

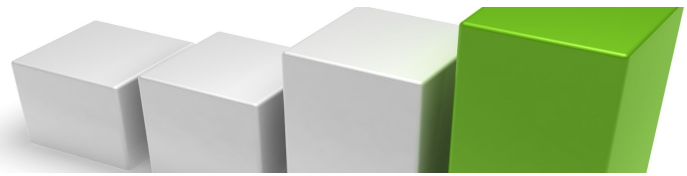
## Transparente RS232/RS485-Kopplung über das Internet

### **1. Aufgabenstellung**

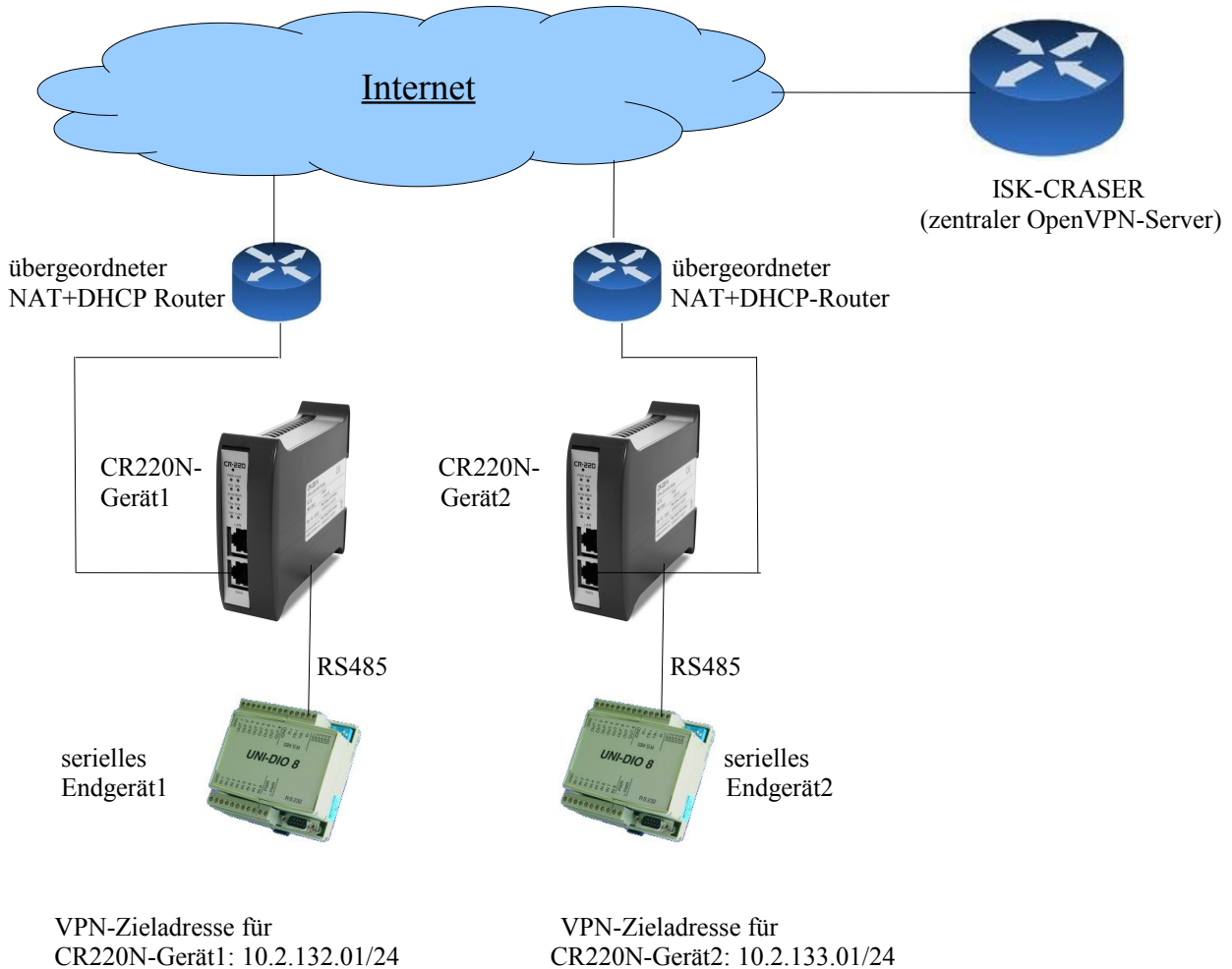
Das RS485-Interface eines seriellen Endgerätes soll über das Internet mit dem RS485-Interface eines 2. seriellen Endgerätes gekoppelt werden. Die Kopplung soll so funktionieren, als wären die beiden seriellen Endgeräte über RS485 direkt miteinander verbunden. Der serielle RS485-Datenverkehr wird auf beiden Seiten vom CR220N in internetgerechte UDP-Frames umgewandelt. Beide CR220N nutzen in dieser Anwendung den Internetzugang eines übergeordneten Routers. Sollte kein übergeordneter Router vorhanden sein, kann auch ein DSL-Modem an den CR220N gekoppelt werden. Falls auch kein DSL-Zugang vorhanden ist, kann die Aufgabe durch den CR230U über UMTS gelöst werden. Die Datenverschlüsselung und Internet-Adresszuordnung übernimmt in allen Fällen der zentrale OpenVPN-Server „CRASER“.

Die Pinbelegungen der COM1 und COM2-Schnittstelle des CR220N finden Sie in unserem Dokument:

„Manual CR-220N.pdf“ auf „<http://isk-automation.de/produkte/industrie-router/cr220-n>“.



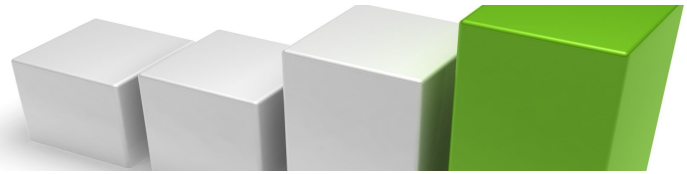
## 2. Netzwerkstruktur der transparenten RS232/RS485-Kopplung



Tipp1: So finden Sie die VPN-Zieladresse für den jeweiligen CR220N

globale Adresse des Fernwartungs-Subnetzes:	10.2.132.0/24
gesuchte Zieladresse:	→ 10.2.132.001
LAN1-Adresse des CR220N:	192.168.1.001/24

Die globale IP-Adresse Ihres Fernwartungs-Subnets ist für jeden am CRASER arbeitenden Router einmalig und ist bereits auf Ihrem Router vorkonfiguriert (siehe VPN → OpenVPN → p12-certificate)



Tipp2: CR220N kann den Internetzugang auch über ein externes DSL-Modem im Bridge-Mode herstellen (z.B. AM100 in Werkseinstellung), so dass die Zugangsdaten des ISP im Router konfiguriert werden können. Die Ankopplung eines DSL-Modems an den CR220N finden Sie in unserem Dokument „Fernwartung-DSL.pdf“ (Checkliste Punkte 1-4).

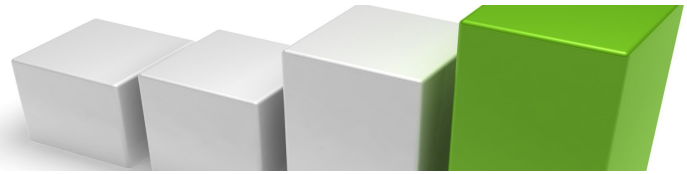
Tipp3: Falls kein übergeordneter Router und kein DSL-Zugang vorhanden sind, kann die Aufgabe auch mit dem CR230U über UMTS gelöst werden.

Tipp4: Neben der RS232/RS485-Kopplung sind auch die LAN-Subnetze beider Router über den CRASER gekoppelt. Näheres dazu finden Sie in unserem Dokument „Fernwartung-EXT-Internetzugang.pdf“.

#### **4. Checkliste zur Inbetriebnahme eines Fernwartungs-CR220N für die transparente RS232/RS485-Kopplung**

##### Ausgangszustand:

- ISK-Automation liefert einen für Fernwartungszwecke vorkonfigurierten CR220N. Das OpenVPN-Zertifikat und die Firewalldatei sind bereits installiert.



#### 1. Vorbereitungen

- Die seriellen Endgeräte werden mit dem RS485-Interface des jeweiligen CR220N verbunden.
- Das mit "WAN" bezeichnete Interface wird mit dem Netzwerk des übergeordneten Routers verbunden.
- Die Alias-Adresse kann genutzt werden, um den CR220N während der Konfiguration ohne Umschaltung des PC-Subnets ansprechen zu können.
- Web-Konfiguration des "CR220N" aufrufen: <http://192.168.0.126:7777>
- login: admin

#### 2. LAN1-Adresse konfigurieren und DHCP-Client einrichten (siehe Bild1)

Network → LAN → LAN1:

- IP address: 192.168.1.1 (Beispiel)
- Subnet mask: 255.255.255.0 (Subnetzmaske muss auf 255.255.255.0 konfiguriert werden).

Network → LAN → LAN2:

- DHCP-client: aktiv
- Apply-Schalter betätigen.
- Statusseite des CR220N aufrufen (siehe Bild2)  
Testen Sie, ob das LAN2-Interface eine IP-Adresse vom DHCP-Server bezogen hat. Im Falle keine Adresse per DHCP zugewiesen wurde, Router neu booten (power down/power up).  
LAN1- und LAN2-Subnetz auf Überschneidungen testen (siehe Bild2).

#### 3. OpenVPN-Client aktivieren. (siehe Bild3)

VPN → OpenVPN:

- Enable/Disable OpenVPN: aktivieren
- "Apply" betätigen.
- die Verbindung zum CRASER baut sich nach einigen Sekunden auf. Während des Verbindungsaufbaus blinkt die CON-LED. Nachdem die Verbindung aufgebaut ist, leuchtet die CON-LED statisch.

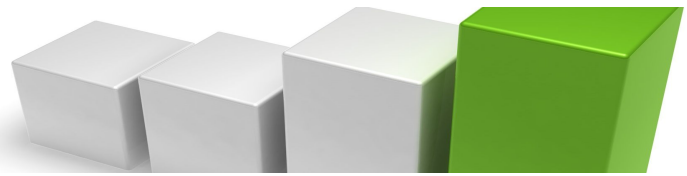
#### 4. COM2-Interface konfigurieren. (siehe Bild4)

Network → COM → COM2 Properties

- Application: UDP Socket
- Destination address: 10.2.132.126 (siehe Abschnitt 2 dieser Dokumentation)
- Portnummer: 2002 (Beispiel)
- Bits per second: 9600 (Beispiel)
- Data bits: 8 (Beispiel)
- Parity: None (Beispiel)
- Stop bits: 1 (Beispiel)
- Flow control: None
- Forwarding Timeout: 200ms
- Hardware line driver: RS485
- Apply-Schalter betätigen.

#### 5. Test der übertragenen Daten. (siehe Bild5)

- Schalter „COM2-LOG“ betätigen und übertragene Daten überprüfen.
- Anzeigefenster schließen.



## 5. Darstellung der zugehörigen Konfigurationsseiten zum Kapitel 4 dieser Doku

Bild 1 LAN1-Adresse und DHCP-client für LAN2 konfigurieren:

CR-220N V.10

Status

Network

- WAN
- LAN
- COM
- Logging

VPN

Services

Proxies

System

Logout

**LAN configuration**

**LAN1 configuration**

Enable/Disable interface LAN1 :	<input checked="" type="checkbox"/>
DHCP-client :	<input type="radio"/>
Use the following IP address :	<input checked="" type="radio"/>
IP address :	192 . 168 . 1 . 1
Subnet mask :	255 . 255 . 255 . 0
Enable/Disable alias IP address :	<input checked="" type="checkbox"/>
Alias IP address :	192 . 168 . 0 . 126
Alias subnet mask :	255 . 255 . 255 . 0

**LAN2 configuration**

Enable/Disable interface LAN2 :	<input checked="" type="checkbox"/>
Use device for DSL :	<input type="radio"/>
DHCP-client :	<input checked="" type="radio"/>
Use the following IP address :	<input type="radio"/>
IP address :	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Subnet mask :	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>

**DNS configuration**

Use a DNS server address :	<input type="checkbox"/>
----------------------------	--------------------------

**Default gateway configuration**

Use a gateway address :	<input type="checkbox"/>
-------------------------	--------------------------

© 2010 ISK-Automation

OK Apply Cancel

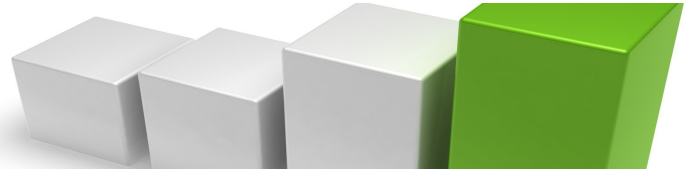


Bild 2 Status des CR220N  
(DHCP-Zuweisungen für LAN2 vom übergeordneten Router überprüfen).

<p><u>CR-220N V.10</u></p> <p>Status</p> <p>Network</p> <ul style="list-style-type: none"> <li>• WAN</li> <li>• LAN</li> <li>• COM</li> <li>• Logging</li> </ul> <p>VPN</p> <p>Services</p> <p>Proxies</p> <p>System</p> <p>Logout</p> <p>© 2010 ISK-Automation</p>	<p><b>Status</b></p>															
<p><b>System status</b></p>																
<table border="1"> <tr> <td>System name :</td> <td>CR220N</td> <td>System host name</td> </tr> <tr> <td>System location :</td> <td>ISK-Automation GmbH</td> <td>Location information</td> </tr> <tr> <td>Contact :</td> <td>info@isk-automation.de</td> <td>Contact information</td> </tr> <tr> <td>Time and date :</td> <td>Tue, 31.05.2011 16:21:00</td> <td>Time and date of this system</td> </tr> </table>		System name :	CR220N	System host name	System location :	ISK-Automation GmbH	Location information	Contact :	info@isk-automation.de	Contact information	Time and date :	Tue, 31.05.2011 16:21:00	Time and date of this system			
System name :	CR220N	System host name														
System location :	ISK-Automation GmbH	Location information														
Contact :	info@isk-automation.de	Contact information														
Time and date :	Tue, 31.05.2011 16:21:00	Time and date of this system														
<p><b>Status LAN1</b></p>																
<table border="1"> <tr> <td>IP address :</td> <td>192.168.1.1</td> <td>LAN1 IP address</td> </tr> <tr> <td>Subnet mask :</td> <td>255.255.255.0</td> <td>LAN1 subnet mask</td> </tr> <tr> <td>MAC address :</td> <td>02:80:AD:21:32:56</td> <td>Physical media address</td> </tr> <tr> <td>Alias IP address :</td> <td>192.168.0.126</td> <td>LAN1 alias IP address</td> </tr> <tr> <td>Alias subnet mask :</td> <td>255.255.255.0</td> <td>LAN1 alias subnet mask</td> </tr> </table>		IP address :	192.168.1.1	LAN1 IP address	Subnet mask :	255.255.255.0	LAN1 subnet mask	MAC address :	02:80:AD:21:32:56	Physical media address	Alias IP address :	192.168.0.126	LAN1 alias IP address	Alias subnet mask :	255.255.255.0	LAN1 alias subnet mask
IP address :	192.168.1.1	LAN1 IP address														
Subnet mask :	255.255.255.0	LAN1 subnet mask														
MAC address :	02:80:AD:21:32:56	Physical media address														
Alias IP address :	192.168.0.126	LAN1 alias IP address														
Alias subnet mask :	255.255.255.0	LAN1 alias subnet mask														
<p><b>Status LAN2</b></p>																
<table border="1"> <tr> <td>IP address :</td> <td>192.168.0.22</td> <td>LAN2 IP address</td> </tr> <tr> <td>Subnet mask :</td> <td>255.255.255.0</td> <td>LAN2 subnet mask</td> </tr> <tr> <td>MAC address :</td> <td>02:80:AD:21:32:57</td> <td>Physical media address</td> </tr> </table>		IP address :	192.168.0.22	LAN2 IP address	Subnet mask :	255.255.255.0	LAN2 subnet mask	MAC address :	02:80:AD:21:32:57	Physical media address						
IP address :	192.168.0.22	LAN2 IP address														
Subnet mask :	255.255.255.0	LAN2 subnet mask														
MAC address :	02:80:AD:21:32:57	Physical media address														
<p><b>Status DNS</b></p>																
<table border="1"> <tr> <td>Primary DNS server :</td> <td>192.168.0.1</td> <td>1st DNS server address</td> </tr> </table>		Primary DNS server :	192.168.0.1	1st DNS server address												
Primary DNS server :	192.168.0.1	1st DNS server address														
<p><b>Status route</b></p>																
<table border="1"> <tr> <td>Default gateway :</td> <td>192.168.0.1</td> <td>Default gateway for device</td> </tr> </table>		Default gateway :	192.168.0.1	Default gateway for device												
Default gateway :	192.168.0.1	Default gateway for device														

Achtung: Das per DHCP zugewiesene LAN2-Subnetz darf sich nicht mit dem konfigurierten LAN1-Subnetz überschneiden. Ändern Sie in einem solchen Fall das LAN1-Subnetz.

Beispiel: LAN1 192.168.1.1/255.255.255.0 ← vom Anwender konfiguriert.  
 LAN2 192.168.1.20/255.255.255.0 ← per DHCP zugewiesen.

→ LAN1 ändern auf z.B.: 192.168.2.1/255.255.255.0

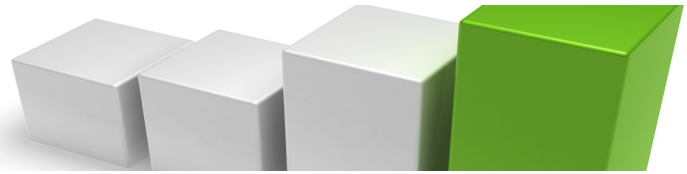


Bild 3 OpenVPN aktivieren:

CR-220N V.10

**OpenVPN configuration**

<b>OpenVPN configuration</b>	
Enable/Disable OpenVPN :	<input checked="" type="checkbox"/>
Work as :	<input type="radio"/> Server <input checked="" type="radio"/> Client
Status :	Running

**OpenVPN client configuration**

Server address :	<input type="text" value="83.169.44.109"/>
Protocol :	<input checked="" type="radio"/> UDP <input type="radio"/> TCP
Port :	<input type="text" value="1194"/>
VPN compression :	Enable ▾

**OpenVPN certificates and keys**

Authentication :	p12-Certificate ▾		
P12-certificate :	ISK-P2-NET5(10.2.132.0).p12	Info	
Import p12-certificate :	<input type="text"/>	Durchsuchen...	Import

OK **Apply** Cancel

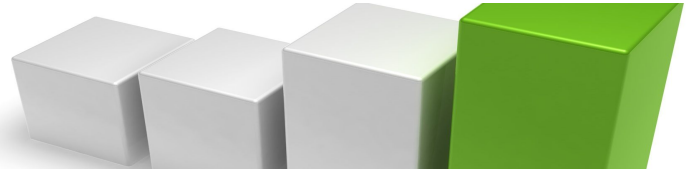


Bild 4 COM2-Interface konfigurieren:

CR-220N V.10

Status  
Network  
• WAN  
• LAN  
• **COM**  
• Logging  
VPN  
Services  
Proxies  
System  
Logout

### Serial port configuration

COM1 Properties	
Application :	None

COM2 Properties	
Application :	UDP-Socket
Destination address :	10.2.133.1
Portnumber :	2002
Bits per second :	9600
Data bits :	8
Parity :	None
Stop bits :	1
Flow control :	None
Forwarding Timeout:	20ms
Hardware line driver :	<input type="radio"/> RS232 <input checked="" type="radio"/> RS485
Show COM2-Logfile:	COM2-LOG

© 2010 ISK-Automation

OK Apply Cancel

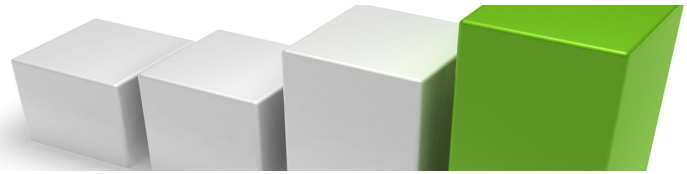


Bild 5: Test der übertragenen Daten:

```

330787.95: COM1-BAUD=9600bps
330787.95: COM1-DATA=8
330787.95: COM1-PARI=n
330787.95: COM1-STOP=1
330787.95: COM1-FLOWCONTROL=noflow
330787.95: COM1-CHARACTER-DELAY=200ms
330788.15: COM1-PEER-IP=10.0.64.127
330788.15: COM1-UDP-Port=2001
330820.51: ->RXD: 31
330820.88: ->RXD: 32
330821.33: ->RXD: 33
330821.95: ->RXD: 0D
330822.36: ->RXD: 0D
330823.19: ->RXD: 34
330823.39: ->RXD: 35
330823.65: ->RXD: 36
330823.90: ->RXD: 37
330824.16: ->RXD: 38
330824.43: ->RXD: 39
330824.84: ->RXD: 0D
330913.56: ->RXD: 01 02 03 04 05 06 07 08 09 0A
330930.20: ->RXD: 01 02 03 04 05 06 07 08 09 0A
330930.69: ->RXD: 01 02 03 04 05 06 07 08 09 0A
330931.04: ->RXD: 01 02 03 04 05 06 07 08 09 0A
330931.28: ->RXD: 01 02 03 04 05 06 07 08 09 0A
332028.69: ->RXD: 01 02 03 04 05 06 07 08 09 0A ... 20 (32Bytes)
332029.37: ->RXD: 01 02 03 04 05 06 07 08 09 0A ... 20 (32Bytes)

```

Zeitstempel in x.xxs (Uptime)

Datenrichtung  
RXD, TXD

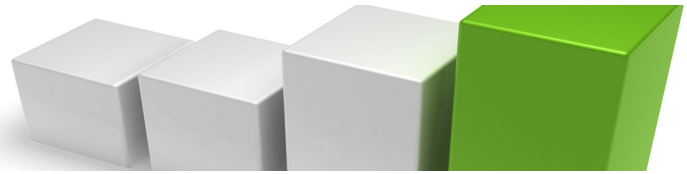
Nutzdatenprotokoll

Längenzähler

**Zeitstempel:** Der Zeitstempel zeigt den Zeitpunkt des Empfangs der Nutzdaten im CR220N. Die Granularität des verwendeten Timers beträgt 10ms.

**Datenrichtung:** „→ RXD“ bedeutet, die angezeigten Daten wurden von der RS485-Schnittstelle seriell empfangen und als UDP-Frame verpackt zur VPN-Gegenstelle gesendet.  
„← TXD“ bedeutet, die angezeigten Daten wurden als UDP-Frame von der VPN-Gegenstelle empfangen und über die RS485-Schnittstelle seriell gesendet.

**Nutzdatenprotokoll:** Darstellung der über den CR220N vermittelten Daten. Sollte ein Datenpaket > 10 Bytes sein, werden nur die ersten 10 Bytes und nach 3 Punkten das letzte Byte des Pakets dargestellt. Am Ende der Zeile erscheint dann in Klammern



ein Längenzähler, der die Byteanzahl des Gesamtpaketes protokolliert.

Achtung: Vergessen Sie nicht, das Anzeigefenster zu schließen. Nur dann kann es nach fortschreitender Datenübertragung erneut mit dem Schalter „COM2-LOG“ geöffnet werden, um die jeweils aktuellen Daten zu sehen.