

## **APPLICATION NOTES**

### **TCP Erweiterungen PPP, SNTP, DNS, DHCP, SNMP**

Version: 3.0  
Datum: 16.7.2010

Erstellt von:

Namen	Company
S. Bättig	SCB

Änderungen:

Version	Wer	Beschreibung	Datum
V1.0	S. Bättig	AN TCP Erweiterungen PPP und SNTP, DNS, DHCP	8. Juli 2008
V1.1	S. Bättig	Anpassungen, Korrekturen bei PG5 Beispielen	14. Juli 2008
V1.2	S. Bättig	Korrektur config.txt in 2.3	17. Juli 2008
V1.3	S. Bättig	Hinzufügen des Verweises auf die Datei ipservices.inc	31. Juli 2008
V1.3.1	S. Bättig	Korrekturen	15. Jan. 2009
V1.3.2	S. Bättig	Korrekturen	20. Feb. 2009
V2.0	S. Bättig	2 neue Kapitel, Korrekturen	22. Mai 2009
V3.0	S. Bättig	Komplett überarbeitet (Device configurator)	6. Juli 2010

## Inhaltsverzeichnis

<b>1. EINLEITUNG</b>	<b>5</b>
<b>2. ANWENDUNGEN MIT PPP-FUNKTION</b>	<b>6</b>
<b>2.1. Anwendungsbeispiel PPP über serielle Leitung</b>	<b>6</b>
2.1.1. Beschreibung	6
2.1.2. Benötigtes Material	6
2.1.3. Anwendungsmöglichkeiten	7
2.1.4. Konfiguration und Inbetriebnahme	7
2.1.5. Bemerkungen	13
<b>2.2. Verbindungen mit Analog- oder GSM-Modems (direkt über Tel.-Netz, ohne Internet)</b>	<b>14</b>
2.2.1. Beschreibung	14
2.2.2. Benötigtes Material	14
2.2.3. Anwendungsmöglichkeiten	15
2.2.4. Konfiguration und Inbetriebnahme	15
<b>2.3. Senden von E-Mails mit GSM-Modem (im GPRS Modus)</b>	<b>21</b>
2.3.1. Beschreibung	21
2.3.2. Benötigtes Material	21
2.3.3. Anwendungsmöglichkeiten	22
2.3.4. Konfiguration und Inbetriebnahme	23
2.3.5. Bemerkungen	28
<b>2.4. Fernzugriff via Internet</b>	<b>29</b>
2.4.1. Beschreibung	29
2.4.2. Benötigtes Material	29
2.4.3. Anwendungsmöglichkeiten	30
2.4.4. Konfiguration und Inbetriebnahme	30
2.4.5. Bemerkungen	31
<b>2.5. SBUS Master – Slave Kommunikation (Ether-SBUS over PPP)</b>	<b>32</b>
2.5.1. Beschreibung	32
2.5.2. Benötigtes Material	33
2.5.3. Anwendungsmöglichkeiten	33
2.5.4. Konfiguration und Inbetriebnahme	33
2.5.5. Bemerkungen	34
2.5.6. Allgemeine Bemerkungen zu GPRS-Verbindungen	35
<b>3. ANWENDUNGEN DER SNTP-FUNKTION</b>	<b>36</b>
<b>3.1. Anwendungsbeispiel SNTP</b>	<b>36</b>
3.1.1. Beschreibung	36
3.1.2. Benötigtes Material	36
3.1.3. Anwendungsmöglichkeiten	37
3.1.4. Konfiguration und Inbetriebnahme	37
3.1.5. Bemerkungen	38
<b>4. ANWENDUNGEN MIT DNS / (DHCP)-FUNKTION</b>	<b>39</b>
<b>4.1. Anwendungsbeispiel DNS-Funktion</b>	<b>39</b>
4.1.1. Beschreibung	39
4.1.2. Benötigtes Material	39

4.1.3.	Anwendungsmöglichkeiten	39
4.1.4.	Konfiguration und Inbetriebnahme	40
4.1.5.	Bemerkungen	41
<b>5.</b>	<b>ANWENDUNGEN MIT DHCP UND DNS-FUNKTION IM LOKALEN NETZWERK</b>	<b>42</b>
<b>5.1.</b>	<b>Anwendungsbeispiel DHCP und DNS-Funktion im LAN</b>	<b>42</b>
5.1.1.	Beschreibung	42
5.1.2.	Anwendungsmöglichkeiten	42
5.1.3.	Benötigtes Material	43
5.1.4.	Konfiguration und Inbetriebnahme	43
5.1.5.	Bemerkungen	47
<b>6.</b>	<b>ANWENDUNGEN MIT SNMP-FUNKTION</b>	<b>48</b>
<b>6.1.</b>	<b>Anwendungsbeispiel SNMP</b>	<b>48</b>
6.1.1.	Beschreibung	48
6.1.2.	Anwendungsmöglichkeiten	48
6.1.3.	Benötigtes Material	49
6.1.4.	Konfiguration und Inbetriebnahme	49
6.1.5.	Bemerkungen	52

# 1. Einleitung

## **! Wichtiger Hinweis:**

Für alle Beispiele in diesem Dokument muss eine Firmware Version 1.14.21 (oder höher) auf die Steuerung geladen werden.

Um die Firmware 1.14.21 zu laden, ist eine Hardware mit 4MB Flash erforderlich.

- PCD3.M32x0, PCD3.M33x0, PCD3.M5xx0, PCD3.M6xx0 HW Version D oder neuer
- PCD3.M30x0, PCD3.M31x0 HW Version E Modifikation: 48 oder neuer
- PCD3.M2x30V6 oder PCD3.M2x30A4Tx: Alle HW Versionen unterstützt
- Die Firmware 1.14.21 kann nicht auf ältere Hardwareversionen geladen werden

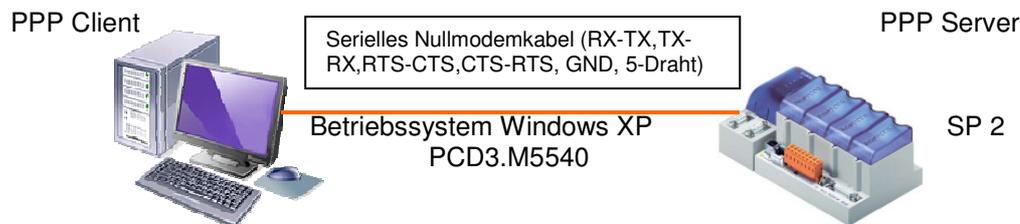
## 2. Anwendungen mit PPP-Funktion

### 2.1. Anwendungsbeispiel PPP über serielle Leitung

#### 2.1.1. Beschreibung

In diesem Beispiel wird eine Möglichkeit zum Testen der neuen PPP-Funktion gezeigt. Dazu braucht man einen Laptop, eine PCD3 und ein Nullmodemkabel. Obwohl es nicht sehr breite Anwendungsmöglichkeiten für diese Konfiguration gibt, eignet sich das Beispiel gut um die Funktionsweise von PPP zu testen und zu verstehen.

Schema:



#### 2.1.2. Benötigtes Material

- 1 Laptop / PC mit PG5 Utilities  
Für die Konfiguration und die Programmierung ist die Software PG5 2.150 erforderlich.
- Für diese Anwendung wird 1 PCD benötigt  
Es können folgende Typen verwendet werden: PCD3.M3xx0, PCD3.M5xx0 oder PCD2.M5xx0, PCD3.M6xx=, PCD3.M2x30V6 oder PCD3.M2x30A4Tx
- Beim PCD3.M3xx0: benötigt man zusätzlich ein PCD3.F121 Modul (Serielle Schnittstelle). Beim PCD3.M2x30V6 und PCD3.M2x30A4Tx braucht es lediglich ein PCD7.F121 Modul
- Serielles Nullmodemkabel + Genderchanger 9-Polig (m/m) oder ein PGU-Kabel PCD8.K111  
Für die Bei PCD3.M2x30V6 oder PCD3.M2x30A4Tx benötigt man ein spezielles Adapterkabel für die die serielle Schnittstelle.

Für dieses Beispiel wurden folgende Geräte verwendet:

- PCD3.M5540
- USB-Serial Konverter (Digitus)
- Laptop HP Compaq 6715b
- Serielles Nullmodemkabel + Gender-Changer

### 2.1.3. Anwendungsmöglichkeiten

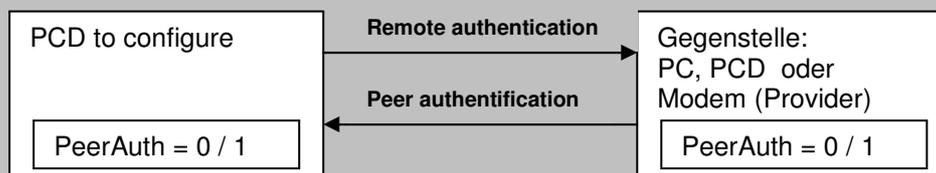
Diese Konfigurationsmöglichkeit kann in der Praxis wie folgt eingesetzt werden:

- Wenn kein Netzwerk vorhanden ist und man nur über eine serielle Leitung als Zugriffsmöglichkeit verfügt.
- Wenn man eine PCD ohne Ethernetanschluss besitzt z.B. PCD3.M3020, kann man via FTP auf das Filesystem im Flashspeicher zugreifen. Es ist möglich eine HTTP-Verbindung aufzubauen ohne die Software Webconnect zu verwenden.

### 2.1.4. Konfiguration und Inbetriebnahme

Grundlage PPP-Login

Da diese Problematik bei jeder Anwendung vorkommt, wird sie bereits hier gezeigt.



Es gibt die Möglichkeit ohne Login zu arbeiten. Bei einer Verbindung über das serielle Kabel, wenn die Verbindung nicht übers WAN geht, ist die Verwendung der Authentifizierung normalerweise nicht nötig.

Wenn das Ziel ist, mit der PCD eine GPRS Verbindung herzustellen, kann es vorkommen, dass der Provider login und password verlangt. D.h. es ist eine so genannte remote authentication erforderlich. Dabei werden von der PCD die Parameter gesendet, die unter "RemoteAuthUsername" und "RemoteAuthPassword" konfiguriert wurden. (Wenn hier der Parameter PeerAuth = 1 gesetzt wurde, ist das normalerweise ein Konfigurationsfehler, da der Provider seinerseits die konfigurierten login-Parameter auf unserer Seite nicht kennt)

Bei einer anderen Anwendung, wie sie später im Beispiel 2.2 gezeigt wird, nimmt die PCD PPP Verbindungen als Server über ein Modem entgegen. Dabei sollte zur optimalen Sicherheit auf der Serverseite die Peer authentication verwendet werden. (PeerAuth = 1) Die PCD verlangt dann von der Gegenstelle (vom Client) die Parameter login und ein password. Standardmässig wird login:root und password:rootpasswd. Diese Parameter können im Device Configurator unter IP Transfer Protocols (FTP) konfiguriert werden. Es kann nun sein, dass der Client (oder eine andere Steuerung) seinerseits auch PeerAuth=1 gesetzt hat. Jetzt wird auch vom Server verlangt auch login und password zu übermitteln, die mit den Einstellungen des Clients übereinstimmen müssen. Es werden die Parameter gesendet, die beim PPP-Server unter "RemoteAuthUsername" und "RemoteAuthUsername" konfiguriert wurden.

Beim PPP-Verbindungsaufbau wird nicht nur gegenseitig vereinbart, wer wem login und password senden soll, sondern auch, ob es im Klartext (PAP) oder mit MD5 Verschlüsselung (CHAP oder MS-CHAP) übertragen werden soll. Bei der PCD kann hier zwar nichts konfiguriert werden, sie kann sich aber immer auf den besten Standard anpassen. D.h. wenn die Gegenstelle nur PAP kann, wird PAP gemacht, sonst CHAP,MSCHAP v1 oder MSCHAP v2.

Folgende Konfigurationsschritte sind nötig:

- A) Konfiguration der Verbindung auf dem Client-PC
- B) PPP-Konfiguration auf der PCD
- C) Aufbau der Verbindung
- D) Kontrolle der Verbindung
- E) Testen der Applikationen über diese neue Verbindung

Diese Konfigurationsschritte gleichen ein wenig der Konfiguration von Internetverbindungen über Analog- oder ISDN-Modems.

Konfiguration Seite PC-Client:

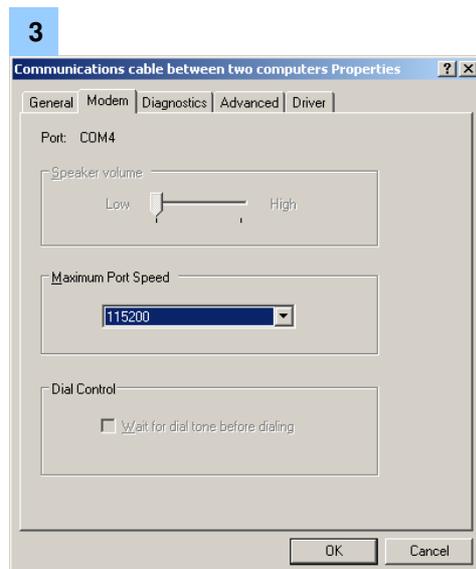
- A) Konfiguration der Verbindung auf dem Windows Client PC

Es muss als erstes der Client unter dem Windowsbetriebssystem konfiguriert werden. Es wird die Konfiguration für Windows XP gezeigt. Die Konfiguration für andere Windows-Betriebssysteme ab Windows 2000 ist ähnlich. Es kann vorkommen, dass die Menus anders angeordnet sind und die Bezeichnungen ändern. Die nachfolgend gezeigten Print-Screens zeigen wie die Konfiguration bei Windows XP für den Anschluss einer direkten seriellen Kabelverbindung erfolgen muss.



**2**

Anstelle eines Modems wird Kabel zwischen 2 Computer ausgewählt.



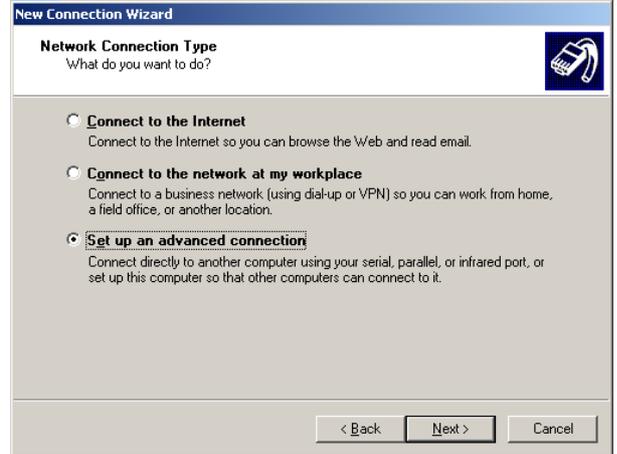
Man hat die Möglichkeit die Verbindungsgeschwindigkeit zu wählen -> 115200

Nun folgen weitere Einstellungen für die Konfiguration der Verbindung.

4

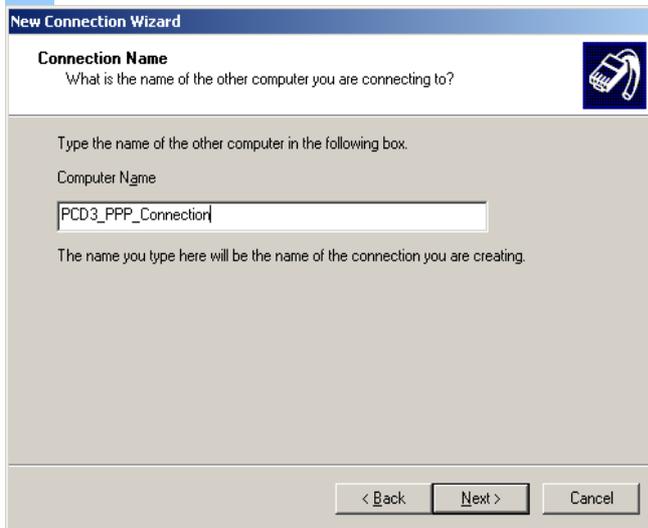


5



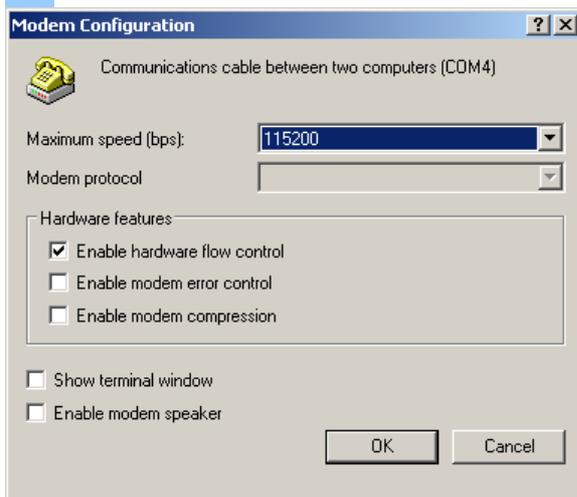
Auswahl: Erweiterte Verbindungen konfigurieren

6



Name wählen: z.B PCD3\_PPP\_Connection

8



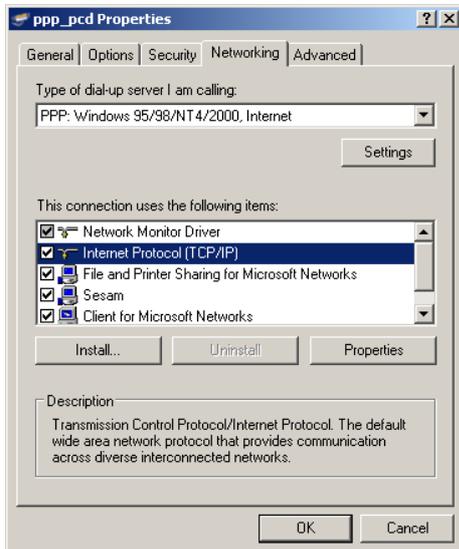
7



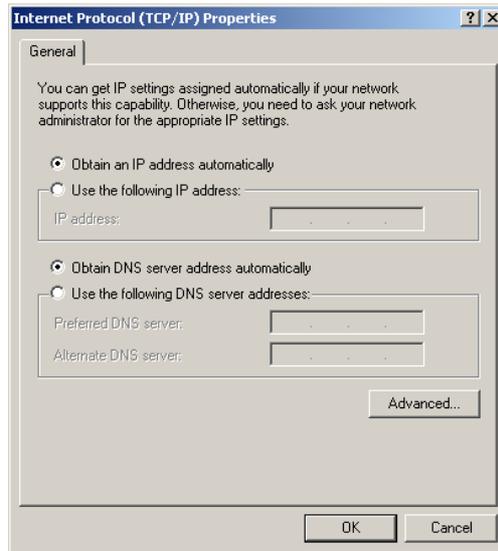
Die Geschwindigkeit, die hier gewählt wird muss identisch wie bei der Kabelverbindung sein und muss mit dem Parameter Baudrate vom Device Configurator übereinstimmen. Es ist wichtig mit Hardware Handshaking zu arbeiten.

Folgende weitere Einstellung muss vorgenommen werden, falls man parallel zu diesem Test weiterhin mit dem Webbrowser, Email-Client und anderen Internetprogrammen via LAN weiterarbeiten will.

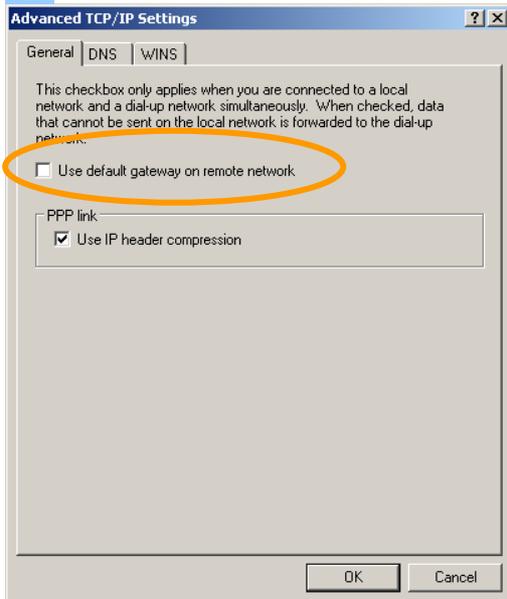
1



2



3



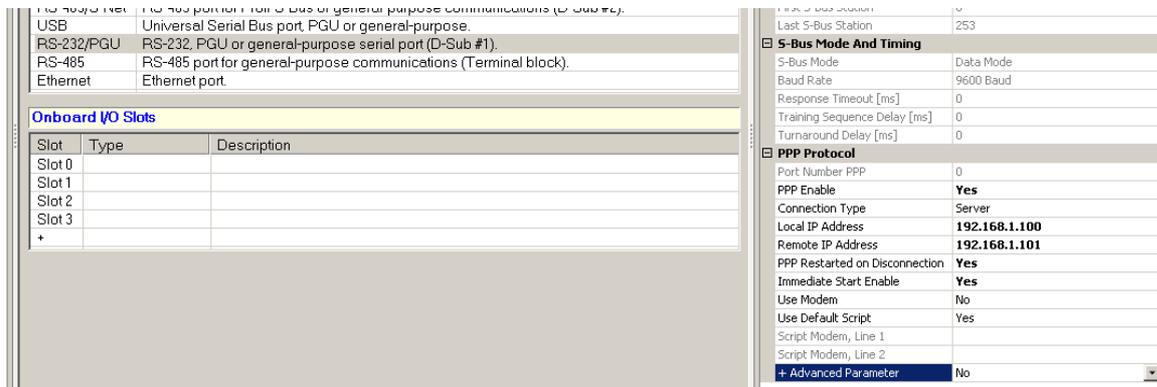
## B) PPP-Konfiguration auf der PCD

Die PCD3 muss auf die Funktion PPP-Server eingestellt werden.

Im Saia Device Configurator werden folgende Einstellungen vorgenommen.

- ➔ Auf dem Port 0 / RS 232/PGU (oder Port 1 bei CPU Typen ohne Port 0) wird folgende Konfiguration eingetragen:

Wenn man das vorhandene Beispielprojekt für die PCD3M5540 verwendet, sind alle Einstellungen im Device Configurator bereits korrekt eingestellt.



Das PPP-Protokoll im Server-Modus wird aktiviert, sobald ein Download der Konfiguration durchgeführt wurde.

Nachdem das Userprogramm heruntergeladen wurde, stehen 2 HTML-Webseiten mit Diagnosemöglichkeiten zur Verfügung:

PPPStatusH.html -> Status der PPP Verbindung

PPPConfigH.html -> Aktuelle Konfigurationseinstellungen

Die PPP-Funktionen sind auch ohne Userprogramm, d. h. auch im Halt- und Stop-Modus aktiviert. Die PPP-Funktionen werden von der Firmware verwaltet. Es gibt allerdings die Möglichkeit mit **CSF** oder **CGI-Befehlen** Einstellungen vorzunehmen. Im vorliegenden Beispiel werden diese Funktionen nicht verwendet.

Der Austausch der Texte: Client sendet „CLIENT“ und erwartet CLIENTSERVER“ ist eine Konvention die von Microsoft Windows verlangt wird. Dank diesem Script kann sich die PCD gleich verhalten wie ein Microsoftsystem.

Bei Linux / Unix Betriebssystemen funktioniert es ohne dieses Script. Tests wurden jedoch nur mit Windows durchgeführt.

➔ Für weitergehende Informationen zu den einzelnen Parametern siehe **PPP User Manual**

### C) Aufbau der Verbindung

Der Verbindungsaufbau hat Ähnlichkeit mit dem Aktivieren der Internetverbindung auf einem Laptop mit eingebautem Modem. Die Eigenschaften von Netzwerk öffnen und den neu erstellten Link: **PCD3\_PPP\_Connection** doppelklicken: Es öffnet sich folgende Dialogbox:



Bei diesem Beispiel wurde der Parameter Peer Authentication auf 0 gesetzt deshalb ist es egal, was bei User name und Password eingegeben wird

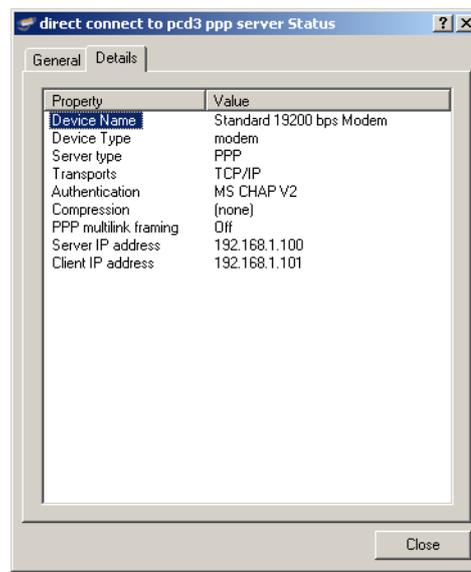
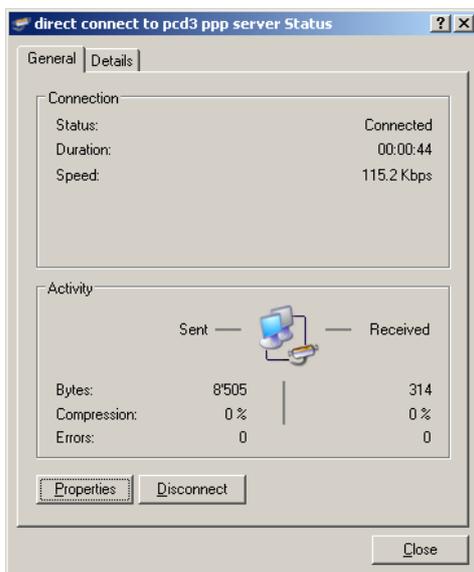
Folgende Eingaben müssen gemacht werden:

Username: beliebiger text oder leer (ROOT, falls Peer Authentication = 1)

Password: beliebiger text oder leer (ROOTPASSWD, falls Peer Authentication = 1)

Danach muss **CONNECT** durchgeführt werden.

Bei erfolgreichem Verbindungsaufbau erscheint ein zusätzliches Symbol mit 2 PC's unten in der Taskleiste. Es ist möglich den Status dieser Verbindung anzuzeigen. Man kann sehen, wie lange die Verbindung bereits besteht. Welche IP-Adresse Server (PCD) und Client (PC) bekommen haben. Die Authentifizierung, die angewendet wurde: MS CHAP V2. Es wurde diese Authentifizierung verwendet, weil es aus Sicht des Microsoft Windows XP Clients die Beste ist und der Server (PCD) alle Varianten (PAP, CHAP, MSCHAP v1 MSCHAPv2) unterstützt.



#### D) Kontrolle der Verbindung

So bald die Verbindung da ist, kann man die unterschiedlichen Anwendungen über TCP/IP testen:

-> PING 192.168.1.100, diesen Befehl aus einem CMD-Fenster ausführen (zum Testen der Verbindung)

#### E) Testen der Applikationen über diese neue Verbindung

HTTP: Direkter Zugriff auf den Webserver, download von Webeditorprojekten, ausführen von CGI-Befehlen. Die Software Webconnect kann verwendet werden, ist aber nicht erforderlich.

URL: <http://192.168.1.100> eingeben. Es erscheint die Standardwebseite der PCD

FTP: File Up- und Download. Z.B. mit Filezilla (mit Modus aktiv). Verbindung zum Server 192.168.1.100

OpenDataMode

SBUS Kommunikation (z.B. PG5 Socket Connection)

### 2.1.5. Bemerkungen

Beim Konfigurieren des Kommunikationskabels zwischen 2 Computer gab es bei Windows XP das Problem, dass nachträglich auf dem gleichen seriellen Port (Digitus USB-Seriell Konverter) installierte Modems dazu führten, dass die Konfiguration fürs Kommunikationskabel (Nullmodem) nicht mehr funktionierte. Abhilfe brachte das Entfernen des Drivers fürs Kommunikationskabel und die Neukonfiguration des Modems „Kommunikationskabel zwischen 2 Computer“. Dies musste jedes Mal erneut gemacht werden, wenn ein anderes Modem auf dem gleichen Port konfiguriert wurde.

## 2.2. Verbindungen mit Analog- oder GSM-Modems (direkt über Tel.-Netz, ohne Internet)

### 2.2.1. Beschreibung

Mit dieser Technik kann man 2 Geräte verbinden z.B 2 PCD's oder 1 PC und eine PCD, Es wird eine direkte Punkt-Punkt-Wählverbindung aufgebaut. Z.B. über eine Telefonzentrale oder das öffentliche Telefonnetz (PSTN). Beim öffentlichen Telefonnetz entstehen die Kosten je nach Dauer der Verbindung und nicht pro Datenvolumen wie bei GPRS.

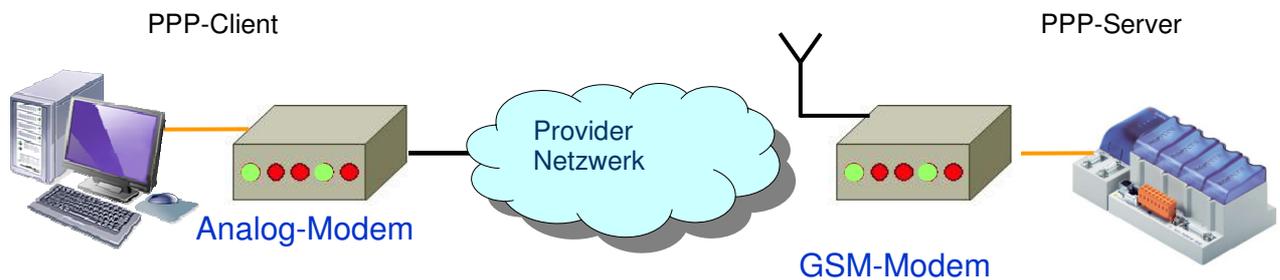
In diesem Anwendungsbeispiel soll eine Verbindung zwischen einem Laptop und einer PCD über PPP hergestellt werden. Es wird das interne Modem des Laptop verwendet (man kann auch ein externes Modem verwenden z.B das Ludwig M716-K). An die PCD schliessen wir wahlweise ein Ludwig M716-KS1 oder ein Enfora GSM1208 GSM Modem an. Der PC ist als PPP-Client konfiguriert und die PCD ist PPP-Server. Die Verbindung wird auf dem Laptop gestartet. Der Benutzer startet die Verbindung mit dem gleichen Verfahren wie eine DFÜ-Verbindung hergestellt wird.

Der Test wurde mit 2 Modems vom Typ Ludwig Systemtechnik M716-K gemacht. Einmal mit eingebautem Modem im Laptop und ein M716-K auf der Seite der PCD (siehe Print-Screens)

Schema 1: PCD mit Analogmodem



Schema 2: PCD mit GSM-Modem



Betriebssystem Windows XP SP 2

PCD3.M5540  
FW 10.9.25

### 2.2.2. Benötigtes Material

- 1 Laptop / PC mit PG5 Utilities

Für die Konfiguration und die Programmierung ist die Software PG5 2.150 erforderlich.

- Für diese Anwendung wird 1 PCD benötigt  
Es können folgende Typen verwendet werden: PCD3.M3xx0, PCD3.M5xx0 oder PCD2.M5xx0,  
PCD3.M6xx=, PCD3.M2x30V6 oder PCD3.M2x30A4Tx

- Beim PCD3.M3xx0: benötigt man zusätzlich ein PCD3.F121 Modul (Serielle Schnittstelle). Beim  
PCD3.M2x30V6 und PCD3.M2x30A4Tx braucht es lediglich ein PCD7.F121 Modul  
Beim PCD3.M2x30A4T5 verwendet man mit Vorteil das eingebaute Modem anstelle des externen  
Modems. (In diesem Fall braucht es kein F121 Modul)

Für dieses Beispiel wurden folgende Geräte verwendet:

- PCD3.M5540
- USB-Serial Konverter (Digitus)
- Laptop HP Compaq 6715b
- Modemkabel

- 1 Stk. Enfora Modems GSM1208 (GPRS-fähig, Speisung 5-30V)
- 1 Stk. Analogmodem Ludwig Systemtechnik M716-K

### **2.2.3. Anwendungsmöglichkeiten**

- Diese Konfiguration ist interessant für Fernwartung.
- Es ist ein Zugriff mit FTP oder HTTP direkt möglich
- Das Herunterladen von Webseiten ist schneller im Vergleich zu den konventionellen SBUS-  
Verbindungen.
- Es ist möglich über Ether-S-Bus mit PG5 Online zu gehen, das Programm zu Debuggen und Online  
zu gehen.

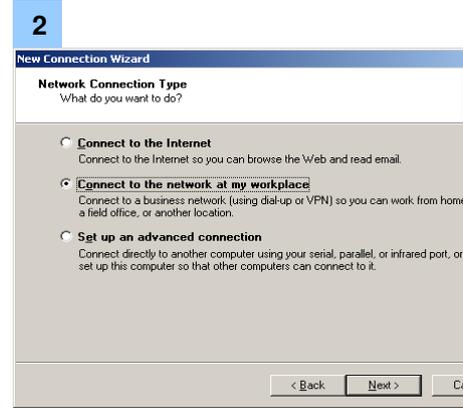
### **2.2.4. Konfiguration und Inbetriebnahme**

Folgende Konfigurationsschritte sind nötig:

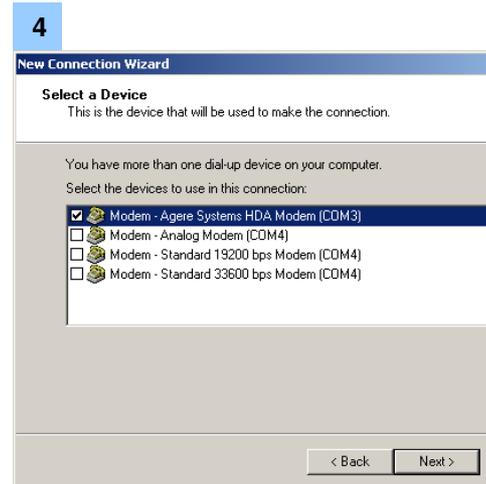
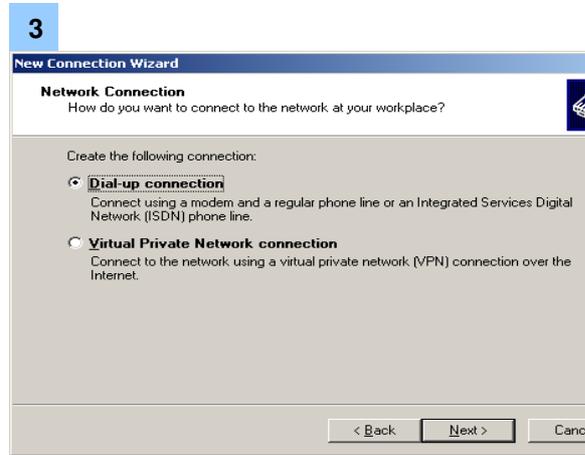
- A) Konfiguration der Verbindung auf dem Client-PC
- B) PPP-Konfiguration auf der PCD
- C) Aufbau der Verbindung
- D) Kontrolle der Verbindung
- E) Testen der Applikationen über diese neue Verbindung

## A) Konfiguration der Verbindung auf dem Client-PC:

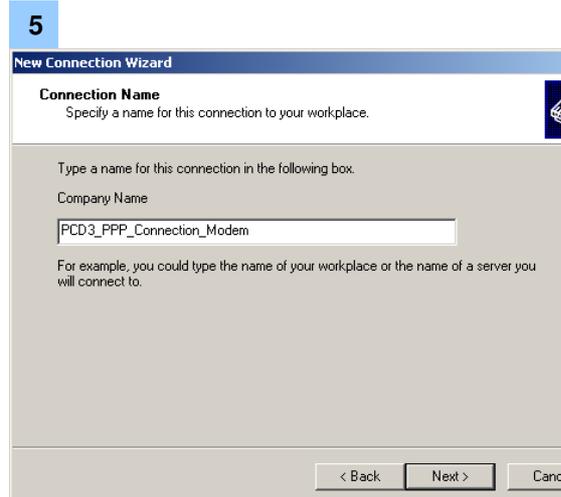
Es muss eine PPP-Modemverbindung konfiguriert werden.



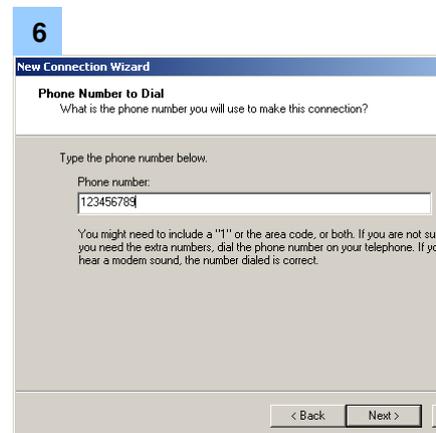
## Netzwerkverbindungen: Neue Verbindung erstellen



## Wählleitungsverbindung erstellen



## Auswahl des eingebauten Analogmodems

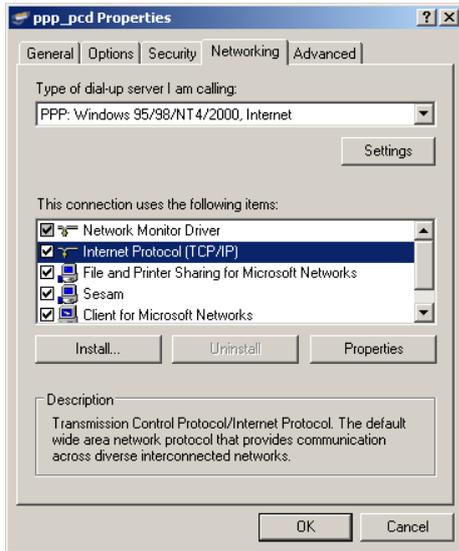


## Telefonnummer des Modems eingeben

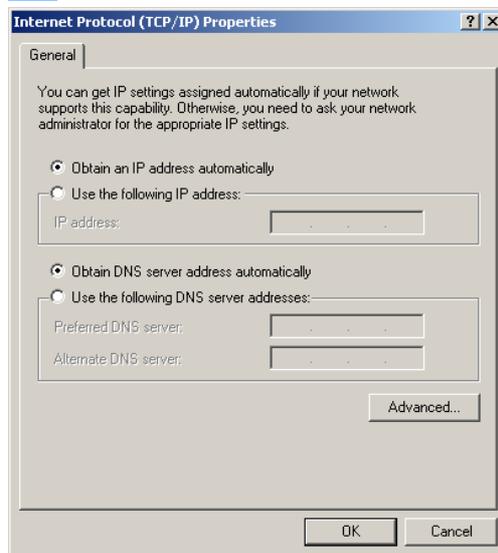
Wenn man anstelle des internen Modems ein externes Modem auf der PC-Client Seite verwenden will, kann man anstelle des unter Punkt 4 gewählten Modems Agere Systems ein Standardmodem an z.B. COM4 wählen. Hier ist COM 4 ein USB-Seriell Konverter.

Folgende weitere Einstellung muss vorgenommen werden, falls man parallel zu diesem Test weiterhin mit dem Webbrowser, Email-Client und anderen Internetprogrammen via LAN weiterarbeiten will.

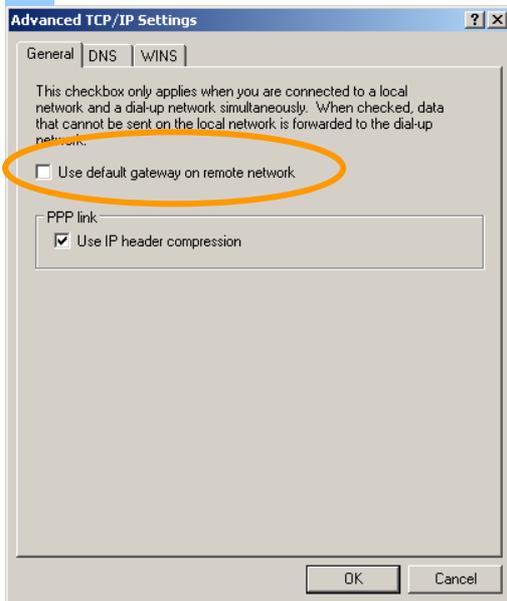
1



2



3



## B) PPP-Konfiguration auf der PCD

Die PCD3 muss auf die Funktion PPP-Server eingestellt werden. Damit diese Einstellungen nicht alle von Hand vorgenommen werden müssen, kann man das Backup des entsprechenden Beispielprojekts verwenden.

### Enfora GSM Modem

The screenshot shows the configuration interface for the Enfora GSM Modem. It is divided into three main sections:

- Onboard Communications:** A table listing communication types and their descriptions:
 

Type	Description
RS-485/S-Net	RS-485 port for Profi-S-Bus or general-purpose communications (D-Sub #2).
USB	Universal Serial Bus port, PGU or general-purpose.
RS-232/PGU	RS-232, PGU or general-purpose serial port (D-Sub #1).
RS-485	RS-485 port for general-purpose communications (Terminal block).
Ethernet	Ethernet port.
- Onboard I/O Slots:** A table listing I/O slots and their descriptions:
 

Slot	Type	Description
Slot 0		
Slot 1		
Slot 2		
Slot 3		
+		
- PPP Protocol:** A detailed configuration panel for the PPP protocol, including:
  - Port Number PPP: 0
  - PPP Enable: **Yes**
  - Connection Type: Server
  - Local IP Address: 192.168.1.100
  - Remote IP Address: 192.168.1.101
  - PPP Restarted on Disconnection: **Yes**
  - Immediate Start Enable: **Yes**
  - Use Modem: **Yes**
  - Use Default Script: **No**
  - Script Modem, Line 1: ATH\r;OK;0;1;0;5
  - Script Modem, Line 2: ATZ\r;OK;0;2;0;5
  - Script Modem, Line 3: AT50=1\r;OK;0;3;0;5
  - Script Modem, Line 4: 0;RING;0;4;0;0
  - Script Modem, Line 5: 0;CONNECT;0;-1;0;60
  - Script Modem, Line 6: 0;NO CARRIER;0;-1;-1;0
  - Script Modem, Line 7: 0;NO DIAL TONE;0;-1;-1;0
  - Script Modem, Line 8: 0;BUSY;0;-1;-1;0
  - Script Modem, Line 9: (empty)
  - Script Modem, Line 10: (empty)
  - + Advanced Parameter: **Yes**
  - Start Delay: 5
  - Default IP Route: No
  - Baudrate: 115200 Baud
  - Remote User Name: (empty)
  - Remote Password: (empty)
  - Peer Authentication: **Yes**
  - IP Forwarding Enable: No
  - Echo Request Enable: No
  - Echo Interval Time: 5
  - Echo Number before Closing: 6
  - DCD Checking Enable: No DCD check
  - DCD Check Timeout: 1000
  - DTR Cleared Enable: No

### Ludwig M716-KS1

The screenshot shows the configuration interface for the Ludwig M716-KS1. It is divided into three main sections:

- Onboard Communications:** A table listing communication types and their descriptions:
 

Type	Description
RS-485/S-Net	RS-485 port for Profi-S-Bus or general-purpose communications (D-Sub #2).
USB	Universal Serial Bus port, PGU or general-purpose.
RS-232/PGU	RS-232, PGU or general-purpose serial port (D-Sub #1).
RS-485	RS-485 port for general-purpose communications (Terminal block).
Ethernet	Ethernet port.
- Onboard I/O Slots:** A table listing I/O slots and their descriptions:
 

Slot	Type	Description
Slot 0		
Slot 1		
Slot 2		
Slot 3		
+		
- PPP Protocol:** A detailed configuration panel for the PPP protocol, including:
  - Port Number PPP: 0
  - PPP Enable: **Yes**
  - Connection Type: Server
  - Local IP Address: 192.168.1.100
  - Remote IP Address: 192.168.1.101
  - PPP Restarted on Disconnection: **Yes**
  - Immediate Start Enable: **Yes**
  - Use Modem: **Yes**
  - Use Default Script: **No**
  - Script Modem, Line 1: ATH\r;OK;0;1;0;5
  - Script Modem, Line 2: ATZ\r;OK;0;2;0;5
  - Script Modem, Line 3: AT&F1%c0&K3\N3525=050=1\
  - Script Modem, Line 4: 0;RING;0;4;0;0
  - Script Modem, Line 5: 0;CONNECT;0;-1;0;60
  - Script Modem, Line 6: 0;NO CARRIER;0;-1;-1;0
  - Script Modem, Line 7: 0;NO DIAL TONE;0;-1;-1;0
  - Script Modem, Line 8: 0;BUSY;0;-1;-1;0
  - Script Modem, Line 9: (empty)
  - Script Modem, Line 10: (empty)
  - + Advanced Parameter: **Yes**
  - Start Delay: 5
  - Default IP Route: No
  - Baudrate: 115200 Baud
  - Remote User Name: (empty)
  - Remote Password: (empty)
  - Peer Authentication: **Yes**
  - IP Forwarding Enable: No
  - Echo Request Enable: No
  - Echo Interval Time: 5
  - Echo Number before Closing: 6
  - DCD Checking Enable: No DCD check
  - DCD Check Timeout: 1000
  - DTR Cleared Enable: No

→ Für weitergehende *Informationen zu den einzelnen Parametern siehe PPP User Manual*

Das PPP-Protokoll im Server-Modus wird aktiviert, sobald ein Download der Konfiguration durchgeführt wurde.

Nachdem das Userprogramm heruntergeladen wurde, stehen 2 HTML-Webseiten mit Diagnosemöglichkeiten zur Verfügung:

PPPStatusH.html -> Status der PPP Verbindung

PPPConfigH.html -> Aktuelle Konfigurationseinstellungen

Die PPP-Funktionen sind auch ohne Userprogramm, d. h. auch im Halt- und Stop-Modus aktiviert. Die PPP-Funktionen werden von der Firmware verwaltet. Es gibt allerdings die Möglichkeit mit **CSF** oder

**CGI-Befehlen** Einstellungen vorzunehmen. Im vorliegenden Beispiel werden diese Funktionen nicht verwendet.

### C) Aufbau der Verbindung

Der Verbindungsaufbau hat Ähnlichkeit mit dem Aktivieren einer Internetverbindung mit einem Laptop und dem eingebauten Modem. Die Eigenschaften von Netzwerk öffnen und den neu erstellten Link: **PCD3\_PPP\_Connection\_Modem** doppelklicken: Es öffnet sich folgende Dialogbox:



Folgende Eingaben müssen gemacht werden:

Username: ROOT

Password: ROOTPASSWD

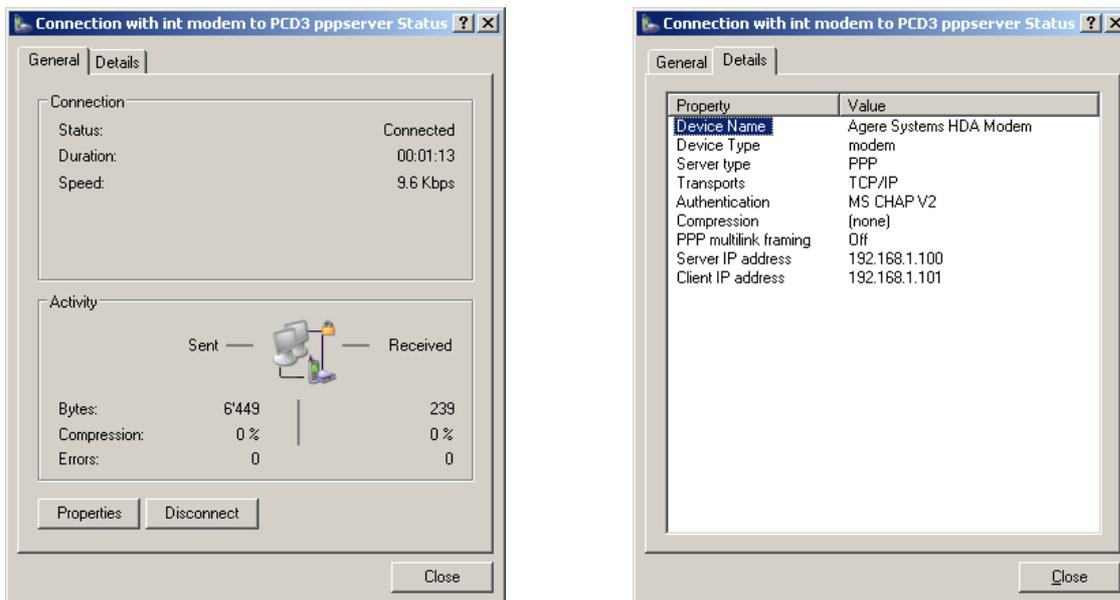
Da bei der Einstellung des PPP-Servers Peer Authentication = 1 gewählt wurde, ist es wichtig, die Login Parameter korrekt einzustellen. Beim Password und beim User Namen muss die Gross- und Kleinschreibung der Buchstaben berücksichtigt wird. (ROOT / ROOTPASSWD)

Dabei handelt es sich um die voreingestellten Parameter. Bei diesem Beispiel wie auch bei allen folgenden Anwendungen wird dringend angeraten das Default Login / Passwort zu ändern. Sobald man sich mit einer öffentlichen Adresse ins Internet verbindet ist diese Vorsichtsmassnahme unverzichtbar. Es können mehrere User-Accounts erstellt werden. Diese gelten sowohl für den Zugriff über PPP (Server) sowie für den Zugriff auf den FTP-Server. Diese Parameter werden im Device Configurator unter IP Transfer Protocols (FTP) konfiguriert.

Bei "Dial": muss die Telefonnummer des Analog-Anschlusses an welchen das Modem der PCD angeschlossen ist oder die Telefonnummer der SIM-Karte bei Verwendung eines GSM-Modems eingegeben werden. Es muss beachtet werden, ob eine vorgängige 0 für die Amtsleitung gewählt werden muss. Bei manchen Zentralen muss man dem Modem im Laptop spezielle Befehle schicken, damit nicht auf einen Summton gewartet wird.

Danach muss **CONNECT** durchgeführt werden.

Bei erfolgreichem Verbindungsaufbau erscheint ein zusätzliches Symbol mit 2 PCs unten in der Taskleiste. Es ist möglich den Status dieser Verbindung anzuzeigen. Man kann sehen, wie lange die Verbindung bereits besteht. Welche IP-Adresse Server (PCD) und Client (PC) bekommen haben. Die Authentifizierung, die angewendet wurde: MS CHAP V2. Es wurde diese Authentifizierung verwendet, weil es aus Sicht des Microsoft Windows XP Clients die Beste ist und der Server (PCD) alle Varianten (PAP, CHAP, MSCHAP v1 MSCHAPv2) unterstützt.



#### D) Kontrolle der Verbindung

So bald die Verbindung da ist, kann man die unterschiedlichen Anwendungen über TCP/IP testen:

PING 192.168.1.100, Befehl aus einem CMD-Fenster ausführen (zum Testen der Verbindung)

#### E)

HTTP: Direkter Zugriff auf den Webserver, download von Webeditorprojekten, ausführen von CGI-Befehlen. Die Software Webconnect kann verwendet werden, ist aber nicht erforderlich

URL: <http://192.168.1.100> eingeben. Es erscheint die Standardwebseite der PCD

FTP: File Up- und Download. Z.B. mit Filezilla (mit Modus aktiv). Verbindung zum Server 192.168.1.100

OpenDataMode

SBUS Kommunikation (z.B PG5 Socket Connection)

## 2.3. Senden von E-Mails mit GSM-Modem (im GPRS Modus)

### 2.3.1. Beschreibung

Bei diesem Anwendungsfall wird gezeigt, wie man mit der neuen PPP-Funktion und einem GSM/GPRS-Modem Emails senden kann.

Schema:



### 2.3.2. Benötigtes Material

- 1 Laptop / PC mit PG5 Utilities

Für die Konfiguration und die Programmierung ist die Software PG5 2.150 erforderlich.

- Für diese Anwendung wird 1 PCD benötigt

Es können folgende Typen verwendet werden: PCD3.M3xx0, PCD3.M5xx0 oder PCD2.M5xx0, PCD3.M6xx-, PCD3.M2x30V6 oder PCD3.M2x30A4Tx

- Beim PCD3.M3xx0: benötigt man zusätzlich ein PCD3.F121 Modul (Serielle Schnittstelle). Beim PCD3.M2x30V6 braucht es lediglich ein PCD7.F121 Modul.

Beim PCD3.M2x30A4T5 verwendet man mit Vorteil das eingebaute Modem anstelle des externen Modems. (In diesem Fall braucht es kein F121 Modul)

Für dieses Beispiel wurden folgende Geräte verwendet:

- PCD3.M5540
- USB-Serial Konverter (Digitus)
- Laptop HP Compaq 6715b
- Modemkabel

- 1 Stk. Enfora Modems GSM1208 (GPRS-fähig, Speisung 5-30V)

- 1 Stk. Analogmodem Ludwig Systemtechnik M716-K

### 2.3.3. Anwendungsmöglichkeiten

Senden von E-Mails über GPRS beim Eintreffen von bestimmten Ereignissen und zur Alarmierung.

Beispiele: Die Anlage hat einen Alarmzustand festgestellt.

Es gab eine Unterschreitung / Überschreitung von Füllständen, Temperaturen etc.

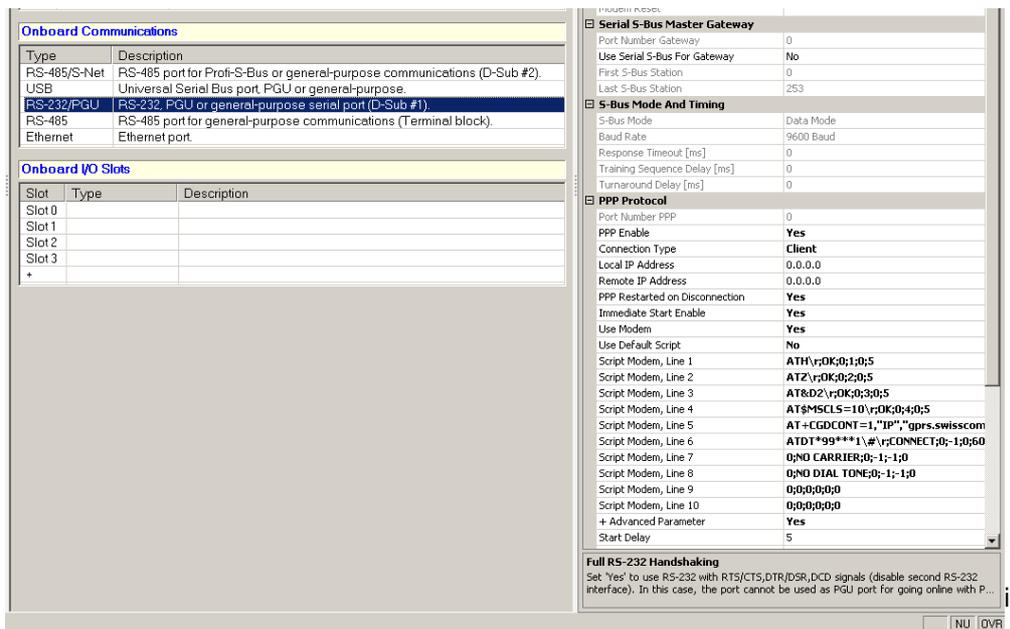
Senden von E-Mails mit Anhängen. Mit dem E-Mail können direkt Files aus dem File-System mitgeschickt werden z.B. Log-Dateien, die eine Fehlfunktion dokumentieren oder File-Protokollierung von periodischen Messwerten. Als spezielle Funktion könnte man bei der Verwendung von dynamischen, öffentlichen IP-Adressen auch die aktuelle IP-Adresse an einen Server oder an ein Fernwartungs-Mailkonto senden.

## 2.3.4. Konfiguration und Inbetriebnahme

PPP-Konfiguration auf der PCD:

Mit dem PPP-Protokoll wird der GPRS-Modus aktiviert, sobald ein Download der Konfiguration durchgeführt wird.

Bei diesem Beispiel wird der APN (Access Point Name) **GPRS.SWISSCOM.CH** von SWISSCOM verwendet. Jeder Internetprovider verwendet meistens seinen eigenen APN-Namen. Der APN-Name muss in der entsprechenden Modem Script Line eingetragen werden.



PPPStatusH.html -> Status der PPP Verbindung  
 PPPConfigH.html -> Aktuelle Konfigurationseinstellungen

Die PPP-Funktionen sind auch ohne Userprogramm, d. h. auch im Halt- und Stop-Modus aktiviert. Die PPP-Funktionen werden von der Firmware verwaltet. Es gibt allerdings die Möglichkeit mit **CSF** oder **CGI-Befehlen** Einstellungen vorzunehmen. Im vorliegenden Beispiel werden diese Funktionen nicht verwendet.

→ Für weitergehende Informationen zu den einzelnen Parametern siehe **PPP User Manual**

Als erstes sollte durch Aufruf von:

**Error! Hyperlink reference not valid.** überprüft werden, dass eine aktive GPRS-Verbindung besteht. Es muss eine IP-Adresse vorhanden sein.

Damit Emails gesendet werden können, müssen einige Einstellungen vorgenommen werden.

Vor allem wenn man nicht sicher ist, ob die Maileinstellungen (smtp-Server, username, pwd etc.) richtig konfiguriert sind, ist es sinnvoll zu erst zu testen, ob es gelingt E-Mails zum Beispiel über Ethernet und eine bereits geprüfte ADSL-Router-Verbindung zu senden und anschliessend für die GPRS-Konfiguration zu verwenden.

Folgende Parameter müssen für die Advanced Mail-Fbox richtig konfiguriert werden.

### - E-Mailserver z.B. 212.1.2.3

Falls man die IP Adresses des Mailservers, den man verwenden möchte nicht kennt, kann man ihn mit der folgenden Methode ausfindig machen:

Beim Command Prompt muss folgender Befehl eingegeben werden:

```
c:\nslookup mail.gmx.net
```

```
Server: .....  
Address: .....
```

```
Name: mail.gmx.net  
Addresses: 213.165.64.21, 213.165.64.20
```

Nun kann man die Adresse 213.165.64.21 beim E-Mailserver konfigurieren.

Als Alternative liefert auch der Befehl ping mail.gmx.net. Die IP-Adresse des Mailservers. In einem der folgenden Kapitel wird gezeigt, wie diese Auflösung automatisch über DNS gemacht werden kann.

- **ename**                      **username**

Dieser Parameter ist nicht immer erforderlich

- **epwd**                      **password**

Dieser Parameter ist nicht immer erforderlich

- **esender**                      **Absender Email Adresse**

hier wird die übliche komplette Absender Adresse eingetragen

- **eto1**                      **Empfänger E-Mail Adresse**

hier wird die übliche komplette Empfänger Adresse eingetragen

Der Versand der Emails kann auf verschiedene Arten ausgelöst werden:

Man kann Mails über das Web-Projekts senden:

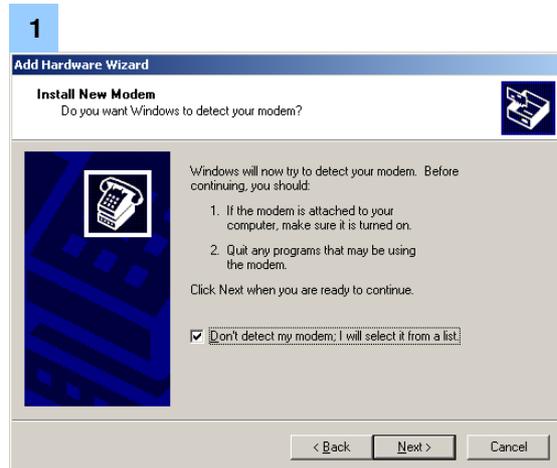
Auf der Page **Error! Hyperlink reference not valid.** hat man 2 Buttons zur Auswahl, die das Versenden eines Mails mit oder ohne Attachment auslösen.

Mit Hilfe des Saia Online Debuggers ist es ebenfalls möglich den Mailversand auszulösen.

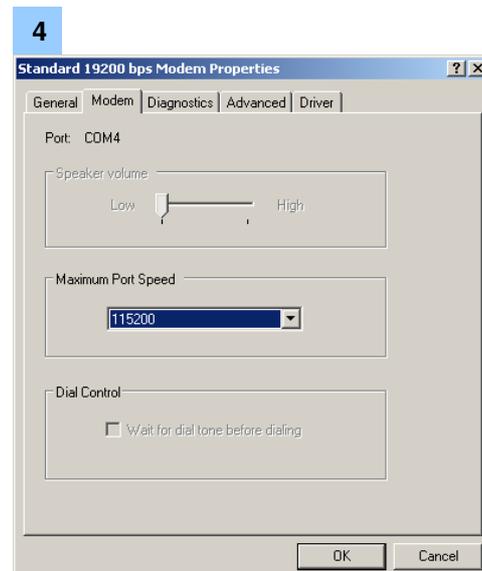
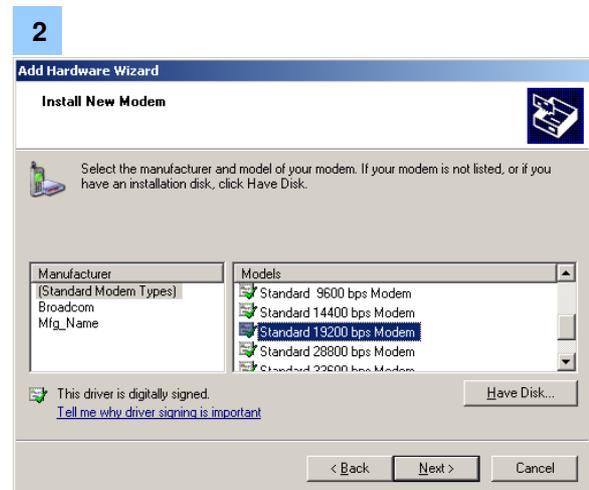
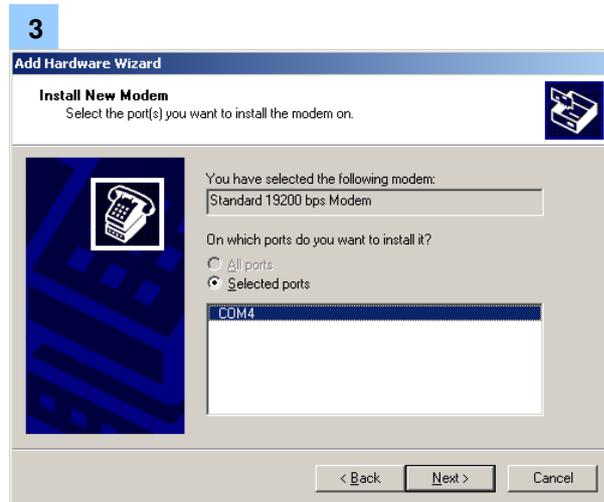
## Konfiguration eines GRPS-Modems auf Windows XP

Falls auf Seite des PC-Clients eine Verbindung über einen ADSL- oder GPRS-Router verwendet werden soll, ist dieses Kapitel nicht relevant. Hier wird gezeigt wie man mit einem Windows XP-Client eine Verbindung ins Internet bei Verwendung des gleichen Modems wie auf der PCD (Enfora Modem GSM1208)

Zunächst folgt die Beschreibung zur Konfiguration des Modems. (Schritte 1-6)

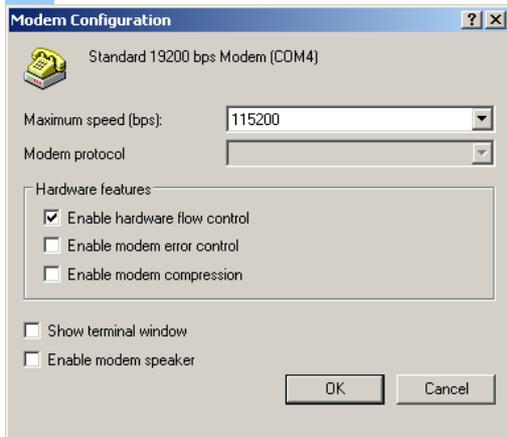


## Neues Modem installieren



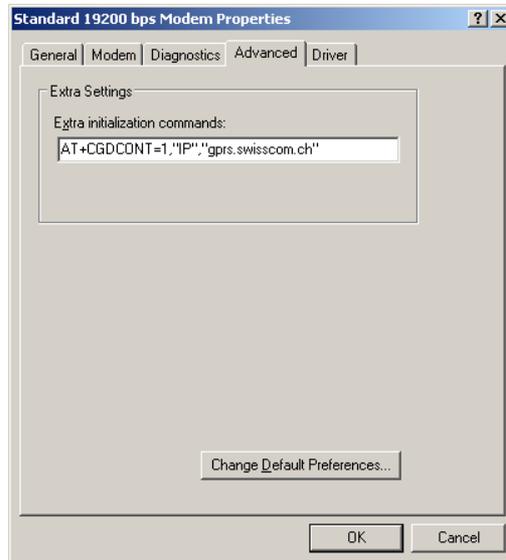
Falls das Modem mit einer festen Baudrate arbeitet ist es sehr wichtig, hier die richtige Geschwindigkeit einzustellen.

5



Es ist zwingend erforderlich  
 Hardware-Handshaking zu verwenden

6



Diese Einstellung ist nötig um den richtigen APN des Providers zu verwenden

Konfiguration der PPP-Modemverbindung (Schritte 1-6)

1



2

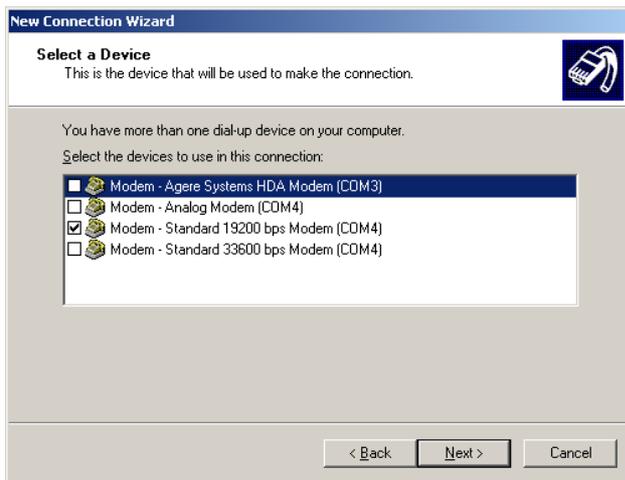


Netzwerkverbindungen: Neue Verbindung erstellen

3



4



Modem an COM4 angeschlossen

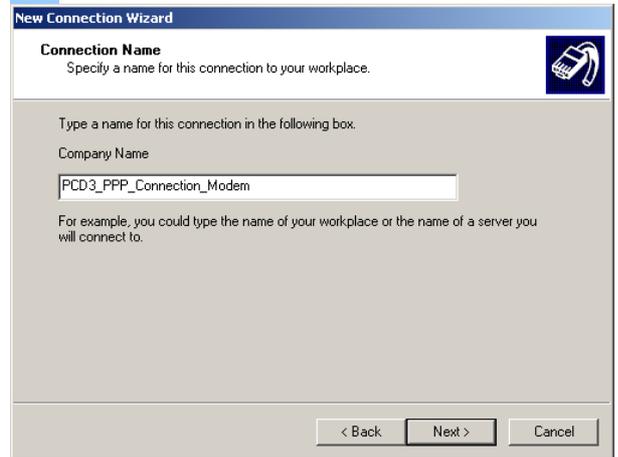
6



Eingabe des speziellen Dialstrings für GPRS-Verbindungen.

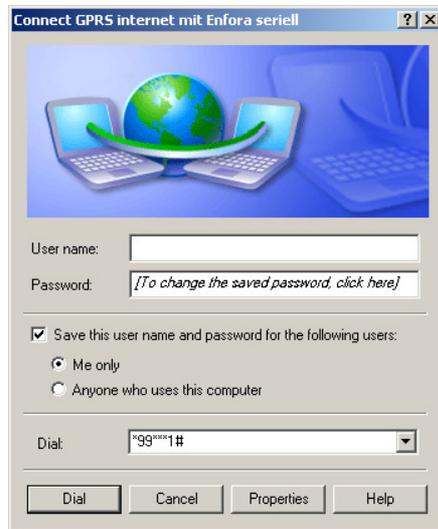
Bemerkung: COM 4 ist bei dieser Konfiguration ein USB-Seriell Konverter.

5



Name für die Verbindung wählen

Der Verbindungsaufbau hat Ähnlichkeit mit dem Aktivieren einer Internetverbindung mit einem Laptop und dem eingebauten Modem. Man öffnet die Eigenschaften von Netzwerk macht einen Doppelklick auf den neu erstellten Link: **PCD3\_PPP\_Connection**: Es öffnet sich folgende Dialogbox:



Je nach Provider und Abonnement muss man hier andere Daten verwenden:  
(swisscom public internet access)

User name: (leer)  
Password: (leer)

Mit dem Button Dial wird der Verbindungsaufbau gemacht.

### 2.3.5. Bemerkungen

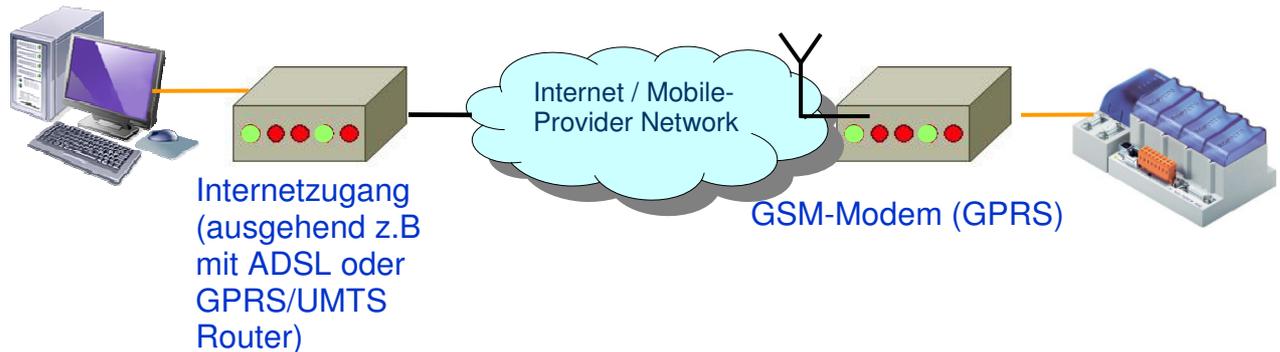
Bei unseren Tests können wir auch E-Mails senden, wenn die PPP-Verbindung über ein Analog-Modem mit PPP zu einem Internetprovider übers öffentliche Telefonnetz (PSTN) aufgebaut wurde. Dies ist jedoch eine Methode, die aus folgenden Gründen nicht mehr besonders empfehlenswert ist: Es fallen für jeden Verbindungsaufbau Kosten an. Die Kosten werden nach Verbindungszeit abgerechnet. Die Zukunftssicherheit ist nicht garantiert. D.h. man weiss nicht genau, wie lange solche Analog- und ISDN-Direkt-Zugänge noch existieren werden.

## 2.4. Fernzugriff via Internet

### 2.4.1. Beschreibung

Bei diesem Beispiel wird gezeigt wie ein typisches Szenario für eine vollständige Fernwartungsmöglichkeit aussehen könnte.

Schema:



Wartungs-PC

Windows XP Professional SP2  
-Keine feste, öffentliche IP-Adresse nötig  
-UDP Port 5050 muss offen für ausgehenden Traffic sein  
-FTP-Zugriff ausgehend freigeschaltet

PCD

(SBUS-Slave aktiviert)  
-PCD3.M5540  
-FW 1.14.21  
-SIM-Karte Swisscom mit öffentlicher (fester oder dynamischer-) IP-Adresse)

### 2.4.2. Benötigtes Material

- 1 Laptop / PC mit PG5 Utilities

Für die Konfiguration und die Programmierung ist die Software PG5 2.150 erforderlich.

- Für diese Anwendung wird 1 PCD benötigt

Es können folgende Typen verwendet werden: PCD3.M3xx0, PCD3.M5xx0 oder PCD2.M5xx0, PCD3.M6xx=, PCD3.M2x30V6 oder PCD3.M2x30A4Tx

- Beim PCD3.M3xx0: benötigt man zusätzlich ein PCD3.F121 Modul (Serielle Schnittstelle). Beim PCD3.M2x30V6 braucht es lediglich ein PCD7.F121 Modul.

Beim PCD3.M2x30A4T5 verwendet man mit Vorteil das eingebaute Modem anstelle des externen Modems. (In diesem Fall braucht es kein F121 Modul)

Für dieses Beispiel wurden folgende Geräte verwendet:

- PCD3.M5540
- USB-Serial Konverter (Digitus)
- Laptop HP Compaq 6715b
- Modemkabel
- 1 Stk. Enfora Modems GSM1208 (GPRS-fähig, Speisung 5-30V)

### 2.4.3. Anwendungsmöglichkeiten

Es gibt verschiedene Anwendungsmöglichkeiten

Es wird ein Fernzugriff mit PG5 über die GPRS/Internet Verbindung (Ether-SBUS-Socket Connection / UDP Port 5050) realisiert.

Es besteht die Möglichkeit Userprogrammupdates durchzuführen. Es ist möglich Online Debugging auf der PCD durchzuführen.

Der User kann übers Internet auf die Applikation via Webinterface (Webeditor-Project) zugreifen.

Ein SCADA-System kann über FTP auf das Filesystem zugreifen oder als SBUS-Master mit den Saia.net Funktionen auf die PCD (SBUS-Slave) zugreifen.

### 2.4.4. Konfiguration und Inbetriebnahme

PPP-Konfiguration auf der PCD:

Mit dem PPP-Protokoll wird der GPRS-Modus aktiviert, sobald ein Download der Konfiguration durchgeführt wird.

Bei diesem Beispiel wird der APN (Access Point Name) **corporate.swisscom.ch** von SWISSCOM verwendet.

Beim Provider Swisscom erhält man mit diesem APN gegen eine monatlichen Aufpreis von 5 CHF Eine öffentliche dynamische IP-Adresse. Es gibt auch Provider, die private, feste IP-Adressen anbieten. Das Beispiel funktioniert auch für diese Zugänge sofern der Internetzugang auf der PC-Seite entsprechend konfiguriert wurde und der Zugriff auf das VPN gewährleistet ist. (z.B OpenVPN Verbindung zum Provider)

Das Default Login und Password des FTP-Servers muss unbedingt geändert werden. Diese Parameter können im Device Configurator unter IP Transfer Protocols (FTP) konfiguriert werden.

Type	Description
RS-485/S-Net	RS-485 port for Profi-S-Bus or general-purpose communications (D-Sub #1)
USB	Universal Serial Bus port, PGU or general-purpose
RS-232/PGU	RS-232, PGU or general-purpose serial port (D-Sub #1)
RS-485	RS-485 port for general-purpose communications (Terminal block)
Ethernet	Ethernet port

Slot	Type	Description
Slot 0		
Slot 1		
Slot 2		
Slot 3		
+		

Parameter	Value
Port Number Gateway	0
Use Serial 5-Bus For Gateway	No
First 5-Bus Station	0
Last 5-Bus Station	253
<b>S-Bus Mode And Timing</b>	
5-Bus Mode	Data Mode
Baud Rate	9600 Baud
Response Timeout [ms]	0
Training Sequence Delay [ms]	0
Turnaround Delay [ms]	0
<b>PPP Protocol</b>	
Port Number PPP	0
PPP Enable	Yes
Connection Type	Client
Local IP Address	0.0.0.0
Remote IP Address	0.0.0.0
PPP Restarted on Disconnection	Yes
Immediate Start Enable	Yes
Use Modem	Yes
Use Default Script	No
Script Modem, Line 1	ATH;rDK;0;1;0;5
Script Modem, Line 2	ATZ;rDK;0;2;0;5
Script Modem, Line 3	ATR;02;rDK;0;3;0;5
Script Modem, Line 4	AT\$MSCLS=10\rDK;0;4;0;5
Script Modem, Line 5	AT+CGDCONT=1,\"corporate.swisscom.ch\";r
Script Modem, Line 6	ATDT*99**1\;#r;CONNECT;0;-1;0;60
Script Modem, Line 7	0;NO CARRIER;0;-1;-1;0
Script Modem, Line 8	0;NO DIAL TONE;0;-1;-1;0
Script Modem, Line 9	0;0;0;0;0
Script Modem, Line 10	0;0;0;0;0
+ Advanced Parameter	Yes
Start Delay	5

**Script Modem, Line 5**  
 There is 10 lines for modem script.  
 Only used lines and two more empty lines are displayed.

**Manual**

Für diese Anwendung kann das gleiche Userprogramm wie bei Kapitel 2.3

Nachdem das Userprogramm heruntergeladen wurde, stehen 2 HTML-Webseiten zu Diagnose zur Verfügung.

Als erstes sollte durch Aufruf von:

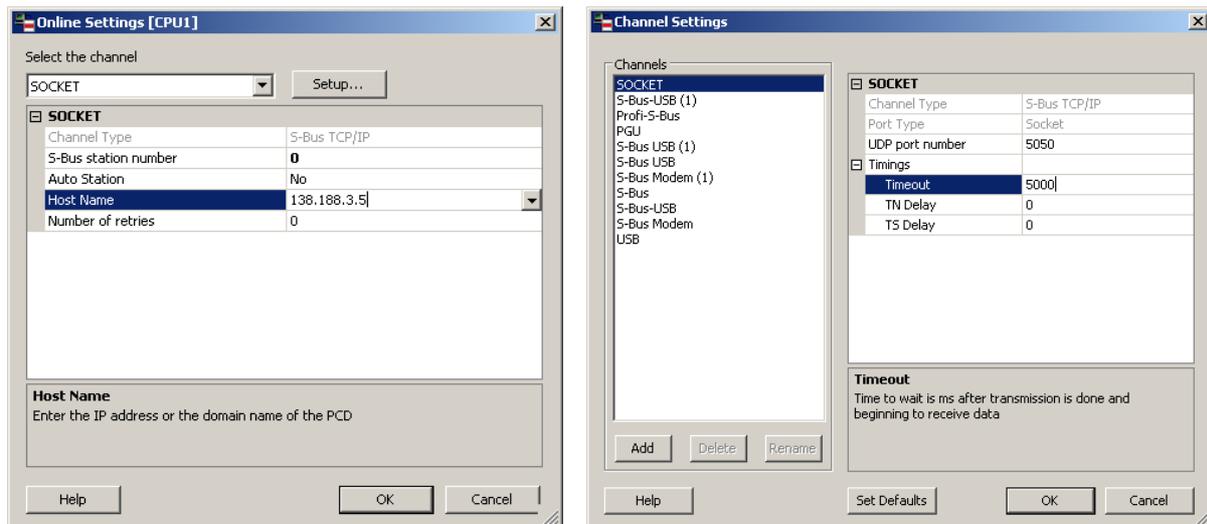
**Error! Hyperlink reference not valid.** überprüft werden, dass eine aktive GPRS-Verbindung besteht. Es muss eine IP-Adresse vorhanden sein. Diese IP-Adresse benötigt man, um die Online-Verbindung aufzubauen.

Falls man öffentliche, dynamische IP-Adressen benutzen will, muss man einen Mechanismus vorsehen, der dem Rechner, der den Fernzugriff machen will, die aktuelle IP-Adresse mitteilt. Es existieren diverse Möglichkeiten für die Übermittlung der aktuellen IP-Adresse (DynDns, Email, Ether-S-BUS, SNMP-Trap, OpenDataMode)

Jetzt muss man in den Online-Settings die richtigen Einstellungen vornehmen.

Als Channel wird Socket gewählt. Bei Hostname trägt man die IP-Adresse der Station ein, auf die man zugreifen will. Anstelle der IP-Adresse kann auch der Hostname eingegeben werden, falls dieser mit DynDns registriert wurde.

Das Default Timeout von 1000 ms ist für das GPRS-Netzwerk zu klein, deshalb muss über die Einstellung Setup der Parameter Timeout auf einen Wert zwischen 5000 -10000 ms eingestellt werden.



Anschliessend kann man mit dem Saia Online Debugger oder mit Fupla verbinden und die aktuellen Werte durch Probes oder im Watch Window anzeigen lassen. Die Funktionalität ist die gleiche wie bei einer Verbindung mit dem USB-Kabel oder über LAN. Da die Ether-S-Bus Telegramme jedoch mit rund 2 Sekunden durch die Übertragung verzögert werden, kann nicht so flüssig gearbeitet werden.

## 2.4.5. Bemerkungen

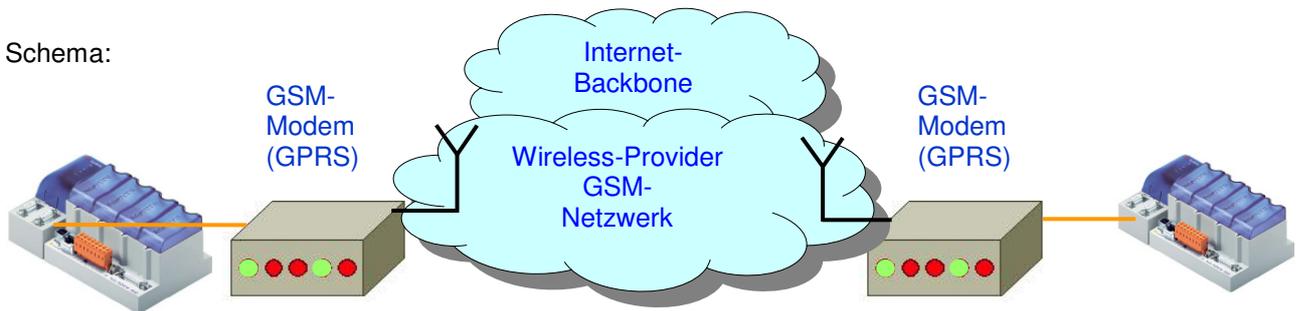
Es gibt Einschränkungen bei der Benutzung bestimmter Protokolle und Anwendungen über WAN-Verbindungen. Davon ist nicht nur diese neue Verbindungsmöglichkeit über PPP und GPRS-Modem betroffen. Allgemein sind alle WAN-Übertragungsarten (Drahtgebundene oder Funkverbindungen) anfälliger für Verzögerungen und Übertragungsfehler als LAN-Verbindungen. Bei der PCD ist speziell die SBUS-UDP Datenübertragung für WAN-Netze nicht optimal. Es wird empfohlen TCP basierte Applikationen zu verwenden (Datenaustausch mit Mails oder Files / FTP). Es sollten Massnahmen getroffen werden, damit bei Web-Projekten das Imaster-jar-File nicht stets von der Steuerung heruntergeladen werden muss.

## 2.5. SBUS Master – Slave Kommunikation (Ether-SBUS over PPP)

### 2.5.1. Beschreibung

Bei diesem Beispiel sollen 2 PCD3-Steuerungen gegenseitig Daten austauschen. Zur Kommunikation wird das bei jeder PCD-Steuerung standardmässig unterstützte SBUS-Protokoll (Ether-SBUS-Protokoll) verwendet. Der Vorteil dabei ist, dass man ohne aufwändige Programmierung mit bereits existierenden Funktionsboxen direkten Zugriff auf alle Ressourcen hat. Man kann Eingänge und Register einer abgesetzten Anlage abfragen und Ausgänge und Register schreiben. Die Anlage lässt sich „fernsteuern“.

Schema:



#### SBUS-Master:

Bei diesem Modem kann eine beliebige SIM-Karte verwendet werden, sofern der Provider IP / UDP Protokoll ausgehend nach Port 5050 erlaubt

#### SBUS-Slave:

Bei diesem Modem muss eine SIM-Karte mit einem APN verwendet werden, der eine öffentliche IP bereitstellt. Wenn die IP dynamisch ist, muss sie beim Slave mit einer geeigneten Methode aktualisiert werden.

Beim SBUS-Slave kann anstelle eines Modems auch ein ADSL-Router verwendet werden. Mit Vorteil bestellt man dazu beim Provider eine fixe IP-Adresse

## 2.5.2. Benötigtes Material

- 1 Laptop / PC mit PG5 Utilities
- Für diese Anwendung werden 2 PCD's benötigt.  
Es können folgende Typen verwendet werden: PCD3.M3xx0, PCD3.M5xx0 oder PCD2.M5xx0, PCD3.M6xx0, PCD3.M2x30V6 oder PCD3.M2x30A4Tx
- Beim PCD3.M3xx0: benötigt man zusätzlich ein PCD3.F121 Modul (Serielle Schnittstelle). Beim PCD3.M2x130V6 benötigt man lediglich ein PCD7.F121 Modul  
Beim PCD3.M2x30A4T5 verwendet man mit Vorteil das eingebaute Modem anstelle des externen Modems. (In diesem Fall braucht es kein F121 Modul)

Für dieses Beispiel wurden folgende Geräte verwendet:

- 2 PCD3.M5540
- USB-Serial Konverter (Digitus)
- Laptop HP Compaq 6715b
- 2 Stk. Enfora Modem GSM1208 GPRS-fähig (Speisung 5-30V)
- Modemkabel

## 2.5.3. Anwendungsmöglichkeiten

Es gibt viele Anwendungsmöglichkeiten für eine solche Konfiguration.  
Datenaustausch zwischen 2 Anlagen mit gleicher oder ähnlicher Funktion. Mit dem Ziel Informationen zu vervollständigen oder Prozesse zu synchronisieren.  
Datenzentralisation auf eine Steuerung (z.B. am Festnetz mit ADSL angeschlossen). Die Remote-Stationen liefern periodische oder ereignisgetriggerte Updates. Ein Server-PC sammelt die Daten zentral.

## 2.5.4. Konfiguration und Inbetriebnahme

Konfiguration auf der PCD:

Auf der Seite des Master-PCD kann man Standard-SIM-Karten von Swisscom mit dem APN „**GPRS.SWISSCOM.CH**“ verwenden.

Auf der Seite der Slave-PCD benötigt man zumindest eine dynamische, öffentliche Adresse  
Bei Swisscom kann man dafür den Zusatzdienst Corporate Application Access verwenden. Als APN muss „**CORPORATE.SWISSCOM.CH**“ (login: 133 / password: 133) verwendet werden. Diesen Dienst kann man für einen monatlichen Aufpreis von 5 CHF benützen. Da die Adresse dynamisch vergeben wird, muss man sie anschliessend manuell oder mit einem geeigneten Mechanismus beim Master aktualisieren. (DynDns, Email, Ether-S-BUS, SNMP-Trap, OpenDataMode)

Es gibt auch Provider, die private, feste IP-Adressen anbieten. Das Beispiel funktioniert auch für diese Zugänge. Es sind dann allerdings 2 identische SIM Karten erforderlich die miteinander über das VPN des Provider kommunizieren können.

→ Für weitergehende Informationen zu den einzelnen Parametern siehe **PPP User Manual**

Beim Laden der PG5-Projekte müssen beim SBUS-Slave im Prinzip nur die Einstellungen mit dem Device-Konfigurator korrekt geladen werden. Die SBUS-Nr. muss auf „0“ eingestellt werden.

Mit dem PPP-Protokoll wird der GPRS-Modus aktiviert, sobald ein Download der Konfiguration durchgeführt wird.

Ein Userprogramm muss beim Slave nicht unbedingt geladen werden. Es ist jedoch praktisch, wenn man das Userprogramm lädt, das beim Projekt dabei ist. So hat man die Möglichkeit durch Aufruf von: **Error! Hyperlink reference not valid.** zu sehen, ob GPRS korrekt funktioniert und die aktuelle IP-Adresse anzeigen. Es ist durchaus möglich das unter 2.3 vorgestellte Projekt als Userprogramm zu laden. So kann erreicht werden, dass die Steuerung als SBUS-Slave funktioniert und bei Bedarf auch die Möglichkeit zum Senden von Emails hat.

Bei der Steuerung, die als Master arbeitet, darf man nicht vergessen die IP-Adresse des Slaves anzupassen. Falls man Probleme mit der Kommunikation hat, kann man vorerst versuchen, ob die Kommunikation wenigstens über Ethernet funktioniert um den Fehler einzugrenzen. Für diesen Test muss man die Variable IPAdresse auf den Hex-Wert 0C0A87824h (192.168.120.36) setzen. Eine Testhilfe ist auch, zu versuchen über einen alternativen Internetzugang (z. B. ADSL) auf den Webserver der beiden Steuerungen zu gelangen.

### 2.5.5. Bemerkungen

Es gibt Einschränkungen bei der Benutzung bestimmter Protokolle und Anwendungen über WAN-Verbindungen. Davon ist nicht nur diese neue Verbindungsmöglichkeit über PPP und GPRS-Modem betroffen. Allgemein sind alle WAN-Uebertragungsarten (Drahtgebundene oder Funkverbindungen) anfällig für Verzögerungen und Übertragungsfehler. Dieses Beispiel ist besonders davon betroffen. Wenn man Datenübertragungen nach diesem Prinzip realisieren will, muss man unbedingt ein besseres „Error-Handling“ einbauen, da es keine Garantie gibt, dass die Datenübertragung nach 2 oder mehr Wiederholungen wirklich erfolgreich war.

Das SBUS-Protokoll wurde für LAN-Netzwerke entwickelt. Die SBUS-UDP Datenübertragung ist nicht für WAN-Netze optimiert worden. Es wird empfohlen wenn möglich eine TCP basierte Applikation zu verwenden (z. B. Datenaustausch mit Mails oder Files / FTP).

## 2.5.6. Allgemeine Bemerkungen zu GPRS-Verbindungen

Zur Erhöhung der Bandbreite sollten Geräte verwendet werden, die mit einer Multislotklasse > 8. D.h. 10, 12 oder noch höher betrieben werden können. Die meisten modernen Modems unterstützen mindestens MS 10.

Man sollte aufpassen, dass das verwendete Gerät optimal konfiguriert ist. Beim Enfora GSM1208 Modem z.B. wird in den Werkeinstellungen (AT&F) nur eine Multislotklasse von 8 konfiguriert. Man muss dem Modem den Befehl AT\$MSCLS=10 senden, damit es optimal arbeitet. Dadurch erhöht sich die maximal mögliche Downloadgeschwindigkeit auf das Doppelte (ca. 2500 Bytes/s)

Bei Webprojekten sollte man versuchen zu verhindern, dass die Benutzer dauernd die imaster\*.jar Datei neu laden müssen. Dies verursacht nicht nur eine zusätzliche Wartezeit (durchschnittlich ca. 2 min.) sondern es entstehen auch zusätzlich Kosten für das wiederholte Herunterladen der 240 kByte-Datei. Es gibt verschiedene Möglichkeiten, dies zu erreichen. Dank dem neuen Webserver kann man die Caching-Funktion von JAVA verwenden. Man kann die Datei mit der Software Webconnect lokal auf dem Client oder auf einem anderen Server im LAN bereitstellen. Man kann das Webprojekt so konfigurieren, dass die JAR-Datei auf einer anderen Steuerung heruntergeladen wird, die über eine ADSL-Verbindung oder eine andere Festnetz-Breitbandverbindung verfügt.

Beim Einsatz vom SBUS-Protokoll muss der Fall vorgesehen werden, dass auch bei 3 Versuchen keine erfolgreiche Übertragung gelungen ist. Das SBUS-Protokoll wurde für LAN-Netzwerke entwickelt. Die SBUS-UDP Datenübertragung ist noch nicht fürs WAN-Netzwerk optimiert worden. Das User-Programm muss das "Acknowledge" für die erfolgreiche Übertragung abwarten und die Daten falls nötig nach einer kurzen Wartezeit noch einmal erneut senden. Es wird empfohlen wenn möglich eine TCP basierte Applikationen zu verwenden (Datenaustausch mit Mails oder Files / FTP)

Einige Provider bieten standardmässig oder mit einem Zusatzabonnement GPRS-Profile an, die dem Benutzer eine dynamische, öffentliche IP-Adresse zuteilen. Bei Swisscom ist dies ein Zusatzservice, den man kaufen kann. Dieser Service nennt sich Corporate Application Access. Die PCD Steuerung kann damit ohne Probleme arbeiten.

Es sollte jedoch beachtet werden, dass man sich damit einem Risiko aussetzt von anderen Internetteilnehmern gestört zu werden. Die Bereiche des Webprojekts die nicht durch ein Passwort geschützt sind, kann man via Internet frei erreichen. Dazu gehört auch das Ausführen von Befehlen über das CGI-Interface. Das Default Login und Password des FTP-Servers muss unbedingt geändert werden. Diese Parameter können im Device Configurator unter IP Transfer Protocols (FTP) konfiguriert werden.

Falls es nötig ist, für Fernwartungszwecke die SBUS-Slave Funktion zu aktivieren. Sollte man auch bedenken, dass dies ein Risikofaktor sein könnte, da diese Funktion nicht über einen Zugangsschutz verfügt. Das Problem wird allerdings dadurch abgeschwächt, dass das S-BUS Protokoll proprietär ist. Die üblichen Hackertools können damit nicht viel anfangen.

Andere Zugangsmethoden wie Public Internet Access (Swisscom), bei dem sich das Endgerät hinter einer Firewall des Providers befindet und Corporate Network Access, die Teilnehmer haben eine VPN- ähnliche Verbindung und sind für sicherheitskritische Anwendungen zu bevorzugen.

## 3. Anwendungen der SNTP-Funktion

### 3.1. Anwendungsbeispiel SNTP

#### 3.1.1. Beschreibung

Bei den TCP-Erweiterungen gibt es neben den PPP-Funktionen neu auch eine SNTP-Client Funktion. Die Zeit wird mit dem SNTP-Protokoll sehr genau übertragen. Beim SNTP-Protokoll wird die Zeit im gleichen Format wie beim NTP-Protokoll übertragen. Die SNTP-Spezifikation ist eine Teilmenge der NTP-Spezifikation. SNTP ist zu NTP kompatibel.

Das Zeitformat ist Total 64 Bit lang. Es werden 32 Bit für den Teil > 1 s und 32-Bit für den Sekundenbruchteil verwendet.

Man kann davon ausgehen, dass die Zeit vom NTP-Server zur PCD mit einer Genauigkeit von der Grössenordnung einer Mikrosekunde ankommt. Die Laufzeit der Abfrage wird durchs Protokoll kompensiert. Diese Genauigkeit kann von der PCD-Steuerung nicht vollständig umgesetzt werden. In der PCD hat es 2 Uhren eine Hardware-Uhr und eine Software-Uhr.

Die Hardware-Uhr auch Realtime-Clock genannt, läuft auch mit Batterie wenn die PCD nicht an eine Spannungsquelle angeschlossen ist. Sie hat nur eine Auflösung von einer Sekunde. Bei solchen Bauteilen ist die Genauigkeit beschränkt. Es kann Abweichungen von mehreren Minuten pro Monat geben.

Die PCD hat auch eine Software-Uhr. Sie wurde implementiert, damit man auch eine Zeit von einigen ms messen kann. Ein weiterer Grund ist, dass das Lesen der Realtime-Clock mehr CPU-Zeit benötigt. Der Takt der Software-Uhr ist abhängig vom Oszillator der den Mikroprozessortakt angibt.

Durch Vergleich der beiden Uhren über längere Zeit berechnet die PCD einen Korrekturfaktor. Er wird dauernd optimiert. Mit diesem Wert wird die Zeit der Hardwareuhr stetig angepasst. (Sprunghafte Änderungen werden vermieden. Die Abweichungen pendeln um den Idealwert)

Wenn der SNTP-Dienst aktiviert wird und die Abweichung (parametrierbar: 100 ms bis 3600 s) der Software-Uhr von der genauen Uhrzeit, die übers Internet erhalten wurde überschritten wurde, so wird die Uhrzeit sprunghaft angepasst. Dies ist für Anwendungen die eine sehr genaue Protokollierung von Ereignissen in einem Netzwerk von mehreren PCD's benötigen unter Umständen nicht ideal.

Schema:



#### 3.1.2. Benötigtes Material

- 1 Laptop / PC mit PG5 Utilities

- Für diese Anwendung wird 1 PCD benötigt

Es können folgende Typen verwendet werden: PCD3.M3120, PCD3.M3330, PCD3.M5540, PCDM6340, PCDM6540, PCD2.M5540, PCD3.M21x30V6 oder PCD3.M2330A4Tx

Für den Test wurde folgendes Material benutzt:

- PCD3.M5540

- Laptop HP Compaq 6715b

### 3.1.3. Anwendungsmöglichkeiten

Dank dieser neuen Funktion ist es möglich Ereignisse auf die Sekunde genau zu protokollieren. Auch wenn man die Zeit auf einem Informationssystem nur als zusätzliches Element anzeigen will, ist es störend, dass die Zeit nicht korrekt auf die Sekunde angezeigt wird, wenn man sie nicht ab und zu von Hand neu einstellt. Mit der SNTP-Funktion hat man die Möglichkeit kostenlos (abgesehen von allfälligen Kommunikationskosten) die Uhrzeit auf einem öffentlich zugänglichen NTP-Server abzufragen.

Die SNTP Funktion kann sowohl über Ethernet, als auch über eine PPP / GPRS-Verbindungen genutzt werden. (siehe Kapitel2)

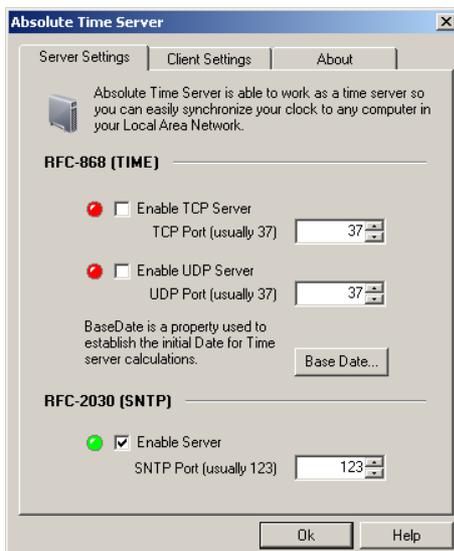
### 3.1.4. Konfiguration und Inbetriebnahme

A) Test Time Server auf dem PC

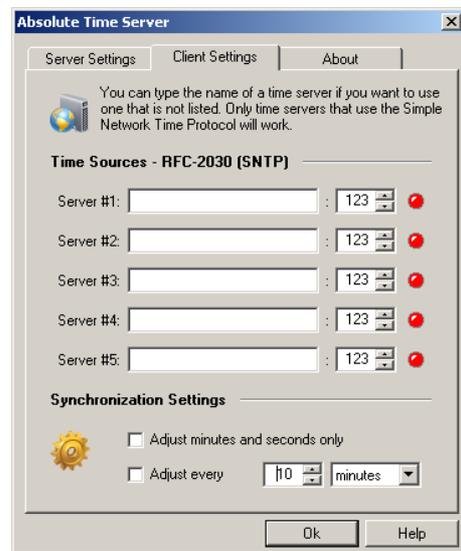
Eine Möglichkeit zum Testen ist die Installation einer Time-Server Software auf dem Windows-PC. Beim dieser Beispielkonfiguration wurde beim PC die IP-Adresse: 192.168.120.251 (Subnetm. 255.255.255.0)

Bei der PCD muss eine Adresse im gleichen Subnet eingestellt werden. (z.B 192.168.120.10)

Als einfaches Testtool ist die Software Absolute Time Server empfehlenswert. (Downloadmöglichkeit unter <http://www.adjustime.com>)



SNTP Server aktivieren



SNTP Client-Funktion deaktivieren (empfehlenswert)

Es handelt sich um eine Shareware. Wenn man sie nicht kaufen will, kann man sie zumindest einen Monat lang für Testzwecke installieren. Der Vorteil bei der lokalen Installation eines NTP-Servers ist, dass man nicht auf eine Infrastruktur angewiesen ist, die unter Umständen nicht überall vorhanden ist. (Z.B ADSL-Zugang oder NTP-Server im eigenen LAN)

Man muss darauf achten, dass der Windows-Firewall oder ein anderer verwendeter Software-Firewall richtig eingestellt ist. Es ist einfacher den Firewall-Dienst komplett zu stoppen. Das Risiko dabei ist klein, da man nur das LAN verwendet. Am Ende des Tests muss der Dienst wieder aktiviert werden.

B) Konfiguration PCD

Im Saia Device Configurator werden folgende Einstellungen vorgenommen.  
 Wenn man das vorhandene Beispielprojekt für die PCD3M5540 verwendet, sind alle Einstellungen im Device Configurator bereits korrekt eingestellt.

The image shows two screenshots of the Saia Device Configurator interface. The top screenshot displays the 'Ethernet Protocols' and 'Memory Slots' sections. The bottom screenshot shows the 'Onboard Communications' and 'Onboard I/O Slots' sections, along with a detailed view of the 'SNTP (Simple Network Time Protocol)' settings.

Section	Description
IP Transfer Protocols	FTP, HTTP Direct Protocols, ODM.
IP Protocols	DHCP, DNS, SNTP, SNMP protocols

Slot	Type	Description
M1		
M2		

Type	Description
RS-485/S-Net	RS-485 port for Profi-S-Bus or general-purpose communications (D-Sub #2).
USB	Universal Serial Bus port, PGU or general-purpose.
RS-232/PGU	RS-232, PGU or general-purpose serial port (D-Sub #1).
RS-485	RS-485 port for general-purpose communications (Terminal block).
Ethernet	Ethernet port.

Slot	Type	Description
Slot 0		
Slot 1		
Slot 2		

Parameter	Value
Automatic Gateway IP Setting	No
Automatic DNS IP Setting	No
DNS Mode	Fixed value
DHCP Server IP to Reject 1	0.0.0.0
DHCP Server IP to Reject 2	0.0.0.0
Host Name	
Fully Qualified Domain Name	
<b>DNS Client Protocol</b>	
DNS Client Enabled	No
DHCP Information Enabled	No
Primary DNS Server IP Address	0.0.0.0
Secondary DNS Server IP Address	0.0.0.0
Response Timeout [ms]	1000
<b>SNTP (Simple Network Time Protocol)</b>	
SNTP Enabled	Yes
SNTP Mode	Use NTP server list
Immediate Start Enabled	Yes
Start Delay [s]	5
Clock Regulation With SNTP	No
Maximum Delta Clock [ms]	2000
Interval Request Clock [s]	10
Server NTP 1	192.168.120.251
Server NTP 2	
Server NTP 3	
<b>SNMP (Simple Network Management Protocol)</b>	

→ Für weitergehende Informationen zu den einzelnen Parametern siehe **SNTP User Manual**

Zum Testen, ob das Korrigieren der Uhrzeit funktioniert, kann man die Zeit der PCD mit der Clock-Funktion des PG5-Online-Konfigurators absichtlich falsch einstellen. Nach maximal 10 Sekunden sollte wieder die richtige Zeit eingestellt sein, sofern die eingestellte Abweichung grösser ist, als der Wert der im Parameter **ClockDelta** eingestellt wurde.

### 3.1.5. Bemerkungen

Mit der Standardeinstellung, findet ca. alle 10 (+/- 0.5) Sekunden eine Abfrage mit dem SNTP-Protokoll statt.

Es kann davon ausgegangen werden, dass bei der Wahl von ClockDelta = 100 ms, die Genauigkeit der Uhr von +/- 1/10 Sekunde erreicht werden kann. Bessere Genauigkeiten können nicht garantiert werden.

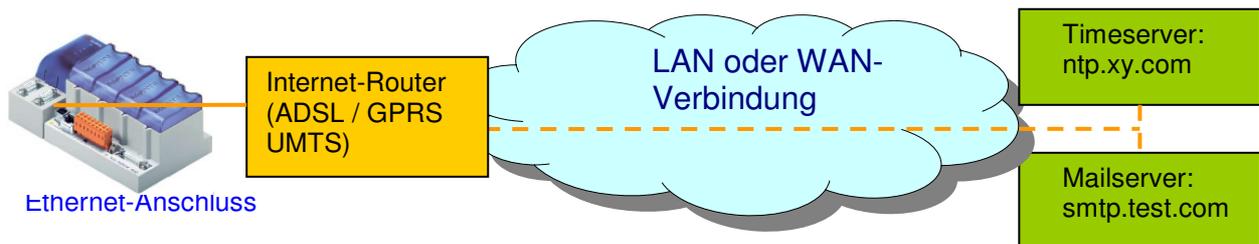
## 4. Anwendungen mit DNS / (DHCP)-Funktion

### 4.1. Anwendungsbeispiel DNS-Funktion

#### 4.1.1. Beschreibung

Wenn eine PCD mit einer anderen PCD oder mit einem Server die sich im Internet befindet kommunizieren wollte, so konnte man bisher nicht direkt mit dem Domain-Namen arbeiten. Man musste vorher mit einem PC und den Tools "nslookup" oder "ping" die entsprechende IP-Adresse ausfindig machen. Diese wurde dem User-Programm als Parameter übergeben. Falls die zu einem Namen gehörende Adresse einmal ändert, hat die PCD keine Möglichkeit dies festzustellen. Eine einwandfreie Kommunikation wäre nicht mehr möglich gewesen. Bei der neuen Firmware kann man die Auflösung der IP-Adresse anhand des Domain Namens zur Laufzeit mit dem Userprogramm durchführen. Beim Versenden einer Email führt das Programm vorgängig die CSF-Funktion Query by Name aus. Die IP-Adresse wird beim Aufruf der CSF für das Senden des Emails by Reference übergeben.

Schema:



#### 4.1.2. Benötigtes Material

- 1 Laptop / PC mit PG5 Utilities
- Für diese Anwendung wird 1 PCD benötigt  
Es können folgende Typen verwendet werden: PCD3.M3120, PCD3.M3330, PCD3.M5540, PCDM6340, PCDM6540, PCD2.M5540, PCD3.M2130V6 oder PCD3.M2330A4Tx
- 1 Router mit Verbindung zum Internet

Für den Test wurde folgendes Material benutzt:

- PCD3.M5540
- Laptop HP Compaq 6715b
- ADSL Router mit DHCP-Funktion

#### 4.1.3. Anwendungsmöglichkeiten

Mit dieser Konfiguration kann man Emails versenden und dabei den Domainnamen des Mailservers anstelle der IP-Adresse verwenden. Mit dem gleichen Prinzip kann man auch mit einem SBUS-Slave kommunizieren, falls dieser einen DNS-Eintrag besitzt siehe auch Kapitel 5.

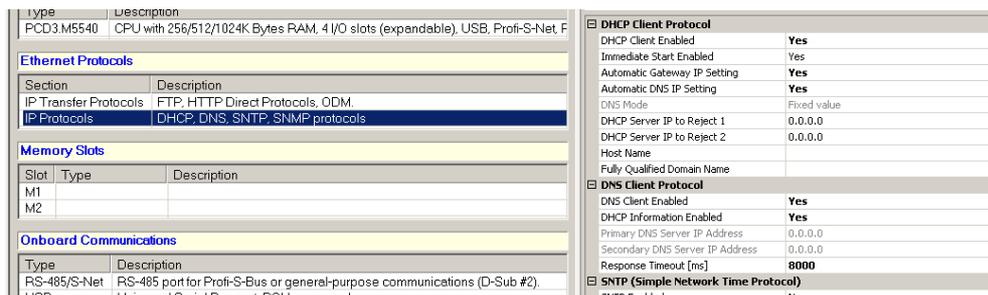
## 4.1.4. Konfiguration und Inbetriebnahme

Im Saia Device Configurator werden folgende Einstellungen vorgenommen. Wenn man das vorhandene Beispielprojekt für die PCD3M5540 verwendet, sind alle Einstellungen im Device Configurator bereits korrekt eingestellt.

Bei dieser Konfiguration wurde der DHCP-Client aktiviert. Durch die Auswahl von Automatic Gateway IP Setting und Automatic DNS IP Setting erreicht man, dass die PCD automatisch vom Router eine IP-Adresse, die Gateway-IP-Adresse sowie die DNS-Server-IP-Adressen erhält. Die Internet-Router, die man bei Vertragsabschluss von den Providern erhält, sind normalerweise so vorkonfiguriert, dass der DHCP-Server aktiviert ist und dieser Vorgang auf Anhieb funktioniert.

Hinweis:

Einige Kabel-Provider (z.B. Cablecom, ein Schweizer TV, Telefon und Internet Betreiber) stellen den Kunden Modems zur Verfügung die über einen Ethernet-Anschluss verfügen und dem angeschlossenen Gerät eine öffentliche Adresse via DHCP zuteilen. Wenn ein solches Gerät zusammen mit einer PCD Steuerung verwendet wird, sollte man bedenken, dass das Gerät (via FTP, HTTP, eventuell Ether-SBUS) auch via Internet erreicht werden kann. Es wird angeraten, ein Zusatzgerät mit NAT-Firewall Funktion zu verwenden, wie es in den meisten ADSL-Routern bereits eingebaut ist.



Beim PG5 Beispiel kann ein Email versendet werden. Im Gegensatz zu bisherigen Lösungen zum Emailversand mit der Saia PCD wird hier mit DNS-Auflösung gearbeitet. Die Mail-Server Adresse wird nicht als parametrierte IP-Adresse sondern als Domainname vorgegeben. Beim Beispiel wird mit der CSF Funktion QueryByName beim DNS-Server des Internetanbieters die IP-Adresse des konfigurierten Mailservernamens angefragt.

Vor dem Kompilieren müssen die Mail-Parameter (SMTP) für die Email-FBox konfiguriert werden. Es handelt sich um die Parameter:

Mail.ServerName,  
 Mail.username,  
 Mail.password,  
 Mail.sender  
 Mail.To1

Das Mail wird gesendet, indem man im Saia Debugger ein Impuls auf das Flag Mail.send gegeben wird lag. Im Watch Window oder mit Hilfe einer Probe kann man anschliessend beobachten, dass am Ausgang IPAddr der QueryIPName FBox die IP-Adresse des SMTP-Servers steht. Anschliessend erfolgt der Mailversand.

## Diagnosemöglichkeiten

Falls der Mailversand nicht auf Anhieb funktioniert kann man mit dem nachfolgenden CGI-Befehl kontrollieren, ob die PCD eine IP-Adresse mit DHCP erhalten hat. (Dafür muss man die Webconnect-Software auf dem Laptop starten, in PG5 2.0.x enthalten)

<http://localhost/48/cgi-bin/readVal.exe?SYS-DHCP,AssignedIPAddr>

Alternativ gibt es die Möglichkeit die IP-Adresse über den Befehl S.IPD.IPGetLocalConfig aus der IPLib.inc abzufragen. Der benötigte Programmteil muss allerdings noch hinzugefügt werden. (siehe FAQ 100952 bei <http://www.sbc-support.ch/faq>)

### 4.1.5. Bemerkungen

Es ist grundsätzlich empfehlenswert, anstelle der IP-Adresse mit dem DNS-Namen zu arbeiten, was die Kommunikation mit öffentlichen Servern betrifft. Zum Zeitpunkt der Erstellung des Programms kann man nicht sicher sein, ob die IP-Adresse des Servers (z.B Mailserver) nicht einmal ändern wird. Ausserdem wird oft auch mit Lastverteilungsmechanismen gearbeitet, die dazu führen, dass hinter einem Servernamen verschiedene IP-Adressen stehen können.

Durch die DNS-Client Funktion hat man neu auch die Möglichkeit mit Gegenstellen zu arbeiten, die über dynamische IP-Adressen verfügen und ihre aktuelle IP-Adresse mit dem entsprechenden Dienst bei DynDns.org registrieren.

Falls man sicher ist, dass die Gegenstelle immer die gleiche IP-Adresse hat z.B weil ein entsprechender Vertrag mit einem Provider für eine öffentliche, permanente IP-Adresse abgeschlossen wurde, bedeutet die Arbeit mit DNS-Registrierung ein Mehraufwand, der sich nur bei einem zukünftigen Wechsel des Providers lohnen würde.

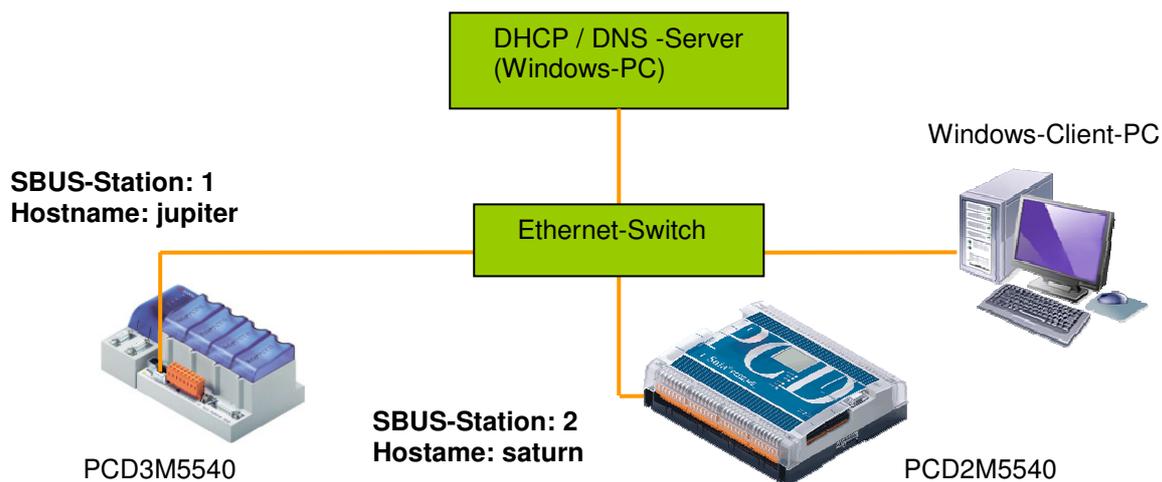
## 5. Anwendungen mit DHCP und DNS-Funktion im Lokalen Netzwerk

### 5.1. Anwendungsbeispiel DHCP und DNS-Funktion im LAN

#### 5.1.1. Beschreibung

Mit Hilfe der DHCP- und DNS Funktion kann man PG5 Projekte realisieren ohne für die Steuerungen konstante, vordefinierte IP-Adressen vorzusehen. Bei der Programmierung verwendet man Hostnamen anstelle von IP-Adressen. Durch ein Broadcast-Telegramm im Netzwerk bezieht die Steuerung die benötigten Informationen von einem DHCP-Server. Der DHCP-Server registriert den Client beim DNS-Server. Neben der IP-Adresse und der Netzwerkmaske enthält die PCD automatisch auch die Adresse vom Default-Gateway.

Schema:



#### 5.1.2. Anwendungsmöglichkeiten

Diese neue Funktion soll es vereinfachen PCD Steuerungen im LAN zu vernetzen. Es gibt verschiedene Serversysteme, die DHCP- und DNS-Serverdienste bereitstellen können. Bekannte Beispiele sind Server PC's mit Microsoft Windows Server oder Linux Betriebssystem. Dank dem Einsatz von DHCP- und DNS kann bei grossen Netzwerken der Administrationsaufwand reduziert werden.

Wenn DHCP- und DNS verwendet wird, kann ein Softwareprojekt mit dem gleichen Netzwerkkonzept an unterschiedlichen Standorten eingesetzt werden, ohne dass der Programmcode, der für den Datenaustausch übers Netzwerk zuständig ist, angepasst werden muss. Der Hostname der Steuerung wird im Saia Device Configurator eingetragen. Die Konfiguration der IP-Adressen wird anschliessend mit dem DHCP / DNS-Server ausgehandelt.

### 5.1.3. Benötigtes Material

- 1 Laptop / PC mit PG5 Utilities
  - 1 separater Windows PC mit DHCP und DNS Server: Software Dual Server
  - Für diese Anwendung werden 2 PCD's benötigt.
- Es können folgende Typen verwendet werden: PCD3.M3120, PCD3.M3330, PCD3.M5540, PCDM6340, PCDM6540, PCD2.M5540, PCD3.M2130V6 oder PCD3.M2330A4Tx

Für den Test wurde folgendes Material benutzt:

- 1 PCD3.M5540
- 1 PCD2.M5540
- Laptop HP Compaq 6715b
- Separater Windows PC mit DHCP und DNS Server: Software Dual Server

(Es kann auch nur mit einem PC gearbeitet werden. Der Nachteil dabei ist, dass man keinen Windows Client-PC zum Testen zur Verfügung hat)

### 5.1.4. Konfiguration und Inbetriebnahme

#### A) Vorbereitung der PCD's

Im Saia Device Configurator werden folgende Einstellungen vorgenommen. Wenn man das vorhandene Beispielprojekt verwendet, sind alle Einstellungen im Device Configurator bereits korrekt eingestellt.

Die PCD3 wird entsprechend dem folgenden Printscreen konfiguriert:

Ethernet Protocols	
Section	Description
IP Transfer Protocols	FTP, HTTP Direct Protocols, ODM.
IP Protocols	DHCP, DNS, SNTP, SNMP protocols.

Memory Slots		
Slot	Type	Description
M1		
M2		

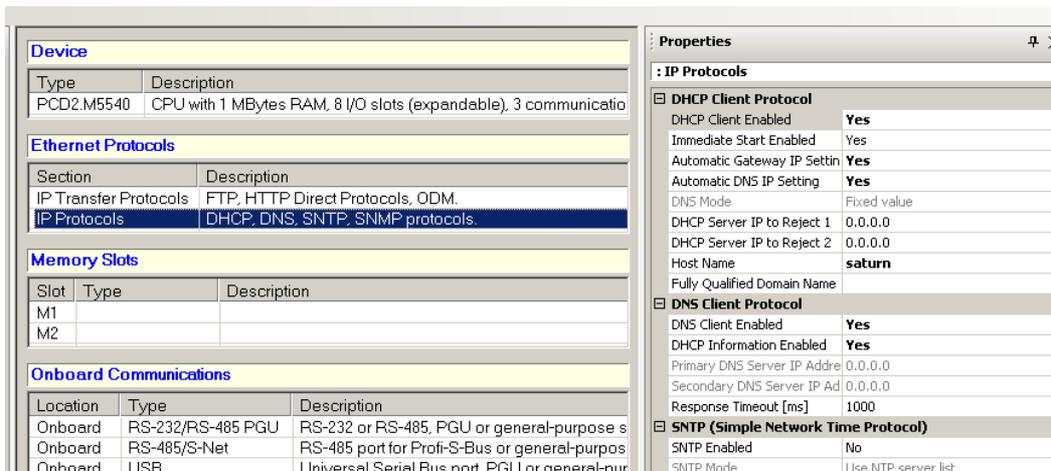
  

Onboard Communications	
Type	Description
RS-422/RS-485	RS-422/RS-485 port for general-purpose communication
USB	Universal Serial Bus port, PGU or general-purpose.
RS-232/PGU	RS-232, PGU or general-purpose serial port (D-Sub #1).
RS-485/S-Net	RS-485 port for Profi-S-Bus or general-purpose commun
Ethernet	Ethernet port.

Immediate Start Enabled	Yes
Automatic Gateway IP Setting	<b>Yes</b>
Automatic DNS IP Setting	<b>Yes</b>
DNS Mode	Fixed value
DHCP Server IP to Reject 1	0.0.0.0
DHCP Server IP to Reject 2	0.0.0.0
Host Name	<b>jupiter</b>
Fully Qualified Domain Name	
<b>DNS Client Protocol</b>	
DNS Client Enabled	<b>Yes</b>
DHCP Information Enabled	<b>Yes</b>
Primary DNS Server IP Address	0.0.0.0
Secondary DNS Server IP Address	0.0.0.0
Response Timeout [ms]	1000
<b>SNTP (Simple Network Time Protocol)</b>	
SNTP Enabled	No
SNTP Mode	Use NTP server list
Immediate Start Enabled	No
Start Delay [s]	0
Clock Synchronization with SNTP	No

Die PCD2 wird entsprechend dem folgenden Printscreen konfiguriert:



Die unterschiedlichen Hostnamen und SBUS-Adressen. (Auch der Devicetype ist bei diesem Beispiel unterschiedlich)

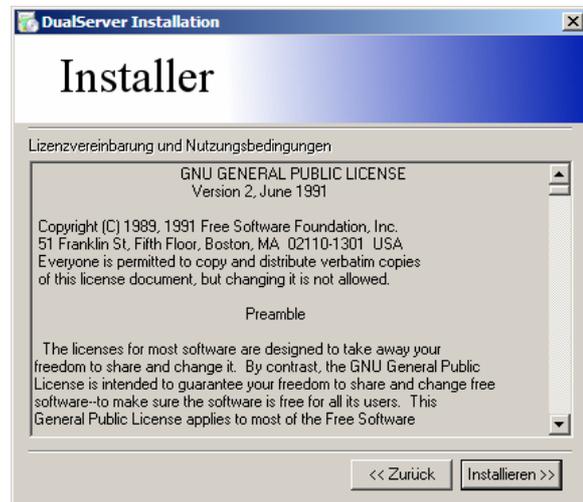
Damit der DHCP-Client aktiviert wird, ist es wichtig, dass man bei den Etherneteinstellungen TCP/IP Enabled „NO“ einstellt.

Als nächstes muss das vorhandene Beispielprojekt auf die Steuerungen geladen werden.

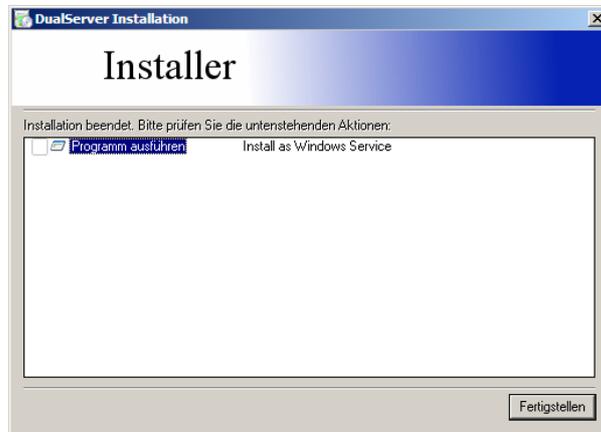
## B) Konfiguration DHCP/DNS Server auf dem Windows PC

Um die DHCP/ DNS Testserver Software zu installieren muss wie folgt vorgegangen werden.

- DualserverInstallerV6.40.exe auf einem PC mit Windows XP Betriebssystem installieren.



- Soll die Software nur provisorisch installiert werden, empfiehlt es sich nicht den Dienst zu installieren. Die Checkbox darf in diesem Fall nicht ausgewählt sein. Anschliessend auf Fertigstellen klicken.



- DualServer.ini im Installationsverzeichnis mit dem ini-File im Zipfile ersetzen.

Dadurch werden folgende Einstellungen vorgenommen:

Domainname: saiatest.net

Für die PCD wird folgende Gateway (Router) Adresse geliefert:

192.168.120.220

Der DHCP Server verwendet den folgenden Bereich für die Vergabe der IP-Adressen:

DHCP\_Range=192.168.120.100-192.168.120.200

Für dieses Beispiel muss die LAN-Adresse des PC wie folgt eingestellt:

192.168.120.20  
255.255.255.0

- Man muss darauf achten, dass der Windows-Firewall oder ein anderer verwendeter Software-Firewall richtig eingestellt ist. Es ist einfacher den Firewall-Dienst komplett zu stoppen. Das Risiko dabei ist klein, da man nur das LAN verwendet. Am Ende des Tests darf man nicht vergessen den Dienst wieder zu aktivieren.
- Durch den Aufruf **Programme -> Dualserver -> Run stand alone** wird der DHCP/ DNS-Server gestartet.

### C) Funktion des Programms / Diagnosemöglichkeiten

Im Kommandofenster des Servers kann man sehen, wenn die Clients ihre Adressen anfordern oder wenn mit einem DNS Request der Name einer Partnersteuerung aufgelöst werden muss.

Als weitere Kontrollmöglichkeit kann man durch Aufruf von „**Programme -> Dualserver -> View lease status**“ im Browser anzeigen lassen, welche Geräte eine Adresse bekommen haben und mit welchem Namen sie registriert wurden.

Der PC oder die PCD's, die eine IP-Adresse erhalten haben können mit PING oder den entsprechenden Clientprogrammen (Internetexplorer, Filezilla etc.) wie folgt erreicht werden.

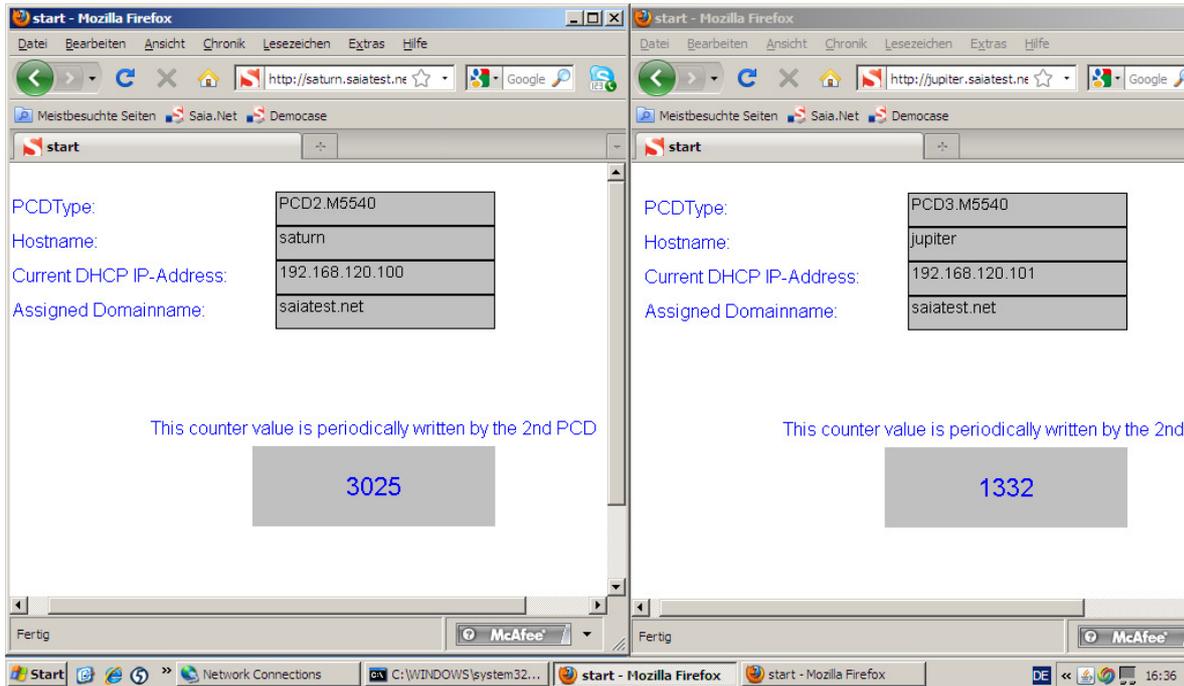
**PING [name].saiatest.net**

Die Beispielprogramme auf den beiden PCD's schreiben sich gegenseitig einen Zählerwert ins Register 100. Dieser Wert wird jede Sekunde erhöht.  
Auf den Steuerungen gibt es jeweils ein Webprojekt, das mit dem Windows-Client aufgerufen werden kann.

Dazu gibt man ein:  
<http://saturn.saiatest.net/start.html> (PCD2)

<http://jupiter.saiatest.net/start.html> (PCD3)

Auf der Webseite wird jeweils das Register 100 angezeigt, das von der anderen Steuerung verändert wird. Man findet auch den PCDTyp und die aktuelle DHCP-IP-Adresse.



Wenn man die aktuelle IP-Adresse im Userprogramm abfragen möchte, gibt es die Möglichkeit diese über den Befehl S.IPD.IPGetLocalConfig aus der IPLib.inc abzufragen. Der benötigte Programmteil muss allerdings noch hinzugefügt werden. (siehe FAQ 100952 bei <http://www.sbc-support.ch/faq>)

## D) Nützliche Windows Diagnosefunktionen

### DNS cache eine Windows clients anzeigen

```
P:\>ipconfig /displaydns
```

#### Windows IP Configuration

```
1.0.0.127.in-addr.arpa
-----
Record Name . . . . . : 1.0.0.127.in-addr.arpa
Record Type . . . . . : 12
Time To Live . . . . . : 602204
Data Length . . . . . : 4
Section . . . . . : Answer
PTR Record . . . . . : localhost

ch02n100.saiatest.net
-----
Record Name . . . . . : ch02n100.saiatest.net
Record Type . . . . . : 1
Time To Live . . . . . : 35995
```

```
Data Length . . . . . : 4  
Section . . . . . : Answer  
A (Host) Record . . . : 192.168.120.107
```

```
pcd3m5540.saiatest.net  
-----  
Record Name . . . . . : pcd3m5540.saiatest.net  
Record Type . . . . . : 1  
Time To Live . . . . . : 35923  
Data Length . . . . . : 4  
Section . . . . . : Answer  
A (Host) Record . . . : 192.168.120.100
```

## Lokalen DNS-Cache löschen

Mit dem folgenden Befehl kann man unter einem Windows 2000/XP/Vista Betriebssystem den lokalen DNS-Cache leeren.

`"ipconfig /flushdns"`

Die bisherigen Tests mit der DHCP/DNS-Funktion mit SAIA PCD haben gezeigt, dass sich die Geräte gemäss den Spezifikationen verhalten. Die Leasetime, die im DHCP Server voreingestellt ist, wird von der PCD (Client) übernommen. Eine Leasetime von 3600 sec. bedeutet, das die PCD die Adresse nach dem Ablauf einer Stunde wieder verwerfen muss d.h. sie hat nicht mehr die Berechtigung mit dieser Adresse weiterzuarbeiten. Nach Ablauf der Hälfte der Leasetime muss der Client versuchen die Adresse zu erneuern. Für die DNS-Konfiguration gibt es ebenfalls Werte, die vom Server übernommen werden, diese bestimmen, wie lange die Einträge im Cache bleiben müssen, bevor die Steuerung erneut eine Anfrage zum DNS-Server senden muss.

## 5.1.5. Bemerkungen

Die Bedürfnisse bei der Konfiguration der Netzwerkeigenschaften von Steuerungen und Server sind vielfältig. Die Verwendung von DNS und DHCP ermöglicht es, auf dem ganzen Netzwerk anstelle von IP-Adressen mit Hostnamen zu arbeiten. Was die Anwendung DHCP betrifft, muss man eine PCD mit einem Server System vergleichen. Wir stellen einen integrierten HTTP- und FTP-Server bereit. In der Regel wird der Netzwerkadministrator für die PCD wie bei einem Mail- oder einem Applicationserver beim DHCP-Server eine IP-Adresse konstant reservieren. Dafür muss bei der Inbetriebnahme ein zusätzlicher zentraler Konfigurationsaufwand beim DHCP-Server gemacht werden. Wenn bei einer späteren Umbau des Netzwerks z.B die IP- und die Gateway-Adresse geändert werden müssen, weil man in einen anderen Raum umziehen muss, so ist man nicht mehr auf den Integrator des Steuerungssystems angewiesen. Diese Umstellung kann von der IT- oder Netzwerk-Abteilung selbst gelöst werden. Es besteht auch kein Risiko, dass die vorhandene Programmier-Software zum Konfigurieren der IP-Adresse nicht mehr kompatibel ist oder dass aus Versehen andere Parameter der Steuerung verändert werden könnten.

Wir verfügen nicht über eine umfangreiche IT-Testinfrastruktur. Unsere bisherigen Tests haben gezeigt, dass DHCP und DNS gemäss Standard implementiert wurden. Wir hatten nicht die Möglichkeit Tests mit einer grossen Zahl von verfügbaren DHCP/DNS-Server durchzuführen. Getestet wurden die Windowsversion von Dualserver und ein Windows Server mit DHCP- und DNS-Server.

## 6. Anwendungen mit SNMP-Funktion

### 6.1. Anwendungsbeispiel SNMP

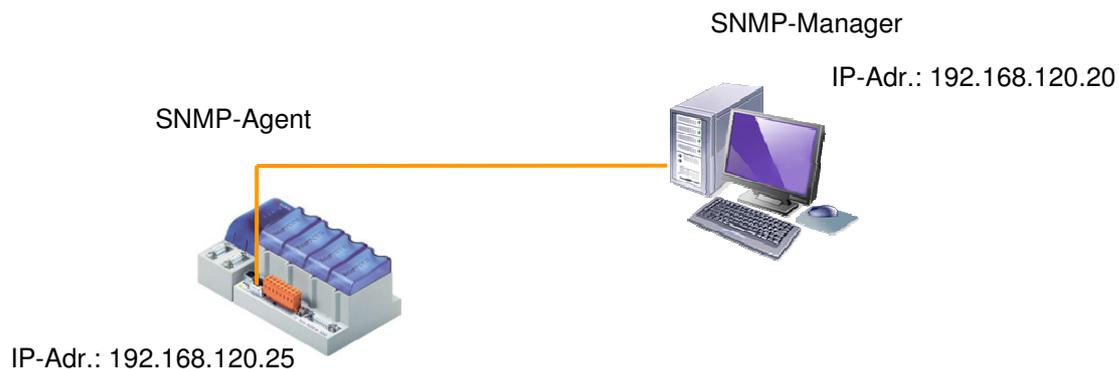
#### 6.1.1. Beschreibung

Das Simple Network Management Protocol (SNMP) wurde entwickelt, um Netzwerkelemente, wie Router, Server und Switches, von einer zentralen Station aus überwachen und steuern zu können. Der SNMP-Manager ist meistens eine Software, die auf einem Server läuft. Er überwacht und steuert die SNMP-Agenten. Dies können beliebige Geräte sein, die über das Netzwerk erreicht werden und SNMP unterstützen. Mit der neuen Firmware unterstützt die Saia PCD die SNMP-Agent Funktionalität. Es gibt folgende SNMP Versionen: v1, v2c, v3 (Sicherheitsmechanismus mit MD5 Authentifizierung, Verschlüsselung mit DES 56 Bit)

Der Standard v3 hat noch keine sehr grosse Verbreitung gefunden. Version v2c ist prinzipiell immer noch der aktuelle Standard. Die Saia PCD unterstützt die Version v2c.

Mit einer PCD und einem Windows PC mit Net-SNMP Tool sollen die Möglichkeiten der SNMP Implementation der Saia PCD gezeigt werden.

Schema:



#### 6.1.2. Anwendungsmöglichkeiten

Dank der Implementierung des SNMP-Protokolls in Saia PCD's kann der Kunde alle seine netzwerkfähigen Geräte: (Router, Server und auch Saia PCD's) auf der gleichen Managementplattform überwachen. SNMP wird von sehr vielen modernen Geräten unterstützt und kann als gemeinsame Schnittstelle für die Verwaltung und Konfiguration verwendet werden. Das Managementsystem kann verschiedene Informationen verknüpfen, die auf dem gesamten Netzwerk verfügbar sind.

Mit SNMP hat man Zugriff auf alle PCD Ressourcen. Es können Parameter abgefragt und verändert werden. Mit einem Konfigurationsfile wird festgelegt, welche Ressourcen gelesen und geschrieben werden können. Wenn die Steuerung den Modus für die Abarbeitung des Userprogramms ändert (Wechsel zwischen RUN / STOP / HALT), kann die PCD automatisch Traps senden. Man kann auch selber definieren, dass ein Messwert (z.B. eine Temperatur) beim Überschreiten eines bestimmten Werts einen Trap auslöst.

### 6.1.3. Benötigtes Material

- 1 Laptop / PC mit PG5 Utilities
  - Für diese Anwendung wird 1 PCD benötigt
- Es können folgende Typen verwendet werden: PCD3.M3120, PCD3.M3330, PCD3.M5540, PCDM6340, PCDM6540, PCD2.M5540, PCD3.M2130V6 oder PCD3.M2330A4Tx

Für den Test wurde folgendes Material benutzt:

- PCD3.M5540
- Laptop HP Compaq 6715b
- Net-SNMP Client Software

### 6.1.4. Konfiguration und Inbetriebnahme

Bei den Beispielen kommt immer eine lange Folge von Zahlen, die mit Punkten getrennt sind vor: Diese Nummer fängt stets wie folgt an: 1.3.6.1.4.1.31977... . Wenn man das SNMP Protokoll zusammen mit einer Saia PCD verwenden will, muss die Adressierung zwingend mit diesen 7 Zahlen beginnen. Die ersten 6 Zahlen (1.3.6.1.4.1) stehen für "iso.org.dod.internet.private.enterprise". Die Zahl 31977 ist die bei IANA registrierte Nummer für Produkte der Saia Burgess Controls AG Diese Nummer ist in der in der Firmware fest eingestellt und kann nicht geändert werden. Das Saia.mib-File setzt diese Nummern-Hierarchie, die mit 1.3.6.1.4.1.31977 anfängt in eine Struktur von Text Definitionen um. Diese beginnen mit: SaiaPCDClassic::.... . Text Definitionen und Zahlen können gemischt werden.

#### A) Konfiguration PCD

Im Saia Device Configurator werden die Einstellungen vorgenommen.

Wenn man das vorhandene Beispielprojekt für die PCD3M5540 verwendet, sind alle Einstellungen im Device Configurator bereits korrekt eingestellt.

Bei dieser Konfiguration handelt es sich um eine Grundkonfiguration, die nur einen lesenden Zugriff auf die Steuerung erlaubt.

The screenshot displays the configuration interface for a Saia PCD. The left pane shows hardware details for PCD3.M5540, including Ethernet protocols, memory slots, and on-board I/O slots. The right pane shows network protocol settings:

- DHCP Client Protocol:** DHCP Client Enabled (No), Automatic Gateway IP Setting (No), Automatic DNS IP Setting (No), DNS Mode (Fixed value), DHCP Server IP to Reject 1 (0.0.0.0), DHCP Server IP to Reject 2 (0.0.0.0), Host Name, Fully Qualified Domain Name.
- DNS Client Protocol:** DNS Client Enabled (No), DHCP Information Enabled (No), Primary DNS Server IP Address (0.0.0.0), Secondary DNS Server IP Address (0.0.0.0), Response Timeout [ms] (1000).
- SNTP (Simple Network Time Protocol):** SNTP Enabled (Yes), SNTP Mode (Use NTP server list), Immediate Start Enabled (No), Start Delay [s] (5), Clock Regulation With SNTP (No), Maximum Delta Clock [ms] (2000), Interval Request Clock [s] (10), Server NTP 1, Server NTP 2.
- SNMP (Simple Network Management Protocol):** SNMP Enable (Yes), sysContact Message (Saia Burgess Controls AG), sysLocation Message (CH-3280 Murten), Life Trap Interval [ms] (0), Trap 1 Port Number (0), Trap 1 IP Address (192.168.120.20), Trap 2 Port Number (0), Trap 2 IP Address (0.0.0.0), + Advanced Parameters (No).

At the bottom of the right pane, there is a note: "Trap 1 IP Address: Up to three SNMP trap receiver can be defined. The IP address defines the IP address of the receiver..."

## B) PC Konfiguration

Installation der Net-SNMP Software

[http://downloads.sourceforge.net/net-snmp/net-snmp-5.4.2.1-ssl-1.win32.exe?use\\_mirror=switch](http://downloads.sourceforge.net/net-snmp/net-snmp-5.4.2.1-ssl-1.win32.exe?use_mirror=switch)

Als nächstes muss das File SaiaMIB.mib in den Ordner  
<Program Files>\net-snmp\share\snmp\mibs/ kopiert werden

Für die nächsten Übungen muss der PC mit einem Ethernet Cross-Cable mit dem PC verbunden werden. Damit man Traps auf dem PC empfangen kann, muss auf dem PC die IP-Adresse 192.168.120.20 eingestellt werden.

Man muss darauf achten, dass der Windows-Firewall oder ein anderer verwendeter Software-Firewall richtig eingestellt ist. Es ist einfacher den Firewall-Dienst komplett zu stoppen. Das Risiko dabei ist klein, da man nur das LAN verwendet. Am Ende des Tests darf man nicht vergessen den Dienst wieder zu aktivieren.

## C) Beispiele Snmpget Funktion

Wert eines Registers abfragen:

```
C:\Program Files\net-snmp\snmpget -v2c -c public -m ALL 192.168.120.25
SaiaPCDClassic::regMedia.1.3.2
  → SaiaPCDClassic::regValueInt.2 = INTEGER: 0
```

Anstelle der Notation mit Textdefinition kann auch die Notation `snmpget -v2c -c public -m ALL 192.168.120.25 1.3.6.1.4.1.31977.4.3.1.3.2` verwendet werden.

Nun kann mit dem Saia Online Debugger den Wert des Registers 2 verändern und den snmpget Befehl erneut durchführen

Run / Stop Switch abfragen:

Position Run

```
C:\Program Files\net-snmp\snmpget -v2c -c public -m ALL 192.168.120.25
SaiaPCDClassic::pcdSwitchState.0
  → SaiaPCDClassic::pcdSwitchState.0 = INTEGER: 1
```

Position Stop

```
C:\Program Files\net-snmp\snmpget -v2c -c public -m ALL 192.168.120.25
SaiaPCDClassic::pcdSwitchState.0
  → SaiaPCDClassic::pcdSwitchState.0 = INTEGER: 0
```

Weitere Beispiele für snmpget Abfragen:

- Inputs or Outputs

z.B. `SaiaPCDClassic::ioMedia.1.2.2` gibt den Wert von Input 2 zurück

- Flags

z.B. `SaiaPCDClassic::flagMedia.1.2.63` gibt den Wert von Flag 63 zurück

- Timers

z.B. `SaiaPCDClassic::timerMedia.1.2.15` gibt den Wert von Timer 15 zurück

- Counters

z.B. `SaiaPCDClassic::counterMedia.1.2.55` gibt den Wert von Counter 55 zurück

- DB's

z.B. 1.3.6.1.4.1.31977.4.6.1.3.2.300 gibt einen 32 Bit signed Wert von DB 2, mit Offset 300 zurück.

## D) Beispiele Snmpset Funktion

Die SNMP Einstellungen müssen für dieses Beispiel angepasst werden. Mit den SNMP Standardeinstellungen ist kein Schreibzugriff auf die PCD erlaubt, d.h. die Medien Bereiche zum Schreiben sind deaktiviert.

Wenn man das vorhandene Beispielprojekt für die PCD3M5540 verwendet, sind alle Einstellungen im Device Configurator bereits korrekt eingestellt.

Beim diesem Beispiel wurde auch für den Parameter Write community ein anderer Wert eingestellt (saia1234). Dies ist ein Schutz gegen den unberechtigten Schreibzugriff. Man muss jedoch bedenken, dass diese Passwörter ohne Verschlüsselung übers Netzwerk geschickt werden.

Wert eines Registers setzen:

```
C:\Program Files\net-snmp>snmpset -v2c -c saia1234 -m ALL 192.168.120.25
SaiaPCDClassic::regMedia.1.3.15 i 123
  → SaiaPCDClassic::regValueInt.15 = INTEGER: 123
```

```
C:\Program Files\net-snmp>snmpset -v2c -c saia1234 -m ALL 192.168.120.25
SaiaPCDClassic::regValueInt.12 i 56
  → SaiaPCDClassic::regValueInt.123 = INTEGER: 123
```

Zustand eines Flags ändern:

Flag 15 setzen

```
C:\Program Files\net-snmp>snmpset -v2c -c saia1234 -m ALL 192.168.120.25
SaiaPCDClassic::flagValue.15 i 1
```

Flag 15 rücksetzen

```
C:\Program Files\net-snmp>snmpset -v2c -c saia1234 -m ALL 192.168.120.25
SaiaPCDClassic::flagValue.15 i 0
```

Output 17 setzen:

```
C:\Program Files\net-snmp>snmpset -v2c -c saia1234 -m ALL 192.168.120.25
SaiaPCDClassic::ioValue.17 i 1
```

Output 17 rücksetzen:

```
C:\Program Files\net-snmp>snmpset -v2c -c saia1234 -m ALL 192.168.120.25
SaiaPCDClassic::ioValue.17 i 0
```

Anstelle der Notation mit Textdefinition kann auch die Notation `snmpset -v2c -c saia1234 -m ALL 192.168.120.25 1.3.6.1.4.1.31977.4.3.1.3.15 i 12345` verwendet werden. Diese Notation kann mit allen SNMP-Management Tools verwendet werden.

Wenn man eine Software verwenden will, bei der sich die Saia MIB nicht importieren lässt, muss man zwingend diese Syntax verwenden.

## E) Beispiele Snmp Trap Funktion

Einige wichtige Traps sendet die Firmware auch ohne Userprogramm. Wenn der Schalter Run/Stop umgeschaltet wird, wird eine Meldung zu den im Device Configurator eingestellten Trap IP-Adressen (1-3) gesendet.

Es ist auch möglich Traps mit Hilfe von CSF-Befehlen zu generieren. Es gibt CSF-Funktionen, die mit den im Device Configurator eingestellten Ziel-IP-Adressen arbeiten. Andere CSF-Funktionen erlauben es die IP-Adresse frei zu konfigurieren.

Die Device-Konfigurator Einstellung vom vorherigen Beispiel ermöglicht es automatisch Traps zu senden, wenn der Schalter RUN/STOP Schalter der PCD3.M5540 von RUN -> STOP gelegt wird. Es wird auch wieder ein Trap gesendet, wenn der Schalter zurück in den ursprünglichen Zustand gelegt wird.

Um zu sehen, wie man Traps mit Hilfe des Userprogramms generiert, lädt man das TrapDemoExample (Beispiel 6.1.4E) auf die PCD.

Durch setzen der folgenden Flags kann man die zur Verfügung stehenden CSF Funktionen testen:

Flag 1: Trap with OID-Reference to Register

Flag 2: Trap with OID-Reference to Flag

Flag 3: Trap with OID-Reference to Register 100. With embedded message (\$R0100)

Flag 4: Trap with OID-Reference to Register (wie Bsp 2, IP-Adresse in Source-code)

Flag 5: Trap with OID-Reference to Flag 10. With embedded message (\$ Flag 10-17).

Mit Hilfe von Wireshark, kann man überprüfen, ob die Traps tatsächlich gesendet werden. Wireshark kann das SNMP-Protokoll interpretieren. Eine andere Möglichkeit, den Empfang von Traps anzuzeigen, ist die Installation der Software IReasoning MIB Browser Personal Edition (<http://www.ireasoning.com/>). Im Menu Tool steht die Funktion Trap Receiver zur Verfügung, mit dieser Funktion kann man die empfangenen Traps anzeigen lassen. Bei einem vollwertigen Managementsystem wird oft auch der trap community string überprüft. Falls dieser nicht übereinstimmt, werden die Traps ignoriert.

### 6.1.5. Bemerkungen

Die Saia PCD hat die SNMP Agent Funktionalität. Es wurde die MIB II und eine Saia.MIB integriert. Es gibt eine grosse Anzahl Softwareprodukte auf dem Markt, die über die SNMP Manager-Funktion verfügen. Es gibt Tools, die Kommandozeilen orientiert sind, sowie kleine Testtools mit GUI. Es existieren auch umfangreiche und meistens recht kostspielige Softwareprodukte. Viele IT-Abteilungen mit grösseren Netzwerken, Server und PCD's benutzen eine leistungsfähige Managementsoftware. Diese Software enthält die SNMP-Funktion zusammen mit anderen Funktionen, die dazu dienen, die Verfügbarkeit der Anlagen zu erhöhen. Eine grosse Anzahl dieser Produkte kann ein MIB-File wie das Saia.mib-File importieren. Unsere bisherigen Tests haben gezeigt, dass SNMP Agent Funktion gemäss dem Standard implementiert wurde. Leider verfügen wir nicht über die Möglichkeit, Tests mit einer grossen Anzahl der verfügbaren SNMP-Management Tools durchzuführen. Getestet wurden die Windowsversion des Net-Snmp Tools und die freie Version der IReasoning MIB Browsing Software.