

WLAN
WLAN

Ethernet
Ethernet

GPRS
GPRS

Virtueller COM-Port

(Version 2.7)

Copyright © November 05 INSYS MICROELECTRONICS GmbH

Jede Vervielfältigung dieses Handbuchs, sowie der beiliegenden Software, ist nicht erlaubt. Alle Rechte an dieser Dokumentation und an den Geräten liegen bei INSYS MICROELECTRONICS GmbH Regensburg.

Einschränkungen der Gewährleistung

Dieses Handbuch enthält eine möglichst exakte Beschreibung. Bei der Zusammenstellung der Texte wurde mit größter Sorgfalt vorgegangen. Trotz aller Bemühungen können Fehler nie vollständig vermieden werden. Für die Richtigkeit des Inhalts kann daher keine Garantie übernommen werden. Für fehlerhafte Angaben und deren Folgen können wir weder eine juristische Verantwortung, noch irgendeine Haftung übernehmen. Für Verbesserungsvorschläge und Hinweise auf Fehler sind wir jederzeit dankbar.

Warenzeichen und Firmenzeichen

Die Verwendung eines hier nicht aufgeführten Waren- oder Firmenzeichens ist kein Hinweis auf die freie Verwendbarkeit desselben.

MNP ist ein eingetragenes Warenzeichen von Microcom, Inc.

IBM PC, AT, XT sind Warenzeichen von International Business Machine Corporation.

INSYS® ist ein eingetragenes Warenzeichen der INSYS MICROELECTRONICS GmbH.

Windows™ ist ein Warenzeichen von Microsoft Corporation.

Herausgeber:

INSYS MICROELECTRONICS GmbH

Waffnergasse 8

93047 Regensburg, Deutschland

Telefon: 0941/58692-0

Telefax: 0941/563471

E-Mail: insys@insys-tec.de

Internet: <http://www.insys-tec.de>

Technische Änderungen sowie Irrtum vorbehalten.

Version 2.7

Stand November 05

31-22-04.012 deutsch

1	Allgemein	2
1.1	History.....	2
1.2	Funktionsübersicht	3
2	Hinweise zur Benutzung.....	3
3	Installation und Einrichtung	4
3.1	Installation.....	4
3.2	Konfiguration des “Write Timeout”	6
3.3	Einrichten als Client	7
3.3.1	Wählen mit ATD.....	8
3.3.2	Automatischer Verbindungsaufbau	10
3.4	Einrichten als Server	12
3.4.1	Automatische Rufannahme (Grundeinstellung).....	13
3.4.2	Rufannahme mit ATA	15
4	Internetkommunikation im Serverbetrieb.....	16
4.1	NAT – Network Adress Translation	16
4.2	Firewall.....	17
4.3	Dynamische IP Adressen	18
5	Diagnosetools	19
5.1.1	TCPView	19
5.1.2	Ping	19
5.1.3	Netzwerkanalyse mit Ethereal	20
6	Begriffserklärung.....	21

1 Allgemein

Der virtuelle COM Port ist eine Software die es erlaubt, serielle Kommunikation durch eine IP-gestützte Kommunikation zu ersetzen, ohne dass die Anwendungssoftware verändert werden muss.

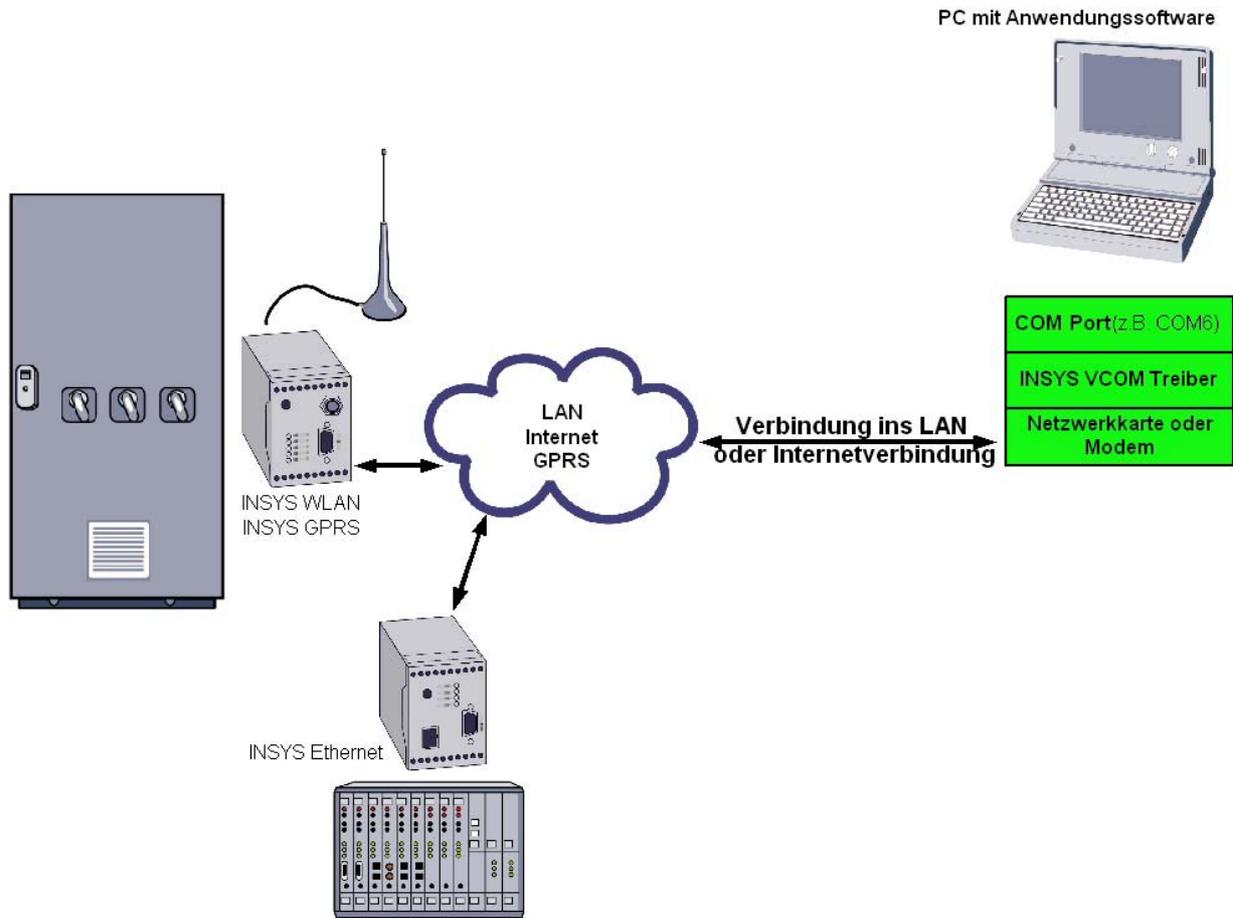
Die Software wird eingesetzt in Verbindung mit INSYS IP-Geräten wie

- INSYS Ethernet und i-modul Ethernet
- INSYS WLAN serial und i-modul WLAN serial
- INSYS GPRS 5.0 und i-modul GPRS 3.0

1.1 History

Treiber-Version	Zusätzliche Funktionen
V2.7	Funktion als Client und Server

1.2 Funktionsübersicht



Der virtuelle COM Port Treiber simuliert eine serielle Schnittstelle am PC. Die Daten, die an diese serielle Schnittstelle von einer beliebigen Anwendung aus gesendet werden, werden über eine TCP/IP Verbindung an ein verbundenes INSYS IP-Gerät weitergeleitet, als ob eine serielle Verbindung bestehen würde.

Damit können beliebige Strecken über vorhandene Netzwerke überbrückt werden, ohne dass vorhandene Systeme (Auslesesoftware, Konfigurationssoftware etc.) geändert werden müssen.

Die Applikation „sieht“ nur eine gewöhnliche Modemstrecke oder gar eine serielle Verbindung, kommuniziert aber über ein TCP/IP Netzwerk.

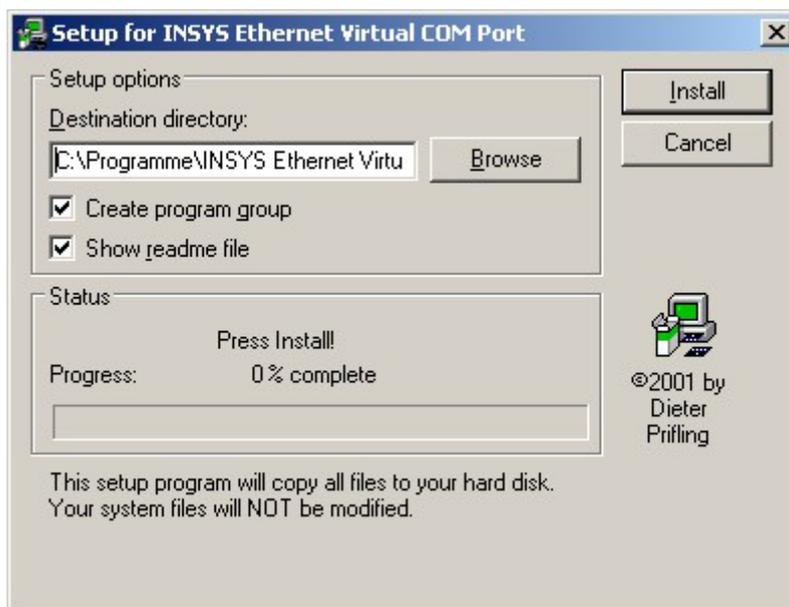
2 Hinweise zur Benutzung

In diesem Handbuch wird das Symbol  für besonders wichtige Hinweise verwendet. Weitere Hinweise sind entsprechend hervorgehoben.

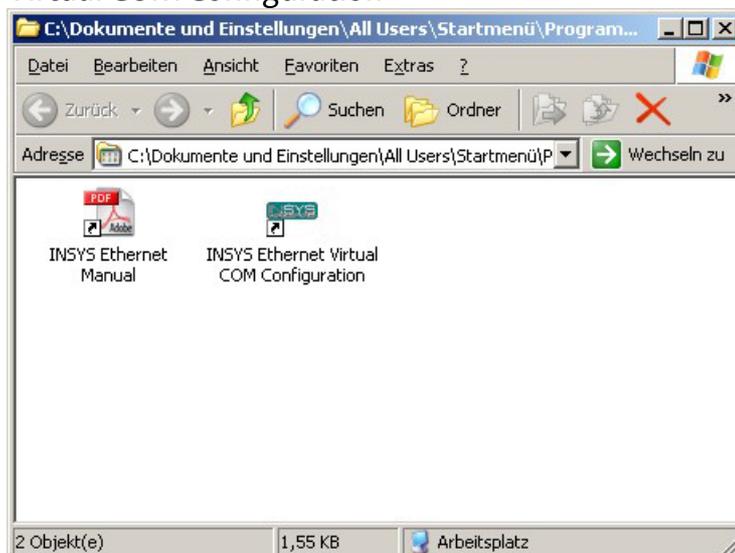
3 Installation und Einrichtung

3.1 Installation

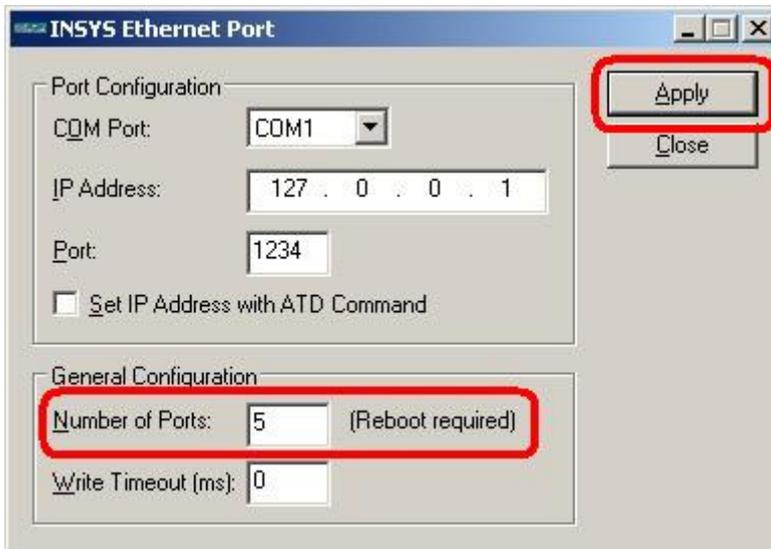
- Entpacken Sie bitte den Treiber in ein temporäres Verzeichnis.
- Prüfen Sie, ob sie auf dem Rechner mit lokalen Administratorrechten eingeloggt sind, anderenfalls schlägt die Installation fehl.
- Doppelklicken Sie auf die Datei „setup.exe“.
- Bestätigen Sie folgendes Fenster mit „Install“, vorher können Sie noch den Installationspfad anpassen.



- Starten Sie das Konfigurationsprogramm durch Doppelklick auf „INSYS Ethernet Virtual COM Configuration“



Stellen sie nun die Zahl an COM-Ports ein, bis zu der virtuelle COM Ports installiert werden sollen. Üblicherweise ist mindestens COM 1 schon von der seriellen Schnittstelle belegt, wollen Sie also beispielsweise vier virtuelle COM Ports installieren, dann setzen Sie die Zahl auf 5. Klicken sie anschließend auf die Schaltfläche „Apply“, um die Änderungen in der Registrierdatenbank zu speichern.



Die Software belegt so viele COM Ports, wie im Konfigurationsfenster angegeben sind. Greifen bereits andere Treiber auf diese Ports zu, so werden die Ports nicht belegt. Üblicherweise ist COM 1 die serielle Schnittstelle des Rechners, diese wird nicht belegt. Aber auch andere virtuelle Treiber (z.B. USB-seriell Wandler, Bluetoothadapter, etc.) können diese Ports belegen, sodass der VCOM-Treiber nicht darauf zugreifen kann. Es können je nach Startzeitpunkt der Treiber beim Booten andere virtuelle Treiber (z.B. USB-seriell Wandler) blockiert werden oder auch der hier beschriebene Treiber blockiert werden.

- Starten Sie ihren Rechner neu ...



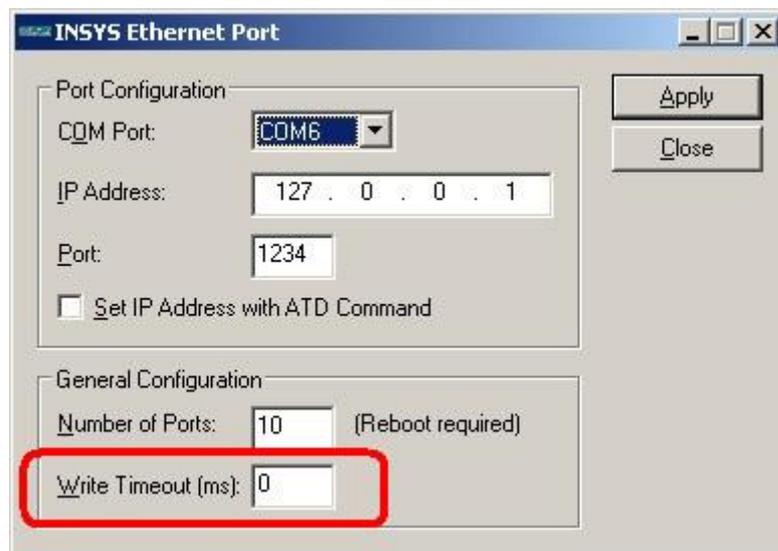
3.2 Konfiguration des “Write Timeout”

Die Daten, die der virtuelle COM Port auf der simulierten seriellen Schnittstelle erhält, werden über einen vorhandenen Internet- oder Netzwerkzugang übertragen.

Zur Übertragung von Daten über ein Netzwerk werden die Daten in TCP/IP Pakete „verpackt“. Diese Pakete enthalten neben den Daten selber auch noch weitere Informationen z.B. Zieladresse und Absenderadresse der Daten. Dazu werden ca. 40 Byte benötigt.

Also wird man, wenn man Zeichen immer einzeln über das Netzwerk schickt, für jedes übertragene Byte zusätzlich 40 Byte übertragen. Daher ist es sinnvoll, die Daten in Paketen zu sammeln.

Ein Paket wird versandt, wenn die Maximalzahl an Nutzdaten (typisch 1500 Bytes) vorliegen oder wenn eine gewisse Zeit abgelaufen ist.



Setzt man den Wert für Write Timeout z.B. auf 100 ms, so wartet der Treiber nach jedem Zeichen, das er von der Applikation erhält, 100 ms, bevor er das Paket verschickt. Erst wenn 100 ms lang keine neuen Daten ankommen, wird das Paket verschickt.

Besonders bei GPRS sollte wegen der volumenbasierten Abrechnung hier niemals 0 ms eingestellt werden, da sonst der Datenverkehr unnötig erhöht wird. Bei der Einstellung von 0 ms wird jedes Zeichen sofort in ein Paket verpackt.

Stellt man den Wert unnötig hoch, werden die Daten immer um den eingestellten Wert verzögert gesendet, was bei einigen Applikationen zu Problemen führen kann.

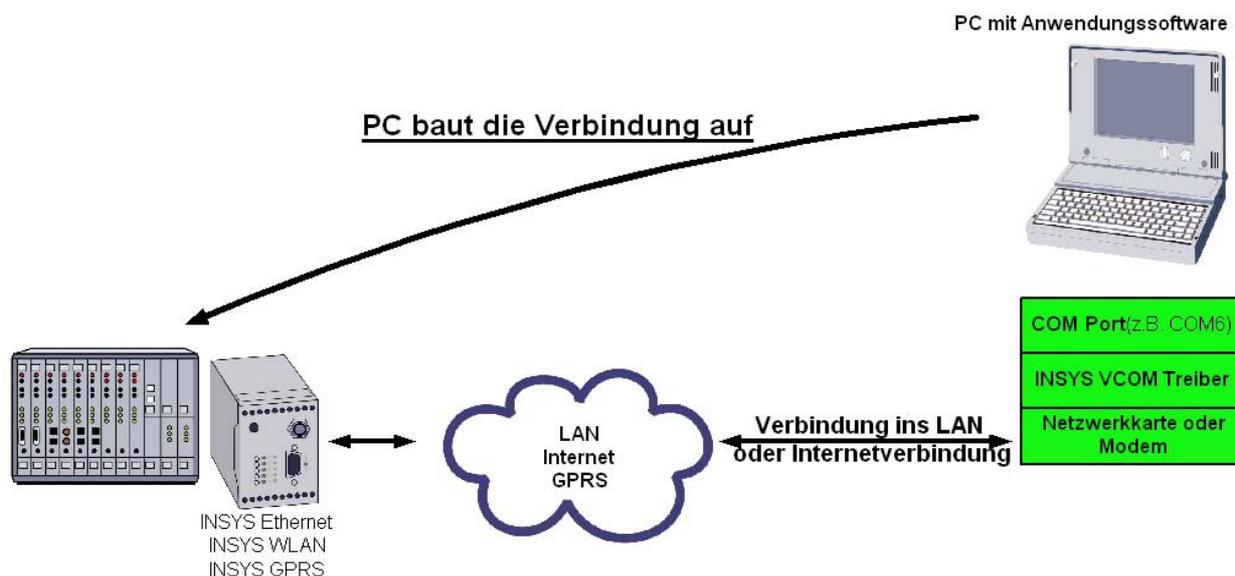
Hier muss also ein vernünftiger Kompromiss für die jeweilige Anwendung gefunden werden.

3.3 Einrichten als Client

Wollen Sie von Ihrem Rechner aus eine Verbindung zu einem INSYS IP- Gerät aufbauen, dann sind Sie in diesem Kapitel richtig. Wollen Sie, dass Ihr PC eingehende Verbindungen von einem INSYS IP-Gerät annimmt, dann können Sie dieses Kapitel überspringen und in Kapitel 3.4 weiterlesen.

Nach dem Verbindungsaufbau ist in beiden Fällen bidirektionaler Datenaustausch möglich!

 Die meisten GSM/GPRS-Provider lassen in Ihren Netzen keine Verbindungen zu GPRS Endgeräten zu. GPRS Geräte müssen die Verbindung immer selber initiieren.

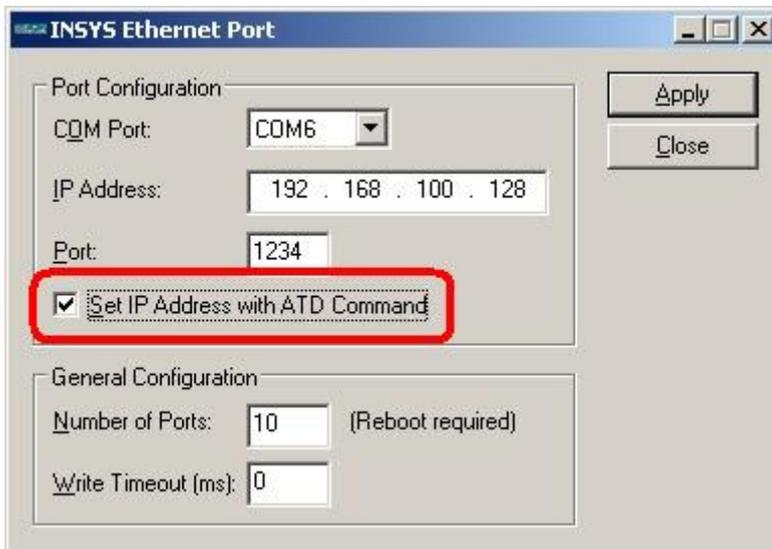


 Bitte achten Sie darauf, dass bei Konfigurationsänderungen durch das Konfigurationsprogramm die betreffenden COM Ports nicht durch Anwendungen geöffnet sind, bzw. dass die Ports nach einer Änderung der Konfiguration einmal geschlossen und wieder geöffnet werden.

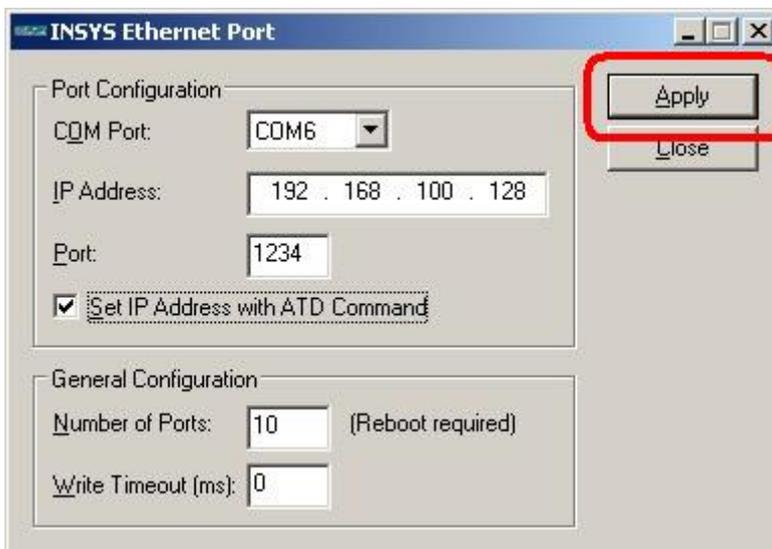
3.3.1 Wählen mit ATD

Soll Ihre Applikation das Endgerät anwählen (wie mit einem Modem), so müssen Sie die folgenden Einstellungen vornehmen:

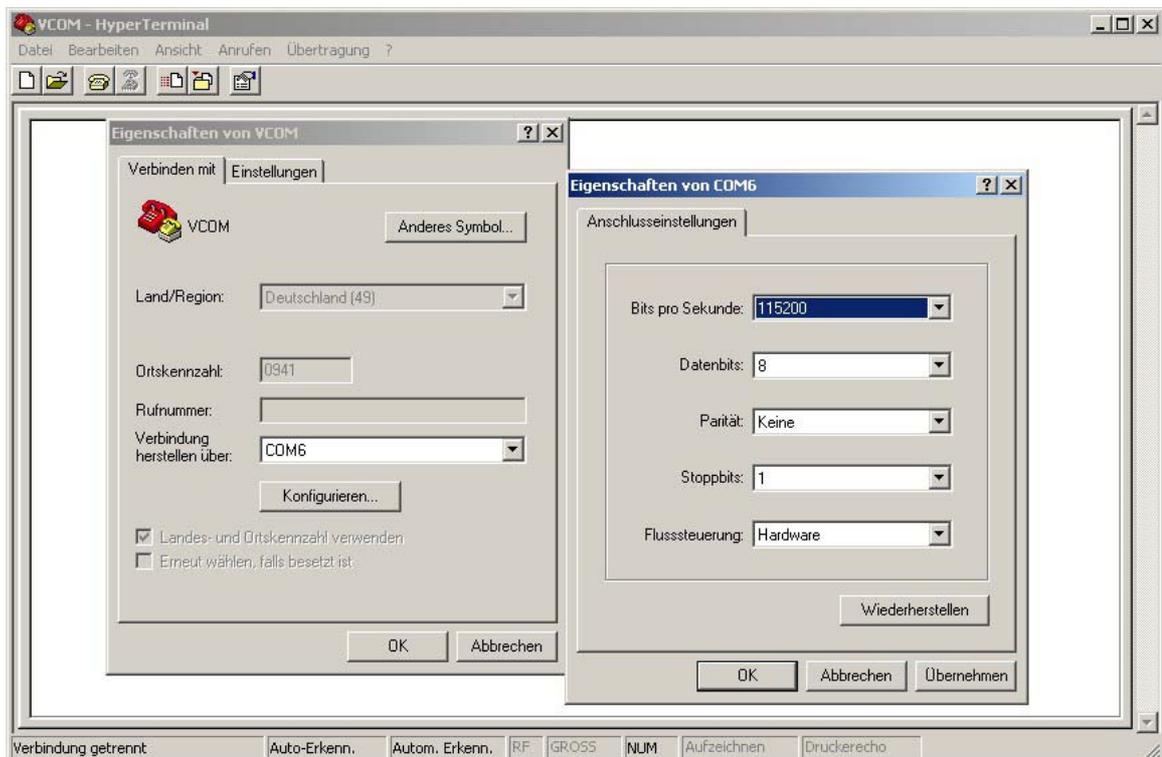
- Aktivieren Sie die Checkbox bei „Set IP Adress with ATD Command“



- Klicken sie auf „Apply“, um die Einstellung für den gewählten COM Port zu übernehmen. Anschließend können Sie das Konfigurationsfenster schließen. Der Treiber arbeitet ohne das Konfigurationsfenster im Hintergrund. Die Einstellung von IP Adresse und Port sind bei dieser Betriebsart nicht nötig.



- Testen Sie den Verbindungsaufbau z.B. mit Hyperterminal, bevor Sie mit Ihrer eigenen Applikation arbeiten. Hierfür stellen Sie in Hyperterminal den gewünschten COM Port ein, und konfigurieren das gewünschte Datenformat und Baudrate.



- Anschließend können Sie mit ATD<IP>:<Port> das gewünschte Endgerät anwählen, und wie bei einer seriellen Verbindung Daten übertragen.

<IP>: die im Endgerät parametrisierte IP Adresse

<Port>: der im Endgerät parametrisierte Port

Achtung: Die INSYS IP-Geräte übernehmen diese Einstellungen erst nach einem Reset.



Nach dem Verbindungsaufbau werden die Daten transparent zwischen dem Terminalprogramm und der seriellen Schnittstelle des INSYS IP-Gerätes ausgetauscht.

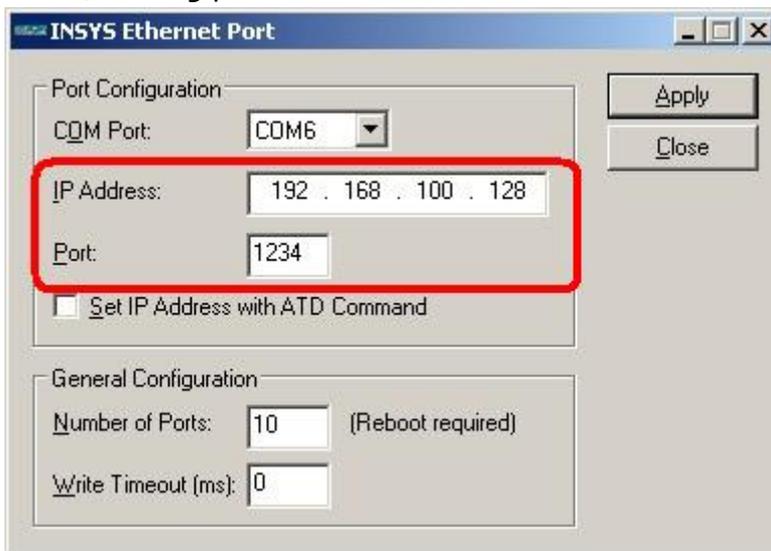
3.3.2 Automatischer Verbindungsaufbau

Diese Anwendung kommt zum Einsatz, wenn Sie Ihre serielle Schnittstelle über das Netzwerk „verlängern“ wollen. Sobald die konfigurierte Schnittstelle von Ihrer Anwendung (z.B. Leitstellensoftware, SPS-Konfigurationsprogramm etc.) geöffnet wird, wird im Hintergrund bereits die Verbindung zum Endgerät aufgebaut.

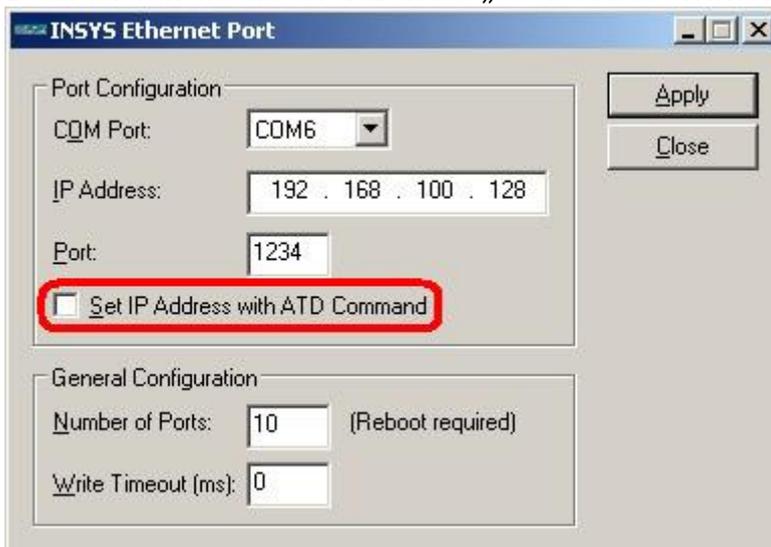
- Konfigurieren Sie die IP-Adresse und den Port des Endgerätes, das Sie erreichen wollen. Die Einstellungen müssen vorher im Endgerät parametrisiert werden, bitte beachten Sie hierfür auch das Handbuch der INSYS IP-Geräte. Im vorliegenden Beispiel wurde ein INSYS Ethernet konfiguriert mit folgenden Einstellungen:

AT#IP=192.168.100.128

AT#PORT=1234

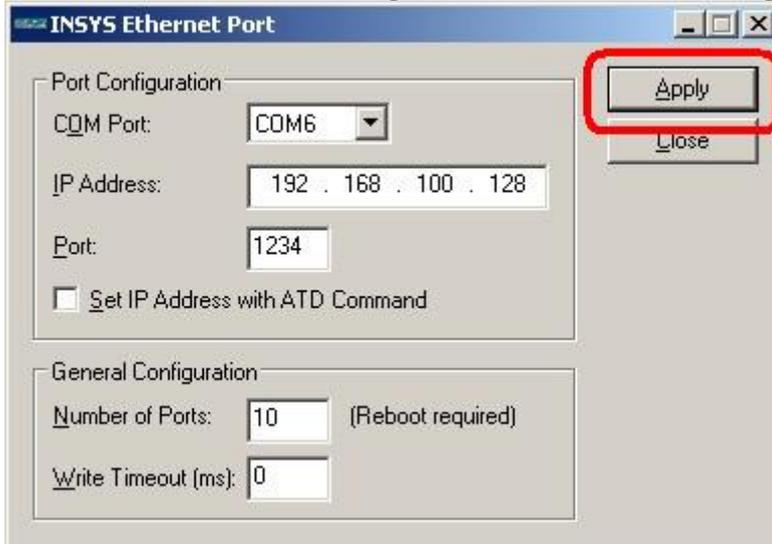


- Deaktivieren Sie die Checkbox bei „Set IP Adress with ATD Command“.

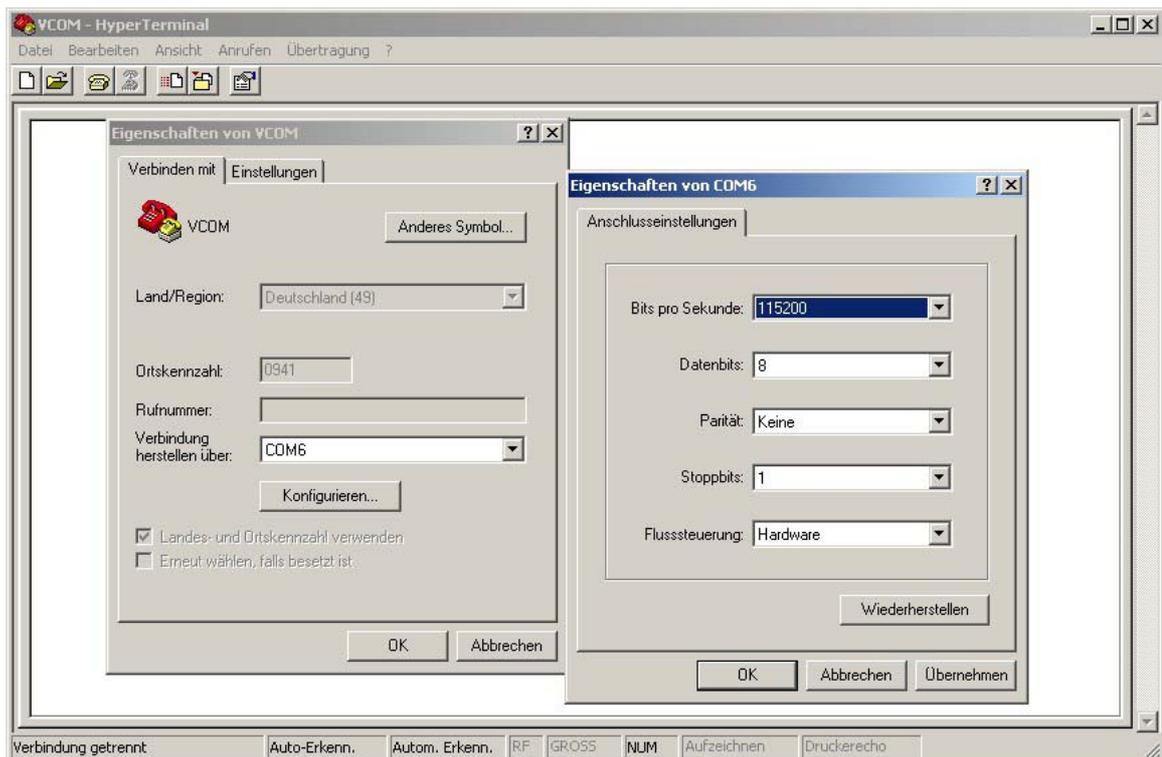


- Klicken Sie auf „Apply“, um die Einstellung für den gewählten COM Port zu übernehmen. Anschließend können Sie das Konfigurationsfenster schließen. Der Trei-

ber arbeitet ohne das Konfigurationsfenster im Hintergrund.



- Testen Sie die Verbindung z.B. mit Hyperterminal. Nach dem Öffnen des COM Ports und Einstellen von Datenformat und Baudrate können Sie direkt mit dem Endgerät kommunizieren.



Nach dem Verbindungsaufbau werden die Daten transparent zwischen dem Terminalprogramm und der seriellen Schnittstelle des INSYS IP-Gerätes ausgetauscht.

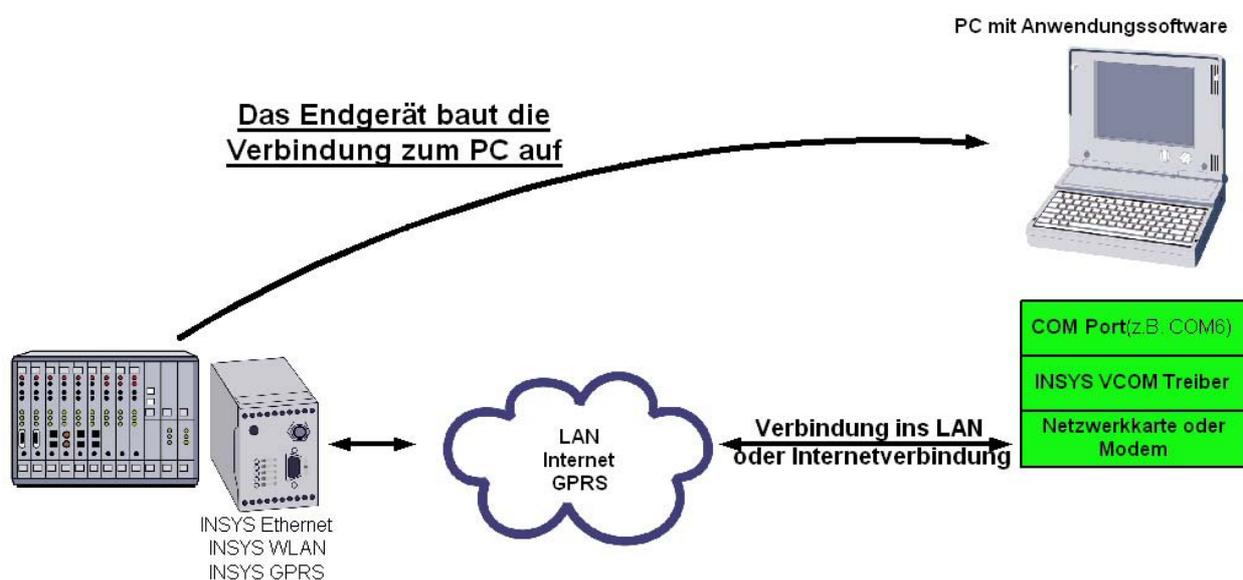
3.4 Einrichten als Server

Wollen Sie von Ihrem Endgerät aus eine Verbindung zu einem PC aufbauen, auf dem der virtuelle COM Port aktiv ist, dann sind Sie in diesem Kapitel richtig.

Wollen Sie mit Ihrem PC eine Verbindung zu einem Endgerät aufbauen, können Sie dieses Kapitel überspringen.

Nach dem Verbindungsaufbau ist in beiden Fällen bidirektionaler Datenaustausch möglich!

 Wenn sie diese Betriebsart in Verbindung mit einem INSYS Ethernet oder INSYS WLAN Gerät verwenden wollen benötigen Sie eine Spezialversion dieses Treibers. Bitte setzen Sie sich hierfür mit Ihrem Vertriebspartner in Verbindung.



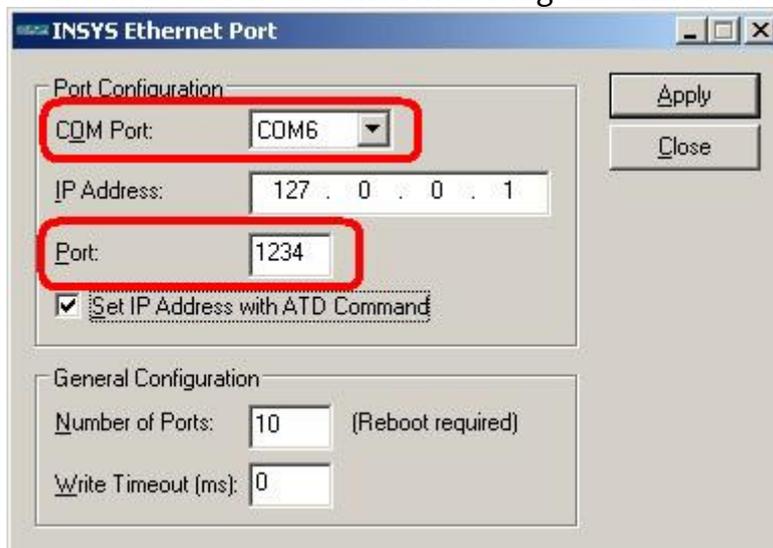
 Bitte achten Sie darauf, dass bei Konfigurationsänderungen durch das Konfigurationsprogramm die betreffenden COM Ports nicht durch Anwendungen geöffnet sind, bzw. dass die Ports nach einer Änderung der Konfiguration einmal geschlossen und wieder geöffnet werden.

3.4.1 Automatische Rufannahme (Grundeinstellung)

Folgende Einstellungen sind nötig, falls Sie eingehende Verbindungen eines INSYS WLAN, INSYS Ethernet oder INSYS GPRS automatisch annehmen wollen:

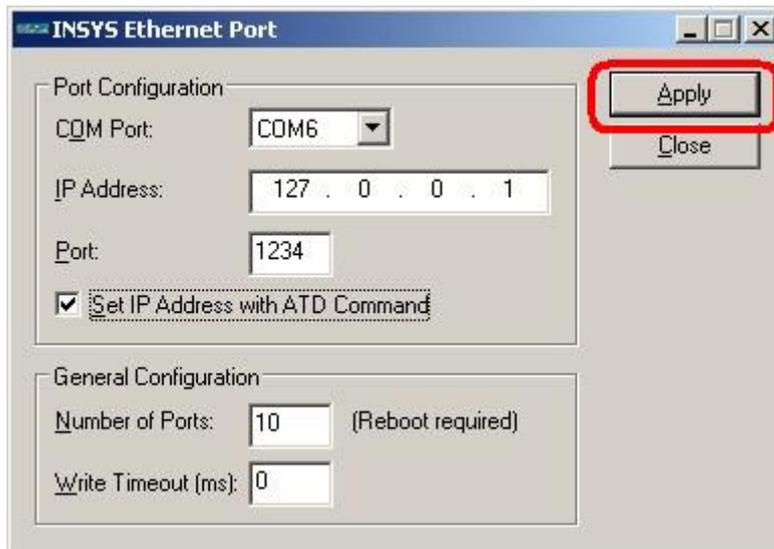
- Stellen sie für den gewünschten COM Port den IP-Port ein, den Sie im INSYS IP-Gerät als Zielport bei der Anwahl verwenden. Genauere Informationen hierzu finden Sie in den jeweiligen Handbüchern. Wenn der Treiber selbst keine Verbindung zum IP-Gerät aufbauen kann, weil das IP-Gerät nicht auf die Annahme einer Verbindung eingerichtet ist, agiert er selbst als Server und wartet auf eine eingehende Verbindung. Dabei beachtet er nur den Port, auf dem die Verbindungsanforderung eingeht.

Beispiel: Wählen Sie Ihren PC von einem INSYS IP Gerät aus mit dem Befehl ATD192.168.100.101:1234 an, so müssen Sie im Feld „Port“ die Nummer 1234 eingeben. Das Eingabefeld „IP Adresse“ und die Checkbox „Set IP Adress with ATD Command“ sind in diesem Anwendungsfall nicht relevant.

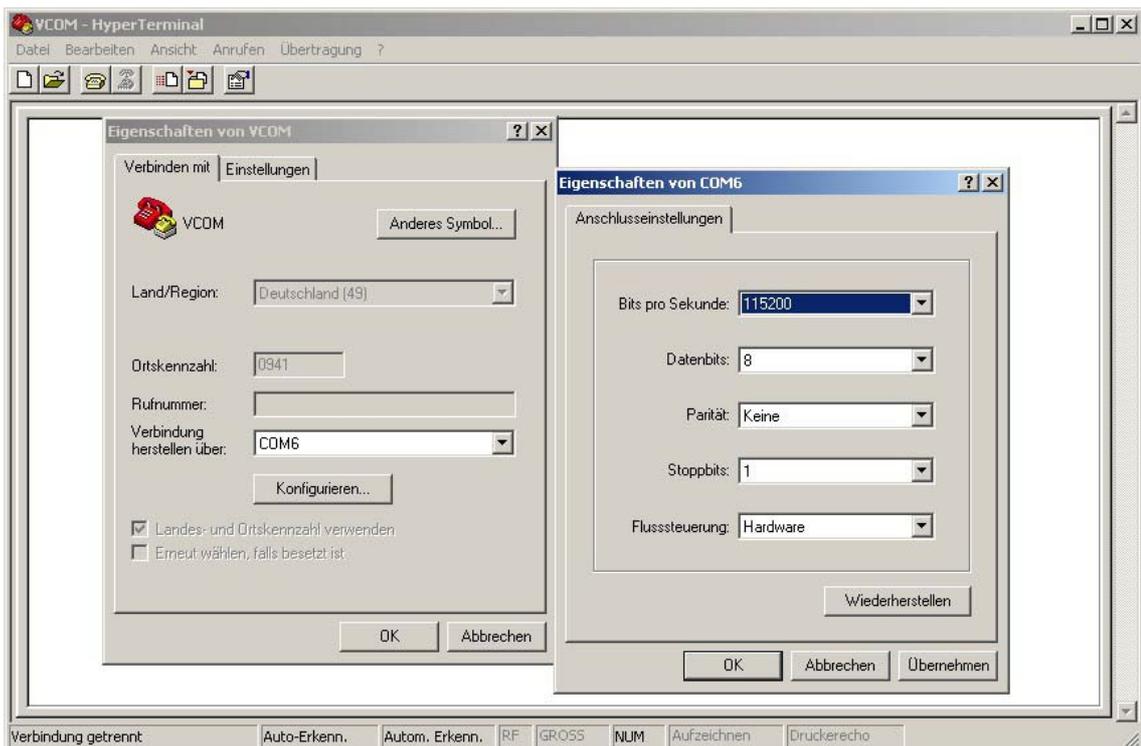


Um zu erfahren, welche IP-Adresse und welchen Port Sie für Ihr Gerät verwenden, können fragen Sie am Besten Ihren Systemadministrator.

- Aktivieren sie die Einstellungen durch einen Klick auf „Apply“. Nun können sie das Konfigurationsfenster schließen.



- Testen Sie die Verbindung am Besten mit einem Terminalprogramm, z.B. Hyperterminal. Hierzu müssen sie nur den konfigurierten COM Port mit den entsprechenden Einstellungen öffnen und anschließend von Ihrem Endgerät aus eine Verbindung zur IP-Adresse des Rechners aufbauen.



3.4.2 Rufannahme mit ATA

Diese Verbindungsart unterscheidet sich in der Konfiguration nicht von Punkt 3.4.1.

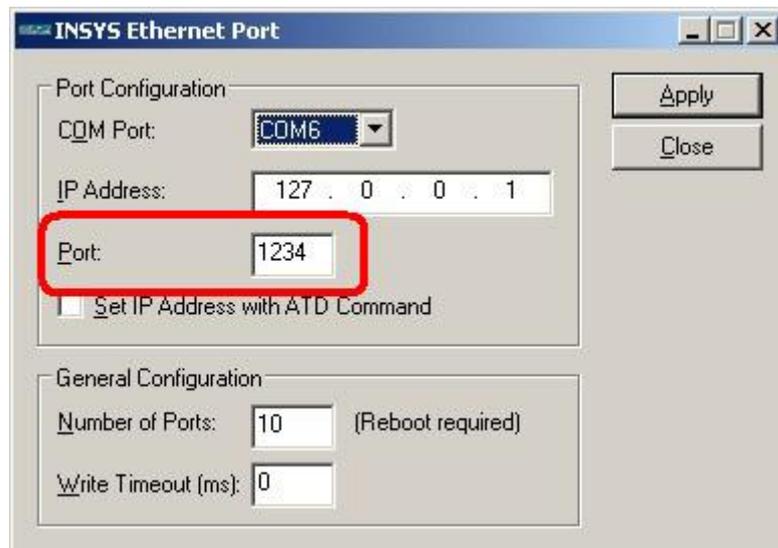
Die Verbindung kann manuell mit ATA angenommen werden. Hierfür muss nach dem Öffnen des COM Ports der Befehl ATSO=0 geschickt werden, um die automatische Rufannahme zu deaktivieren. Da der Treiber aber wissen muss, auf welchem Port der Ruf erwartet werden soll, kann bereits vor einem ankommenden Ruf folgender Befehl gesendet werden:

ATA?:<Port>

<Port> ist der am Endgerät eingestellte Zielport der Verbindung.

z.B. ATA?:1234

Wird dieser Befehl nicht gesendet, sondern nur ATA, wird der im Konfigurationsfenster eingestellte Port überwacht, und bei einem Verbindungswunsch eine RING Meldung ausgegeben.



4 Internetkommunikation im Serverbetrieb

Die obigen Beispiele beziehen sich auf den Einsatz innerhalb eines Netzwerks. Sobald die Kommunikation netzwerkübergreifend stattfinden soll, muss man noch einige Dinge zusätzlich beachten.

Wenn ein Datenaustausch zwischen zwei Netzwerken, z.B. dem Internet und einem Firmennetzwerk stattfinden soll, braucht man ein Koppellement zwischen den beiden Netzwerken. Diese Kopplung und die Organisation des Datenverkehrs zwischen den Netzwerken übernimmt ein Router. Heutzutage sind in Firmennetzen diese Router meist über ein DSL-Modem mit einem Internetprovider verbunden. Der Router hat immer zwei IP-Adressen. Eine aus dem einen Netzwerk (Firmennetz) und eine aus dem anderen (Internet). Der Router muss ja in beiden Netzen kommunizieren können.

Beim Betrieb des virtuellen COM Ports als Server muss man beachten, dass die IP-Adresse des Rechners, auf dem der virtuelle COM Port installiert ist, von außen nicht ohne weiteres erreichbar ist. Es gibt hier einige Dinge, die der Netzwerkadministrator konfigurieren muss:

4.1 NAT – Network Address Translation

Beispiel (siehe auch Abbildung unten):

Ein Firmennetz ist über einen Router und DSL Anschluss mit dem Internet verbunden, und hat folgende IP Adresse vom Provider zugewiesen bekommen:

IP Adresse des Routers im Internet 212.88.46.123

Der Rechner mit dem virtuellen COM Port ist Teil des Firmennetzwerks.

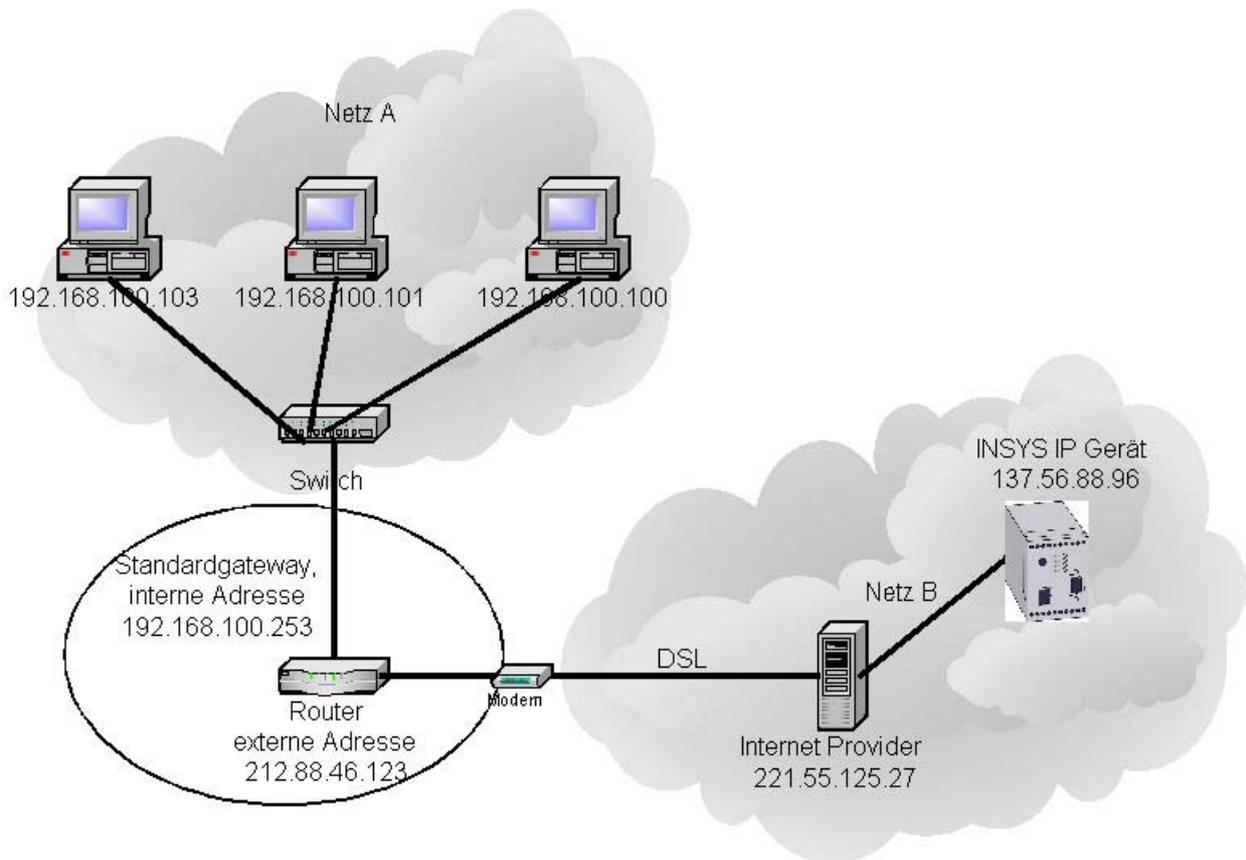
IP Adresse des COM Treibers 192.168.100.101

Normalerweise werden immer nur aus dem Firmennetzwerk Pakete aus dem Internet angefordert (z.B. eine Internetseite). Der Router merkt sich, wer in seinem Netzwerk dieses Paket angefordert hat, und schickt die Anforderung ins Internet unter seiner eigenen Adresse (212.88.46.123). Erhält der Router dann aus dem Internet die Antwort auf diese Anfrage, leitet er die Antwort an den Rechner, der das Paket aus dem Internet angefordert hat, weiter.

Will man den virtuellen COM Port aus dem Internet erreichen, so kann man nicht die IP-Adresse 192.168.100.101 anwählen, da diese Adresse im privaten Netzwerkbereich liegt. Die einzige IP Adresse, die von diesem Firmennetz im Internet bekannt und erreichbar ist, ist die 212.88.46.123, also die Adresse des Routers.

Also wählt man diese Adresse an,
z.B. ATD212.88.46.123:1234

Damit erhält der Router ein Paket mit einer Verbindungsanfrage aus dem Internet für den virtuellen COM Port. Aber nun weiß der Router noch nicht, was er mit diesem Paket machen soll. Woher kann der Router wissen, dass er das Paket an den Rechner mit der Adresse 192.168.100.101 weiterleiten soll?



In unserem Fall will ja ein Gerät im Internet einen Rechner im Firmennetz erreichen. Der Router weiß also erst mal nicht, wo er das Paket hinsenden soll, weil das Paket nicht angefordert wurde. Üblicherweise werden diese Pakete dann verworfen.

Die Lösung für diese Problematik nennt sich „Port Forwarding“. Man kann bei den meisten Routern unter diesem Begriff oder unter den „NAT Einstellungen“ eine IP Adresse vorgeben, auf die eingehende Verbindungen weitergeleitet werden. Hierzu muss auch ein bestimmter Port oder Portbereich festgelegt werden. Bitte kontaktieren sie hierfür Ihren Systemadministrator.

Die Weiterleitung muss für TCP und UDP aktiviert werden.

Beispiel:

Der Router erhält einen Verbindungswunsch zu 212.88.46.123 auf Port 1234. Der Router schlägt in seinen Tabellen nach und findet einen Eintrag, dass eingehende Verbindungen auf Port 1234 immer zum Rechner 192.168.100.101 weitergeleitet werden sollen. Das Paket wird also an 192.168.100.101 gesendet.

So erhält der Rechner mit dem virtuellen COM Port die Verbindungsanfrage und kann die Verbindung annehmen.

4.2 Firewall

Üblicherweise ist in Firmennetzen auch eine Firewall installiert, die eingehende Verbindungen blockiert. Bitten Sie Ihren Systemadministrator, die eingehende Verbindung auf den gewünschten Port freizuschalten für UDP und TCP Pakete.

4.3 Dynamische IP Adressen

Bei der Einwahl ins Internet erhält man üblicherweise immer eine andere IP Adresse. Verfügen Sie über ein Netzwerk mit statischer/fester IP Adresse, können Sie dieses Kapitel überspringen.

Bei Vergabe einer dynamischen IP Adresse für den Server müsste man den Geräten im Feld jedes Mal die neue IP Adresse des Servers mitteilen, damit es das Firmennetzwerk wieder erreichen kann.

Das INSYS GPRS 5.0 bzw. INSYS i-modul GPRS 3.0 unterstützt daher auch die Anwahl über URL und kann damit diese Problematik mithilfe eines DynDNS Dienstes lösen.

Bei einem DynDNS Dienst kann man sich kostenlos eine Internetadresse (URL) zuweisen lassen, die dann mit der jeweils zugewiesenen IP Adresse verknüpft wird.

Jedes Mal, wenn dem Router eine neue IP Adresse zugewiesen wird, meldet sich der Router dem DynDNS Server und teilt diesem die neue Adresse mit. Die meisten aktuellen Router unterstützen dieses automatische Verfahren.

Sie müssen sich nur bei dem entsprechenden Service kostenlos anmelden, z.B. unter <http://www.dyndns.com/>

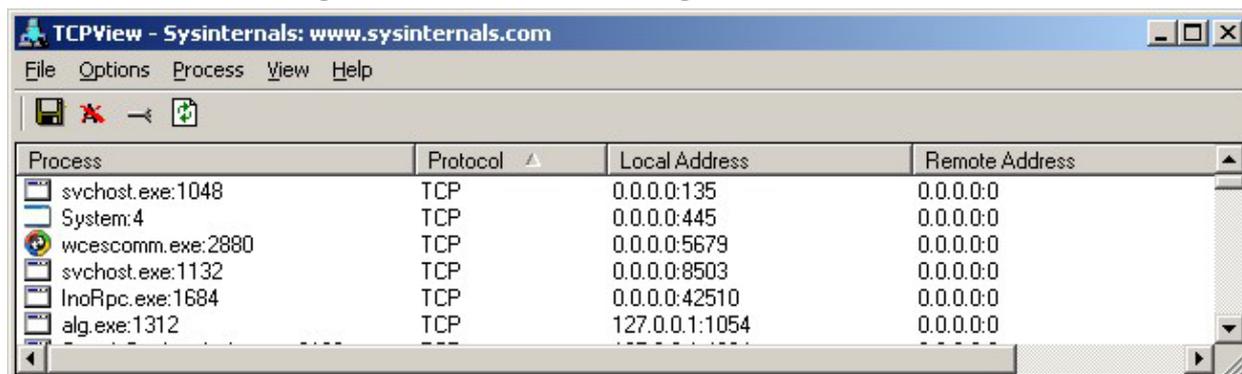
5 Diagnosetools

5.1.1 TCPView

Mit diesem Tool kann man sich alle aktiven TCP und UDP Verbindungen anzeigen lassen, die auf einem Rechner aktiv sind.

Quelle: <http://www.sysinternals.com/NetworkingUtilities.html>

Keine Installation nötig, direkt ausführbares Programm.



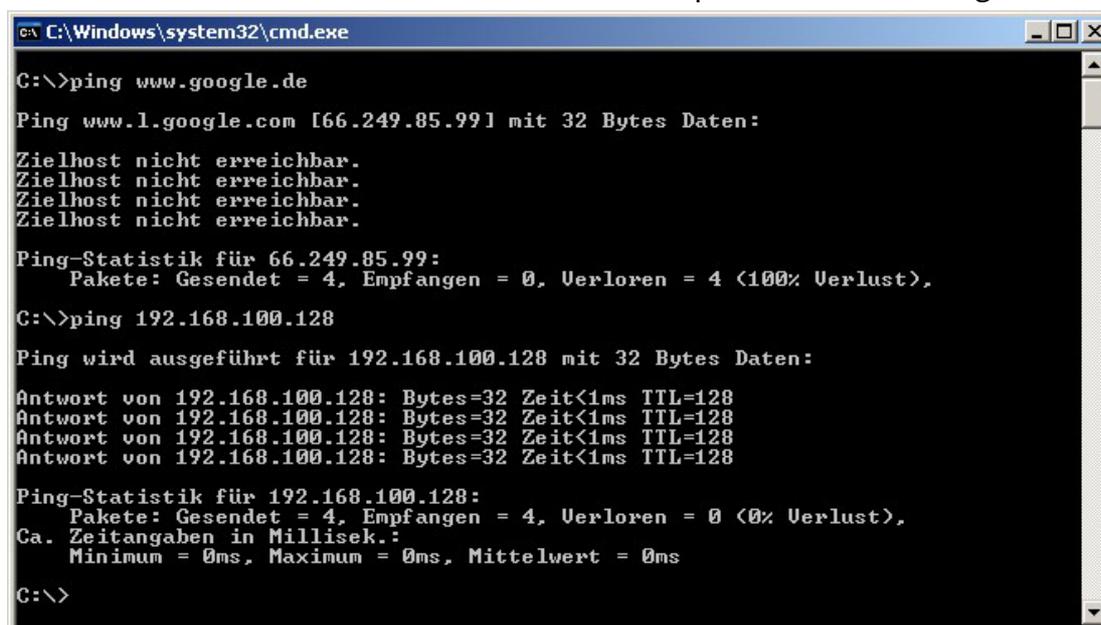
The screenshot shows the TCPView application window. The title bar reads 'TCPView - Sysinternals: www.sysinternals.com'. The menu bar includes 'File', 'Options', 'Process', 'View', and 'Help'. Below the menu bar is a toolbar with icons for file operations. The main area is a table with the following columns: 'Process', 'Protocol', 'Local Address', and 'Remote Address'. The table contains the following data:

Process	Protocol	Local Address	Remote Address
svchost.exe:1048	TCP	0.0.0.0:135	0.0.0.0
System:4	TCP	0.0.0.0:445	0.0.0.0
wcescomm.exe:2880	TCP	0.0.0.0:5679	0.0.0.0
svchost.exe:1132	TCP	0.0.0.0:8503	0.0.0.0
lnorpc.exe:1684	TCP	0.0.0.0:42510	0.0.0.0
alg.exe:1312	TCP	127.0.0.1:1054	0.0.0.0

5.1.2 Ping

Mit dem Kommandozeilenbefehl Ping lässt sich ein einfacher Verbindungstest zu einem Rechner durchführen. Aber Vorsicht, oft blockieren Router oder Firewalls Ping-Anfragen. Ein fehlerhafter Ping heißt also nicht zwangsweise, dass die Gegenstelle nicht erreichbar ist. In der Abbildung unten sehen Sie eine fehlgeschlagene Anfrage an www.google.de, obwohl über den Internetbrowser Google erreichbar ist – das kann daran liegen, daß die Firewall nur das Internetprotokoll (http), nicht aber die Ping-Anfrage passieren läßt.

Die Rechner im internen Netz sind üblicherweise problemlos über Ping erreichbar.



```
C:\Windows\system32\cmd.exe
C:\>ping www.google.de
Ping www.1.google.com [66.249.85.99] mit 32 Bytes Daten:
Zielhost nicht erreichbar.
Zielhost nicht erreichbar.
Zielhost nicht erreichbar.
Zielhost nicht erreichbar.
Ping-Statistik für 66.249.85.99:
    Pakete: Gesendet = 4, Empfangen = 0, Verloren = 4 (100% Verlust),
C:\>ping 192.168.100.128
Ping wird ausgeführt für 192.168.100.128 mit 32 Bytes Daten:
Antwort von 192.168.100.128: Bytes=32 Zeit<1ms TTL=128
Ping-Statistik für 192.168.100.128:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 0ms, Maximum = 0ms, Mittelwert = 0ms
C:\>
```

5.1.3 Netzwerkanalyse mit Ethereal

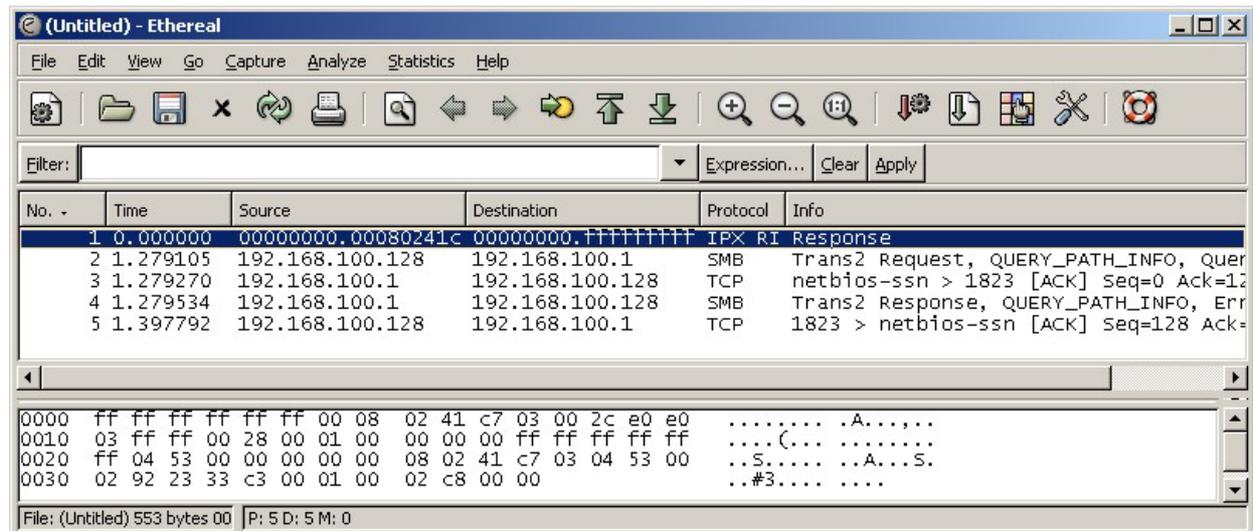
Quelle: <http://www.ethereal.com/>

Ethereal ist ein Freeware Netzwerkprotokoll-Analysetool.

Die Funktion und die Bedienung ist im Internet dokumentiert, hier nur zwei Hinweise:

Üblicherweise sind Rechner mit Switches miteinander und mit dem Server eines Netzwerks verbunden. Ein Switch leitet Pakete immer nur an die an der Kommunikation beteiligten Rechner weiter. Sie können also nicht mit Ihrem Rechner z.B. ein INSYS Ethernet „abhören“, das an einem anderen Port des Switches angeschlossen ist. Hierfür benötigen Sie einen Hub oder einen Switch , der das so genannte „Port Mirroring“ unterstützt.

Ist man über ein Modem ins Internet eingewählt, hat man eine PPP-Verbindung zu seinem Provider. Diese Verbindung kann man mit Ethereal nur mithilfe eines Zusatztreibers (WinPcap) mithört werden.



6 Begriffserklärung

IP-Adresse

Die IP-Adresse ist die Adresse eines Rechners in einem IP Netzwerk und besteht aus vier Zahlen im Bereich zwischen 1 und 255.

Beispiel: 192.168.100.101

Mit Ausnahme der folgenden Adressen sind die IP-Adressen weltweit eindeutig und einmalig:

- 127.0.0.1 ist die Bezeichnung für den lokalen Computer („loopback address“)
- private Adressen (10.0.0.0 - 10.255.255.255, 172.16.0.0 - 172.31.255.255, 192.168.0.0 - 192.168.255.255, 69.254.0.0 - 169.254.255.255) können von jedermann genutzt werden. Pakete von diese IP-Adressen werden im Internet grundsätzlich nicht weitergeleitet.

(Sub)Netzmaske

Die eingestellte Subnetzmaske entscheidet, ob ein Rechner ein IP Paket einfach ins lokale Netzwerk sendet, oder an das Standardgateway.

Beispiel:

Senderadresse:

192.168.1.1 (Binär: 1100 000. 1010 1000. 0000 0001. 0000 0010)

Netzmaske:

255.255.255.0 (Binär: 1111 1111. 1111 1111. 1111 1111. 0000 0000)

Empfängeradresse:

192.168.2.3 (Binär: 1100 0000. 1010 1000. 0000 0010. 0000 0011)

Soll ermittelt werden, ob der Empfänger im lokalen Netzwerk ist, werden folgende Verknüpfungen

durchgeführt:

Verknüpfung 1:

```
11000000 10101000 00000001 00000010
&& 11111111 11111111 11111111 00000000
11000000 10101000 00000001 00000000
```

Verknüpfung 2:

```
11000000 10101000 00000010 00000011
&& 11111111 11111111 11111111 00000000
11000000 10101000 00000010 00000000
```

Sind die beiden Ergebnisse identisch, dann liegt das Ziel im eigenen Netzwerk. In diesem Beispiel sind die Ergebnisse nicht identisch, daher muss das Paket an das in den Netzwerkeinstellungen eingetragene Standardgateway geschickt werden.

Standardgateway

Wenn ein IP-Paket an einen Rechner verschickt werden soll, der nicht im eigenen Netzwerk liegt, muss es einen zentralen Rechner geben, der Zugang zu dem anderen Netzwerk hat. Die IP-Adresse dieses Rechners ist das Standardgateway.

Dies ist z.B. die interne Adresse des DSL-Routers, der die Pakete ins Internet weiterschickt.

Ports

Neben den IP-Adressen gibt es innerhalb der TCP-Kommunikation noch die so genannten Ports, die mit Kanälen vergleichbar sind. Für jede einzelne Verbindung zwischen zwei Rechnern wird ein Port benutzt. Das hat den Vorteil, dass ein Rechner gleichzeitig zu mehreren Rechnern eine Verbindung offen halten kann.

Manche Services im Internet haben bestimmte Ports reserviert, z.B. http auf Port 80.