

## CR230U-Fernwartung über UMTS

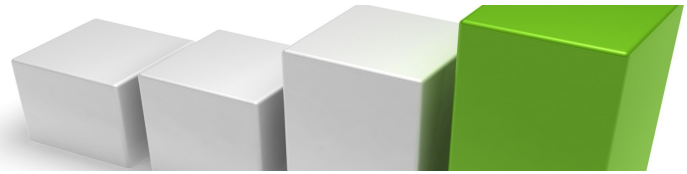
### 1. Allgemeines

In der Internet-Fernwartung wird es immer wichtiger, nicht nur einzelne IP-Adressen anzusprechen, sondern ein ganzes IP-Subnetz fernzuwarten. Der VPN-Router CR230U stellt ein solches Fernwartungs-Subnetz auf seinem LAN1-Interface zur Verfügung. Alle Netzwerkteilnehmer, die mit diesem Interface verbunden sind, nehmen an der Fernwartung teil. Es handelt sich um ein Klasse-C-Subnetz, das heißt, es können bis zu 252 Netzwerkteilnehmer ferngewartet werden. Das Fernwartungs-Subnetz ist frei konfigurierbar, indem die LAN1-IP-Adresse durch den Anwender konfiguriert wird.

Es können alle IP-Protokolle verwendet werden, also nicht nur TCP, sondern beispielsweise auch UDP und ICMP. Das ist für die Inbetriebnahme hilfreich, da somit alle fernzuwartenden Netzwerkteilnehmer auch per „ping-Befehl“ erreicht werden können.

Als Fernwartungs-Client dient ein PC, der ebenfalls mit dem Internet verbunden wird. Die Fernwartungs-Verbindung zwischen PC und CR230U ist durch einen OpenVPN-Tunnel gesichert. Damit ist die Übertragung der Anwenderdaten nach dem neuesten Stand der Technik gegen Fremdzugriffe geschützt. Als VPN-Vermittler arbeitet, für den Anwender unsichtbar, ein schneller OpenVPN-Server im Internet, der „ISK-CRASER“. Für eine komfortable Subnetz-Fernwartung nach heutigem technischen Stand ist die Vermittlung über den „ISK-CRASER“ unumgänglich. Dafür sprechen 3 gewichtige Gründe:

1. CRASER ist 24h Online und hat die Leistungsfähigkeit moderner Serversysteme. Dadurch wird eine gleichzeitige und sichere Kommunikation mit sehr vielen Clients möglich.
2. CRASER ist ein Open-VPN-Server mit einer festen IP-Adresse: Sowohl der Fernwartungs-PC als auch der Fernwartungsrouter melden sich als VPN-Client an. Damit ist weder beim Fernwartungs-PC noch beim Fernwartungsrouter eine public IP-Adresse bzw. eine feste IP-Adresse erforderlich.
3. CRASER kann Open-VPN-Verbindungen routen: Das bedeutet, der Fernwartungs-PC kann mit einer Open-VPN-Verbindung auch Fernwartungs-Subnetze mehrerer CR230U/CR220N gleichzeitig erreichen und die Fernwartungs-Subnetze mehrerer CR230U/CR220N können auch untereinander kommunizieren. Bei Bedarf sind mehrere Fernwartungs-PCs mit unterschiedlichen Zertifikaten möglich. Maximal 64 Fernwartungs-Subnetze lassen sich nach diesem Prinzip gleichzeitig durch den CRASER vermitteln. Die Zugriffsrechte aller Clients können variiert werden.

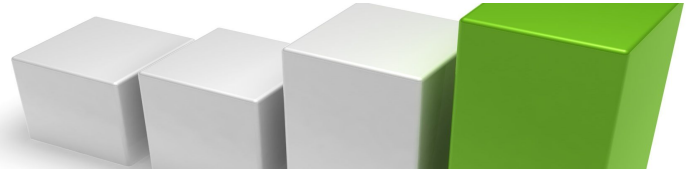


## **2. Aufgabenstellung**

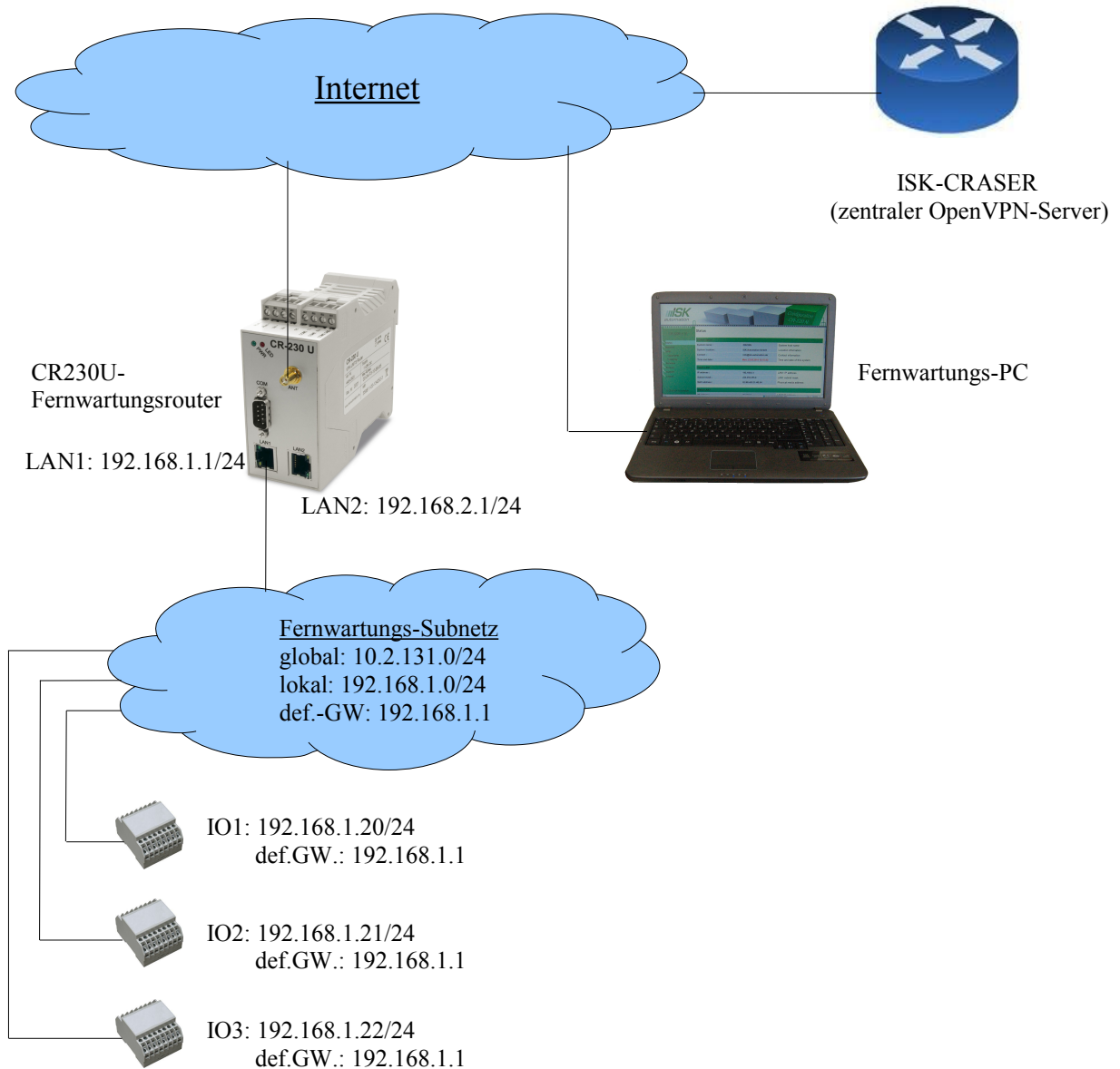
Der VPN-Router CR230U soll über sein eingebautes UMTS-Modem eine Verbindung ins Internet herstellen. Daraufhin soll eine Verbindung zwischen einem Fernwartungs-PC und dem Fernwartungs-Subnet des CR230U über das Internet in Betrieb genommen werden. Diese Inbetriebnahme erfolgt in 6 Schritten:

1. Kabelverbindungen vorbereiten.
2. WAN-Interface (UMTS) konfigurieren.
3. Fernwartungs-Subnetz (LAN1) auf eine zur Anwendung passende IP-Adresse konfigurieren.
4. OpenVPN auf dem CR230U aktiv schalten und Verbindung zum CRASER herstellen.
5. Fernwartungs-PC konfigurieren und eine OpenVPN-Verbindung zum CRASER aufbauen.
6. Fernwartungs-Subnetz durch ping-Kommandos von der Konsole des Fernwartungs-PCs testen.

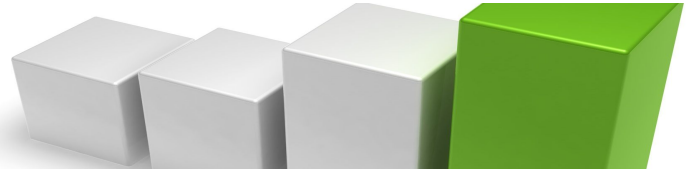
Werfen wir zunächst einen Blick auf die Netzwerkstruktur unserer Anwendung, bevor wir die 6 Schritte zur Inbetriebnahme abarbeiten:



### 3. Netzwerkstruktur der Fernwartung mit Beispieladressen



Testzugriffe:	PC → CR230U	ping 10.2.131.1	(globaler Zugriff)
	PC → IO1:	ping 10.2.131.20	(globaler Zugriff)
	PC → IO2:	ping 10.2.131.21	(globaler Zugriff)
	PC → IO3:	ping 10.2.131.22	(globaler Zugriff)
	IO1 → IO2:	ping 192.168.1.21	(lokaler Zugriff)



Tipp1: Ein globaler Zugriff ist ein Zugriff auf ein Fernwartungs-Subnetz über das Internet.  
Ein lokaler Zugriff ist ein Zugriff innerhalb eines Fernwartungs-Subnetzes.

Tipp2: Die globale IP-Adresse Ihres Fernwartungs-Subnetzes ist für jeden am CRASER arbeitenden Router einmalig und ist bereits auf Ihrem Router vorkonfiguriert (siehe Routerkonfigurationsmenü: VPN → OpenVPN → p12-certificate).

Tipp3: So finden Sie die Zieladresse für einen globalen Zugriff auf den Teilnehmer „IO1“ Ihres Fernwartungs-Subnetzes:

globale Adresse des Fernwartungs-Subnetzes:	10.2.132.0/24
gesuchte Zieladresse:	→ 10.2.132.20
lokale Adresse des Teilnehmers IO1:	192.168.1.20/24

Tipp4: Durch die Zuordnung der globalen IP-Adresse zur lokalen IP-Adresse des Fernwartungs-Subnetzes können Sie die lokale IP-Adresse frei konfigurieren, ohne Rücksicht auf später hinzukommende Fernwartungs-Subnetze nehmen zu müssen.

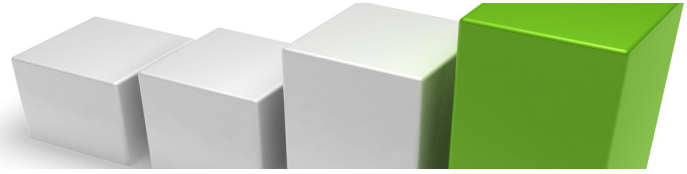
Tipp5: Das LAN2 des CR230U ist von der Fernwartung getrennt und kann für lokale Teilnehmer benutzt werden, auf die die Fernwartung nicht zugreifen darf (z.B. PCs). LAN2-Teilnehmer können mit LAN1-Teilnehmern kommunizieren.

Tipp6: LAN1- und LAN2-Teilnehmer können das Internet benutzen.  
Eine Sperrung dieser Funktion ist durch Laden einer speziellen Firewalldatei möglich.  
Bei Bedarf stellen wir Ihnen diese Datei zur Verfügung.

#### 4. Checkliste zur Inbetriebnahme eines Fernwartungs-CR230U

##### Ausgangszustand:

- ISK-Automation liefert einen für Fernwartungszwecke vorkonfigurierten CR230U.  
Das OpenVPN-Zertifikat und die Firewalldatei sind bereits installiert.
- ISK-Automation liefert die OpenVPN-Konfigurationsdateien für den Fernwartungs-PC.  
Für das Projekt2, PC1 der Firma ISK-Automation würde diese Datei „ISK-P2-PC1.zip“ heißen.



Inbetriebnahme des Fernwartungsrouters CR230U in 6 Schritten:

1. Vorbereitungen

- Das mit "LAN1" bezeichnete Interface wird mit dem Fernwartungs-Subnetz verbunden.
- Das mit "LAN2" bezeichnete Interface wird mit lokalen Teilnehmern verbunden, auf die die Fernwartung keinen Zugriff haben soll.
- Die Alias-Adresse kann genutzt werden, um den CR230U während der Netzwerkkonfiguration ohne Umschaltung des PC-Subnets ansprechen zu können.
- Web-Konfiguration des "CR230U" aufrufen: <http://192.168.0.127:7777>
- login: admin

2. WAN-Interface konfigurieren. (siehe Bild1)

Network → WAN → ISP settings:

- Provider: D2 (Beispiel)
- SIM PIN: 0815 (Beispiel)
- Confirm SIM PIN: 0815 (Beispiel)

Network → WAN → Connection settings:

- Connect type: System start, always reconnect
- Apply-Schalter betätigen.

3. lokale Fernwartungs-Subnetzadresse konfigurieren: (siehe Bild2)

Network → LAN → LAN1:

- IP address: 192.168.1.1 (Beispiel, die lokale Fernwartungsadresse können Sie selbst festlegen)
- Subnet mask: 255.255.255.0 (Die Subnetmaske muss auf 255.255.255.0 konfiguriert werden.)
- Apply-Schalter betätigen.

4. 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 USER-LED. Nachdem die Verbindung aufgebaut ist, leuchtet die USER-LED statisch.

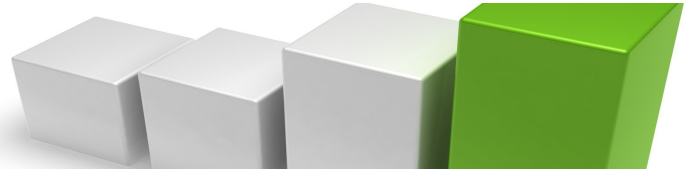
5. OpenVPN-Client auf dem Fernwartungs-PC konfigurieren und starten.

OpenVPN-Client nach unserer Anleitung „VPN\_PC\_Client\_Install.pdf“ auf dem Fernwartungs-PC installieren und mit dem zu diesem Router gelieferten PC-Zertifikatpaket konfigurieren. Danach den OpenVPN-Client auf dem Fernwartungs-PC starten.

6. Subnet des CR230U vom Fernwartungs-PC her pingen:

ping-Befehle siehe Kapitel 3 dieser Dokumentation.

Achtung: Benutzen Sie bei den ping-Befehlen die globale Subnetzadresse Ihres konkreten Fernwartungs-Subnetzes. Diese Adresse ist auf Ihrem Router schon vorkonfiguriert. Sie finden sie unter VPN → OpenVPN → p12 certificate.



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

Bild 1 WAN-Interface konfigurieren:

**CR-230U V.10**

**WAN configuration**

**ISP settings**

Provider : D2

SIM PIN : ●●●●

Confirm SIM PIN : ●●●●

DNS : Automatic

Gateway : Automatic

**Connection settings**

Connect type : System start, always reconnect

Manuell test : Connect Disconnect Check Modem

Connection State : Connected  
signal quality: -69 dBm

OK Apply Cancel

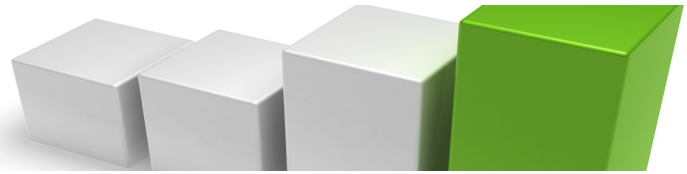


Bild 2 lokale Fernwartungs-Subnetadresse (LAN1) konfigurieren:

CR-230U 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 . 127
Alias subnet mask :	255 . 255 . 255 . 0

LAN2 configuration

Enable/Disable interface LAN2 :	<input checked="" type="checkbox"/>
DHCP-client :	<input type="radio"/>
Use the following IP address :	<input checked="" type="radio"/>
IP address :	192 . 168 . 2 . 1
Subnet mask :	255 . 255 . 255 . 0

DNS configuration

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

Default gateway configuration

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

OK Apply Cancel

Das LAN2 des CR230U ist von der Fernwartung getrennt und kann für lokale Teilnehmer benutzt werden, auf die die Fernwartung nicht zugreifen darf (z.B. PCs). LAN2-Teilnehmer können mit LAN1-Teilnehmern kommunizieren.

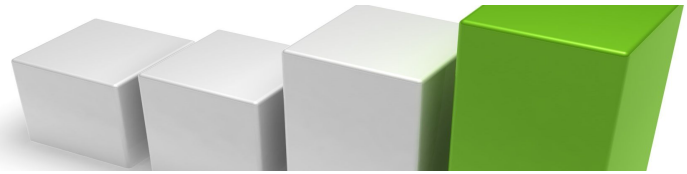


Bild 3 OpenVPN aktivieren:

CR-230U V.10

Status  
Network  
VPN  
• OpenVPN  
• Logging  
Services  
Proxies  
System  
Logout

### OpenVPN configuration

OpenVPN configuration	
Enable/Disable OpenVPN :	<input checked="" type="checkbox"/>
Work as :	<input type="radio"/> Server <input checked="" type="radio"/> Client
Status :	Not 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-NET4(10.2.131.0).p12 <input type="button" value="Info"/>
Import p12-certificate :	<input type="text"/> <input type="button" value="Durchsuchen..."/> <input type="button" value="Import"/>