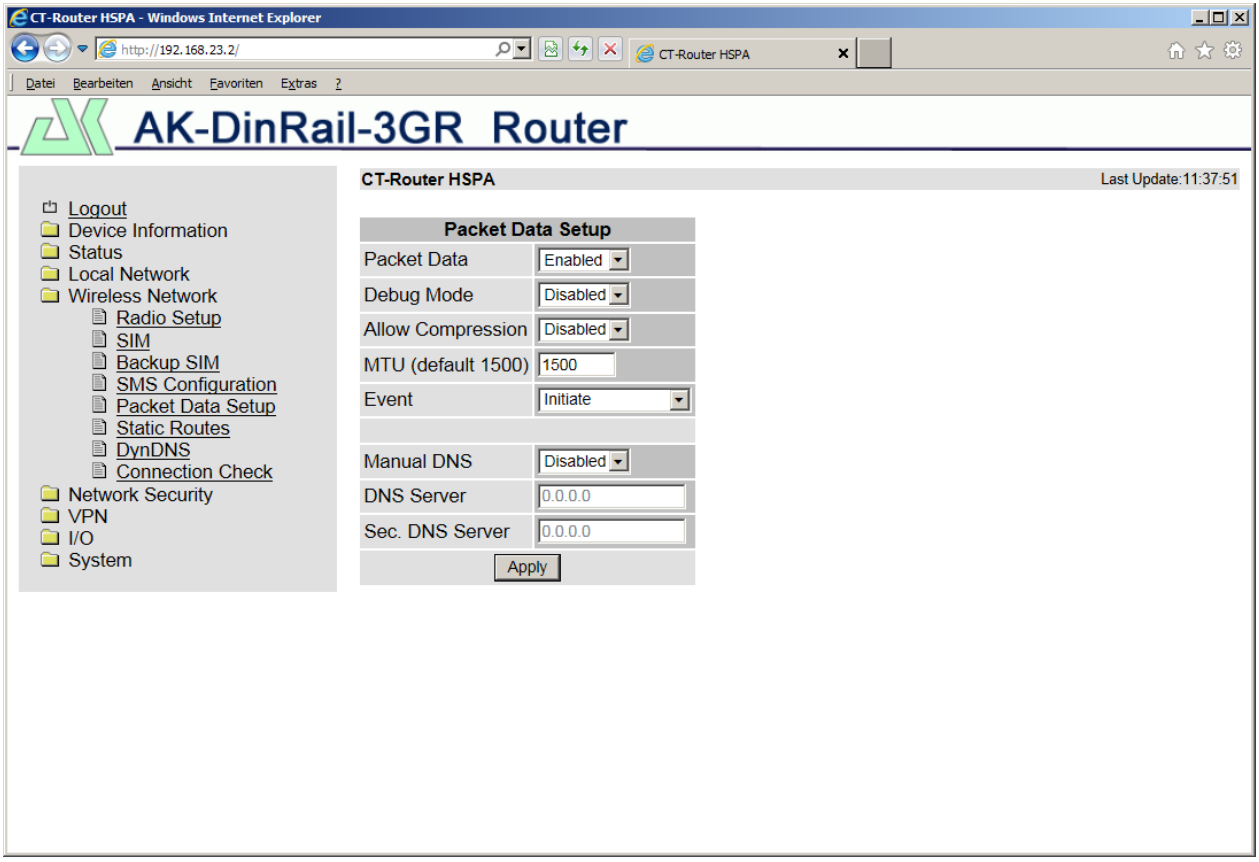
CT-Router HSPA Last Update:11:37:36

SMS Configuration	
SMS control	Disabled
SMS Password	
SMS forward	Disabled
Server IP Address	192.168.0.200
Server Port (default 1432)	1432

Wireless network → SMS configuration	
SMS configuration	**Explanation**
SMS control	**Disable:** Controlling the router via SMS is deactivated. **Enable:** Controlling the router via SMS is activated.
SMS password	SMS password to control via SMS
SMS forward	**Disable:** Forwarding of SMS messages via Ethernet is deactivated. **Enable:** Forwarding of SMS messages via Ethernet is activated.
Server IP address	Forwarding the SMS is performed to this IP address
Server port (default 1432)	Forwarding the SMS is performed to this port.

Wireless network

Package data setup

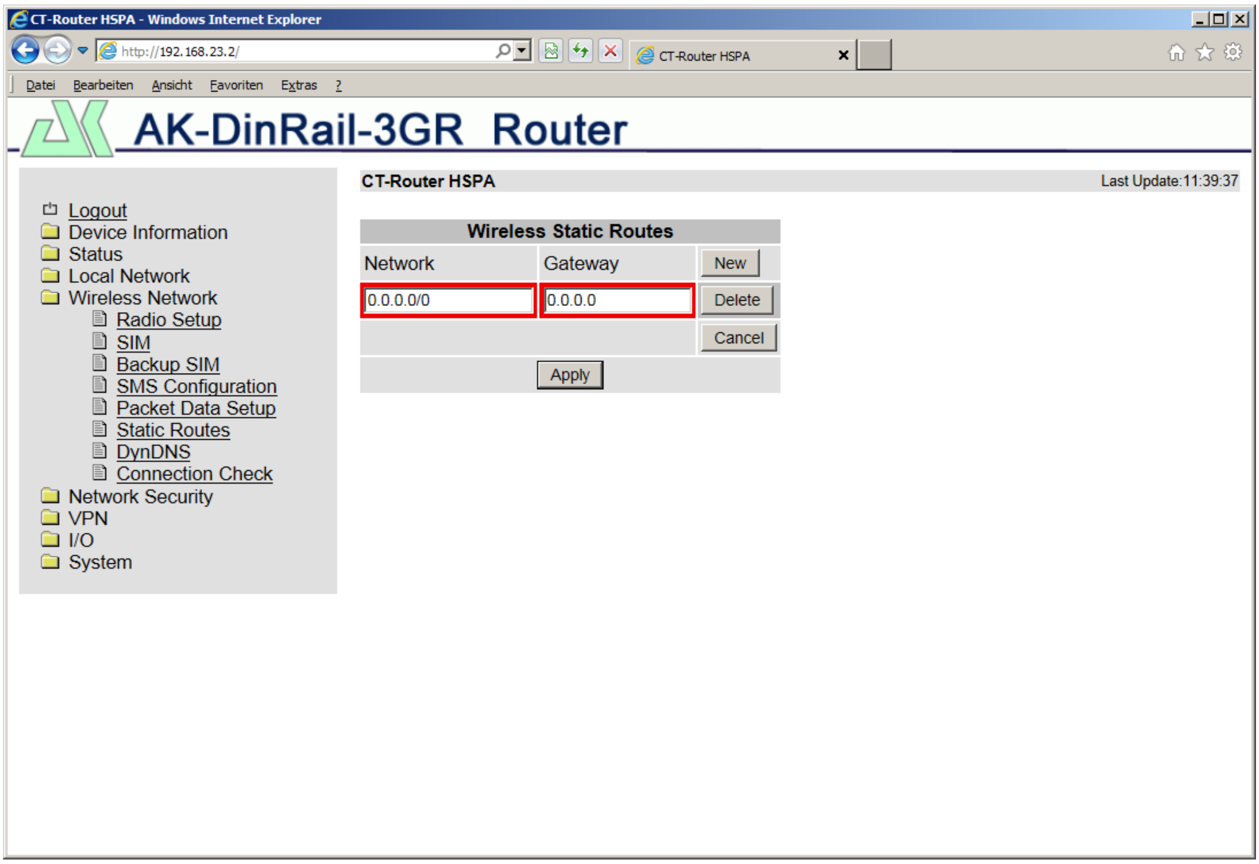


Packet Data Setup	
Packet Data	Enabled
Debug Mode	Disabled
Allow Compression	Disabled
MTU (default 1500)	1500
Event	Initiate
Manual DNS	Disabled
DNS Server	0.0.0.0
Sec. DNS Server	0.0.0.0

Wireless network → Package data setup	
Package data setup	Explanation
Package data	**Disable:** Deactivating the package data connection **Enable:** Activating the package data connection / virtual continuous connection only for real data transfer, traffic is taking place.
Debug mode	For diagnose purposes regarding the package data connection information may be saved in the log file. This option can be activated or deactivated.
Allow compression	**Disable:** Data compression activated **Enable:** Data compression deactivated
MTU (default 1500)	Maximum package size in bytes
Event	**Initiate:** Automatic start-up of the package data connection **Initiate on Input #1... #4:** Manual start-up via gate input
Manual DNS	**Disable:** Deactivating the manual DNS setting (DNS is received by the provider). **Enable:** Activating the manual DNS setting.
DNS server	IP address, primary DNS server in the mobile phone network
Sec. DNS server	IP address, secondary DNS server in the mobile phone network

Wireless network

Static routes

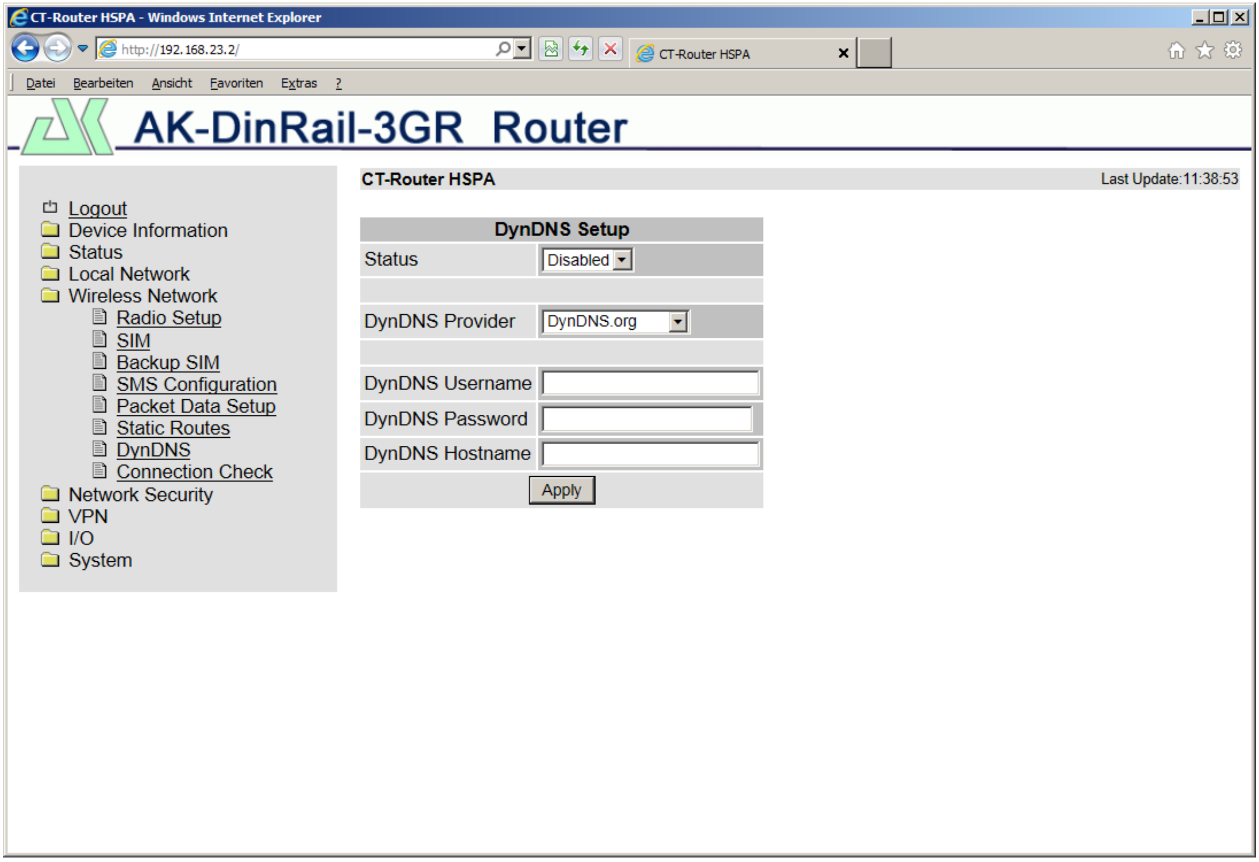


Network	Gateway
0.0.0.0/0	0.0.0.0

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

Wireless network

DynDNS



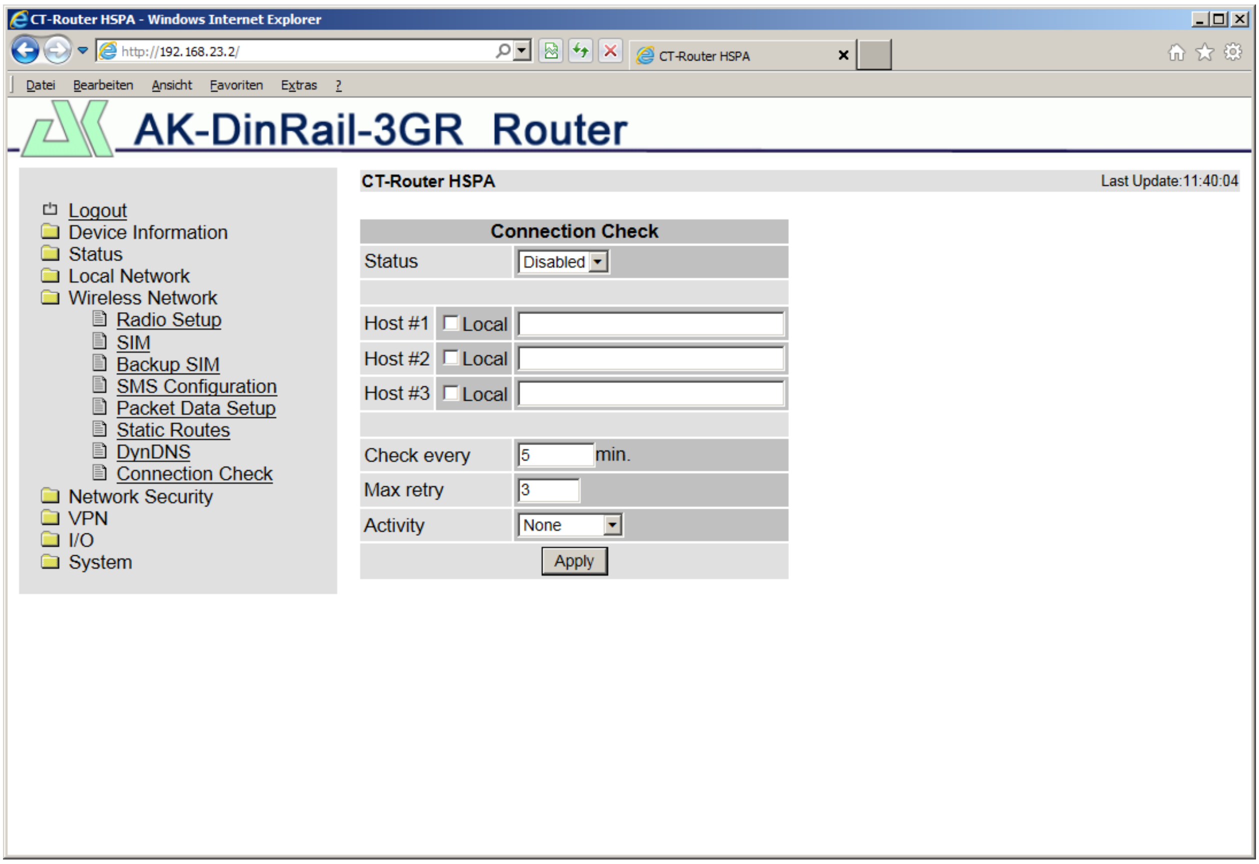
DynDNS Setup

Status	Disabled
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 user name	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

Wireless network

Connection check



Connection Check

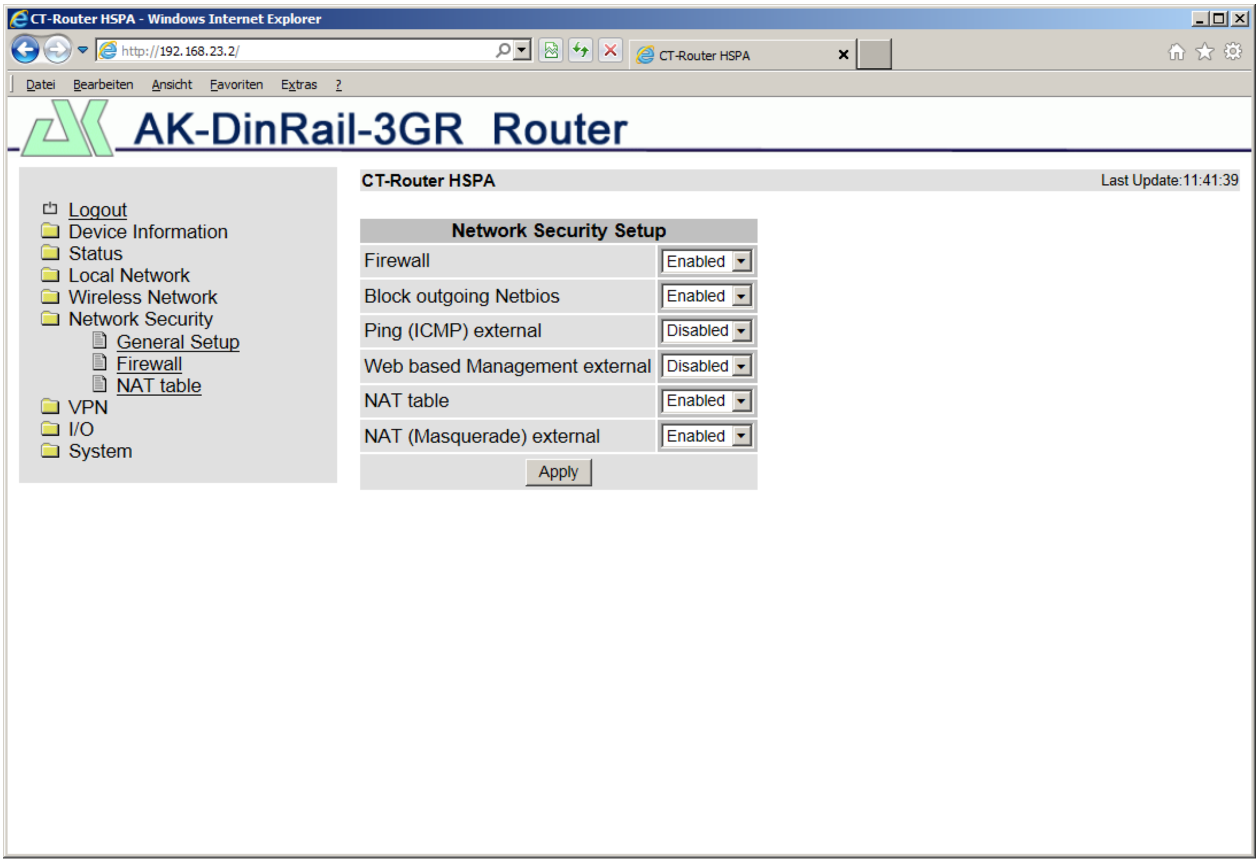
Status	Disabled	
Host #1	□ Local	
Host #2	□ Local	
Host #3	□ Local	
Check every	5 min.	
Max retry	3	
Activity	None	

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

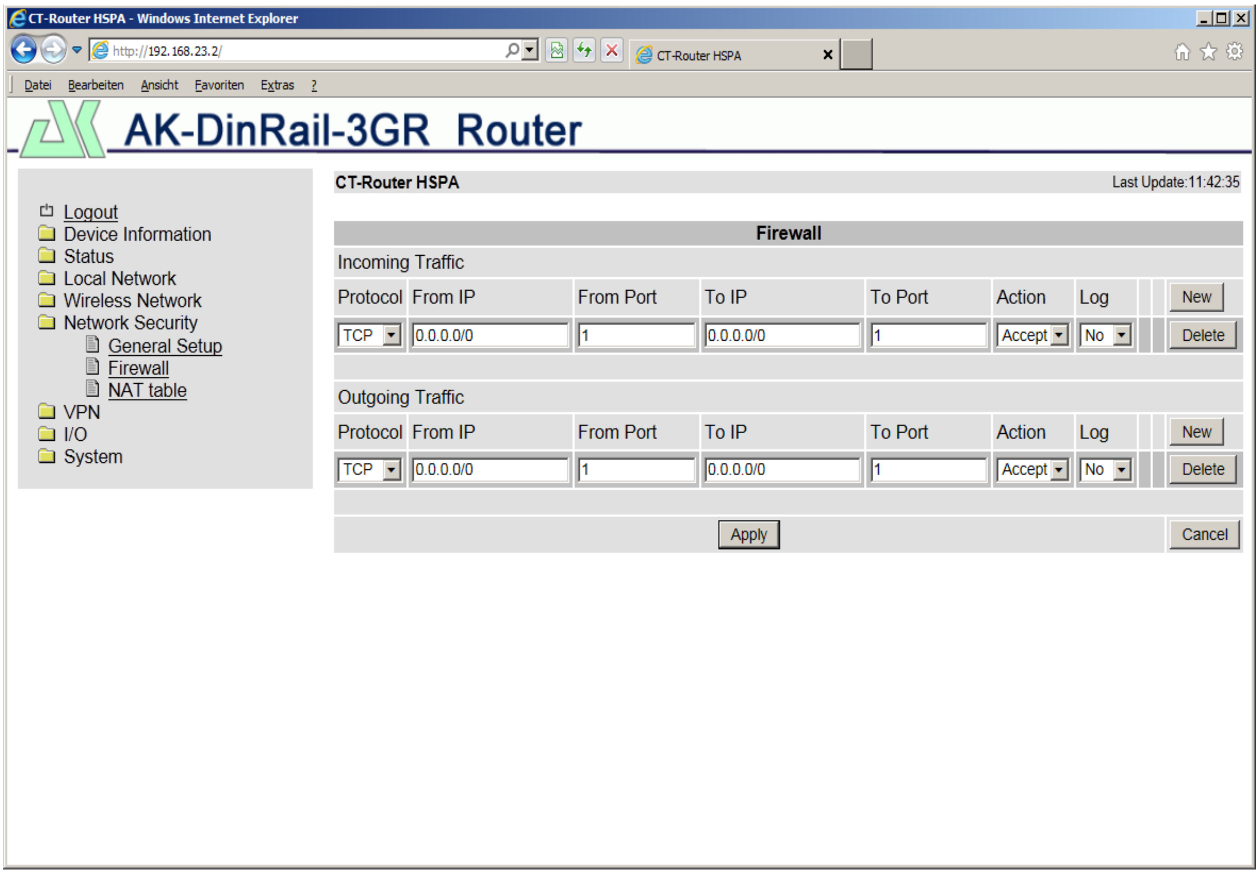


Network Security Setup	
Firewall	Enabled
Block outgoing Netbios	Enabled
Ping (ICMP) external	Disabled
Web based Management external	Disabled
NAT table	Enabled
NAT (Masquerade) external	Enabled

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



CT-Router HSPA Last Update:11:42:35

Firewall

Incoming Traffic

Protocol	From IP	From Port	To IP	To Port	Action	Log	New
TCP	0.0.0.0/0	1	0.0.0.0/0	1	Accept	No	Delete

Outgoing Traffic

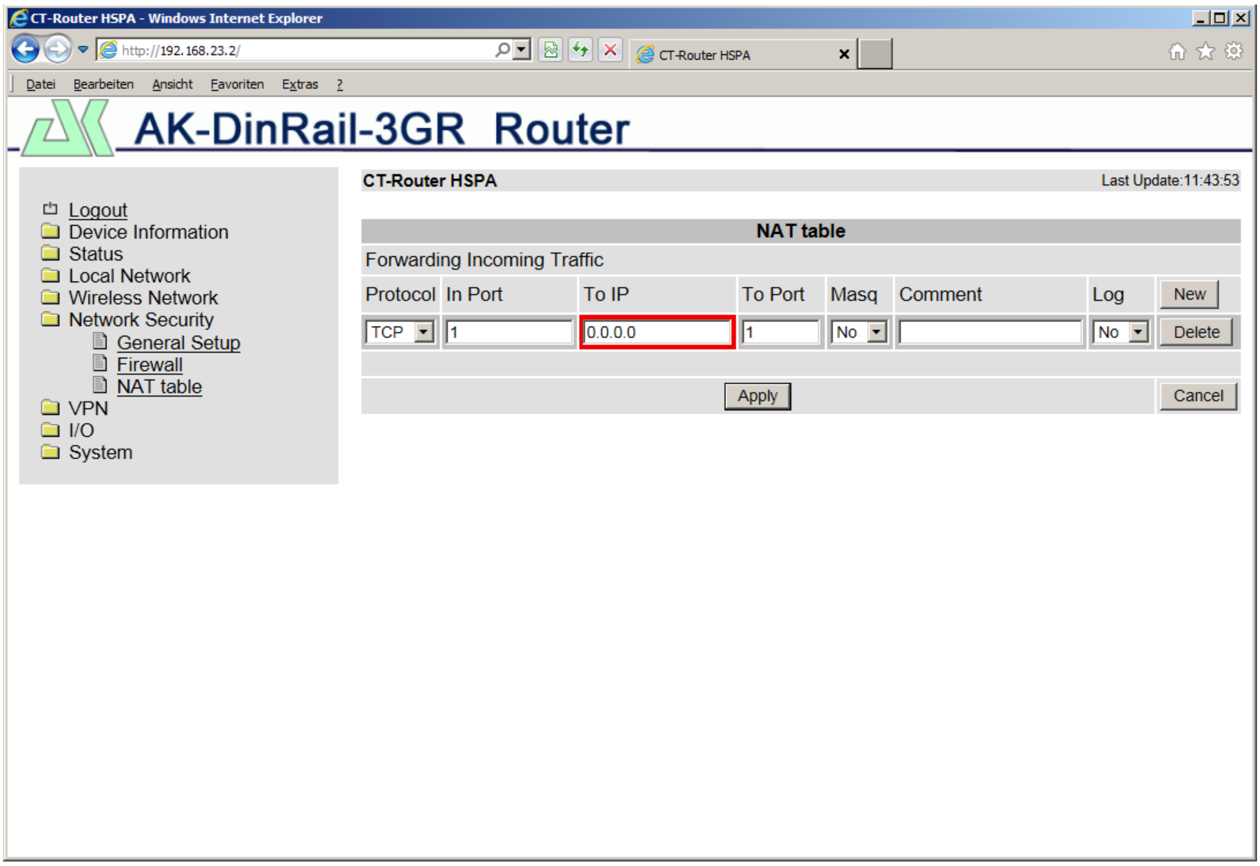
Protocol	From IP	From Port	To IP	To Port	Action	Log	New
TCP	0.0.0.0/0	1	0.0.0.0/0	1	Accept	No	Delete

Apply Cancel

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 rejection.
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



NAT table

Forwarding Incoming Traffic

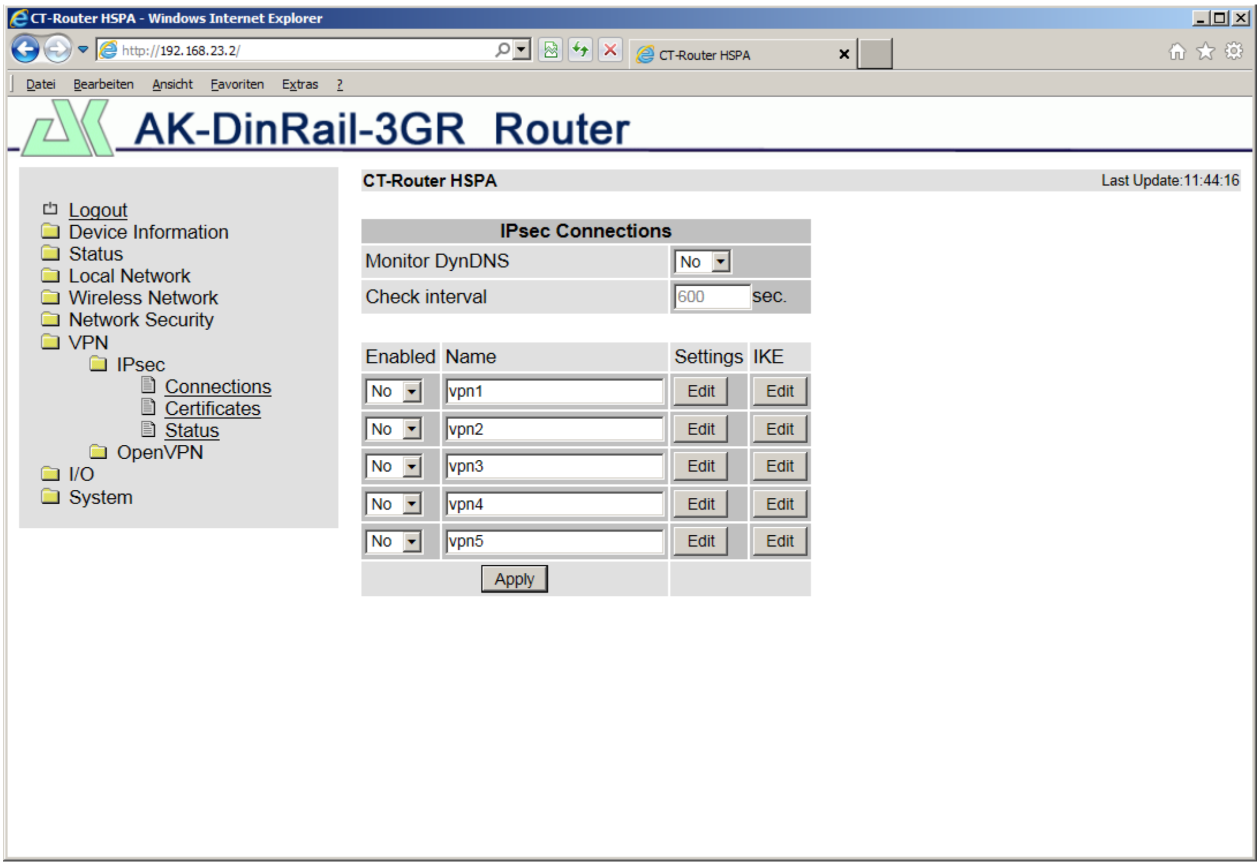
Protocol	In Port	To IP	To Port	Masq	Comment	Log
TCP	1	0.0.0.0	1	No		No

Network security →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-IPsec

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).

Connections



CT-Router HSPA

Last Update:11:44:16

IPsec Connections	
Monitor DynDNS	No
Check interval	600 sec.

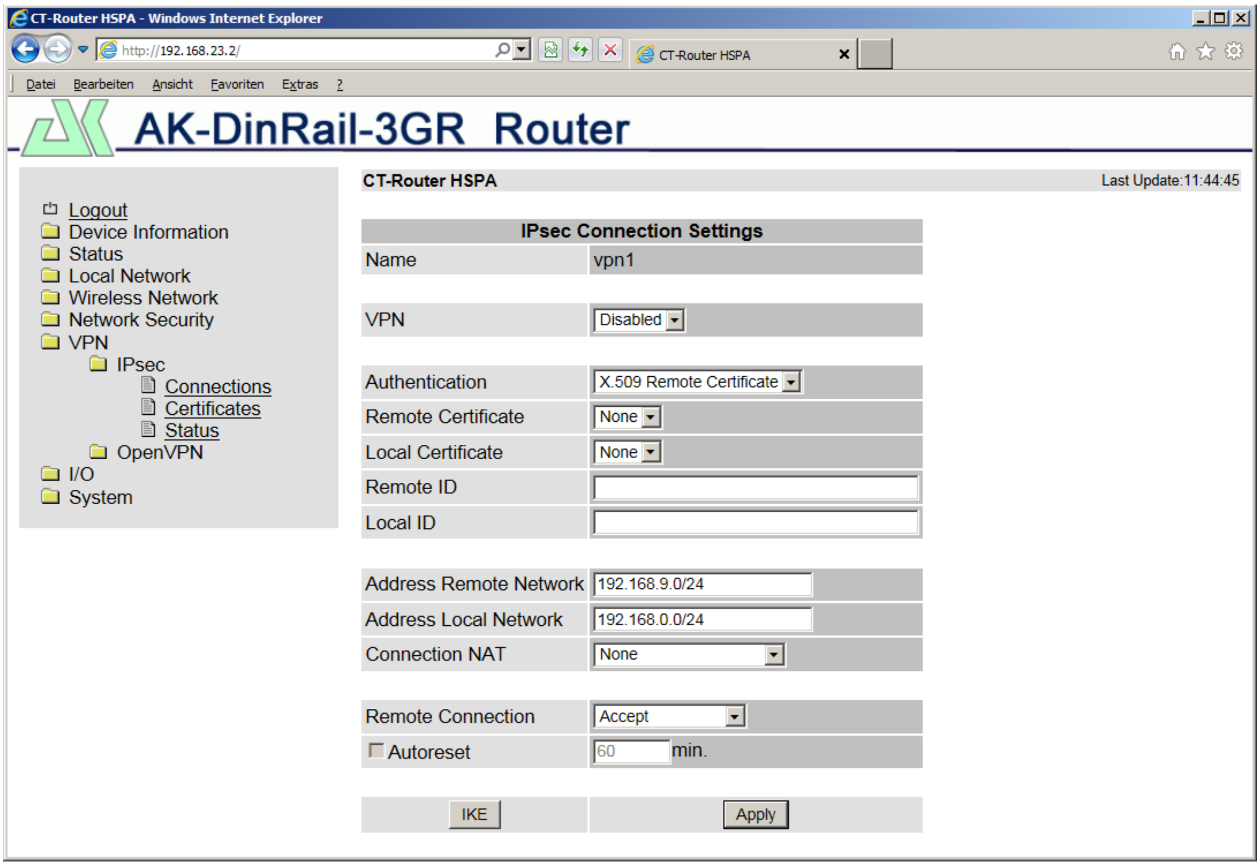
Enabled	Name	Settings	IKE
No	vpn1	Edit	Edit
No	vpn2	Edit	Edit
No	vpn3	Edit	Edit
No	vpn4	Edit	Edit
No	vpn5	Edit	Edit

Apply

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 HSPA Last Update:11:44:45

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.

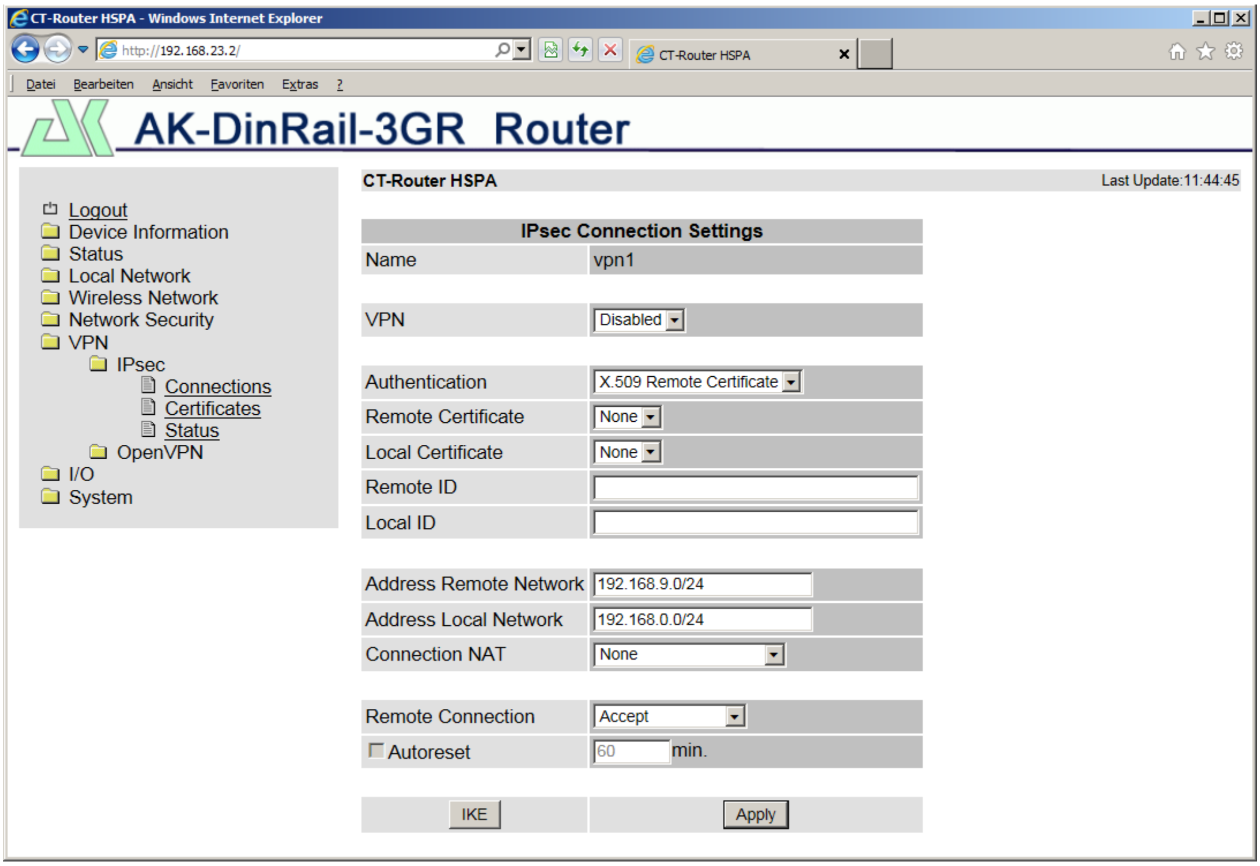
VPN → IPsec → Connections → Settings → Edit	
Settings	**Explanation**
Name	Name of the VPN connection
VPN	Activating (=Enable) or deactivating (=Disable) of the VPN connection
Remote host	IP address / URL of the remote station Can only be set if "Initiate" was selected under remote connection. If "Accept" 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.
Remote connection	**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 HSPA — Last Update:11:44:45

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.

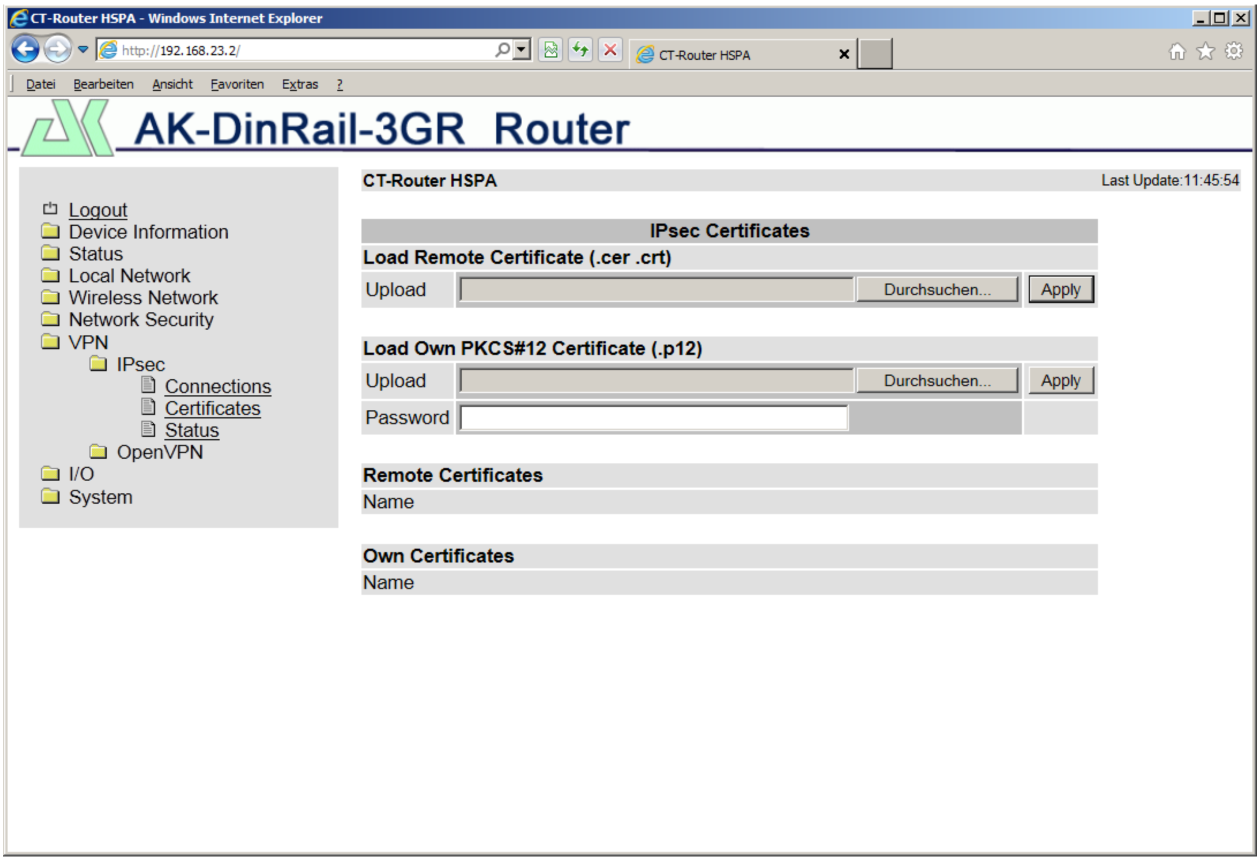
VPN → IPsec → Connections → IKE → Edit	
IKE	Explanation
Name	Name of the VPN connection.
Phase 1 ISAKMP SA	Key exchange
ISAKMP SA Encryption	Choice of encryption algorithm
ISAKMP SA Hash	Choice of hash algorithm
ISAKMP SA Lifetime	Lifetime of the ISAKMP SA key. Standard setting 3600 seconds (1 hour)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

VPN-IPsec

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 HSPA Last Update:11:45:54

IPsec Certificates

Load Remote Certificate (.cer .crt)

Upload

Load Own PKCS#12 Certificate (.p12)

Upload

Password

Remote Certificates

Name

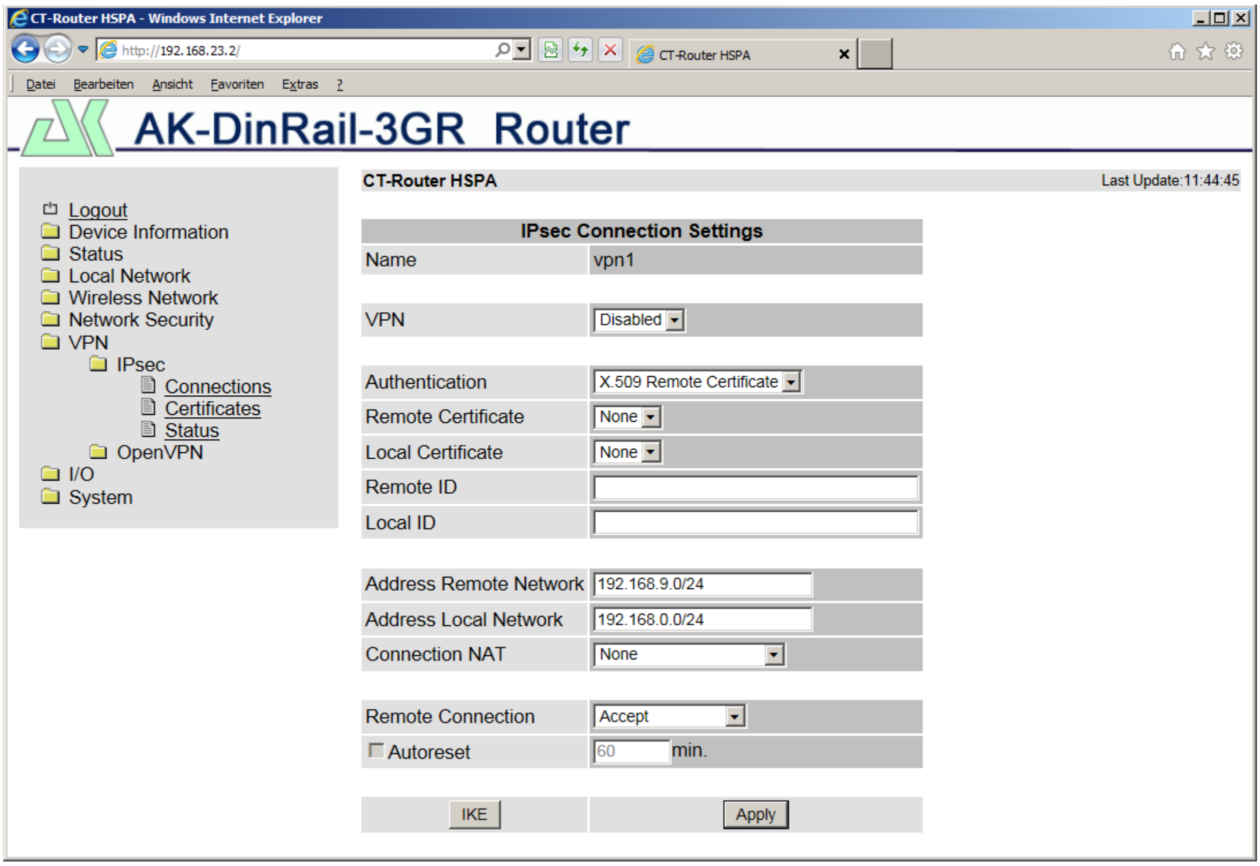
Own Certificates

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



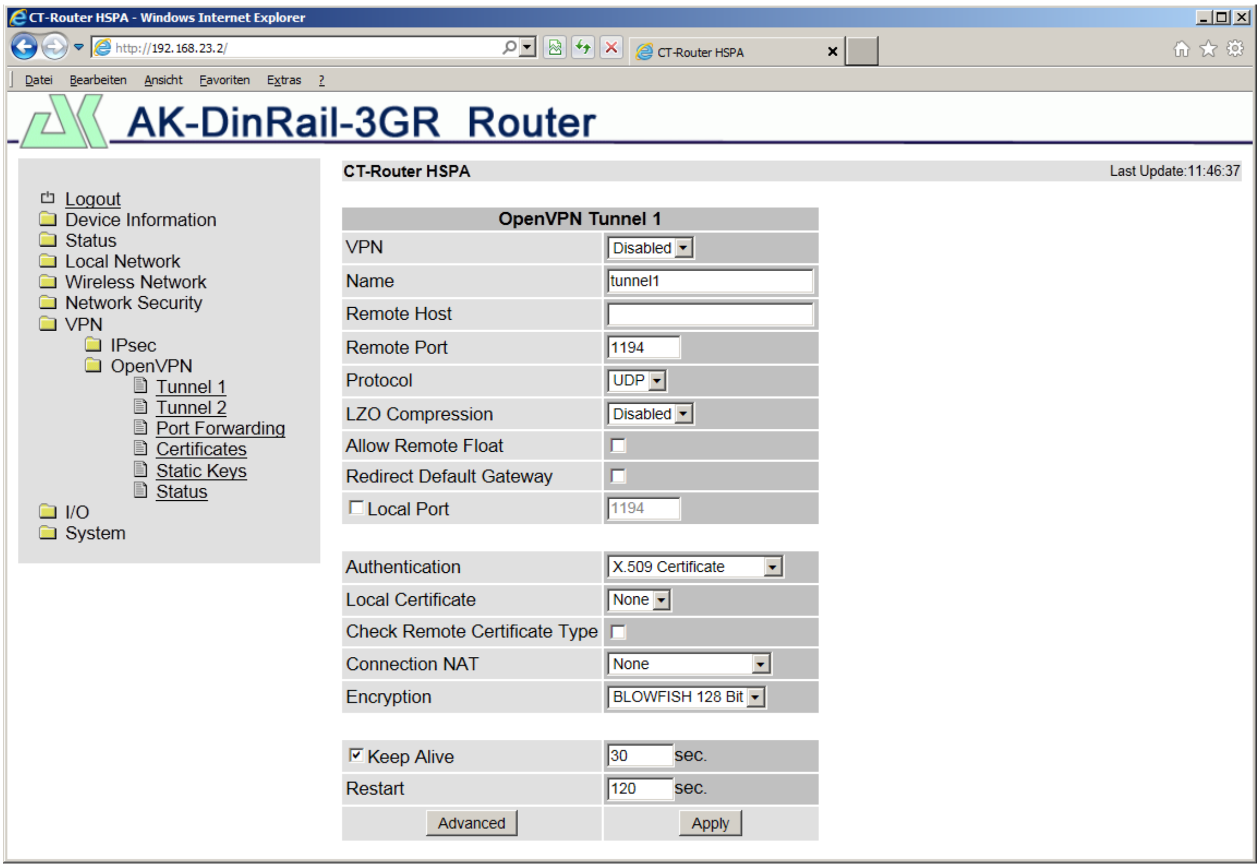
CT-Router HSPA — Last Update:11:44:45

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.
IKE	Apply

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



CT-Router HSPA Last Update:11:46:37

OpenVPN Tunnel 1	
VPN	Disabled
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	None
Encryption	BLOWFISH 128 Bit
☑ Keep Alive	30 sec.
Restart	120 sec.

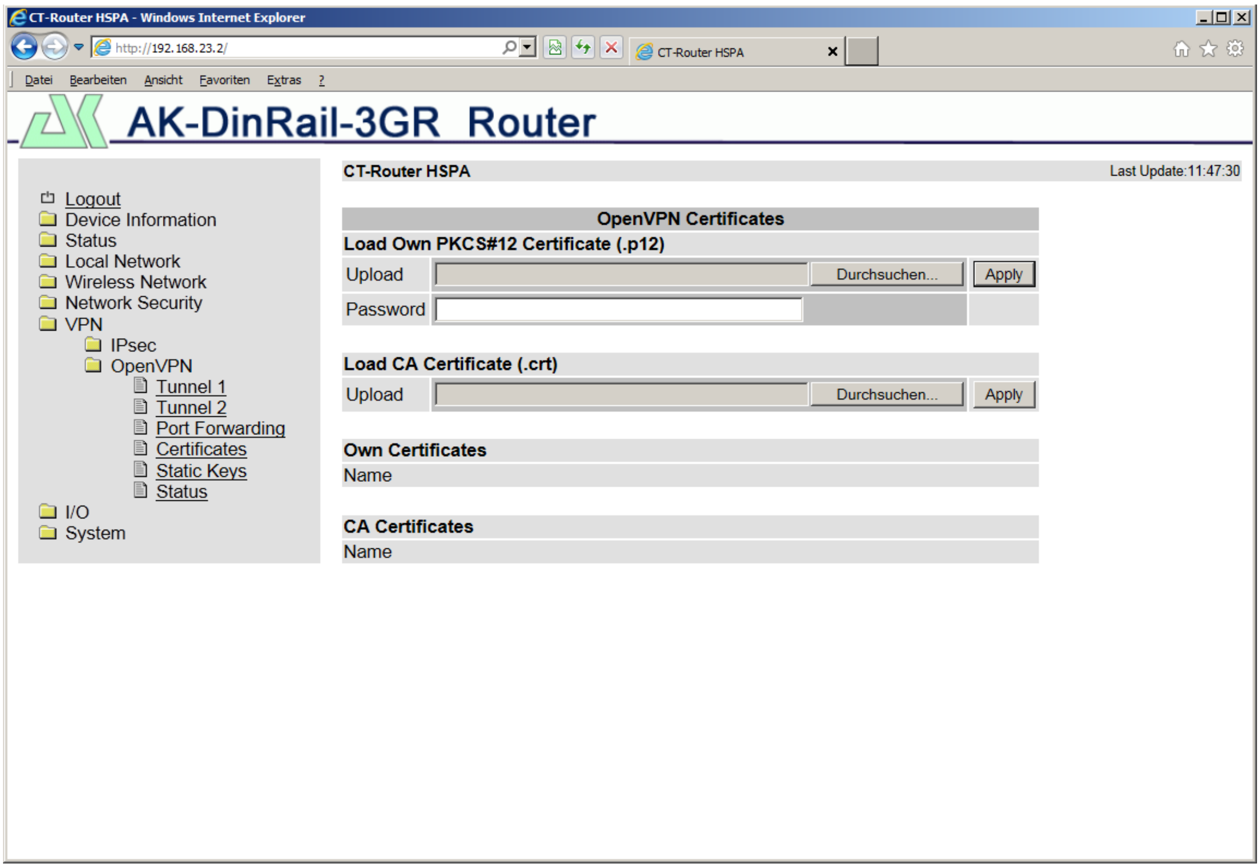
VPN → OpenVPN → Tunnel	
OpenVPN Tunnel	**Explanation**
VPN	OpenVPN Tunnel activated (=Enable) or inactivated (=Disable)
Name	Name of the OpenVPN connection
Remote host	IP address or URL of the remote station
Remote port	Port of the remote station (Standard: 1194)
Protocol	Determine UDP or TCP protocol for the OpenVPN connection!
LZO compression	**Disabled:** No compression **Adaptive:** Adaptive compression **Yes:** Compression activated
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 certification	Certificate of the router for the authentication at the remote station.
Check Type of Remote Certificate	Option: Check certificates of the OpenVPN connection.

VPN-OpenVPN

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/shall be 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

Certificates



CT-Router HSPA Last Update:11:47:30

OpenVPN Certificates

Load Own PKCS#12 Certificate (.p12)

Upload

Password

Load CA Certificate (.crt)

Upload

Own Certificates

Name

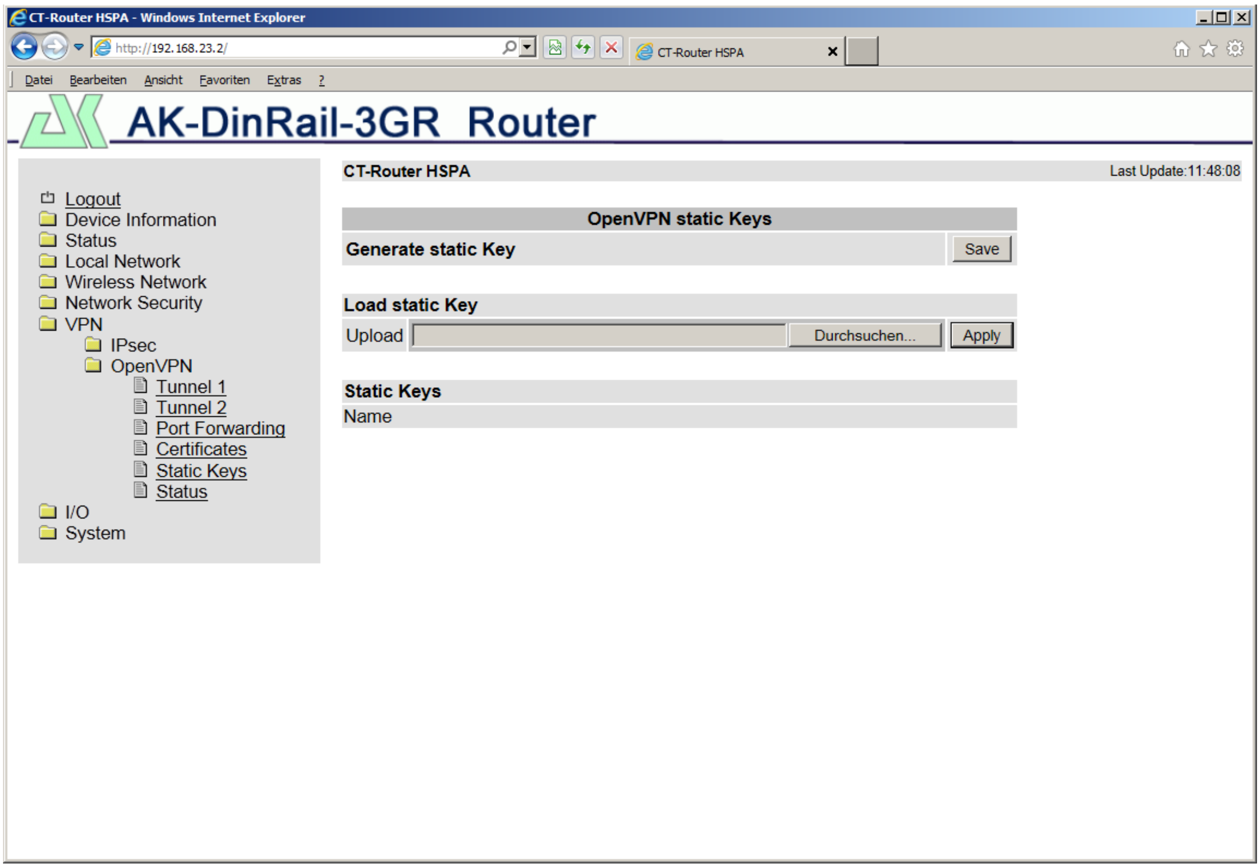
CA Certificates

Name

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 HSPA Last Update:11:48:08

OpenVPN static Keys

Generate static Key

Load static Key

Upload

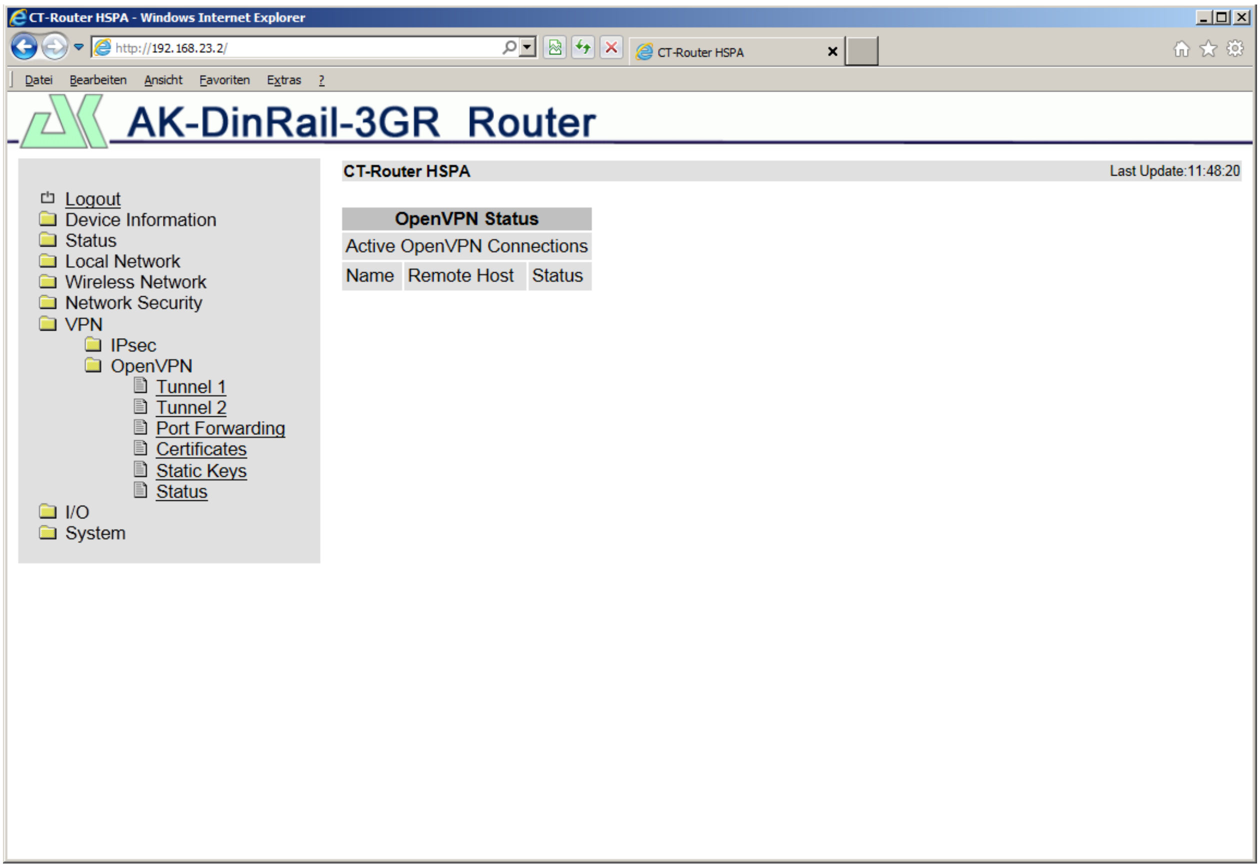
Static Keys

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



CT-Router HSPA

Last Update:11:48:20

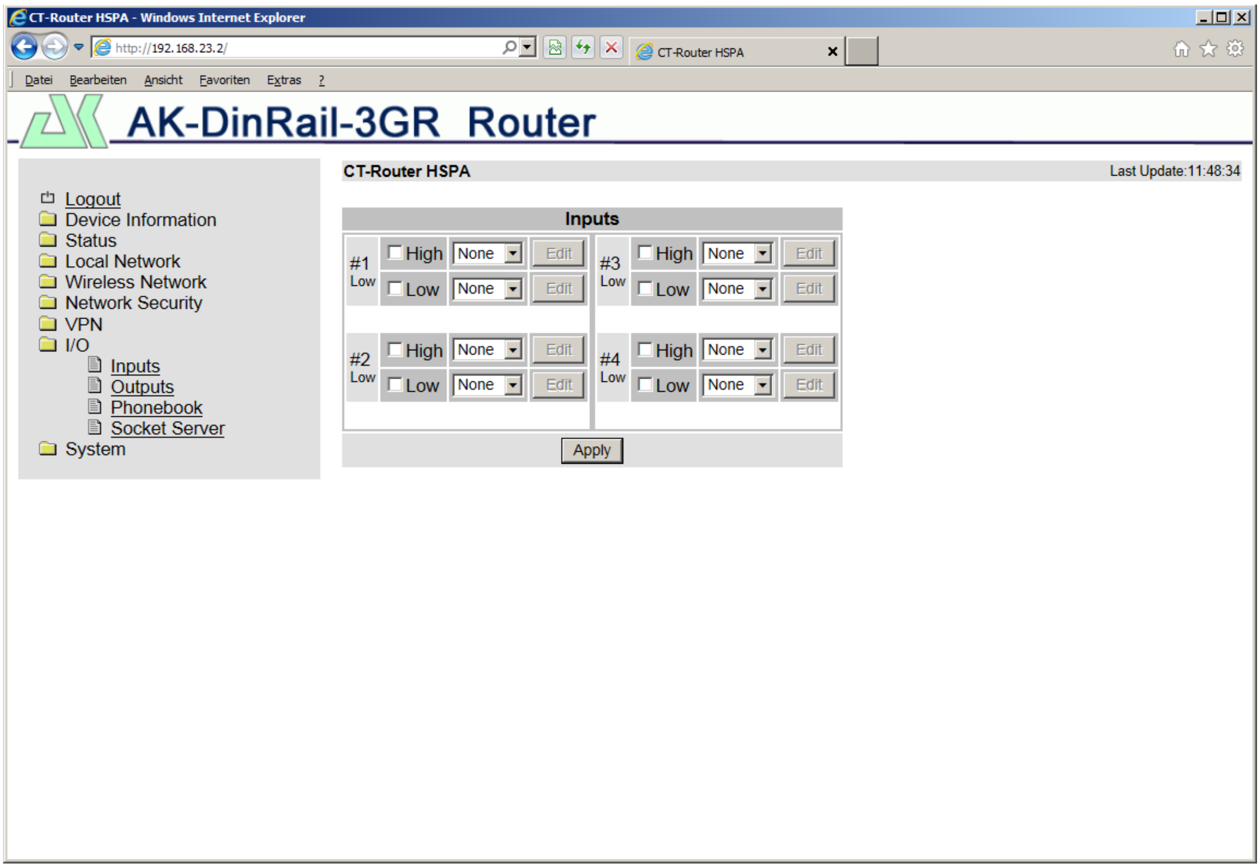
OpenVPN Status		
Active OpenVPN Connections		
Name	Remote Host	Status

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

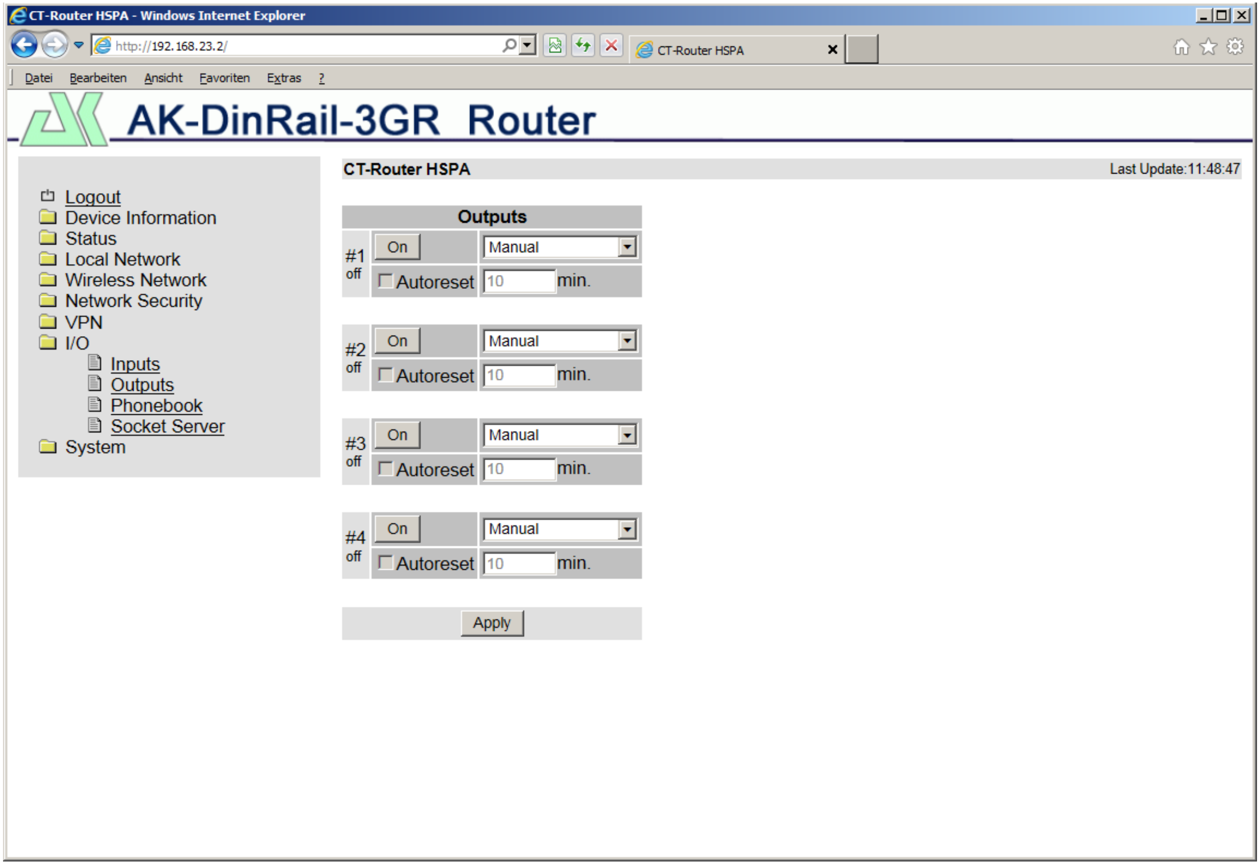
Inputs



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.	

I/O

Outputs



CT-Router HSPA Last Update:11:48:47

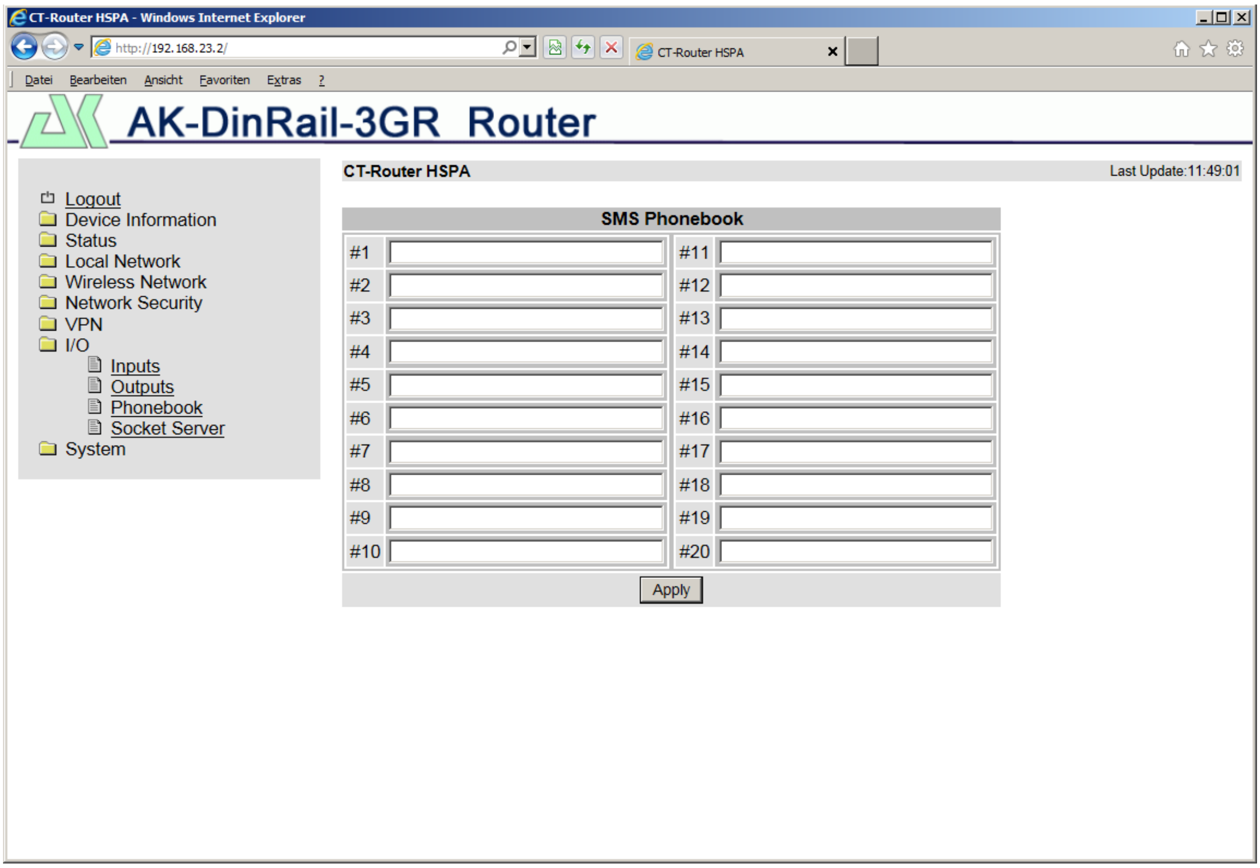
Outputs		
#1 off	On	Manual
	□ Autoreset	10 min.
#2 off	On	Manual
	□ Autoreset	10 min.
#3 off	On	Manual
	□ Autoreset	10 min.
#4 off	On	Manual
	□ Autoreset	10 min.

Apply

I/O →Outputs	
Outputs	Explanation
Options	**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.

I/O

Phonebook



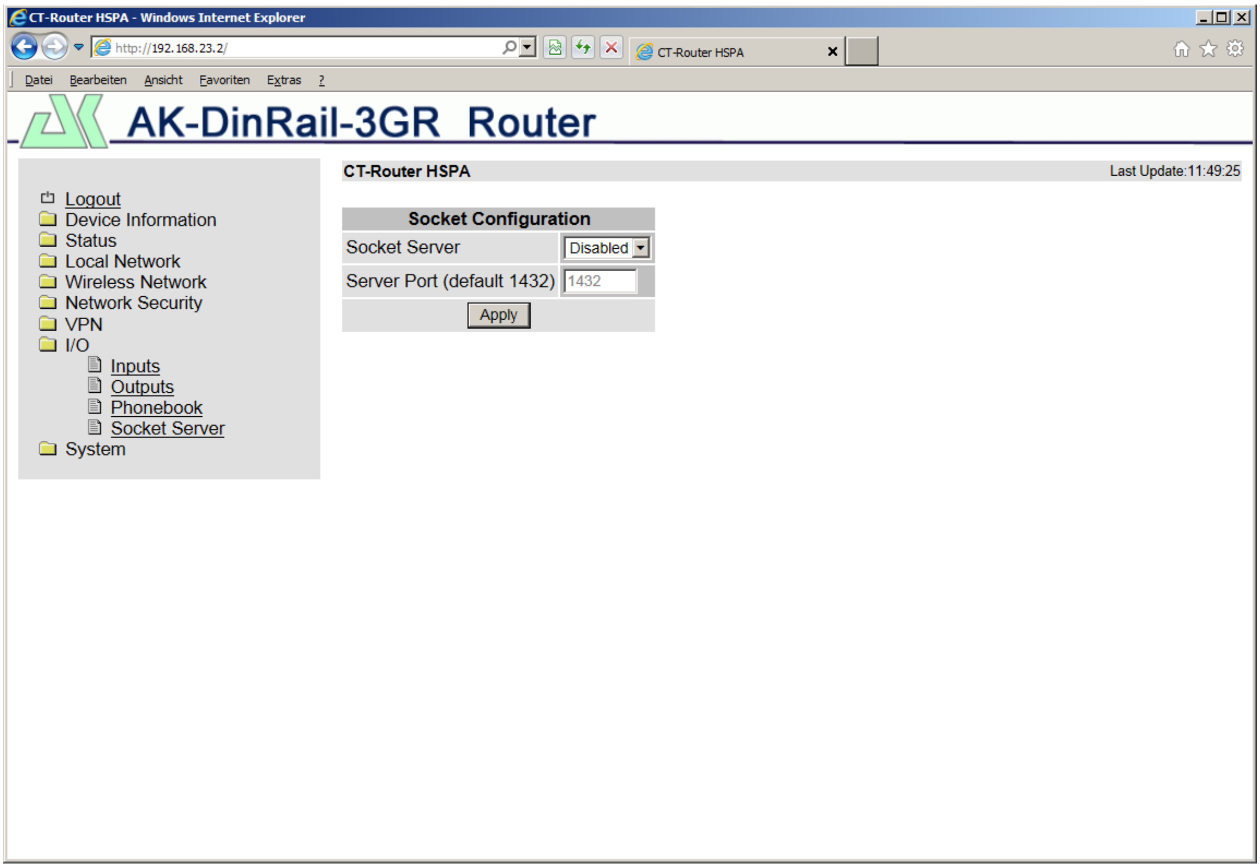
CT-Router HSPA Last Update:11:49:01

SMS Phonebook			
#1		#11	
#2		#12	
#3		#13	
#4		#14	
#5		#15	
#6		#16	
#7		#17	
#8		#18	
#9		#19	
#10		#20	

I/O → Phonebook	
Phonebook	Explanation
#1 … #20	Phone number for I/O input and I/O output

I/O

Socket server



Socket Configuration

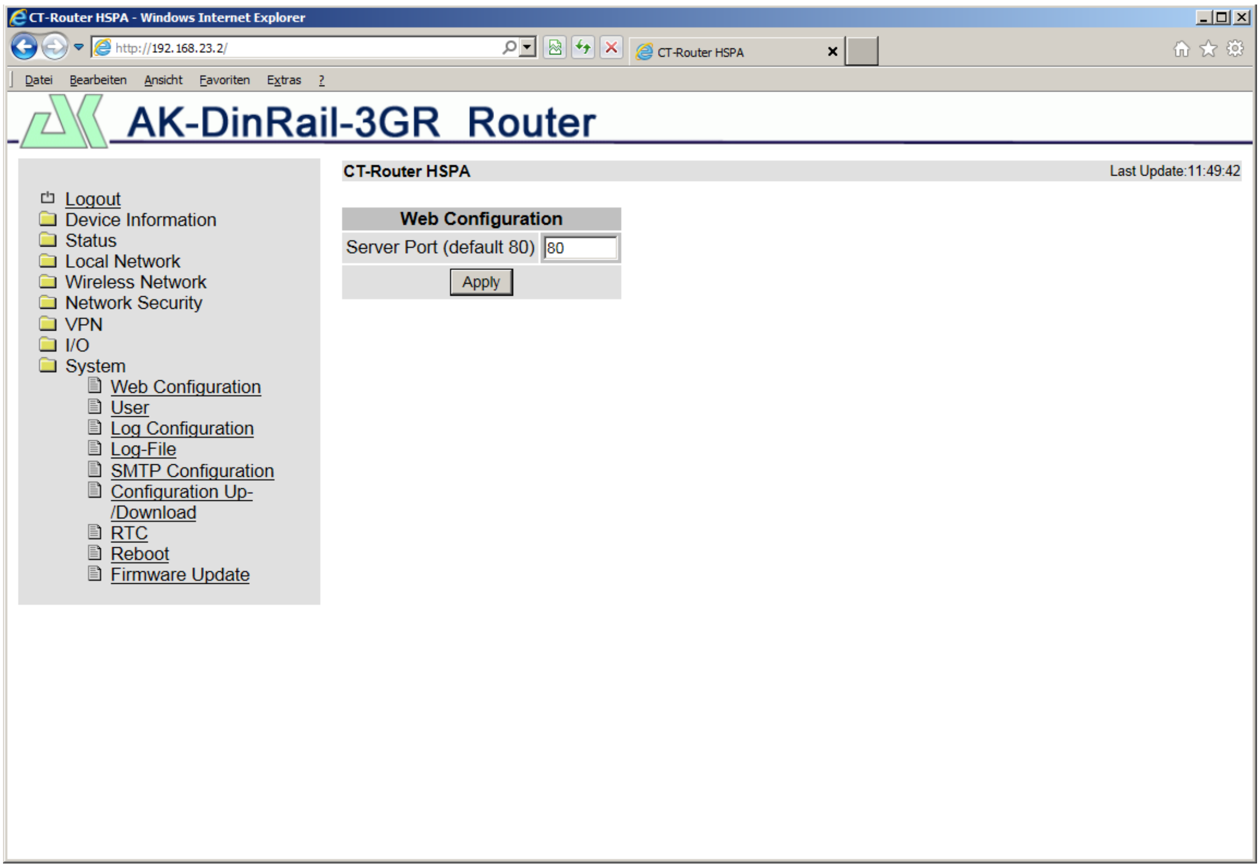
Socket Configuration	
Socket Server	Disabled
Server Port (default 1432)	1432

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-xG-Router in the system menu.

Web configuration



CT-Router HSPA

Last Update:11:49:42

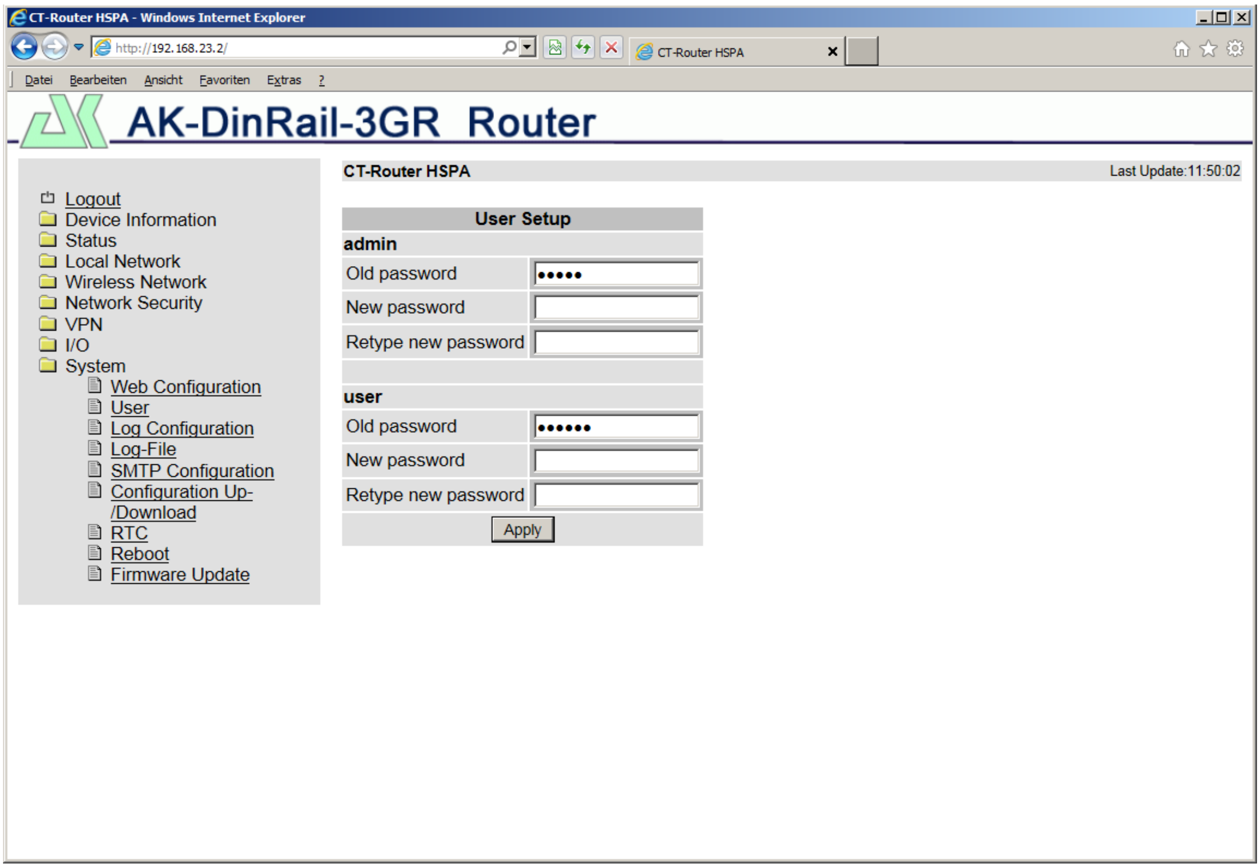
Web Configuration

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 Last Update:11:50:02

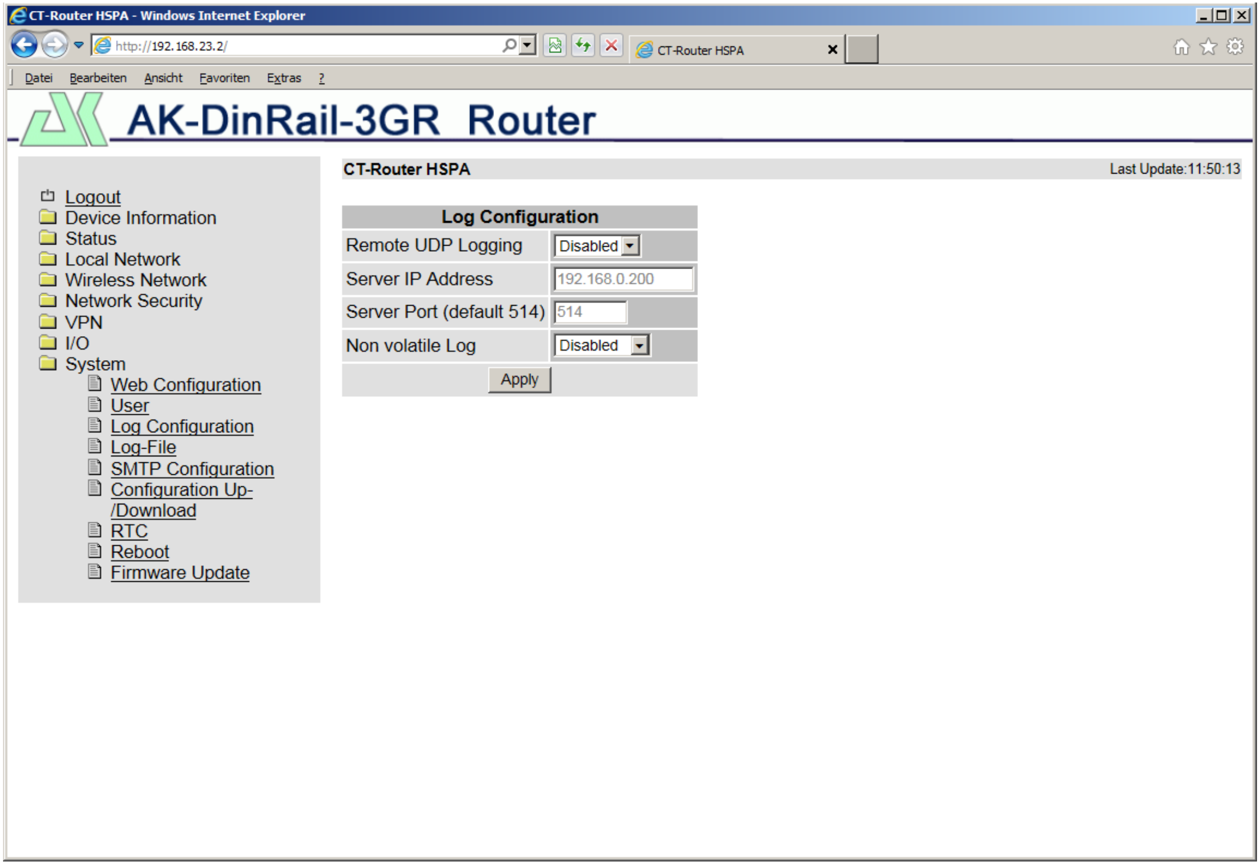
User Setup

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.

System

Log configuration



CT-Router HSPA

Last Update:11:50:13

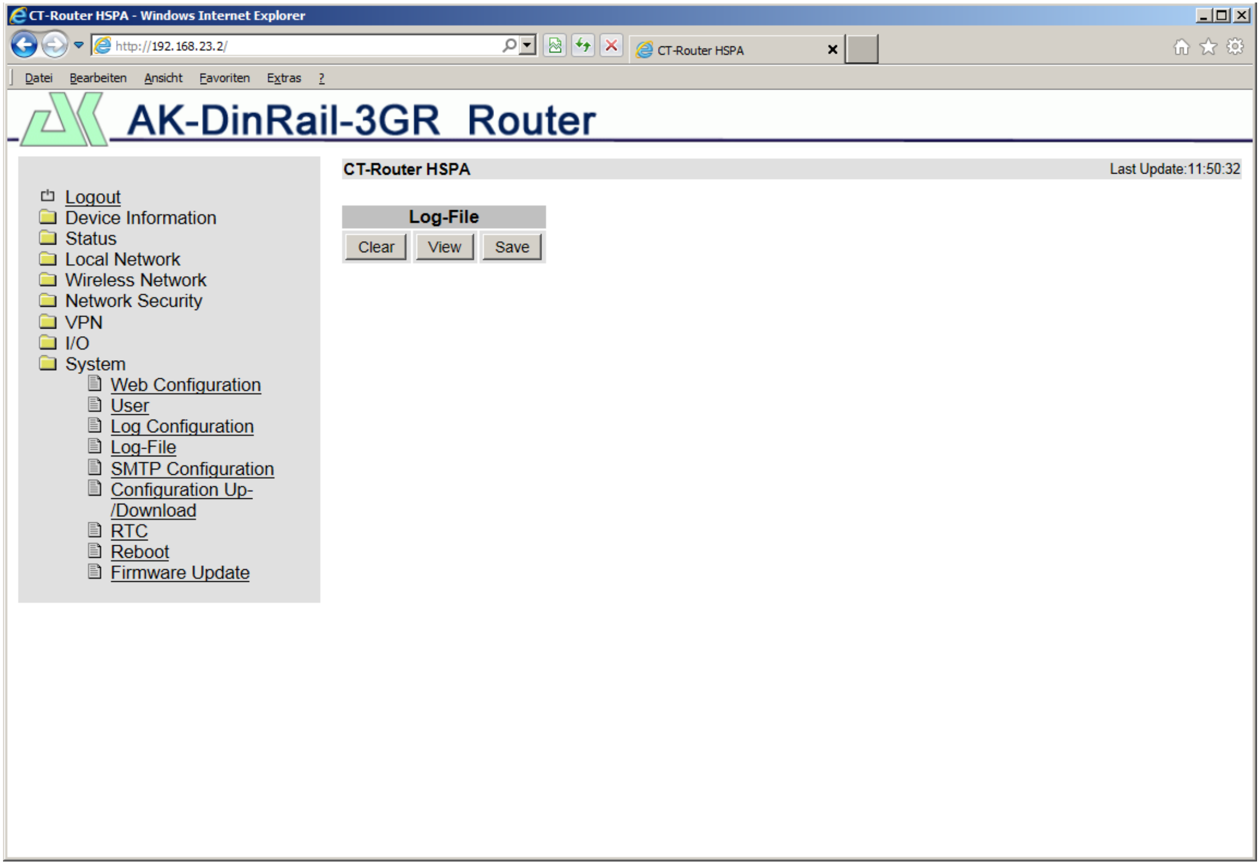
Log Configuration

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

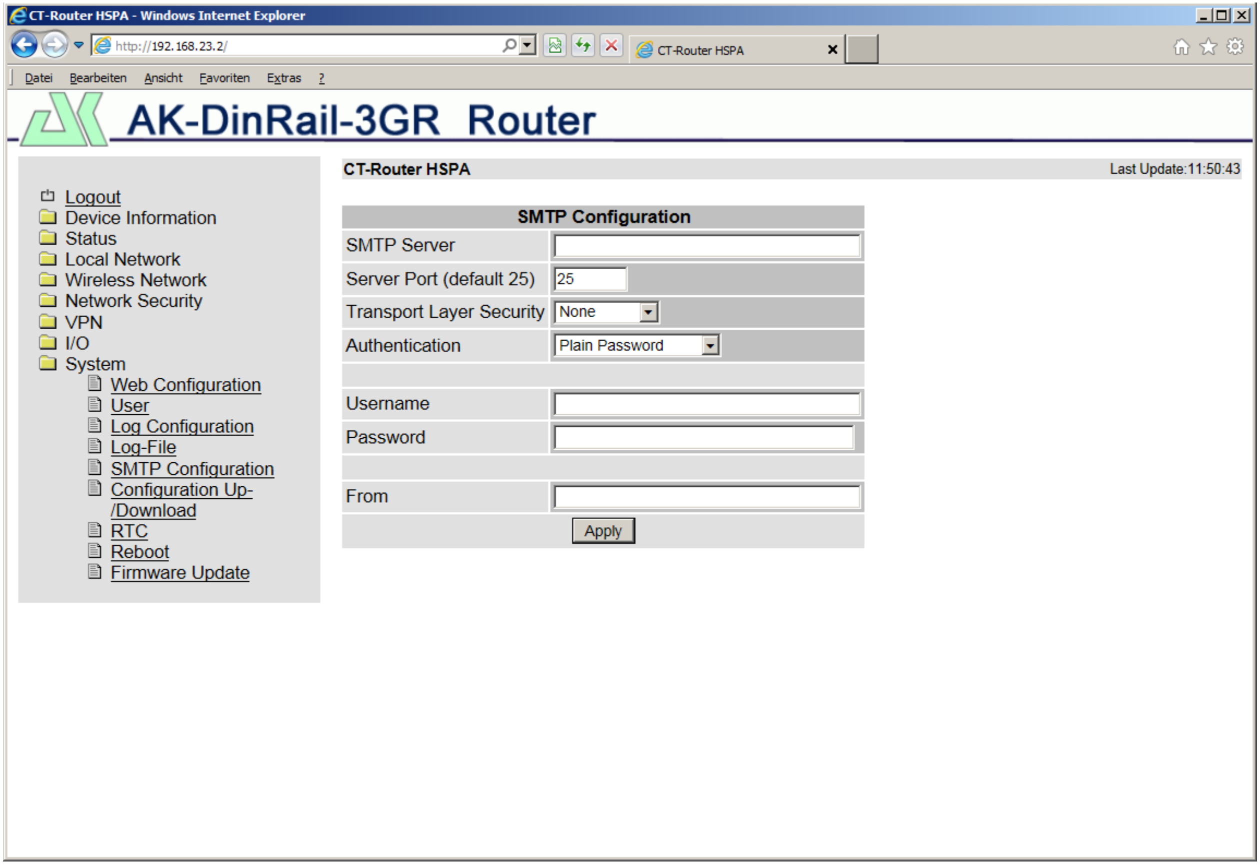
Log file



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

SMTP configuration



CT-Router HSPA Last Update:11:50:43

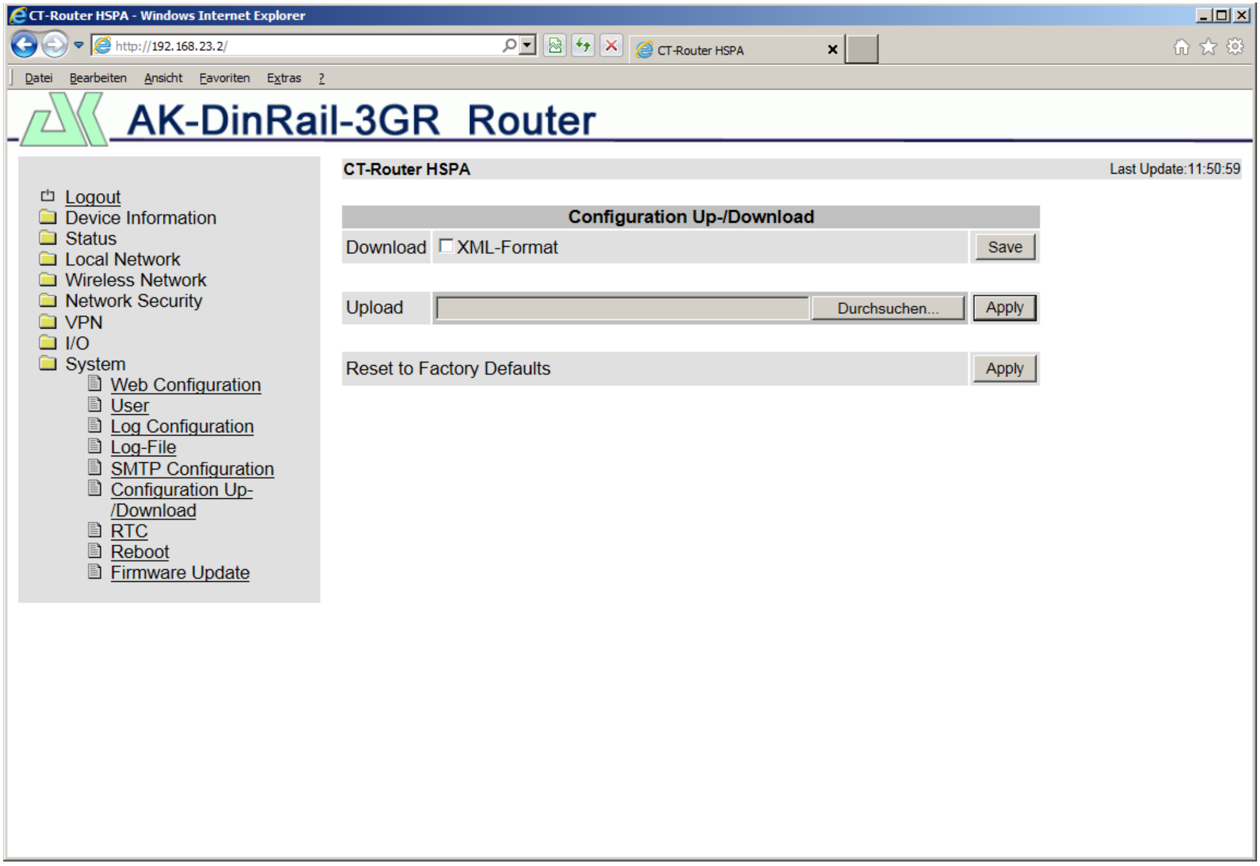
SMTP Configuration

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).
User name	User name
Password	Password
From	sender of the mail

System

Configuration up-/download



CT-Router HSPA Last Update:11:50:59

Configuration Up-/Download

Download □ XML-Format Save

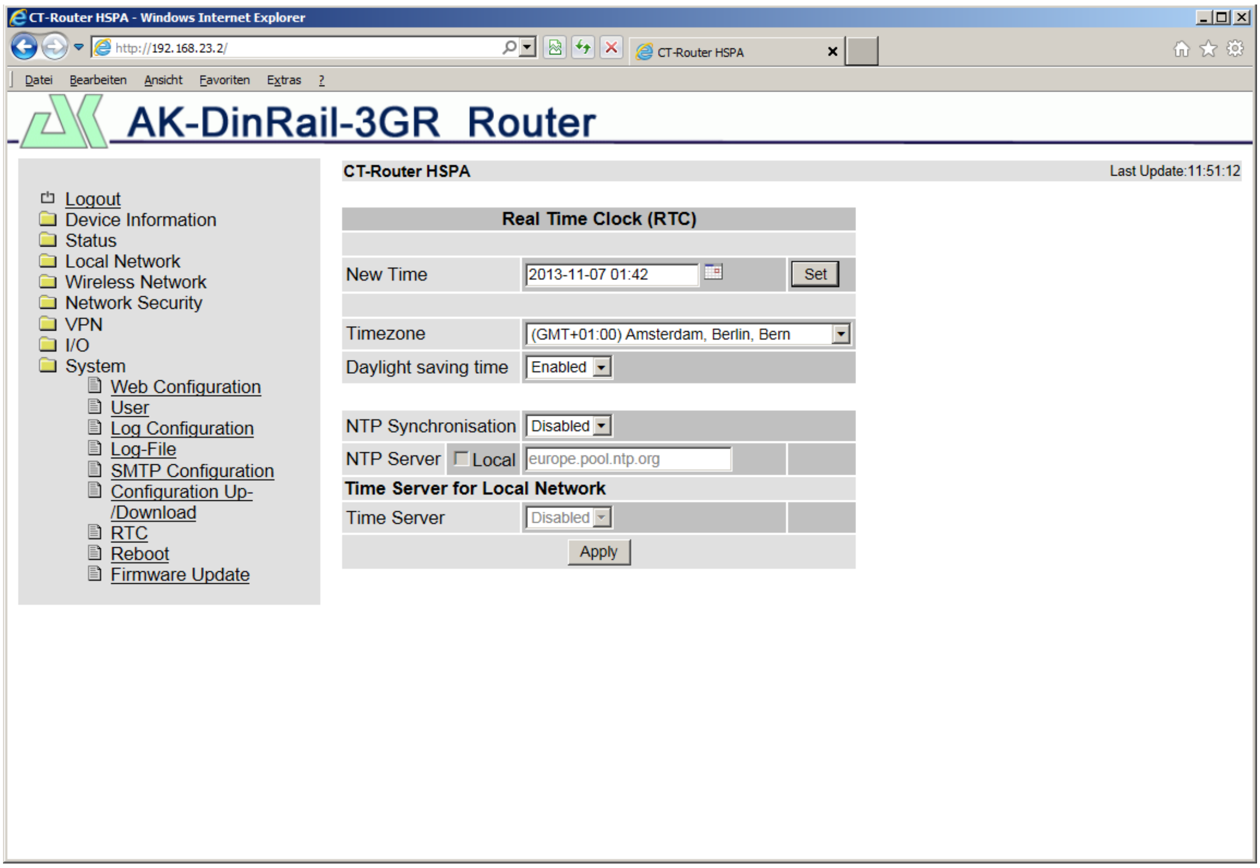
Upload Durchsuchen... Apply

Reset to Factory Defaults Apply

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 Last Update:11:51:12

Real Time Clock (RTC)

New Time: 2013-11-07 01:42

Timezone: (GMT+01:00) Amsterdam, Berlin, Bern

Daylight saving time: Enabled

NTP Synchronisation: Disabled

NTP Server: □ Local europe.pool.ntp.org

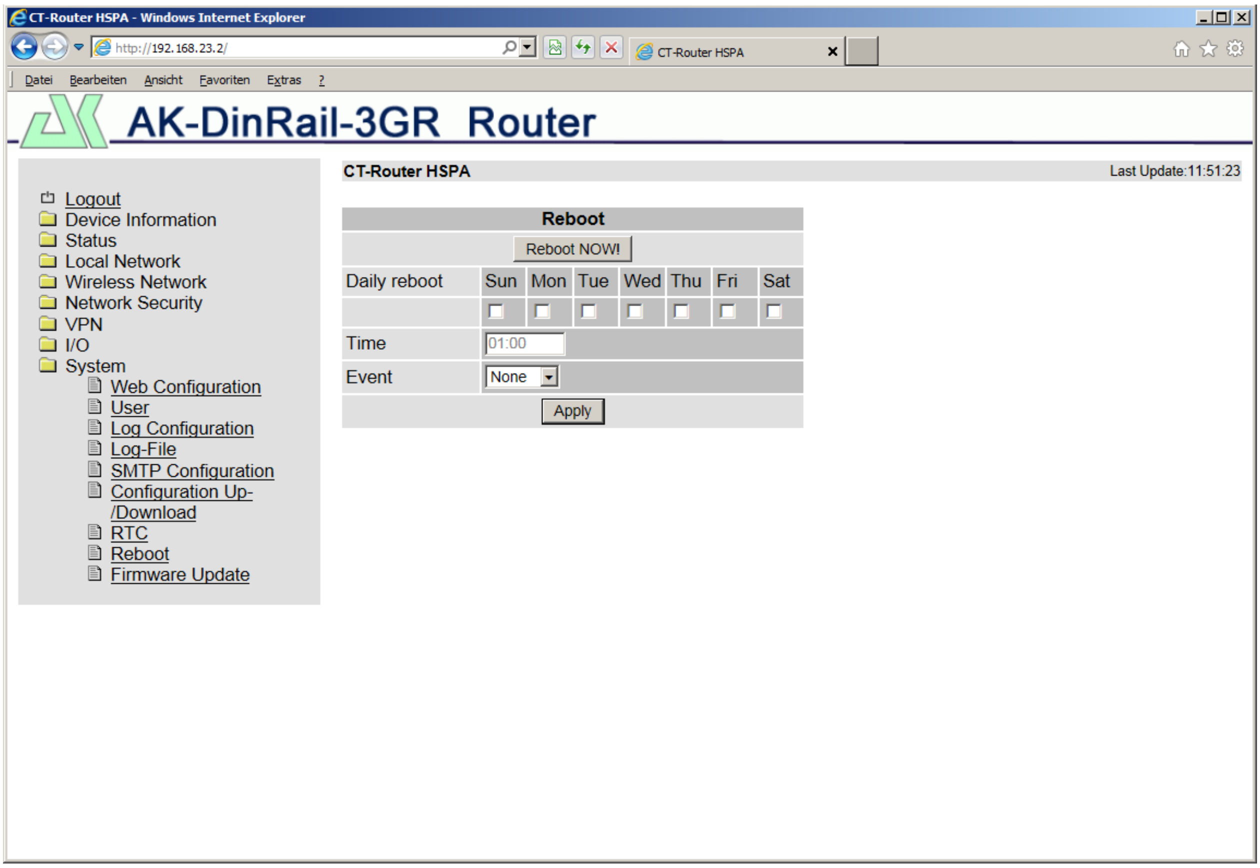
Time Server for Local Network

Time Server: Disabled

System → RTC	
RTC	Explanation
New time	Manual time configuration if no NTP server is available.
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



CT-Router HSPA - Windows Internet Explorer

http://192.168.23.2/

AK-DinRail-3GR Router

CT-Router HSPA

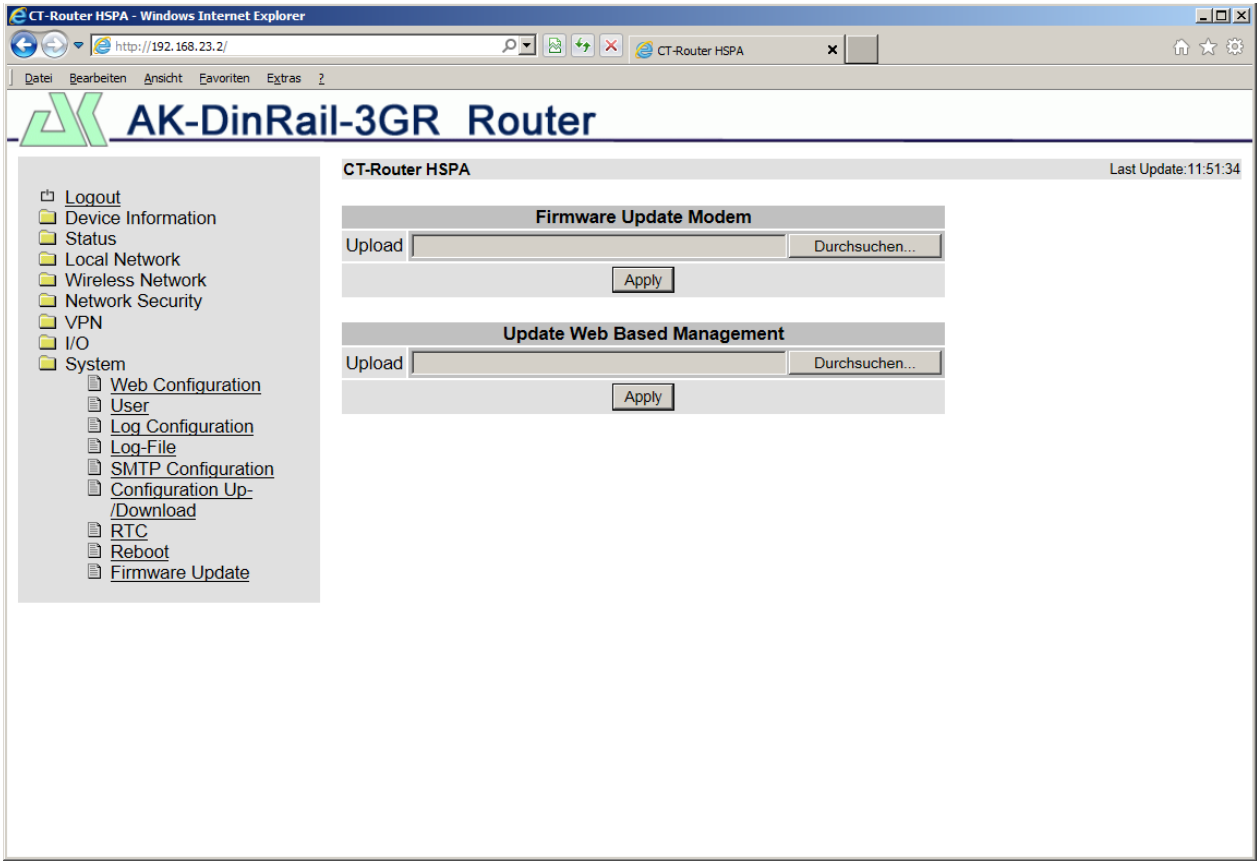
Last Update:11:51:23

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

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



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

1. Format of the XML files

Each file starts with the header:

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

or

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

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

```
<io>            </io> # I/O system
<info>          </info> # Request general informations
<cmgr ...>      </cmgr> # Send SMS (only mobile phones)
<email ...>     </email> # Send e-mail
```

All data are configured in UTF-8. The following characters
have to be transferred as a sequence:

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

2. Examples for the basic entries:

a) I/O system

```
<?xml version="1.0"?>
<io>
<output no="1"/>                    # Request status of output 1
<output no="2" value="on"/>         # Switch on output 2
<input no="1"/>                     # Request status of input 1
</io>
```

Note: It is possible to indicate on/off as well as 0/1 for the "value".
The response will always be on or off.

The response is delivered as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<result>
<io>
<output no="1" value="off"/> # Status of output 1; to be switched on here
<output no="2" value="on"/> # Status of output 2; was switched on here
<input no="1" value="off"/> # Status of input 1; to be switched off here
</io>
</result>
```

Please note that the outputs which shall be remote controlled need to be configured as "Remote controlled".

Inquiry and control via XML files

b) Request general information

```
<?xml version="1.0"?>
<info>
<device /> # Request device data
<radio /> # Request data regarding the phone connection (only mobile phones)
</info>
```

The response is delivered as follows:

```
<?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) Sending an SMS

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

The response is delivered as follows:

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

d) Sending an e-mail

```
<?xml version="1.0"?>
<email to="x.yz@diesunddas.de" cc="info@andere.de">
<subject>Test Mail</subject>
<body>
    This is an e-mail text of several lines.
    Kind regards
    your router
</body>
</email>
```

Inquiry and control via XML files

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.

c) Receive a SMS

Notice: Please activate „SMS configuration“ -> „SMS control“, and use a password. Additionally you can add a TCP-Server to get the sent SMS-Messages.

Syntax of a received SMS:

```
#<password>:<command>[:<subcommand>[:<parameter>]]

  <password>   - ('A'-'Z', 'a'-'z', '0'-'9')    (up to 7 alfanumeric chars)

  <command>    - SET:<subcommand>[:<parameter>]
                 CLR:<subcommand>[:<parameter>]
  <subcommand> - OUTPUT[:<parameter>]
                 IPSEC[:<parameter>]
                 OPENVPN[:<parameter>]
                 OPENVPN.TUNNEL[:<parameter>]
                 OPENVPN.BRIDGE[:<parameter>]
                 GPRS

  <command>    - SEND:<subcommand>
  <subcommand> - STATUS

  <command>    - RESET   // Alarm reset
  <command>    - REBOOT  // Device reboot
```

Special conditions:

If <parameter> is omitted, it defaults to 1.
If all chars in the password field are uppercase at the device configuration then the case of received chars is ignored.

Examples:
password = SECRET

a) set output number 3 to on:
Remark: this works only if the desired output is configured as "Remote Controlled"

```
#SECRET:SET:OUTPUT:3
```

b) set output number 3 to off:
Remark: same as above example.

```
#SECRET:CLR:OUTPUT:3
```

c) start IPsec VPN channel no 2
this works only if the desired IPsec channel is configured as "Initiate on SMS"

```
#SECRET:SET:IPSEC:2
```

d) start packet service
this works only if the packet data event is configured as "Initiate on SMS"

```
#SECRET:SET:GPRS
```

e) send back a status SMS

```
#SECRET:SEND:STATUS
```

The format of the returned SMS:
STATUS INPUT1-<state> .. INPUTx-<state> OUTPUT1-<state> .. OUTPUTx-<state> [CGPADDR=a.b.c.d]

Where <state> is NA for "not activated" and A for "activated".
If valid packet data is available then the IP-Adresse is retuned as "CGPADDR=2.3.4.5".

f) start OpenVPN tunnel no 2
this works only if the desired OpenVPN tunnel is configured as "Initiate on SMS"

```
#SECRET:SET:OPENVPN:2
```

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

4. Datendefinitionen der verwendeten Elemente

4.1 Info Categorie

4.1.2 Device group

- serialno
  Serialnumber
- hardware
  Hardwarerevision
- firmware
  Current firmwareversion
- wbm
  Current version of webmanagement
- imei
  IMEI number

- adslfirmware
  Version of DSP-Firmware

4.1.3 Radio Gruppe

Only for radiomodule

- provider
  Type: Text, name of provider
- rssi
  Signal level:
  Type: 0..99

0	->	-113 dBm r less
1	->	-111 dBm
2..30	->	-109.. -53 dBm
31	->	-51 dBm or more
99	->	could not get value

- creg
  Status of registry within radio
  Type: 0..5
  0 -> not registered. Still searching
  1 -> Registrered at home network
  2 -> not registered. Still searching
  3 -> registration not allowed
  4 -> not used
  5 -> Roaming (Registred in other network)

- lac
  Location Area Code (Aufenthaltsbereich des Gerätes innerhalb eines Mobilfunknetzes)
  Type: Hexadezimalzahl max. 4-digits
- ci
  Cell ID (Identifikation number within LAC)
  Type: Hex max. 8-Stellen
- paket
  Paketdata state
  Type: 0..8
  0 -> offline (no connection)
  1 -> online (connection is going to be established)
  2 -> GPRS online
  3 -> EDGE online
  4 -> UMTS online
  5 -> HSDPA online
  6 -> HSUPA online
  7 -> HSDPA+HSUPA online
  8 -> LTE online
- simstatus
  State of SIM-card
  Type: 0..5
  0 -> unknown
  1 -> no sim detected
  2 -> waiting for PIN
  3 -> wrong PIN
  4 -> waiting for PUK
  5 -> ready

- simselect
  choose the SIM card
  Type: 0..3
  0 -> unknown/no SIM
  1 -> SIM 1
  2 -> SIM 2

4.1.4 Inet Gruppe

- ip
  IP-Adress
  Type: IP-Adress

- rx_bytes
  Amount of received bytes
  Type: 0..4294967295

- tx_bytes
  Amount of transmitted bytes
  Type: 0..4294967295

- mtu
  Maximum paket size
  Type: 128..1500

4.1.5 IO Gruppe

There are two types possible (You need to configure first):
- Verbose: text "off" or "on"
- Numeric: 0 or 1

- gsm
  binary state of GSM/UMTS connection

- inet
  binary state of (paketdata) connection

- vpn
  binary state of the VPN-Tunnels

4.2 SMS Categories

4.2.1 SMS sending

- cmgs
  used attributes:

- destaddr
  Type: Telefon number of receipient.

Note the maximum of 160 chars.
Note that some signs can take space of 2 chars. (^ [ ] { } ~ \ | €)

Use the GSM 03.38 '6.2.1 Default alphabet.
Coding must be done by UTF-8 XML rules.

4.2.2 SMS receiving

- cmgr
  Type: UTF-8 Text

  Used attributes:

- origaddr
  Type: Telefon number of sender.

- timestamp
  Type: Time

- error
  Type: 1..3
  You will only get an error if there really occurred an error.
  1 -> empty
  2 -> busy
  3 -> system error

4.2.3 SMS receipt notice

- cmga
  Type: Text
  If possible you will get an OK

  uzsed attributes:
- error
  Type: 3
  If there is an error, you will receive „system error“

4.3 E-Mail Categorie

- email
  used attributes:
  - to
  - cc
  Type: E-Mail adress

4.3.1 E-Mail Subject

- subject
  Type: UTF-8 coded text

4.3.2 E-Mail Message

- body
  Type: UTF-8 coded text

4.4 IO Categories

4.4.1 Input element

- input
  used attributes:
  - no
  Type: 1..6

4.4.2 Output element

- output
  used attributes:
  - no
  Type: 1..6

- value
  There are two types possible (You need to configure first):
  - Verbose: Text "off" or "on"
  - Numeric: DEZ 0 or 1
  To set or reset the port, both types can be used.

4.4.3 IPsec Element

- ipsec
  used attributes:

- no
  Type: 1..5

- value
  There are two types possible (You need to configure first):
  - Verbose: Text "off" or "on"
  - Numeric: DEZ 0 or 1

To set or reset the port, both types can be used.

4.4.4 OpenVPN Element

- openvpn
  used attributes:

- no
  Type: 1..5

- value
  There are two types possible (You need to configure first):
  - Verbose: Text "off" or "on"
  - Numeric: DEZ 0 or 1

To set or reset the connection, both types can be used.

You can also use typee

- typee
  Type: String {tunnel|bridge} preinstalled is 'tunnel'.

Inquiry and control via XML files

4.4.5 GPRS Element

- gprs
  used attributes:

- value
  There are two types possible (You need to configure first):
  - Verbose: Text "off" or "on"
  - Numeric: DEZ 0 or 1

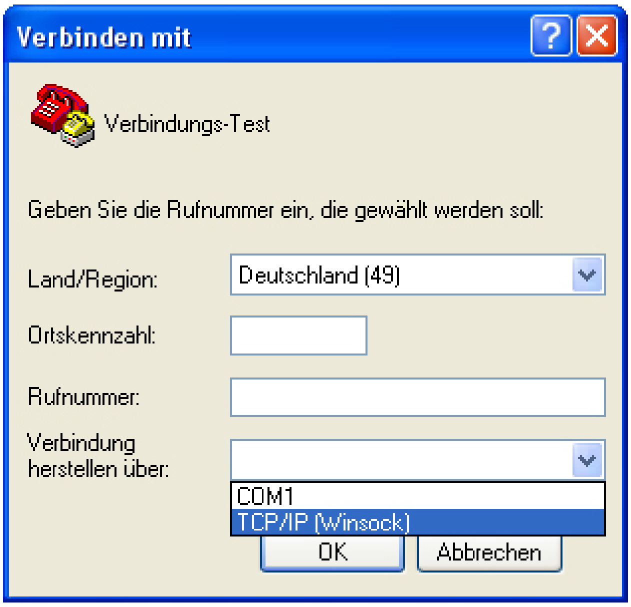
To set or reset the paketdata connection, both types can be used.

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)



Verbinden mit

Verbindungs-Test

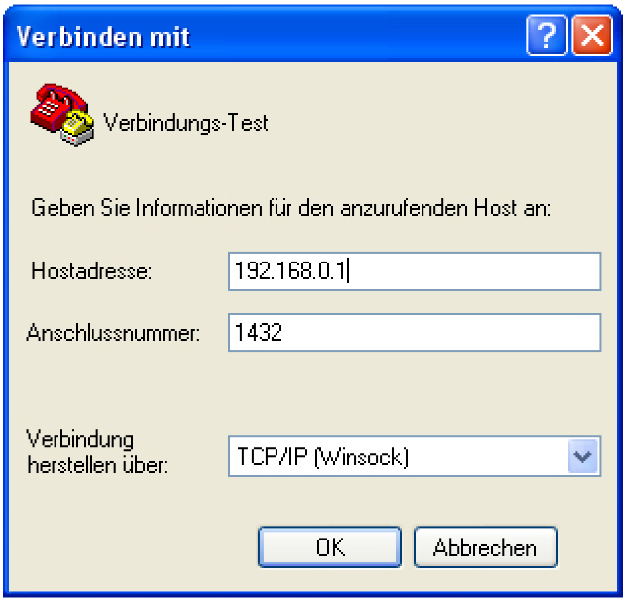
Geben Sie die Rufnummer ein, die gewählt werden soll:

Land/Region: Deutschland (49)

Ortskennzahl:

Rufnummer:

Verbindung herstellen über:



Verbinden mit

Verbindungs-Test

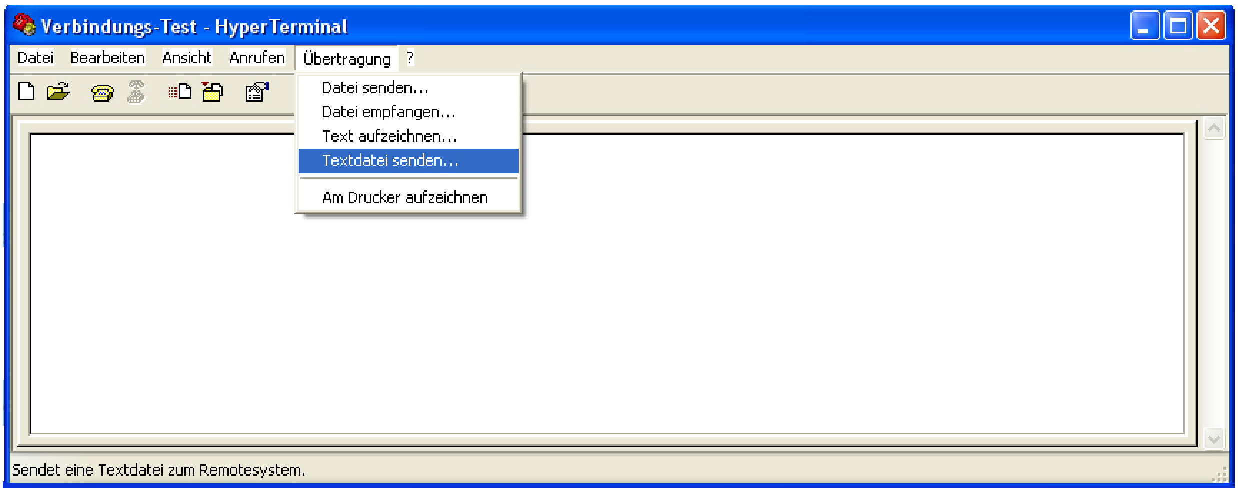
Geben Sie Informationen für den anzurufenden Host an:

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

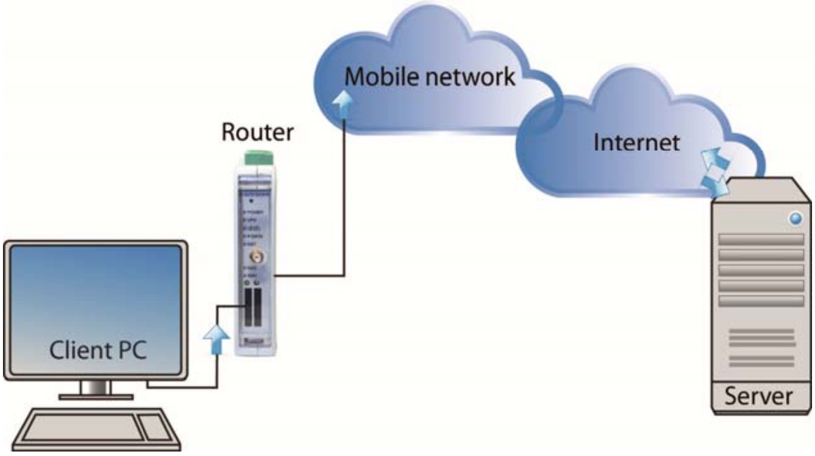
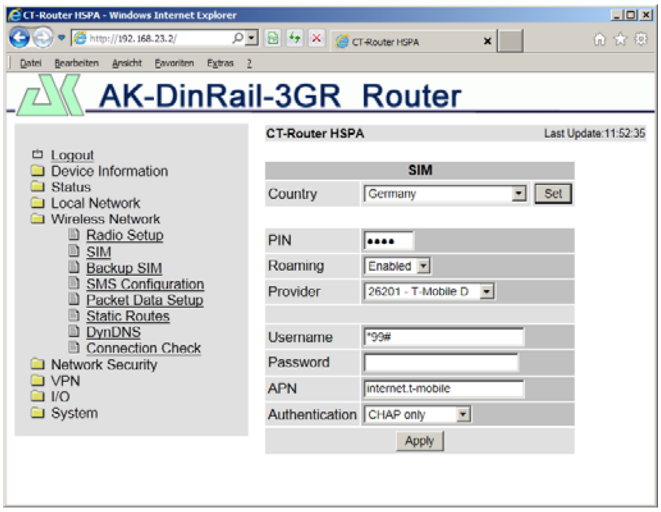


Illustration: Access to the Internet

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.

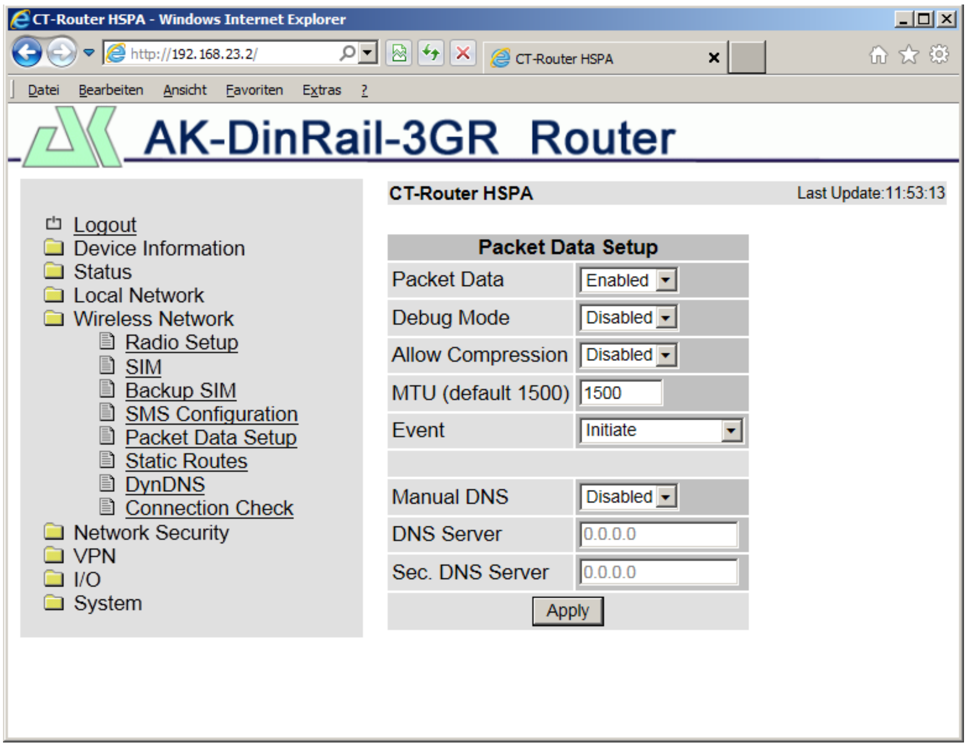


CT-Router HSPA Last Update:11:52:35

SIM	
Country	Germany
PIN	••••
Roaming	Enabled
Provider	26201 - T-Mobile D
Username	*99#
Password	
APN	internet.t-mobile
Authentication	CHAP only

Examples of an application

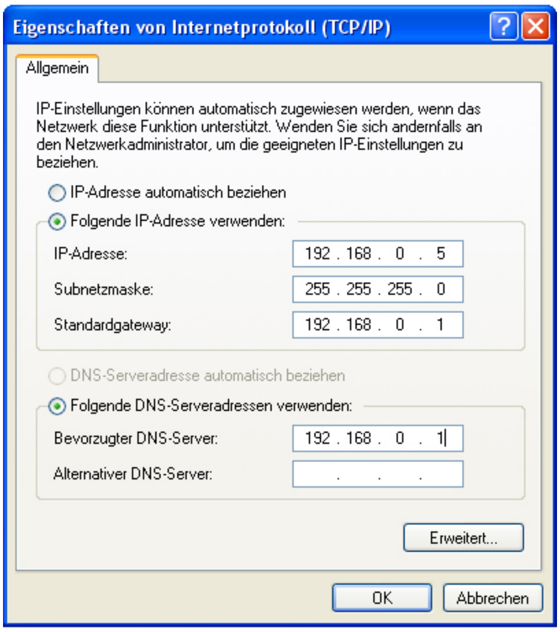
- Change over to a "Wireless network" and "Packed data setup" and activate the package data transfer in the mobile phone network.
  To do so, set "Package data" to "Enable".



CT-Router HSPA — Last Update:11:53:13

Packet Data Setup	
Packet Data	Enabled
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

- 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:	. . .

FAQ

Question	Answer
The router is online, but there is no data transmission possible	Enable the packet data. (Wireless Network → Packet Data Setup)
The router got problems at dial-up	Check your APN
I can't log in to web-based-managent	Please use „admin“ for requested user and password.