

## Net-to-Subnet-Koppler

### 1. Allgemeines

Oftmals besteht die Aufgabe, getrennte Subnets an ein übergeordnetes Netz zu koppeln. Dabei muss berücksichtigt werden, dass mehrere der zu koppelnden Subnets exakt den gleichen Adressbereich, z.B. „192.168.1.0/24“ haben können. Subnets mit gleichen Adressbereichen bieten Vorteile, da sie durch immer gleiche Arbeitsschritte vorkonfiguriert und getestet werden können, ohne Rücksicht auf das spätere Gesamt-Netzwerk nehmen zu müssen. Somit können auch komplizierte Gesamtstrukturen übersichtlicher geplant und gefertigt werden.

Wie können jedoch Subnets mit gleichen Adressbereichen an ein übergeordnetes Netz gekoppelt werden ?

Dazu ordnet der koppelnde Router jedem Subnet 2 Adressbereiche zu:

1. die globale Subnetadresse, z.B. 172.1.10.0/24 und
2. die lokale Subnetadresse, z.B. 192.168.1.0/24.

Die globale Subnetadresse dient dazu, jedes Subnet vom übergeordneten Netz her eindeutig adressieren zu können. Sie wird auch benutzt, um von einem Subnet auf ein anderes Subnet zugreifen zu können.

Die lokale Subnetadresse wird benutzt, um innerhalb eines Subnets kommunizieren zu können.

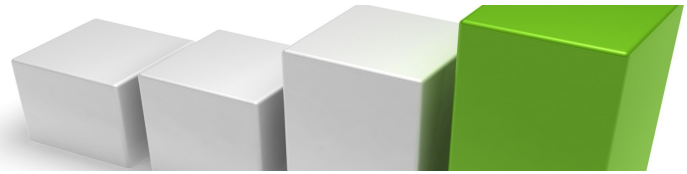
### 2. Aufgabenstellung

Mehrere CR220N sollen mit ihrem LAN2-Interface ein übergeordnetes Netz bilden. Auch PCs oder übergeordnete Router können Teilnehmer dieses Netzes sein. Das LAN1-Interface des CR220N soll jeweils ein vom übergeordneten Netz getrenntes Subnet bilden.

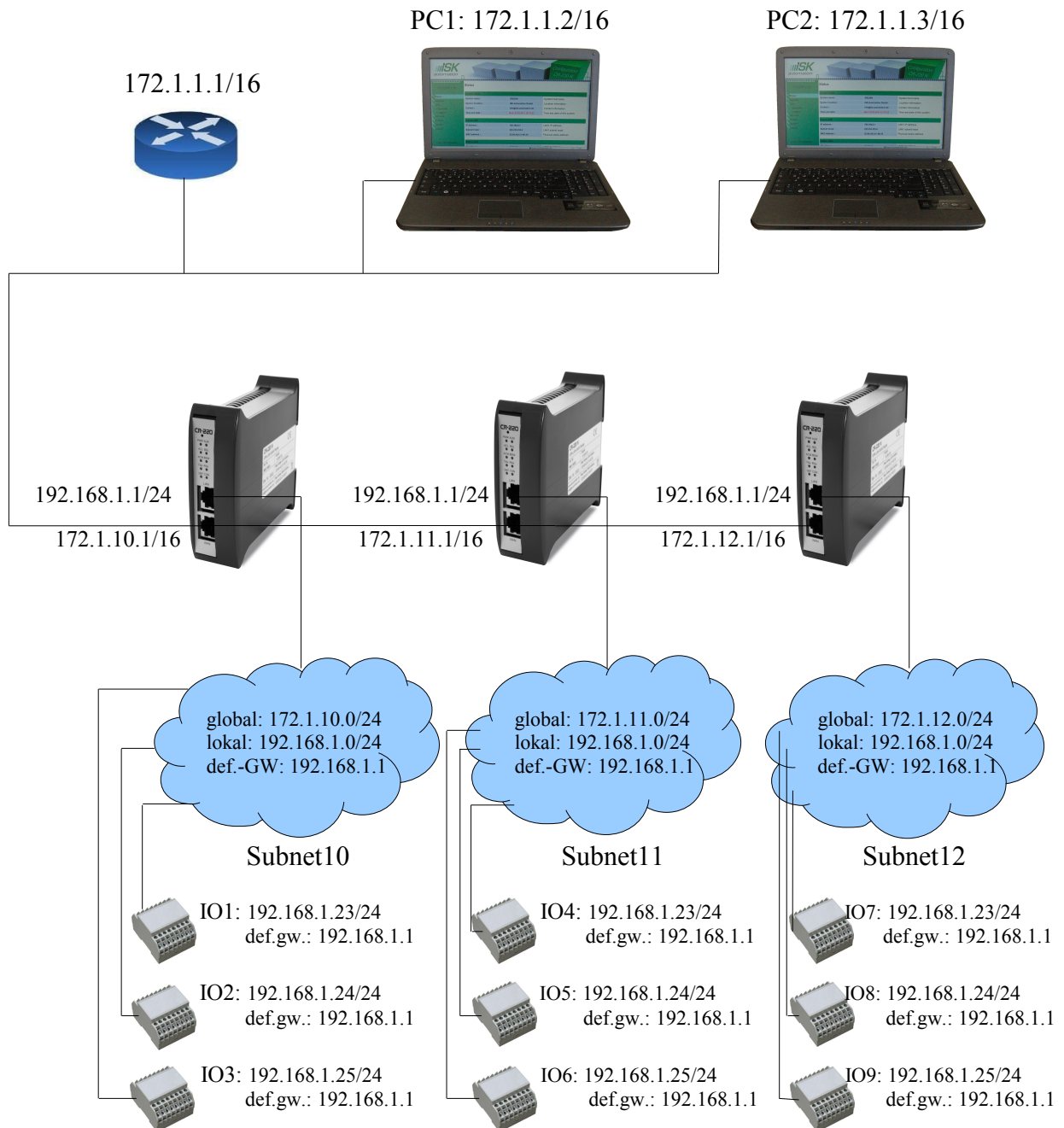
Alle Teilnehmer des übergeordneten Netzes sollen die untergeordneten Subnets adressieren können. Alle Teilnehmer der untergeordneten Subnets sollen sowohl das übergeordnete Subnet als auch alle anderen untergeordneten Subnets adressieren können. Die Lösung soll außerdem ohne Einrichtung spezieller Routen im übergeordneten Netz auskommen.

### 3. Lösungsprinzip

Zur Kopplung der untergeordneten Subnets mit dem übergeordneten Subnet stellt ISK-Automation eine spezielle Firewall bereit. Diese Firewall übersetzt den jeweiligen Adressbereich des untergeordneten Subnets in einen zum übergeordneten Netz passenden Adressbereich. Sie orientiert sich dabei an den IP-Adressen, die auf LAN1 und LAN2 konfiguriert sind. Somit sind alle Netze frei konfigurierbar, ohne die Firewall ändern zu müssen. Die Firewall garantiert außerdem, dass keine speziellen Routen zur Adressierung der untergeordneten Subnets eingerichtet werden müssen.



#### 4. Netzwerkstruktur zur Net-to-Subnet-Kopplung

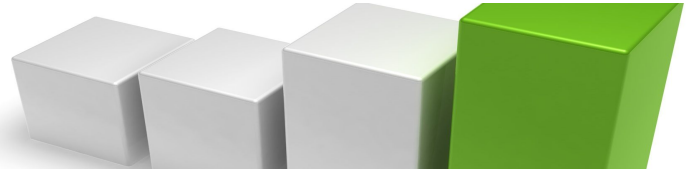


Testzugriffe:

PC1 → IO1: ping 172.1.10.23  
 PC1 → IO2: ping 172.1.10.24  
 PC1 → IO3: ping 172.1.10.25  
 IO1 → IO6: ping 172.1.11.25  
 IO1 → IO2: ping 192.168.1.24

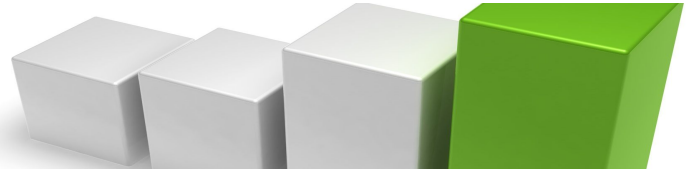
PC1 → IO4: ping 172.1.11.23  
 PC1 → IO5: ping 172.1.11.24  
 PC1 → IO6: ping 172.1.11.25  
 IO4 → IO3: ping 172.1.10.25  
 IO4 → IO5: ping 192.168.1.24

PC1 → IO7: ping 172.1.12.23  
 PC1 → IO8: ping 172.1.12.24  
 PC1 → IO9: ping 172.1.12.25  
 IO7 → IO6: ping 172.1.11.25  
 IO7 → IO8: ping 192.168.1.24



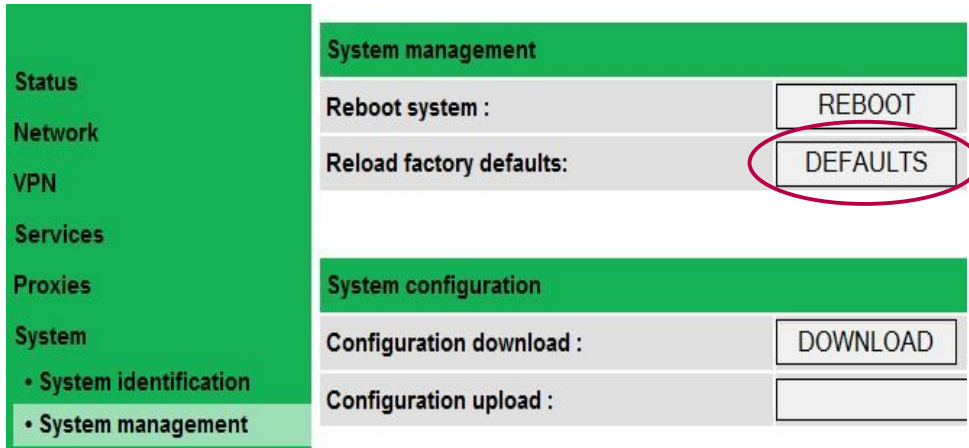
## 5. Checkliste zur Net-to-Subnet-Kopplung

1. ISK-Automation liefert eine passende USER-Firewall für diese Aufgabenstellung.  
Datei "ISK-Net-to-Subnet.sh"
2. Das mit "LAN" bezeichnete Interface (LAN1) wird mit dem zu koppelnden Subnet verbunden.  
Das mit "WAN" bezeichnete Interface (LAN2) wird mit dem übergeordneten Netz verbunden.  
Die Alias-Adresse kann genutzt werden, um den CR220N während der Netzwerkkonfiguration ohne Umschaltung des PC-Subnets ansprechen zu können.
3. Web-Konfiguration des "CR220N" aufrufen: <http://192.168.0.126:7777>  
- login: admin
4. Werkseinstellung herstellen (siehe Bild1):  
System -> System management:  
- Schalter „DEFAULT“ betätigen.  
- 1 min warten.  
- login: admin
5. CR220N LAN-Interface konfigurieren: (siehe Bild2)  
Network → LAN → LAN1:  
- IP address: 192.168.1.1 (Beispiel)  
- Subnet mask: 255.255.255.0  
Network → LAN → LAN2  
- Use the following IP address: aktiv  
- IP address: 172.1.10.1 (Beispiel)  
- Subnet mask: 255.255.0.0  
- Apply-Schalter betätigen.
6. Firewall konfigurieren: (siehe Bild3)  
Services -> Firewall and NAT:  
- Enable/Disable firewall: aktiv  
- User configured script below: aktiv  
- Button "Durchsuchen" anklicken und die Datei "ISK-Net-to-Subnet.sh" im Verzeichnisbaum des PCs suchen und öffnen.  
- Button "Apply" betätigen und warten, bis die Firewall aktiviert ist.  
Danach kann bei Bedarf durch Betätigen des Buttons "Script rules" die geladene Firewalldatei angezeigt werden.
7. Subnet des CR220N von PC1 her anpingen:  
Details siehe Kapitel 4
8. fertig.



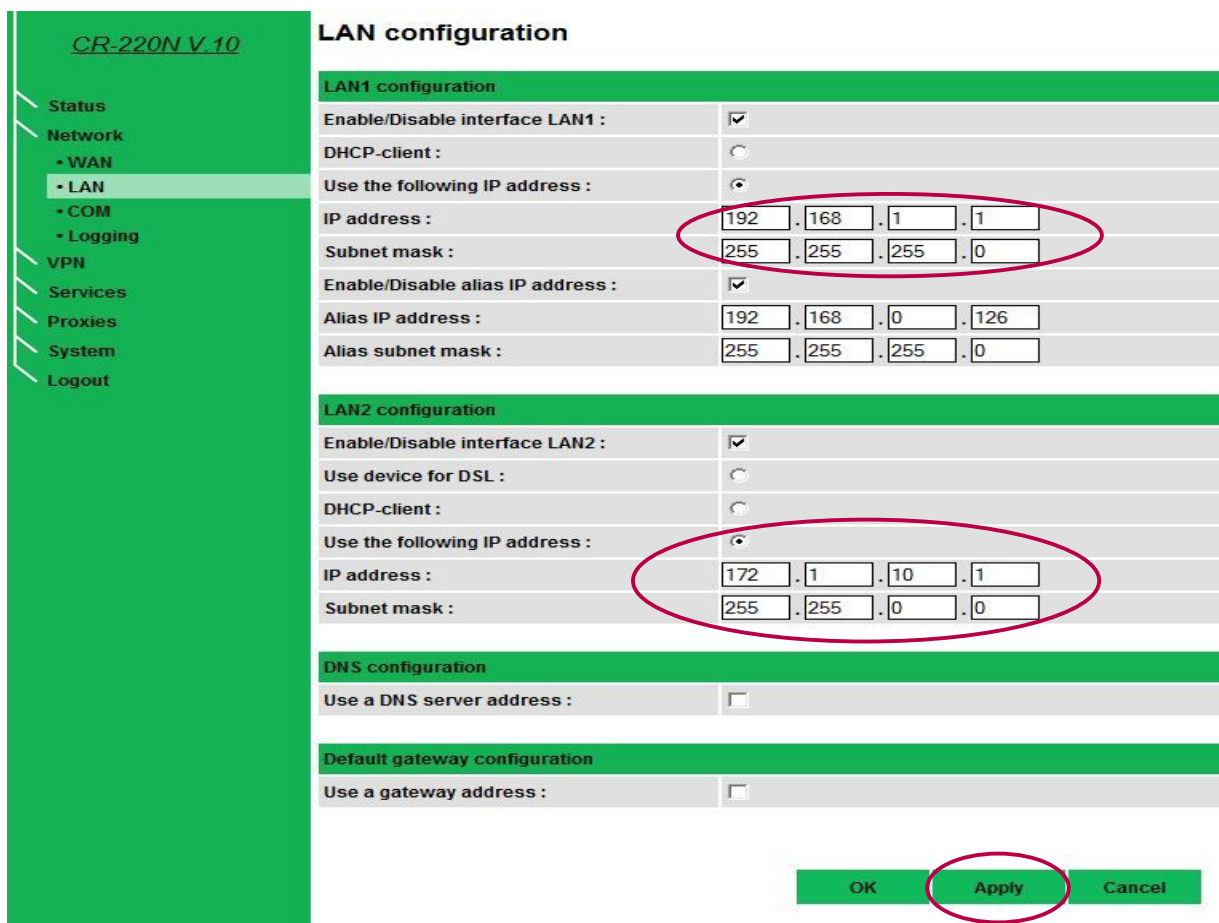
## 6. Darstellung der zugehörigen Konfigurationsseiten zu Kapitel 5

Bild 1 Werkseinstellung herstellen:



<ul style="list-style-type: none"> <li>Status</li> <li>Network</li> <li>VPN</li> <li>Services</li> <li>Proxies</li> <li>System <ul style="list-style-type: none"> <li>• System identification</li> <li>• System management</li> </ul> </li> </ul>	<b>System management</b>	
	Reboot system :	REBOOT
	Reload factory defaults:	DEFAULTS
	<b>System configuration</b>	
	Configuration download :	DOWNLOAD
	Configuration upload :	

Bild 2 LAN1, LAN2 konfigurieren:



CR-220N V.10

<ul style="list-style-type: none"> <li>Status</li> <li>Network <ul style="list-style-type: none"> <li>• WAN</li> <li>• LAN</li> <li>• COM</li> <li>• Logging</li> </ul> </li> <li>VPN</li> <li>Services</li> <li>Proxies</li> <li>System</li> <li>Logout</li> </ul>	<b>LAN configuration</b>	
	<b>LAN1 configuration</b>	
	Enable/Disable interface LAN1 :	<input checked="" type="checkbox"/>
	DHCP-client :	<input type="checkbox"/>
	Use the following IP address :	<input 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
	<b>LAN2 configuration</b>	
	Enable/Disable interface LAN2 :	<input checked="" type="checkbox"/>
	Use device for DSL :	<input type="checkbox"/>
	DHCP-client :	<input type="checkbox"/>
	Use the following IP address :	<input type="radio"/>
IP address :	172 . 1 . 10 . 1	
Subnet mask :	255 . 255 . 0 . 0	
<b>DNS configuration</b>		
Use a DNS server address :	<input type="checkbox"/>	
<b>Default gateway configuration</b>		
Use a gateway address :	<input type="checkbox"/>	
<input type="button" value="OK"/> <input checked="" type="button" value="Apply"/> <input type="button" value="Cancel"/>		

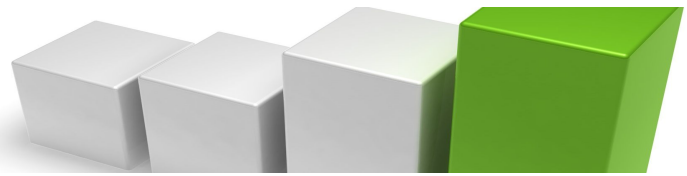


Bild 3 Firewall konfigurieren, Datei "ISK-Net-to-Subnet.sh" auswählen:

**CR-220N V.06**

**Firewall and NAT configuration**

**Firewall configuration**

Enable/Disable firewall :

**Firewall and NAT rules preconfigured sets**

All incoming ports closed, VPN allowed :

Selective ports allowed :

User configured script below :

**Firewall and NAT rules script**

Show current settings :

Upload new rules :

Firewall is on.