

SIEMENS

I-GATE 11M Benutzerhandbuch



Copyright (C) Siemens Schweiz AG 2000

Herausgegeben von Information and Communication Mobile
Haidenauplatz 1
D-81667 München
Änderungen vorbehalten

Inhaltsverzeichnis

1	Einleitung	10
1.1	Systemanforderungen	14
1.2	Was Sie für den Internet-Zugriff benötigen.....	14
1.3	Was Sie zur Installation des I-GATE 11M benötigen.....	14
1.4	Falls Sie Hilfe brauchen	15
1.5	Die I-GATE 11M Produkte	16
1.5.1	I-GATE 11M ISDN	17
1.5.2	I-GATE 11M I/LAN	18
1.5.3	I-GATE 11M PCI.....	19
1.5.4	I-GATE 11M PC Card.....	19
1.5.5	I-GATE 11M PC Card plus.....	20
1.5.6	I-GATE 11M USB.....	20
1.6	Betriebsarten	21
1.6.1	WLAN im Infrastruktur-Modus	22
1.6.2	WLAN mit Internet-Zugang	23
1.6.3	WLAN mit Remote Access (RAS).....	24
1.6.4	Wireless LAN-LAN Kopplung	24
1.6.5	WLAN Roaming über Funk	25
1.6.6	WLAN-LAN Kopplung	25
1.6.7	WLAN Roaming über Kabel	26
1.6.8	WLAN-LAN Internet-Zugang.....	27
1.6.9	WLAN im Ad-hoc-Modus	28
1.7	I-GATE 11M und I-GATE 2 Mbit Interoperabilität	29
1.8	Installationsablauf	29
1.8.1	Standard Installation.....	30
2	MobilePort Hardware installieren	32
2.1	I-GATE 11M PCI in den PC einbauen	32
2.2	I-GATE 11M PC Card oder I-GATE 11M PC Card plus in das Notebook einschieben	32
2.3	I-GATE 11M USB anschliessen.....	33
3	I-GATE 11M PCI Software installieren	34
3.1	Treiber für I-GATE 11M PCI installieren	35
3.1.1	Treiber für I-GATE 11M PCI unter Windows 95.....	35
3.1.2	Treiber für I-GATE 11M PCI unter Windows 98.....	44

3.1.3	Treiber für I-GATE 11M PCI unter Windows NT	49
3.1.3.1	NT-Netzwerkunterstützung installieren	49
3.1.3.2	BIOS Einstellungen	51
3.1.3.3	MobilePort Treiber-Installation	51
3.1.4	Treiber für I-GATE 11M PCI unter Windows 2000.....	58
3.2	MobilePort Manager installieren.....	63
4	I-GATE 11M PC Card und I-GATE 11M PC-Card plus Software installieren	66
4.1	Treiber für I-GATE 11M PC Card installieren.....	67
4.1.1	Treiber für I-GATE 11M PC Card unter Windows 95	67
4.1.2	Treiber für I-GATE 11M PC Card unter Windows 98	76
4.1.3	Treiber für I-GATE 11M PC Card unter Windows NT.....	81
4.1.3.1	NT-Netzwerkunterstützung installieren	81
4.1.3.2	BIOS Einstellungen	83
4.1.3.3	MobilePort Treiber-Installation	83
4.1.4	Treiber für I-GATE 11M PC Card unter Windows 2000.....	90
4.2	MobilePort Manager installieren.....	94
5	I-GATE 11M USB Software installieren	96
5.1	Treiber für I-GATE 11M USB installieren.....	97
5.1.1	Treiber für I-GATE 11M USB unter Windows 98	97
5.1.2	Treiber für I-GATE 11M USB unter Windows 2000.....	102
5.2	MobilePort Manager installieren.....	106
6	MobilePort Management	109
6.1	Monitoring und Konfiguration mit dem MobilePort Manager	109
6.1.1	Monitoring mit dem MobilePort Manager	109
6.1.2	Konfiguration mit dem MobilePort Manager	111
6.1.2.1	Configuration.....	111
6.1.2.2	MobilePort WEP Verschlüsselung.....	113
6.2	Konfiguration über den erweiterten Einstellungen des MobilePort Treibers	117
6.2.1	Power Management.....	118
7	Anwendung ohne AccessPoint (nur im Ad-hoc-Modus)	120
7.1	Grundlagen	120
7.2	Windows "Peer-to-Peer" Netzwerke ohne AccessPoint	120
7.2.1	"Peer-to-Peer" Netzwerke unter Windows 98.....	121

7.2.2	Automatische Konfiguration des TCP/IP-Stacks eines "Peer-to-Peer" Netzwerks (ohne AccessPoint) nur bei Windows 98 und 2000	123
7.2.3	Konfiguration des TCP/IP-Stacks mit festen Werten bei Windows 95 und Windows NT	124
8	I-GATE 11M AccessPoint Hardware anschliessen	125
8.1	I-GATE 11M ISDN AccessPoint Hardware anschliessen	125
8.2	I-GATE 11M I/LAN AccessPoint Hardware anschliessen	128
9	I-GATE 11M AccessPoint Software und Grundeinstellungen	137
9.1	I-GATE AccessPoint Tools installieren.	137
9.2	AccessPoint Grundeinstellungen	139
9.2.1	AccessPoint Grundeinstellung über Siemens AccessPoint Manager	139
9.3	AccessPoint Setup-Assistent für Anwendungen	144
9.4	ISDN Internet-Zugang einrichten	145
9.5	SSID (= WLAN Domain) ändern	147
9.6	Access Control mittels MAC-Adressenliste	150
9.7	AccessPoint WEP Verschlüsselung	152
9.8	Konfiguration mit dem AccessPoint Manager	156
9.9	Monitoring mit dem AccessPoint Monitor	162
10	Anwendungen mit AccessPoint - Überblick	166
10.1	Grundlagen	166
10.2	Windows "Peer-to-Peer" Netzwerke mit AccessPoint.	167
10.3	Remote Access mit I-GATE 11M	169
10.4	Wireless LAN-LAN-Kopplung mit I-GATE 11M.	170
10.5	Die I-GATE 11M AccessPoints als CAPI-Server.	171
11	AccessPoint - Konfigurationsmöglichkeiten	172
11.1	Funk oder Kabel: Wege für die Konfiguration	172
11.2	Alternativ: Adreßverwaltung mit dem DHCP-Server.	173
11.2.1	Konfiguration über Siemens AccessPoint Manager	173
11.2.2	Konfiguration mit Siemens WEBconfig.	174
11.2.3	Konfiguration über Telnet	174
11.3	Der Fernzugang: Konfiguration über DFÜ-Netzwerk.	175
11.3.1	Das brauchen Sie für die Fernkonfiguration.	175
11.3.2	So bereiten Sie die Fernkonfiguration vor.	175
11.3.3	Die erste Fernverbindung mit DFÜ-Netzwerk (Siemens AccessPoint Manager).	175

11.3.4	Die erste Fernverbindung mit PPP-Client und Telnet.....	176
11.3.5	Fernkonfiguration einschränken	176
11.4	Neue Firmware mit FirmSafe	178
11.4.1	So funktioniert FirmSafe.....	178
11.4.2	So spielen Sie eine neue Firmware ein.....	179
11.5	Was ist los auf der Leitung?	180
11.5.1	Siemens AccessPoint Monitor.....	180
11.6	Konfiguration über SNMP	181
11.7	Siemens I-GATE 11M I/LAN AccessPoint DSL-Firmware.....	182
12	AccessPoint - Funktionen und Betriebsarten	184
12.1	Sicherheit für Ihre Konfiguration.....	184
12.1.1	Paßwortschutz	185
12.1.2	Die Login-Sperre	185
12.1.3	Zugangskontrolle über TCP/IP	186
12.2	Sicherheit für Ihr LAN	186
12.3	Die Kontrolle	186
12.3.1	Der Rückruf	188
12.3.2	Das Versteck – IP-Masquerading (NAT, PAT).....	189
12.3.3	WEP - Sicherheit für Ihr WLAN.....	189
12.4	Gebührenmanagement.....	190
12.4.1	Einstellungen im Gebührenmodul	190
12.5	ISDN-Verbindungen.....	190
12.5.1	ISDN-Namenliste.....	191
12.5.2	Interface-Einstellungen.....	192
12.5.3	Router-Interface-Einstellungen	193
12.5.4	CAPI-Interface-Einstellungen.....	194
12.5.5	Layer-Liste	194
12.5.6	Round-Robin-Liste	195
12.5.7	Script.....	196
12.5.8	Rufannahme	196
12.5.9	Nummernliste	197
12.6	Point-to-Point Protocol	198
12.7	Das Protokoll.....	198
12.7.1	Die PPP-Liste	200
12.7.2	Alles o.k.? Leitungsüberprüfung mit LCP.....	202
12.8	IPX-Routing	203

12.8.1	IPX-Adressierung	203
12.8.2	Informationen über das LAN	204
12.8.3	IPX-Routing-Tabelle	204
12.8.4	Was passiert bei der Datenübertragung im IPX-Netz?	206
12.8.5	RIP- und SAP-Tabellen	206
12.8.6	So viele Router hier	207
12.8.7	Redundante Routen	207
12.8.8	Exponential-Backoff	208
12.8.9	Filter für die IPX-Pakete	208
12.9	IP-Routing	211
12.9.1	Die IP-Routing-Tabelle	211
12.9.2	Filter für die TCP/IP-Pakete	213
12.9.3	Proxy-ARP	213
12.9.4	Lokales Routing	214
12.9.5	Dynamisches Routing mit IP-RIP	215
12.9.6	IP-Masquerading (NAT, PAT)	217
12.9.7	DNS-Forwarding	219
12.9.8	Zeitsteuerung für die Default-Route	220
12.9.9	Policy Based Routing	221
12.10	Automatische Adreßverwaltung mit DHCP	221
12.10.1	Der DHCP-Server	222
12.10.2	DHCP – 'Ein', 'Aus' oder 'Auto'?	222
12.10.3	So werden die Adressen zugewiesen	223
12.10.4	Konfiguration des DHCP-Servers	226
12.11	DHCP-Relay-Agent	228
12.11.1	Netzwerkconfiguration über ISDN übertragen	228
12.11.2	DHCP-Informationen aus dem entfernten Netz holen	229
12.11.3	DHCP-Informationen anpassen	230
12.11.4	Boot-Images aus dem entfernten Netz holen	230
12.12	DNS	231
12.12.1	Was macht ein DNS-Server?	231
12.12.2	So stellen Sie den DNS-Server ein	232
12.13	NetBIOS-Proxy	234
12.13.1	Kurz und bündig: Was ist NetBIOS?	234
12.13.2	Behandlung von NetBIOS-Paketen	235
12.13.3	Welche Voraussetzungen müssen erfüllt sein?	236
12.13.4	So verbinden Sie zwei Windows-Netze	238

12.13.5	So wählt sich ein Remote-Access-Rechner ein.....	239
12.13.6	Gesucht – Gefunden: Die Netzwerkumgebung.....	240
12.14	Der Least-Cost-Router.....	241
12.14.1	So arbeitet der Least-Cost-Router im I-GATE 11M AccessPoint.....	242
12.14.2	So stellen Sie den Least-Cost-Router ein.....	245
12.15	Bürokommunikation und Siemens CAPI.....	247
12.15.1	Die Siemens CAPI.....	247
12.16	Reservierung von B-Kanälen.....	250
12.17	Accounting.....	251
12.17.1	Konfiguration des Accountings.....	252
12.17.2	Ablesen der Accounting-Informationen.....	253
13	Fehlersuche.....	254
13.1	Ist der MobilePort Treiber erfolgreich geladen?.....	254
13.2	Stimmt die SSID (= WLAN-Domain) Ihrer MobilePort Rechner?.....	258
13.3	Ist das TCP/IP-Protokoll geladen und richtig konfiguriert?.....	259
13.4	Ist eine IP-Kommunikation zwischen zwei WLAN-Rechnern oder zwischen Rechner und AccessPoint möglich?.....	264
13.5	Ist der AccessPoint nicht erreichbar oder funktioniert er nicht mehr?.....	264
14	Technische Daten.....	267
14.1	Funkkanäle.....	267
14.2	Technische Daten.....	268
14.3	Artikelnummern.....	268
15	Allgemeine Garantiebedingungen.....	270
15.1	Garantieumfang.....	270
15.2	Garantiezeit.....	270
16	Service.....	272
16.1	Falls Sie Hilfe brauchen.....	272
16.2	Servicenummern.....	272
17	Stichwörter.....	275

1 Einleitung

Die I-GATE 11M Familie - eine Erweiterung der 2 Mbit Familie

Wir gratulieren Ihnen zum Kauf eines oder mehrerer der folgenden Produkte aus der neuen I-GATE 11Mbit Familie, I-GATE 11M - eine Erweiterung der Siemens Funk-LAN (WLAN) Lösungen:

- I-GATE 11M PC Card MobilePort
- I-GATE 11M PCI MobilePort
- I-GATE 11M ISDN AccessPoint mit steckbarem WLAN-Interface
- I-GATE 11M I/LAN AccessPoint(ISDN/Ethernet oder xDSL) mit steckbarem WLAN-Interface

Wie die Siemens I-GATE 2Mbit Familie, bestehend aus

- MobilePort M2P PC Card
- MobilePort M2D ISA
- BasisPort N2 ISDN mit steckbarem WLAN-Interface
- BasisPort N2 Ethernet (LAN 2) mit steckbarem WLAN-Interface

ist I-GATE 11M die Lösung in allen Fällen, in denen eine konventionelle Ethernet- und ISDN-Verkabelung problematisch ist, oder die Mobilität der Arbeitsplatzrechner im Vordergrund steht.

Mit I-GATE 11M lassen sich bis zu fünfzehn PCs und/oder Notebooks kabellos vernetzen – und das über eine Distanz von ca. 30 bis 100 Meter. Mit einem ISDN- oder ADSL Anschluss besteht die Möglichkeit, ebenfalls kabellos im Internet zu surfen oder andere ISDN-Dienste wie Fax und Filetransfer zu nutzen.

Installation in 4 Schritten

1. MobilePort Hardware einstecken/einbauen
2. MobilePort Software installieren
3. AccessPoint Hardware anschliessen
4. AccessPoint Tools installieren und Grundkonfiguration

Dieses Handbuch zeigt Ihnen in 4 Schritten, wie Sie ihr I-GATE WLAN über die beschriebene **Standard Installation** möglichst schnell in Betrieb nehmen. Dabei ist es egal, ob es sich um den Internet-Zugang eines reinen WLANs mit dem I-GATE 11M ISDN AccessPoint (**Bild 1.2**) oder eines kombinierten Netzes (WLAN + LAN) mit dem I-GATE 11M I/LAN AccessPoint (**Bild 1.8**) handelt. Bezüglich ihrer ISDN-Funktionalität sind die beiden AccessPoints

identisch. Auch bei reinem Bridge-Betrieb des I-GATE 11M I/LAN AccessPoints für eine Ankopplung von Rechnern mit I-GATE MobilePorts an ein kabelgebundenes Netzwerk ([Bild 1.6](#)) gelten die gleichen Schritte, es entfällt lediglich die Konfiguration des ISDN Teiles. Mit einer speziellen Firmware wird es in Zukunft auch möglich sein, den I-GATE 11M I/LAN auch für den breitbandigen Internetzugang über ein ADSL-Modem einzusetzen.

Wenn Sie mehr wissen wollen

Dieses Handbuch führt Sie knapp, jedoch verständlich durch die Installation und die entsprechenden Funktionen Ihrer I-GATE 11M Produkte ein. PC- und Netzwerk-Profis, aber auch Anwender die eine Einführung in die Grundlagen von Funknetzwerken möchten, werden dabei etwas zu kurz kommen. Ihnen empfehlen wir Kapitel "[11 AccessPoint - Konfigurationsmöglichkeiten](#)" und "[12 AccessPoint - Funktionen und Betriebsarten](#)" dieses Handbuchs. Dazu empfehlen wir die Technischen Grundlagen und die Beschreibungen für die Konfiguration über Telnet sowie über SNMP im umfassenden Referenzhandbuch auf der I-GATE CD-ROM.

Kennzeichnung von wichtigen Hinweisen



Informationen, die auf besondere Gegebenheiten hinweisen und denen Sie Aufmerksamkeit widmen sollten, sind im Text durch das I-GATE Logo hervorgehoben.

Annahme: kein Netzwerk installiert



Die Installationsbeschreibung bezieht sich auf den Fall, dass auf Ihrem PC bisher kein Netzwerk installiert ist. Ist auf Ihrem PC bereits ein Netzwerk installiert, so werden einige in diesem Handbuch beschriebene Schritte fehlen oder in leicht anderer Reihenfolge ablaufen. Verfahren Sie in diesem Fall sinngemäss.

Wenn Sie bereits 2 Mbit Produkte haben

Für den Fall, dass Sie I-GATE 2 Mbit und 11 Mbit Produkte zusammen betreiben möchten, werden die Möglichkeiten in Kapitel "[1.7 I-GATE 11M und I-GATE 2 Mbit Interoperabilität](#)" erklärt.

Das ist noch nicht alles...

Die I-GATE 11Mbit Familie bekommt demnächst Zuwachs. Um Sie vorab zu orientieren, finden Sie bereits in diesem Handbuch Hinweise über

- I-GATE 11M USB MobilePort
- I-GATE 11M PC Card plus MobilePort

Besuchen Sie uns



Weil wir unsere Produkte entsprechend Neuerungen in der Technik laufend verbessern, lohnt sich nachdem Sie die Standard Installation durchgeführt haben, einen Besuch bei

www.siemens.com/i-gate

Dort können Sie prüfen, ob aktuellere Softwareversionen und Anleitungen, als die, die auf dem CD mit ihrem Produkt geliefert wurden, verfügbar sind.

CE-Konformität

Diese Geräte wurden getestet und erfüllen unter praxisgerechten Bedingungen die Anforderungen nach der Richtlinie des europäischen Parlaments und des Rates zur Angleichung der Rechtsvorschriften der Mitgliedstaaten über Funkanlagen und Telekommunikations-end-einrichtungen und die gegenseitige Anerkennung ihrer Konformität (R&TTE - Richtlinie 99/5/EWG) entsprechend den folgenden Normen:

- EN 55022 Klasse B und EN 55024 sowie ETS 300 826 (EMV)
- EN 60950 (Produktsicherheit)
- ETS 300 328 & ETS 300 328 A1 (Funkverbindung)
- ETS 300 047-3 (Safety & Protection)
- TBR 3 (S₀-Schnittstelle)

CE-Kennzeichnung:



Wichtige Hinweise zur Produktsicherheit



Der I-GATE 11M ISDN AccessPoint und der I-GATE 11M I/LAN AccessPoint sind für den Basisanschluss S_0 des ISDN-Netzes vorgesehen, der als hausinterne Schnittstelle definiert ist (SELV-Stromkreis). Der Anschluss erfolgt über das mitgelieferte ISDN-Kabel.

Die AccessPoints dürfen nur mit dem mitgelieferten Netzgerät betrieben werden.

Die AccessPoints sind an einer leicht zugänglichen 230 V Steckdose anzuschliessen.

Das System entspricht den Anforderungen gemäss EN 60950. Angeschlossene Geräte müssen die relevanten Sicherheitsbestimmungen erfüllen.

Wichtiger Hinweis für die Funkzulassung



Die Geräte sind in ganz Europa zugelassen. Da der verwendete Frequenzbereich in Frankreich eingeschränkt ist, prüfen Sie dringend in der Tabelle von Kapitel "14.1 Funkkanäle", welche Frequenzen Sie in Frankreich verwenden dürfen. Stellen Sie sicher, dass Sie in Frankreich nur MobilePorts mit den Bezeichnungen V4411-Z9-X101 (I-GATE 11M PC Card), V4411-Z9-X102 (I-GATE 11M PC Card plus) oder V4411-Z11-X101 (I-GATE 11M PCI) verwenden.

1.1 Systemanforderungen

Vergewissern Sie sich, dass Ihr PC oder Notebook die folgenden Anforderungen erfüllt:

- Pentium 90 MHz oder höher
- Mindestens 32 MB RAM
- Mindestens 25 MB freie Festplattenkapazität
- CD-ROM Laufwerk
- Freier PC Card Typ II- bzw. PCI- Steckplatz, bzw. USB-Port

Betriebssysteme für das I-GATE 11M PCI MobilePort, den I-GATE 11M ISDN AccessPoint und den I-GATE 11M I/LAN AccessPoint:

- Windows 95/98/2000 oder NT 4.0 (Service Pack 6 oder höher) auf CD-ROM

Betriebssystem für das I-GATE 11M PC Card MobilePort und das I-GATE 11M PC Card plus MobilePort:

- Windows 95/98/2000 oder NT 4.0 (Service Pack 6 oder höher) auf CD-ROM
- Windows CE auf Anfrage

Betriebssystem für das I-GATE 11M USB MobilePort:

- Windows 98/2000

1.2 Was Sie für den Internet-Zugriff benötigen

- Zugangsdaten für einen Internet-Provider
- ISDN (S₀)-Anschluss oder ADSL-Modem mit LAN-Anschluss

1.3 Was Sie zur Installation des I-GATE 11M benötigen

- Ungefähr 1 Stunde Zeit für ein Notebook (Anwendungen wie Internet Browser u.s.w. ausgeschlossen)
- **CD-ROM mit Ihrem Betriebssystem**
- Original-Handbücher zu Ihrem PC resp. Notebook sowie zu Ihrem Betriebssystem
- I-GATE 11M Produkte in Kapitel 1.5 je nach gewählte Betriebsart (Kapitel 1.6).

Wichtige Hinweise zur Installation



Persönliche Daten müssen vor der Installation gesichert werden.

Die Installation muss gemäss dem **Installationsablauf** in Kapitel **1.8** durchgeführt werden.

1.4 Falls Sie Hilfe brauchen

Wenn Sie mit der Installation oder dem Betrieb mit I-GATE 11M Probleme haben, stehen Ihnen folgende Möglichkeiten offen:

- Tipps im Kapitel "**13 Fehlersuche**"
- Internet: **www.siemens.com/i-gate**
- Ihr Fachhändler
- Die am Ende dieses Handbuchs aufgeführte Servicenummer für Ihr Land

Ihr **Fachhändler** beantwortet gerne Fragen betreffend Gerätebedienung. **Siemens Service** hilft Ihnen gerne weiter bei Geräteproblemen. Kontaktieren Sie Ihre **Telefongesellschaft** mit Fragen betreffend Ihrem ISDN - respektiv DSL - Anschluss. Kontaktieren Sie Ihren **Internet Service Provider** mit Fragen betreffend Ihres Internet Anschlusses.

1.5 Die I-GATE 11M Produkte

Artikelnummern

Nicht alle Produkte dürfen in jedem Land verwendet werden. Eine Liste mit den gültigen Artikelnummern für Produkte in Ihrem Land finden Sie als PDF auf der I-GATE 11M CD-ROM unter **CD durchsuchen -> document -> Ihre Sprache -> Daten** oder auf dem Internet unter **www.siemens.com/i-gate**.

Technische Daten

Die technischen Daten Ihrer I-GATE 11M Produkte finden Sie in den PDF Datenblätter auf der I-GATE 11M CD-ROM unter **CD durchsuchen -> document -> Ihre Sprache -> Daten** oder auf dem Internet unter **www.siemens.com/i-gate**.

Haben Sie alles erhalten? Prüfen Sie den Inhalt:

Alle in der 11 Mbit-Familie verwendeten PC Cards (PC Card Typ II) sind identisch und somit austauschbar!

1.5.1 I-GATE 11M ISDN

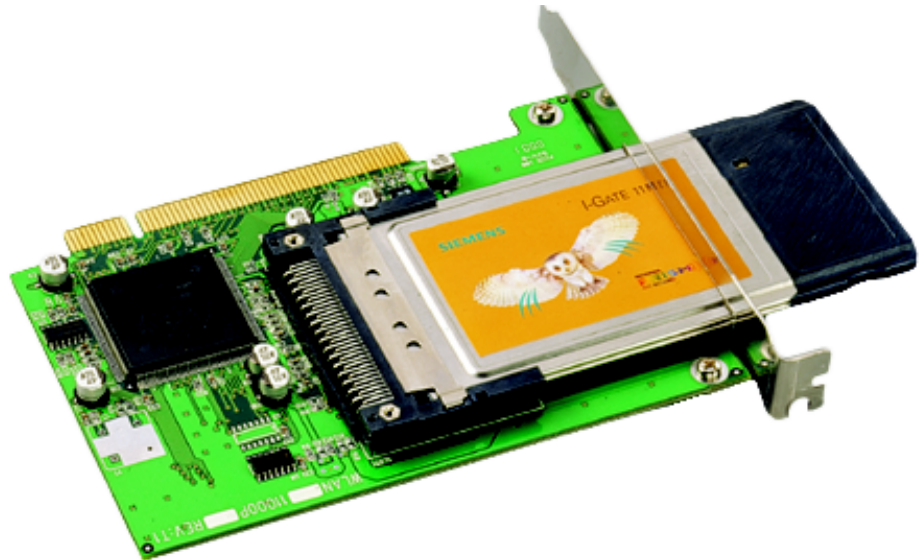
- I-GATE 11M ISDN AccessPoint
- I-GATE 11M PC Card MobilePort (PC Card Typ II)
- Steckernetzgerät für I-GATE 11M ISDN AccessPoint
- ISDN Anschlusskabel
- I-GATE 11M CD-ROM mit Hülle

1.5.2 I-GATE 11M I/LAN



- I-GATE 11M I/LAN AccessPoint
- I-GATE 11M PC Card MobilePort (PC Card Typ II)
- Steckernetzgerät für I-GATE 11M I/LAN AccessPoint
- ISDN Anschlusskabel - das weniger steife Kabel
- Ethernet Anschlusskabel (RJ45 für Ethernet oder ADSL) - das steifere Kabel
- I-GATE 11M CD-ROM mit Hülle

1.5.3 I-GATE 11M PCI



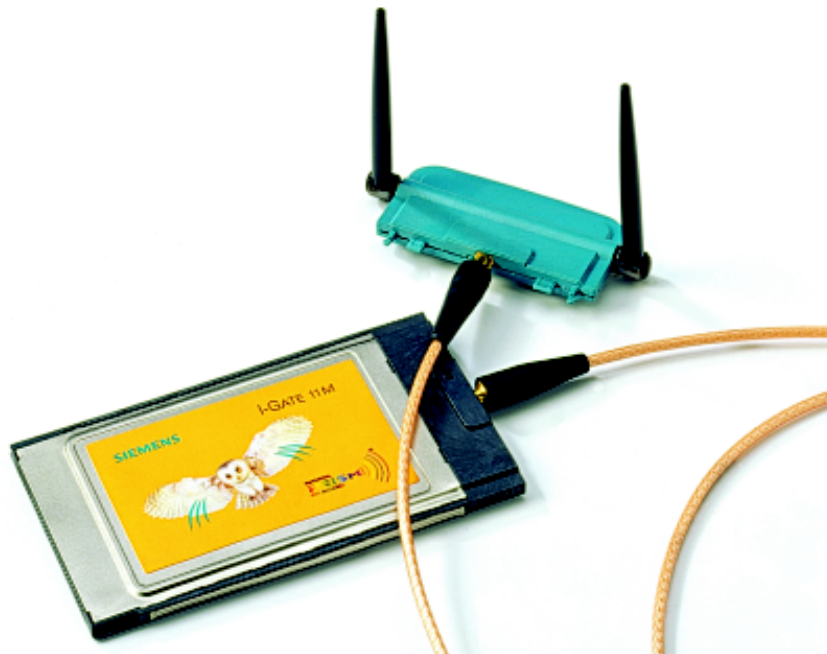
- I-GATE 11M PC Card MobilePort (PC Card Typ II)
- PCI-Adapterkarte
- I-GATE 11M CD-ROM mit Hülle

1.5.4 I-GATE 11M PC Card



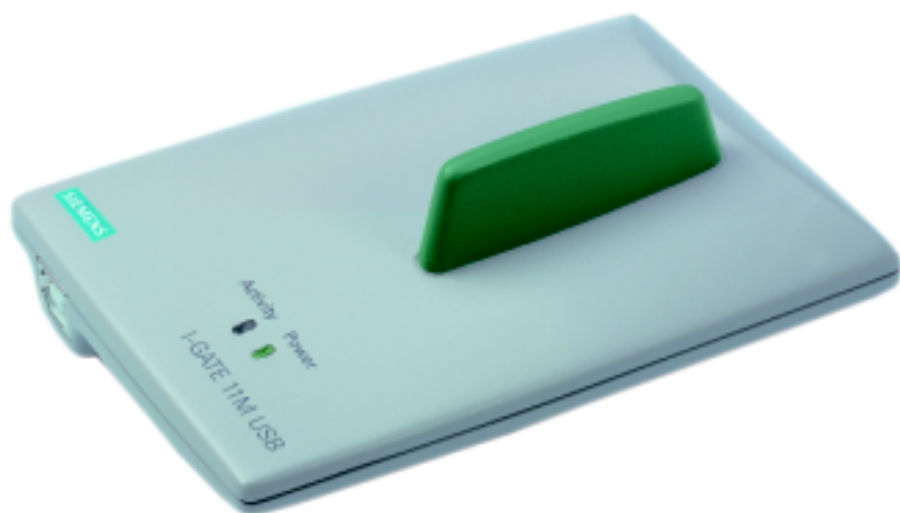
- I-GATE 11M PC Card MobilePort (PC Card Typ II)
- I-GATE 11M CD-ROM mit Hülle

1.5.5 I-GATE 11M PC Card plus



- I-GATE 11M PC Card plus MobilePort (PC Card Typ II) inkl. Kabel & Antenne
- I-GATE 11M CD-ROM mit Hülle

1.5.6 I-GATE 11M USB



- I-GATE 11M USB MobilePort
- USB Anschlusskabel
- I-GATE 11M CD-ROM mit Hülle

1.6 Betriebsarten

Ab Kapitel 1.8.1 führt Sie das I-GATE 11M Benutzerhandbuch durch eine **Standard Installation** im Infrastruktur-Modus mit ISDN (in Zukunft auch xDSL) Internet-Zugang mit dem I-GATE 11M ISDN AccessPoint (**Bild 1.2** unten) und dem I-GATE 11M I/LAN AccessPoint (**Bild 1.8** unten). Sie können die **Standard Installation** auch verwenden um den I-GATE 11M I/LAN AccessPoint für den reinen LAN Betrieb (**Bild 1.6**) oder den LAN Betrieb mit ISDN (z.B. **Bild 1.8**) vorzubereiten. Besuchen Sie **www.siemens.com/i-gate** wenn Sie bei folgenden Installationen Hilfe möchten: Unsere Installateure, Fachhändler und Distributoren beraten Sie gerne. Bei Bedarf führen wir auch Schulungen durch. Als Einführung in WLAN-Netzwerke und auch die Erklärung von Begriffen wie Ad-hoc- und Infrastruktur-Modus empfehlen wir das Kapitel 'Technische Grundlagen' des Referenzhandbuchs (auch auf der I-GATE 11M CD-ROM unter **CD durchsuchen -> document -> Ihre Sprache**).

Im folgenden sehen Sie einen Überblick über die wichtigsten Betriebsarten mit der I-GATE 11M Familie. Die Betriebsarten in "**Bild 1.2 Wireless LAN mit Internet-Zugang**", "**Bild 1.6 WLAN-LAN Kopplung**" und "**Bild 1.8 WLAN-LAN Internet-Zugang**" werden in der **Standard Installation** beschrieben. Für die restlichen Betriebsarten verweisen wir auf die Kapitel "**10 Anwendungen mit AccessPoint - Überblick**", "**11 AccessPoint - Konfigurationsmöglichkeiten**" und "**12 AccessPoint - Funktionen und Betriebsarten**" sowie das Referenzhandbuch auf der I-GATE 11M CD-ROM.

1.6.1 WLAN im Infrastruktur-Modus

Im Infrastruktur-Modus läuft die Kommunikation immer über den AccessPoint. Platziert man den AccessPoint im Zentrum der WLAN-Funkzelle, so ist der Durchmesser der Funkzelle zweimal die Distanz einer Ad-hoc-Verbindung im Ad-hoc-Netzwerk (siehe [1.6.9](#)).



Bild 1.1 WLAN im Infrastruktur-Modus

1.6.2 WLAN mit Internet-Zugang

Der eingebaute ISDN Internetzugangsrouten der I-GATE 11M AccessPoints erlaubt allen Netzteilnehmern den gleichzeitigen Zugriff auf das Internet über die WLAN-Verbindung. Die Zugangsdaten zu einem Internetprovider (Telefonnummer, Benutzername und Passwort) müssen auf dem AccessPoint konfiguriert werden. **Diese Betriebsart wird durch die folgende Standard Installation abgedeckt und ist mit beiden AccessPoints möglich.**

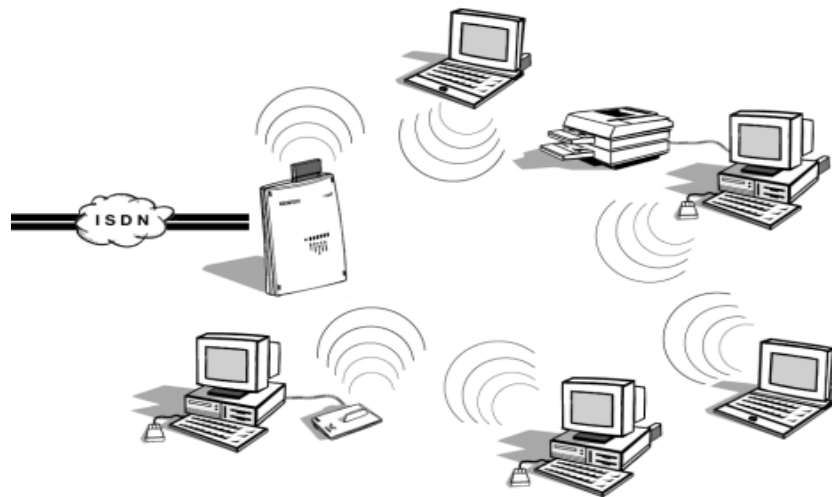


Bild 1.2 Wireless LAN mit Internet-Zugang

1.6.3 WLAN mit Remote Access (RAS)

Auf dieser Weise lässt sich ein Mitarbeiter an einem Aussenstandort über ISDN mit dem Firmennetz (WLAN) verbinden. Gehen Sie zu Kapitel 10.3 um mehr über diese Betriebsart zu erfahren.

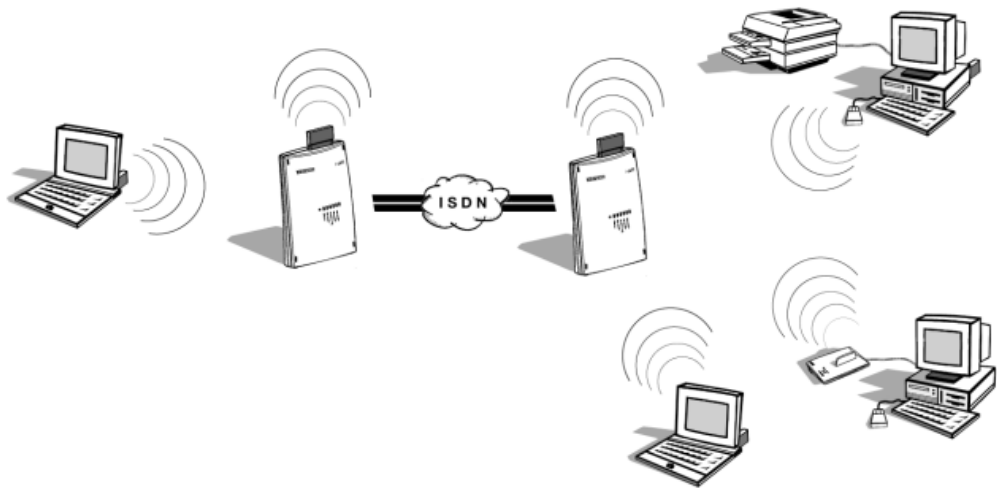


Bild 1.3 WLAN mit Remote Access (RAS)

1.6.4 Wireless LAN-LAN Kopplung

Auf dieser Weise lassen sich zwei separate WLANs über ISDN verbinden. Auf Windows-Ebene (z.B. Explorer) werden die Daten beider WLANs so dargestellt, als ob es sich nur um ein WLAN handeln würde. Damit lassen sich z.B. zwei oder mehrere geographisch getrennte Büros elektronisch koppeln. Gehen Sie zu Kapitel 10.4 um mehr über diese Betriebsart zu erfahren.

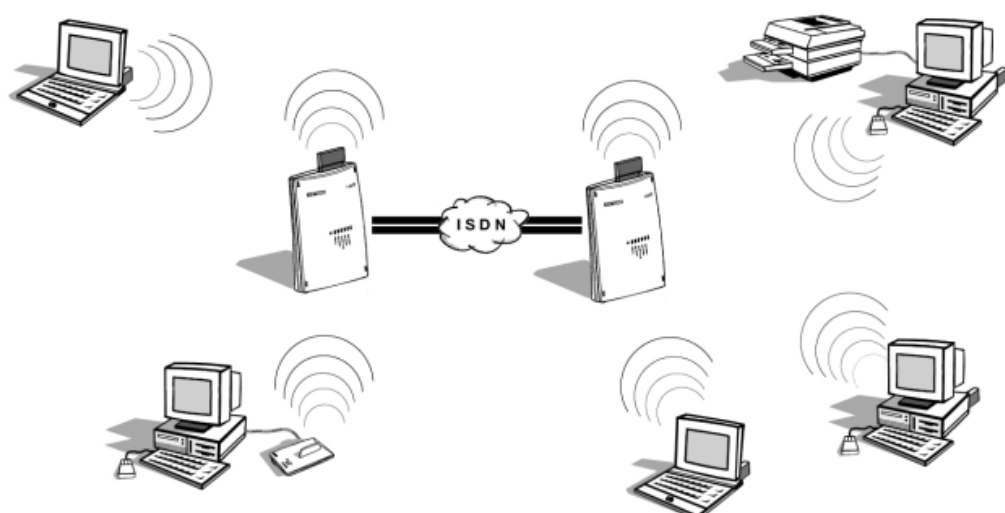


Bild 1.4 Wireless LAN-LAN Kopplung

1.6.5 WLAN Roaming über Funk

Liegen mobile Rechner nicht alle innerhalb der Reichweite eines AccessPoints können weitere AccessPoints dazu genommen werden. Die AccessPoints verwalten dann untereinander das Handover der mobilen Rechner.

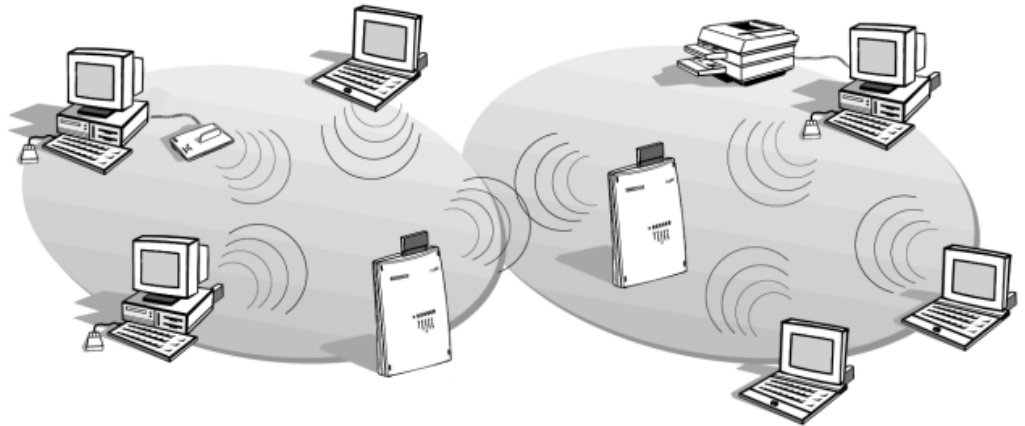


Bild 1.5 WLAN Roaming über Funk

1.6.6 WLAN-LAN Kopplung

Der I-GATE 11M I/LAN AccessPoint dient als Verbindung zwischen WLAN und kabelgebundenem LAN. **Diese Betriebsart wird durch die folgende Standard Installation abgedeckt.**

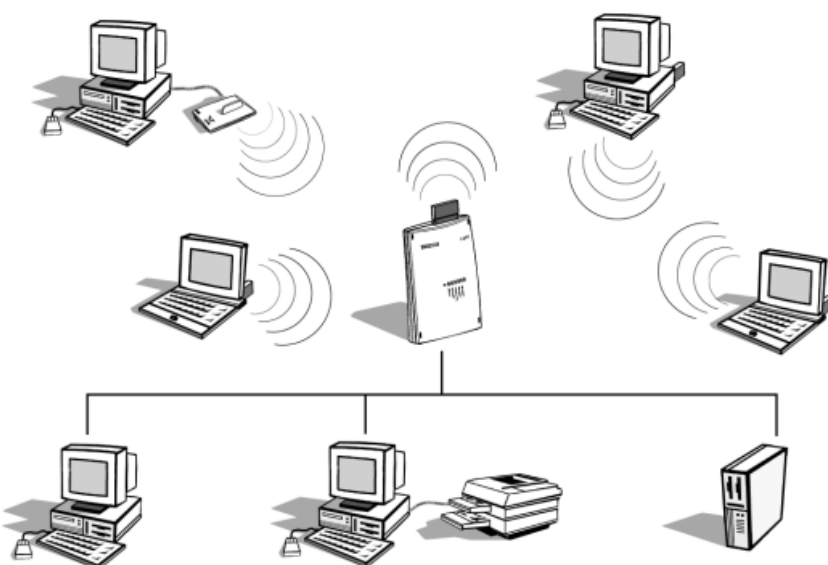


Bild 1.6 WLAN-LAN Kopplung

1.6.7 WLAN Roaming über Kabel

Wenn die Reichweite einer Funkzelle nicht mehr ausreicht, um alle mobilen Rechner zu einem WLAN zusammenschliessen, können auch mehrere AccessPoints eingesetzt werden. Damit wird das Netzkabel zur Überbrückung der fehlenden Reichweite genutzt.

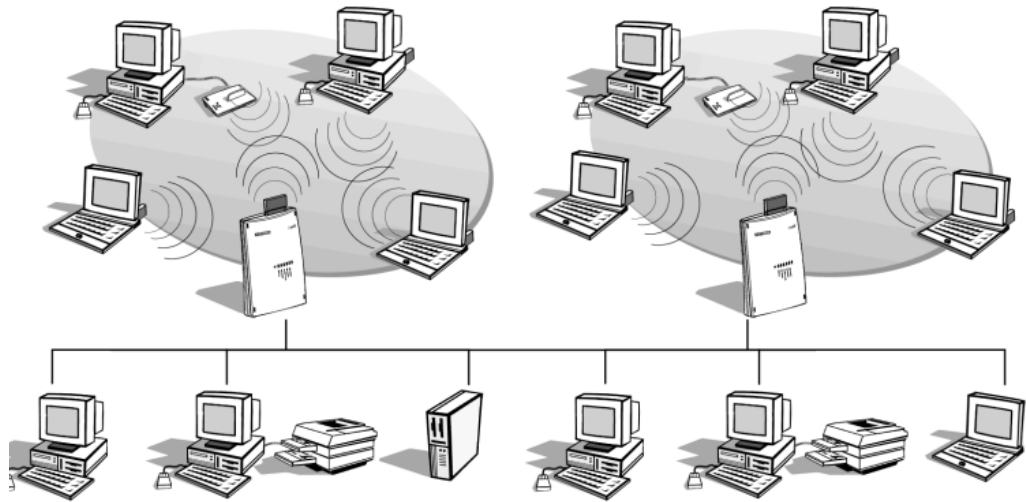


Bild 1.7 WLAN Roaming über Kabel

1.6.8 WLAN-LAN Internet-Zugang

Der I-GATE 11M I/LAN AccessPoint dient als Verbindung zwischen WLAN und kabelgebundenem LAN. Der eingebaute ISDN Internetzugangsrouter des I-GATE 11M I/LAN AccessPoints erlaubt allen Netzteilnehmern den gleichzeitigen Zugriff auf das Internet über die WLAN-Verbindung. Die Zugangsdaten zu einem Internetprovider (Telefonnummer, Benutzername und Passwort) müssen auf dem AccessPoint konfiguriert werden. **Diese Betriebsart wird durch die folgende Standard Installation abgedeckt.**

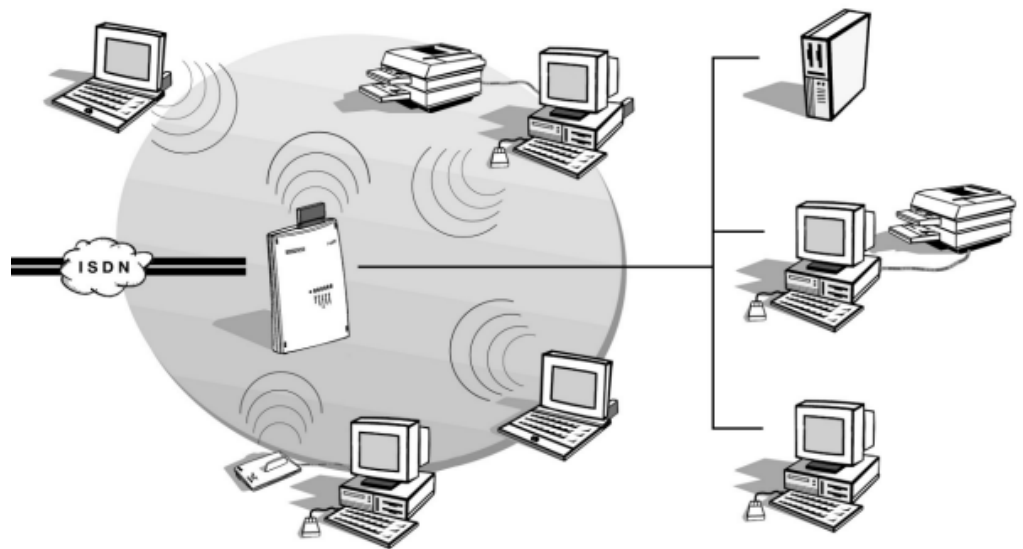


Bild 1.8 WLAN-LAN Internet-Zugang

1.6.9 WLAN im Ad-hoc-Modus

Im Ad-hoc-Modus kommunizieren Die WLAN Teilnehmer (Mobile-Port Rechner und AccessPoints) direkt miteinander (auch "Peer-to-Peer" genannt). Ein AccessPoint kann wahlweise vorhanden sein. Vorteil gegenüber Infrastruktur-Modus: doppelter Datendurchsatz; Nachteile gegenüber Infrastruktur-Modus: geringere Reichweite, kein Roaming, kein Power Saving, keine Kanal-Garantie.

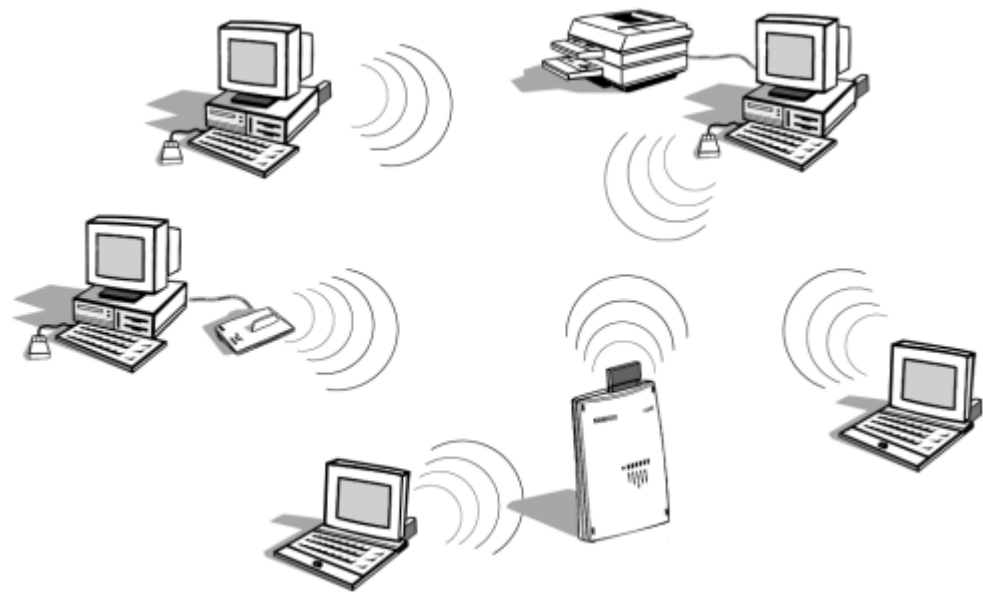


Bild 1.9 WLAN im Ad-hoc-Modus

1.7 I-GATE 11M und I-GATE 2 Mbit Interoperabilität

Sie haben bereits I-Gate 2 Mbit Produkte installiert und wollen nun anstelle der 2 Mbit Produkte die 11Mbit Produkte verwenden? Haben Sie es eilig oder möchten Sie das 2 Mbit MobilePort Tool ('Wireless LAN Configuration Utility') und die 2 Mbit BasisPort Tools ('I-Manager' und 'I-Screen') eventuell doch noch verwenden, so deinstallieren Sie diese nicht. Das 11 Mbit MobilePort Tool ('Siemens MobilePort Manager') und die 11 Mbit AccessPoint Tools ('Siemens AccessPoint Manager', 'Siemens AccessPoint Monitor' und 'Siemens CAPI') überschreiben die 2 Mbit Tools nicht, sondern werden separat installiert.

Sie können also ein 2 Mbit BasisPort N2 (ISDN) und ein 2 Mbit BasisPort LAN 2 (Ethernet) mit einem I-GATE 11M ISDN AccessPoint und einem I-GATE 11M I/LAN AccessPoint in einem WLAN-Netzwerk und vom selben Rechner aus betreiben. Sie können hierzu auch beliebige 2 Mbit und 11 Mbit MobilePorts einsetzen. Dazu stellen Sie auf dem BasisPort resp. auf dem AccessPoint sowie auf allen MobilePorts die selbe SSID (=WLAN Domain) ein. 'Mode' stellen Sie überall auf 'Infrastruktur' ein.

Zudem können Sie mit den I-GATE 11M I/LAN AccessPoint Tools einen I-GATE 11M ISDN AccessPoint konfigurieren.



Die 11Mbit Produkte und 2 Mbit Produkte sind nur im Infrastruktur-Mode interoperabel. Um mit den 11Mbit Produkte interoperabel zu sein, muss der 2 Mbit BasisPort N2 (ISDN) mit der Software Version 1.71 betrieben werden. Sie können diese von www.siemens.com/i-gate unter **Support -> 2 Mbps Produkte Downloads -> Software Release V1.1 -> Update BasisPort N2: update n2.exe** herunterladen. Falls Sie den sich dort ebenfalls befindende **Update MobilePort M2P: update m2p.exe** auf Ihre 2 Mbit MobilePorts noch nicht durchgeführt haben, empfehlen wir zur Leistungssteigerung diesen Update auch durchzuführen.

1.8 Installationsablauf

Je nachdem welche I-GATE 11M Produkte (Kapitel 1.5) und welche Betriebsart (Kapitel 1.6) Sie gewählt haben, können sie nun mit der **Standard Installation** beginnen.

1.8.1 Standard Installation

Mit dem I-GATE 11M Benutzerhandbuch führen wir Sie durch eine **Standard Installation** im Infrastruktur-Modus für einen kabellosen ISDN (in Zukunft auch xDSL) Internet-Zugang mit den I-GATE 11M AccessPoints (**Bild 1.2** und **Bild 1.8**). Diese **Standard Installation** verwenden Sie auch um den I-GATE 11M I/LAN AccessPoint für den reinen LAN Betrieb (**Bild 1.6**) und den LAN Betrieb mit ISDN (**Bild 1.8**) vorzubereiten. AccessPoint Grundeinstellungen werden über den Siemens AccessPoint Manager (für Windows 95, 98, NT4 und 2000) durchgeführt.

In unserer **Standard Installation** gehen wir davon aus, dass Sie ein TCP/IP-Netzwerk betreiben und dass Sie Ihre IP-Adressen über die DHCP-Server Funktion des AccessPoints automatisch (dynamisch) beziehen. Für den Fall, dass Sie fixe IP-Adressen verwenden möchten, haben wir diesen jeweils alternativ beschrieben.

Bevor Sie mit Punkt 2 der **Standard Installation** beginnen, sollten Sie also wissen, ob Sie Ihr TCP/IP-Netzwerk mit dynamischen oder fixen IP-Adressen betreiben wollen. Bevor Sie mit Punkt 4 der **Standard Installation** beginnen, sollten Sie auch wissen ob Sie die DHCP-Server Funktion des AccessPoints nutzen wollen.

Wenn Sie mit Netzwerken und IP-Adressen vertraut sind, können Sie jetzt mit der **Standard Installation** beginnen.

Wenn Sie nicht mit Netzwerken und IP-Adressen vertraut sind und dazu Entscheidungshilfen möchten, lesen Sie in diesem Handbuch die Kapitel "**9.2.1 AccessPoint Grundeinstellung über Siemens AccessPoint Manager**" und "**12.10 Automatische Adreßverwaltung mit DHCP**". Lesen Sie auch im Kapitel Technische Grundlagen des Referenzhandbuchs die Abschnitte 'Netzwerk-Arten' und 'IP-Adressierung'. Sie können jetzt mit der **Standard Installation** beginnen.

Wenn Sie nicht mit Netzwerken und IP-Adressen vertraut sind und jetzt keine Zeit haben dies zu werden, empfehlen wir Ihnen die DHCP-Server Funktion des AccessPoints zu nutzen und die IP-Adresse aller Netzteilnehmer vom AccessPoint automatisch zu beziehen. In diesem Fall wählen Sie unter Punkt 2 im jeweiligen Kapitel über die MobilePort Software Installation "IP-Adresse automatisch beziehen." Genauso wählen Sie unter Punkt 4 im Kapitel "**9 I-GATE 11M AccessPoint Software und Grundeinstellungen**" den Unterkapitel "**9.2.1 AccessPoint Grundeinstellung über**

Siemens AccessPoint Manager" und die Option "Alle Einstellungen automatisch durchführen". Sie können jetzt mit der **Standard Installation** beginnen.

Für die **Standard Installation** gehen Sie mit mindestens einem I-GATE 11M MobilePort und einem AccessPoint in folgenden 4 Schritten entsprechend den Anweisungen in den genannten Kapiteln vor. Schritt 1 und 2 führen Sie an jedem Rechner der im WLAN teilnehmen soll durch. Schritt 1, 2 und 4 führen Sie an jedem WLAN Rechner von dem aus der AccessPoint konfiguriert werden soll durch. Wenn Sie in Schritt 3 ein I-GATE 11M I/LAN AccessPoint mit einem kabelgebundenen LAN verbunden haben können Sie Schritt 4 auch auf einem Rechner im kabelgebundenen LAN durchführen.

1**MobilePort Hardware einstecken/einbauen**

gemäß Kapitel

"2.1 I-GATE 11M PCI in den PC einbauen" oder**"2.2 I-GATE 11M PC Card oder I-GATE 11M PC Card plus in das Notebook einschieben"** oder**"2.3 I-GATE 11M USB anschliessen"****2****MobilePort Software installieren**

gemäß Kapitel

"3 I-GATE 11M PCI Software installieren" oder**"4 I-GATE 11M PC Card und I-GATE 11M PC-Card plus Software installieren"** oder**"5 I-GATE 11M USB Software installieren"****3****AccessPoint Hardware anschliessen**

gemäß Kapitel

"8 I-GATE 11M AccessPoint Hardware anschliessen"**4****AccessPoint Tools installieren und ISDN Internet-Zugang einrichten**

gemäß Kapitel

"9 I-GATE 11M AccessPoint Software und Grundeinstellungen"

2 MobilePort Hardware installieren

2.1 I-GATE 11M PCI in den PC einbauen

1. Schalten Sie Ihren PC aus und trennen Sie ihn vom Stromnetz. Öffnen Sie den PC gemäss den Anweisungen im PC-Manual.
2. Das I-GATE 11M PCI besteht aus der I-GATE 11M PC Card und der PCI-Adapterkarte. Der Einfachheit halber ziehen Sie die PC Card aus der PCI-Adapterkarte heraus und stecken die PCI-Adapterkarte in einen freien PCI-Slot ein.
3. Notieren Sie sich die auf der PC Card gedruckte MAC-Adresse.
4. Schrauben Sie die PCI-Adapterkarte am Gehäuse fest und schieben Sie die PC Card in die PCI-Adapterkarte ein.
5. Schliessen Sie den PC und schalten Sie ihn ein.



Die I-GATE 11M PC Card darf bei eingeschaltetem PC weder in die PCI-Adapterkarte eingeschoben noch herausgezogen werden. Nichtbeachtung kann die Beschädigung der I-GATE 11M PC Card zur Folge haben.

6. Weiter zu "**3.1.1 Treiber für I-GATE 11M PCI unter Windows 95**" oder
7. "**3.1.2 Treiber für I-GATE 11M PCI unter Windows 98**" oder
8. "**3.1.3 Treiber für I-GATE 11M PCI unter Windows NT**" oder
9. "**3.1.4 Treiber für I-GATE 11M PCI unter Windows 2000**"

2.2 I-GATE 11M PC Card oder I-GATE 11M PC Card plus in das Notebook einschieben

1. Notieren Sie sich die auf der PC Card gedruckte MAC-Adresse.
2. Schalten Sie das Notebook ein und schieben Sie nach dem Hochlauf die I-GATE 11M PC Card oder I-GATE 11M PC Card plus ein.
3. Wenn Sie die I-GATE 11M PC Card oder I-GATE 11M PC Card plus auf Windows NT installieren, stellen Sie sicher, dass Sie PC Card Software (zur Spannungsumschaltung auf 3,3 Volt) installiert haben. Wenn Sie diese nicht installiert haben und Sie keine auf der mit dem Notebook gelieferten CDs finden, besuchen Sie z.B. **www.systemsoft.com** und laden Sie SystemSoft's 'CardWizard' Software herunter.

4. Wenn Sie die I-GATE 11M PC Card oder I-GATE 11M PC Card plus auf Windows NT installieren und nicht mindestens Service Pack 6 installiert haben, spielen Sie dieses jetzt auf. Service Pack 6 resp. 6a finden Sie auf der I-GATE 11M CD-ROM unter **CD durchsuchen -> misc -> nt4spx** in Ihrer Sprache.
5. **Weiter zu "4.1.1 Treiber für I-GATE 11M PC Card unter Windows 95" oder**
6. **"4.1.2 Treiber für I-GATE 11M PC Card unter Windows 98" oder**
7. **"4.1.3 Treiber für I-GATE 11M PC Card unter Windows NT" oder**
8. **"4.1.4 Treiber für I-GATE 11M PC Card unter Windows 2000"**

2.3 I-GATE 11M USB anschliessen

1. Starten Sie den PC oder das Notebook und schliessen Sie das I-GATE 11M USB an einer freien USB-Schnittstelle des PC's oder an einem stromversorgten USB-Hub an.
2. **Weiter zu "5.1.1 Treiber für I-GATE 11M USB unter Windows 98" oder**
3. **"5.1.2 Treiber für I-GATE 11M USB unter Windows 2000"**

3 I-GATE 11M PCI Software installieren

In dieser **Standard Installation** gehen wir davon aus, dass Sie ein TCP/IP-Netzwerk betreiben und dass Sie Ihre IP-Adressen über die DHCP-Server Funktion des AccessPoints automatisch (dynamisch) beziehen. Für den Fall, dass Sie fixe IP-Adressen verwenden möchten, haben wir diesen jeweils alternativ beschrieben.

Bevor Sie mit der Installation weiterfahren sollten Sie also wissen, ob Sie Ihr TCP/IP-Netzwerk mit dynamischen oder fixen IP-Adressen betreiben wollen und ob Sie die DHCP-Server Funktion des AccessPoints nutzen wollen.

Wenn Sie mit Netzwerken und IP-Adressen vertraut sind, gehen Sie zu Punkt 1 auf der folgenden Seite.

Wenn Sie nicht mit Netzwerken und IP-Adressen vertraut sind und dazu Entscheidungshilfen möchten, lesen Sie in diesem Handbuch die Kapitel "**9.2.1 AccessPoint Grundeinstellung über Siemens AccessPoint Manager**" und "**12.10 Automatische Adreßverwaltung mit DHCP**". Lesen Sie auch im Kapitel Technische Grundlagen des Referenzhandbuchs die Abschnitte 'Netzwerk-Arten' und 'IP-Adressierung'. Gehen Sie dann zu Punkt 1 auf der folgenden Seite.

Wenn Sie nicht mit Netzwerken und IP-Adressen vertraut sind und jetzt keine Zeit haben dies zu werden, empfehlen wir Ihnen die DHCP-Server Funktion des AccessPoints zu nutzen und die IP-Adresse aller Netzteilnehmer vom AccessPoint automatisch zu beziehen. So wählen Sie den Punkt 'IP-Adresse automatisch beziehen' wenn Sie zum Auswahl des Punkts 'IP-Adresse automatisch beziehen' oder des Punkts 'Fixe IP-Adresse' in diesem Kapitel kommen. Gehen Sie jetzt zu Punkt 1 auf der folgenden Seite.

3.1 Treiber für I-GATE 11M PCI installieren

3.1.1 Treiber für I-GATE 11M PCI unter Windows 95



Die I-GATE 11M PC Card und die I-GATE 11M PC Card plus dürfen bei eingeschaltetem PC weder in die PCI-Adapterkarte eingeschoben noch herausgezogen werden. Nichtbeachtung kann die Beschädigung der PC Cards zur Folge haben.

1

Treiber suchen

Nachdem Sie die I-GATE 11M PCI (gemäß Kapitel "2.1 I-GATE 11M PCI in den PC einbauen") installiert haben und der PC wieder hochgefahren haben, öffnet sich der Assistent für Gerätetreiber-Updates mit der Meldung, dass er nach Treibern für 'PCI Network Controller' sucht. Überspringen Sie in diesem Falle den Punkt 2 und fahren Sie weiter mit Punkt 3, Automatische Hardware-Erkennung. Sollte der Assistent für Gerätetreiber-Updates mit der Meldung nicht erscheinen, fahren Sie weiter bei Punkt 2.

2

Manuelle Hardware-Erkennung

Sollte sich der Assistent für Gerätetreiber-Updates nicht öffnen, starten Sie die Installation unter **Start -> Einstellungen -> Systemsteuerung -> Hardware** und bestätigen Sie mit **Weiter**.

Beantworten Sie die Frage nach der Hardware-Suche mit **Nein** und **Weiter**.

Selektieren Sie in der Liste der 'Hardware-Typen' den Eintrag **Netzwerkkarten** und klicken Sie auf **Weiter**. Im nächsten Fenster klicken Sie auf den Button **Diskette** und geben im Feld 'Herstellerdateien kopieren von' den Laufwerksbuchstaben für Ihr CD-ROM Laufwerk (z.B. F: \) ein (**Bild 3.1**).

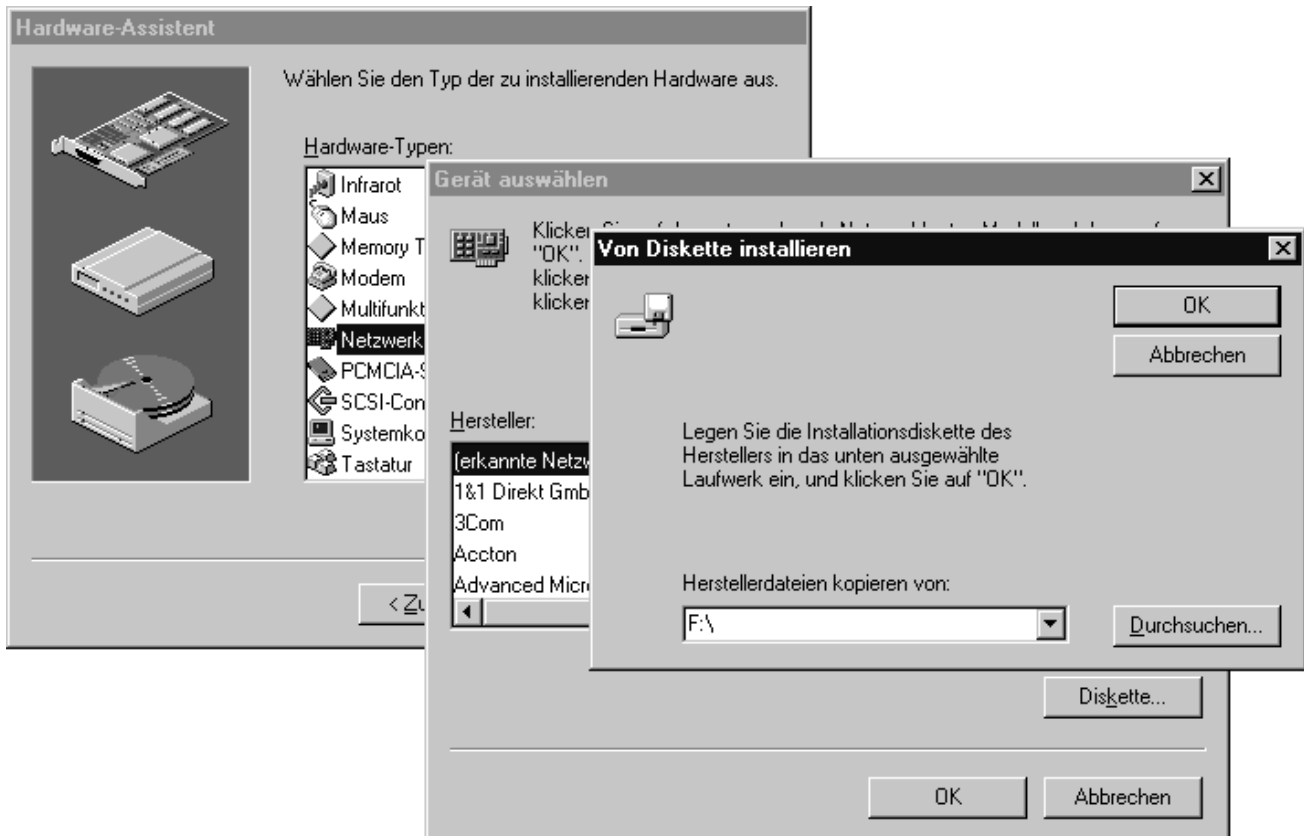


Bild 3.1 Pfad eingabe MobilePort-Treiber bei manueller Hardware-Erkennung

Legen Sie die I-GATE 11M CD-ROM ein und bestätigen Sie nach dem Hochlaufen des CD-ROM Laufwerks mit **Weiter**.

Sollte sich das I-GATE 11M CD-Einstiegsbild öffnen, so schließen Sie es. Selektieren Sie im Fenster 'Gerät auswählen' den Eintrag 'I-GATE 11M PCI'. Bestätigen Sie mit **OK** und anschließend mit **Weiter**.

Fahren Sie nun weiter mit Punkt 4, Namen des Computers und der Arbeitsgruppe eingeben.

3 Automatische Hardware-Erkennung

Legen Sie die I-GATE 11M CD-ROM ein und klicken Sie nach dem Hochlaufen des CD-ROM Laufwerks auf **Weiter**. Sollte sich das I-GATE 11M CD-Einstiegsbild öffnen, schließen Sie dieses mit **Beenden**.

Der Treiber 'I-GATE 11M PCI' wird gefunden. Bestätigen Sie erneut mit **Weiter**. Sie werden daraufhin vom System nochmals aufgefor-

dert, die CD-ROM einzulegen. Da diese bereits eingelegt wurde, können Sie mit **OK** bestätigen. Sollte anschliessend eine Datei nicht gefunden werden, geben Sie im Feld 'Quelle' den Laufwerksbuchstaben für Ihr CD-ROM Laufwerk (z.B. F: \) ein und bestätigen Sie mit **OK**.

4

Namen des Computers und der Arbeitsgruppe eingeben

Sie werden vom System aufgefordert, Computer- und Arbeitsgruppennamen anzugeben. Schliessen Sie die Meldung mit **OK**. Falls Sie nicht aufgefordert wurden, Computernamen und Arbeitsgruppennamen einzugeben, öffnen Sie die Netzwerkeinstellungen mit Start -> Einstellungen -> Systemsteuerung -> Netzwerk, klicken Sie auf das Register Identifikation und überprüfen Sie den Computer- und Arbeitsgruppennamen. Sie können Computernamen und Arbeitsgruppennamen frei wählen. Beachten Sie dabei, dass alle Computer, die miteinander Daten austauschen, der gleichen Arbeitsgruppe angehören. Sie müssen den gleichen Arbeitsgruppennamen, aber verschiedene Computernamen aufweisen.

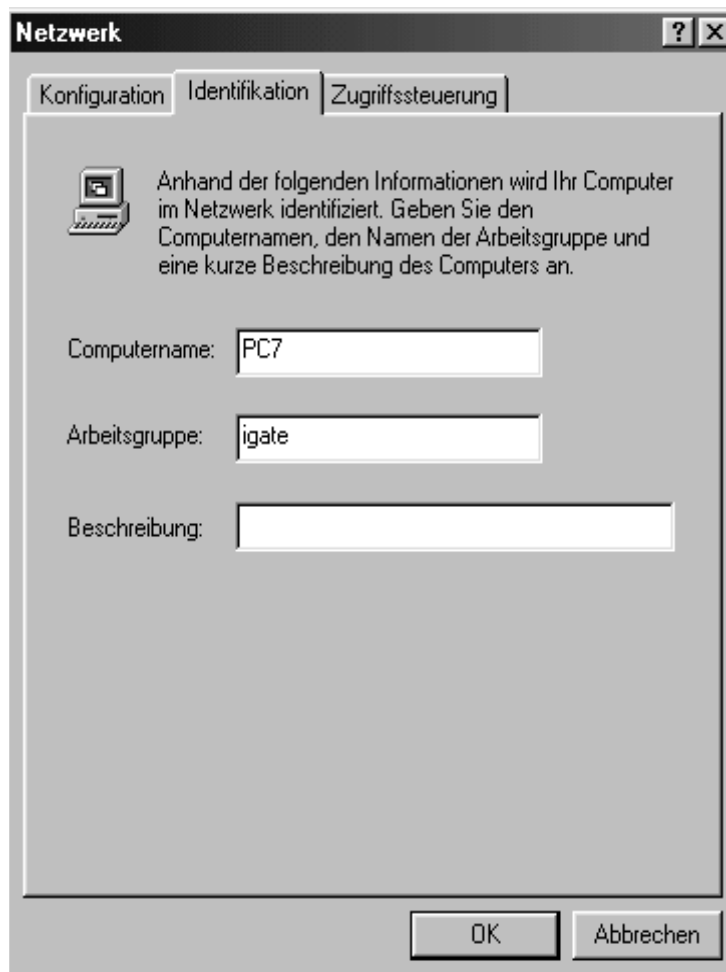


Bild 3.2 Eingabe Computer- und Arbeitsgruppennamen

Geben Sie im Fenster 'Netzwerk' in der Registerkarte 'Identifikation' den Computer- und Arbeitsgruppennamen ein. Bestätigen Sie die Eingabe mit 'OK'.

5 SSID (= WLAN-Domain) eingeben (siehe Bild 3.3)

Markieren Sie im sich automatisch öffnenden Fenster 'Eigenschaften von I-GATE 11M PCI' die Zeile **SSID** (Service Set Identifier) und geben Sie in das Feld 'Wert' die Seriennummer des AccessPoints ein. Diese finden Sie auf dem Typenschild auf der Rückseite des AccessPoints. Die ersten 5 Stellen sind Buchstaben wobei der Buchstabe 'O' nicht verwendet wird. Beachten Sie die Gross-/Kleinschreibung! Die folgenden 7 Stellen sind Zahlen. (Bild 3.3)

Die Eingabe der SSID ist bei der Erstinstallation zwingend. (Falls die SSID bereits geändert wurde, muss der aktuelle Wert eingegeben werden.)

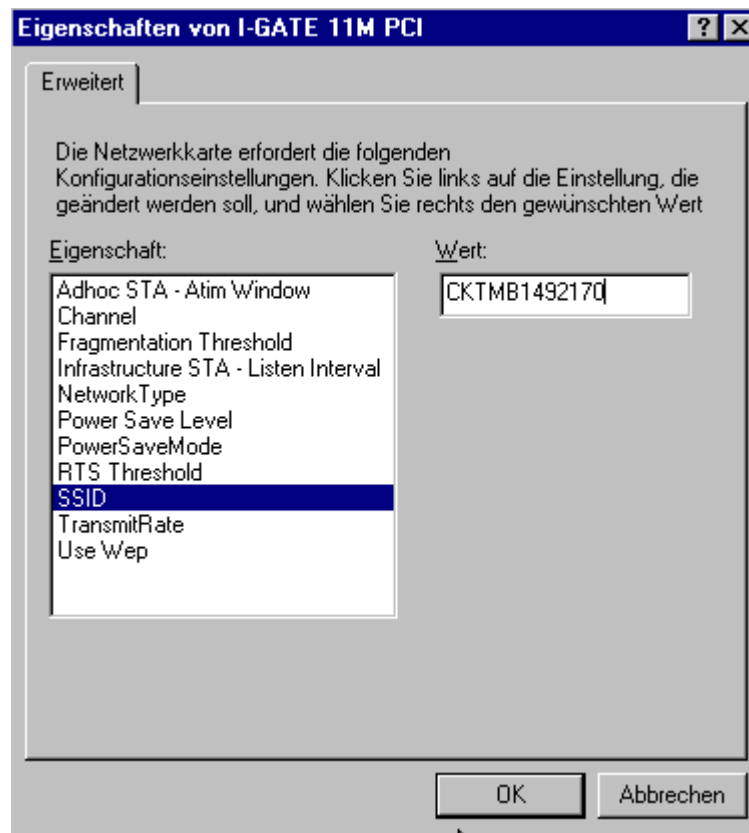


Bild 3.3 SSID eingeben unter Windows 95/98

6 Bestätigen Sie Ihre Eingabe mit **OK.**



Sicherheit nach der Erstinstallation

Die SSID dient lediglich der Zuordnung zu einem AccessPoint und entspricht damit noch keiner Sicherheitsvorkehrung. Wir empfehlen Ihnen trotzdem die SSID nach der Erstinstallation zu ändern (siehe Kapitel "9.5 SSID (= WLAN Domain) ändern").

Nach der Erstinstallation empfehlen wir Ihnen die Kapitel "12.1 Sicherheit für Ihre Konfiguration" bis und mit Kapitel "12.3.3 WEP - Sicherheit für Ihr WLAN" zu lesen und Sicherheitsmerkmale entsprechend Ihren Bedürfnissen einzurichten. Einige in den vorgenannten Kapiteln beschriebenen Sicherheitseinrichtungen:

Aus Sicherheitsgründen empfehlen wir Ihnen nach der Erstinstallation die Erstellung einer Liste der MobilePorts, die über den AccessPoint Zutritt (oder keinen Zutritt) zum WAN haben sollen. Sehen Sie dazu Kapitel "9.6 Access Control mittels MAC-Adressenliste".

Eine weitere Sicherheitsvorkehrung nach der Erstinstallation ist WEP (Wired Equivalent Privacy). Für die Einstellungen am AccessPoint sehen Sie Kapitel "9.7 AccessPoint WEP Verschlüsselung", für die Einstellungen am MobilePort, Kapitel "6.1.2.2 MobilePort WEP Verschlüsselung".

7

CD-ROM wechseln und Fehlermeldung 'Datei nicht gefunden'

Legen Sie nun wie aufgefordert, die Windows 95 CD-ROM ein. Starten Sie nach dem Hochlaufen den Kopiervorgang durch Klick auf **OK**. Erscheint die Fehlermeldung, dass eine Datei nicht gefunden wurde, geben Sie unter 'Quelle' den Buchstaben Ihres CD-ROM Laufwerks ein (z.B. F), gefolgt vom Pfad : \WIN95 und bestätigen Sie mit **OK**. Die Dateien werden fertig kopiert. Beantworten Sie die Fragen, ob der Computer neu gestartet werden soll, jeweils mit **Nein**.

8 TCP/IP-Protokoll installieren & IP-Adresse automatisch beziehen (I-GATE 11M AccessPoint als DHCP-Server)

Doppelklicken Sie in der 'Systemsteuerung' (**Start -> Einstellungen -> Systemsteuerung**) das Icon **Netzwerk**. Das Fenster Netzwerk öffnet sich. Wählen Sie das Register **Konfiguration**. Klicken Sie auf **Hinzufügen**, sofern im Register 'Konfiguration' TCP/IP fehlen sollte. Das Fenster 'Netzwerkkomponententyp auswählen' öffnet sich. Markieren Sie **Protokoll** und bestätigen Sie mit **Hinzufügen**. Das Fenster 'Netzwerkprotokoll auswählen' öffnet sich. Markieren Sie unter 'Hersteller' **Microsoft** und unter 'Netzwerkprotokolle' **TCP/IP**. Bestätigen Sie mit **OK**. Im Fenster 'Netzwerk' sehen Sie neu den Eintrag 'TCP/IP'. Markieren Sie den Eintrag **TCP/IP** und klicken Sie auf **Eigenschaften**. Das Fenster 'Eigenschaften für TCP/IP' öffnet sich. Wählen Sie das Register 'IP-Adresse' und aktivieren Sie die Option **IP-Adresse automatisch beziehen**. Schliessen Sie das Fenster 'Eigenschaften für TCP/IP' mit **OK**. Schliessen Sie ebenfalls das Fenster 'Netzwerk' mit **OK**.

Wenn Sie mit fixen IP-Adressen arbeiten wollen, verfahren Sie gemäss Punkt 9. Sonst gehen Sie zu Punkt 10.

9 Fixe IP-Adresse

Doppelklicken Sie in der 'Systemsteuerung' (**Start -> Einstellungen -> Systemsteuerung**) das Icon **Netzwerk**. Das Fenster 'Netzwerk' öffnet sich.

Im Register 'Konfiguration' markieren Sie den Eintrag **TCP/IP -> I-GATE 11M PCI MobilePort** und klicken Sie auf **Eigenschaften**. Das Fenster 'Eigenschaften von TCP/IP' öffnet sich.

Wählen Sie das Register 'IP-Adresse' und aktivieren Sie die Option **IP-Adresse festlegen**. Geben Sie in den nun freigegebenen Eingabefeldern die gewünschten fixen Daten (IP-Adresse, Subnet-Mask und Gateway) des TCP/IP -Stacks des Rechners ein. Vergessen Sie nicht den DNS-Server anzugeben; dieser wird für den Internet-Zugang unbedingt benötigt. In der Betriebsart nach **Bild 1.2** oder **Bild 1.8** (I-GATE 11M AccessPoint als Internet-Zugangsrouten für ein WLAN) muss das Gateway und der DNS-Server auf die IP-Adresse des AccessPoints konfiguriert werden.

Sie haben nun alle erforderlichen Einstellungen für fixe IP-Adressen vorgenommen und können deshalb den Netzwerkdialog mit **OK** beenden.

10 Windows 95 CD-ROM einlegen

Sie werden jetzt aufgefordert, die Windows 95 CD-ROM einzulegen. Da diese bereits eingelegt ist, bestätigen Sie mit **OK**. Eventuell müssen Sie den Pfad analog Punkt 7 anpassen. Die Dateien werden nun kopiert.

11 Computer neu starten

Das System fragt, ob der Computer neu gestartet werden soll. Entfernen Sie die Windows 95 CD-ROM und antworten Sie mit **Ja**.



Möglicherweise erscheint nach dem Neustart der Hinweis, dass der DHCP-Client keine IP-Adresse erhalten konnte. Das ist normal, solange keine Verbindung zum AccessPoint besteht. Schliessen Sie das Fenster 'DHCP Client' durch Drücken des Buttons **Nein**. Sollte der Hinweis nicht erscheinen, fahren Sie weiter bei Punkt 12.

12 Betriebsanzeigen (LEDs)



Der I-GATE 11M PCI ist mit einer LED versehen. Bei einem erfolgreich installierten Treiber muss diese permanent grün blinken.

grün blinken = MobilePort sucht AccessPoint (Scanning)

grün leuchten = MobilePort hat AccessPoint gefunden (Associated)

Wie Sie Probleme beheben können, lesen Sie im Kapitel "[13.1 Ist der MobilePort Treiber erfolgreich geladen?](#)" nach.

13 Benutzernamen und Kennwort eingeben

Das System fordert Sie eventuell auf, einen Benutzernamen und ein Kennwort einzugeben. Beide Werte sind frei wählbar.



Beachten Sie, dass Sie in Zukunft nach jedem Neustart nach den von Ihnen festgelegten Benutzernamen und Kennwort gefragt werden. Sie können das Feld 'Kennwort' leer lassen. In diesem Fall müssen Sie auch in Zukunft kein Kennwort eingeben. Wiederholen Sie Ihre erste Eingabe und bestätigen Sie anschliessend mit **OK**.

14

Zurück zu Kapitel "[2 MobilePort Hardware installieren](#)", wenn Sie weitere MobilePorts installieren möchten, sonst weiter zu Kapitel "[3.2 MobilePort Manager installieren](#)".

3.1.2 Treiber für I-GATE 11M PCI unter Windows 98



Die I-GATE 11M PC Card und die I-GATE 11M PC Card plus dürfen bei eingeschaltetem PC weder in die PCI-Adapterkarte eingeschoben noch herausgezogen werden. Nichtbeachtung kann die Beschädigung der PC Cards zur Folge haben.

1 Treiber suchen - automatische Kennung

Nachdem Sie Ihre I-GATE 11M PCI gemäss Kapitel "2.1 I-GATE 11M PCI in den PC einbauen" installiert haben und nachdem Ihr PC wieder hochgefahren ist, öffnet sich der Hardware-Assistent mit der Meldung, dass er nach neuen Treibern für 'PCI Network Controller' sucht. Klicken Sie auf **Weiter**. Der Hardware-Assistent fragt nun, wie Sie vorgehen möchten. Stellen Sie sicher, dass 'Nach einem passenden Treiber für das Gerät suchen' angewählt ist und gehen Sie zu Punkt 2.

Treiber suchen - manuelle Kennung

Sollte sich der Hardware-Assistent nicht öffnen, starten Sie die Installation mit **Start -> Einstellungen -> Systemsteuerung -> Hardware** und klicken Sie viermal auf **Weiter**. Gehen Sie zu Punkt 2.

2 I-GATE 11M CD-ROM einlegen

Legen Sie die I-GATE 11M CD-ROM ein. Sollte sich das I-GATE 11M CD-Einstiegsbild öffnen, so schliessen Sie es. Klicken Sie auf **Weiter**.

Im folgenden Fenster selektieren Sie nur die Option 'CD-ROM Laufwerk' und bestätigen Sie mit **Weiter**.

3 Treiberdatei gefunden

Der Treiber für 'I-GATE 11M PCI' wird gefunden. Klicken Sie auf **Weiter**.

4 SSID (= WLAN-Domain) eingeben

Markieren Sie im sich automatisch öffnenden Fenster 'Eigenschaften von I-GATE 11M PCI' die Zeile **SSID** (Service Set Identifier) und geben Sie in das Feld 'Wert' die Seriennummer des AccessPoints ein. Diese finden Sie auf dem Typenschild auf der Rückseite des AccessPoints. Die ersten 5 Stellen sind Buchstaben wobei der Buchstabe 'O' nicht verwendet wird. Beachten Sie die Gross-/Kleinschreibung! Die folgenden 7 Stellen sind Zahlen. (Bild 3.4)

Diese Vorgabe ist bei der Erstinstallation zwingend. (Falls die SSID bereits geändert wurde, muss der aktuelle Wert eingegeben werden.)

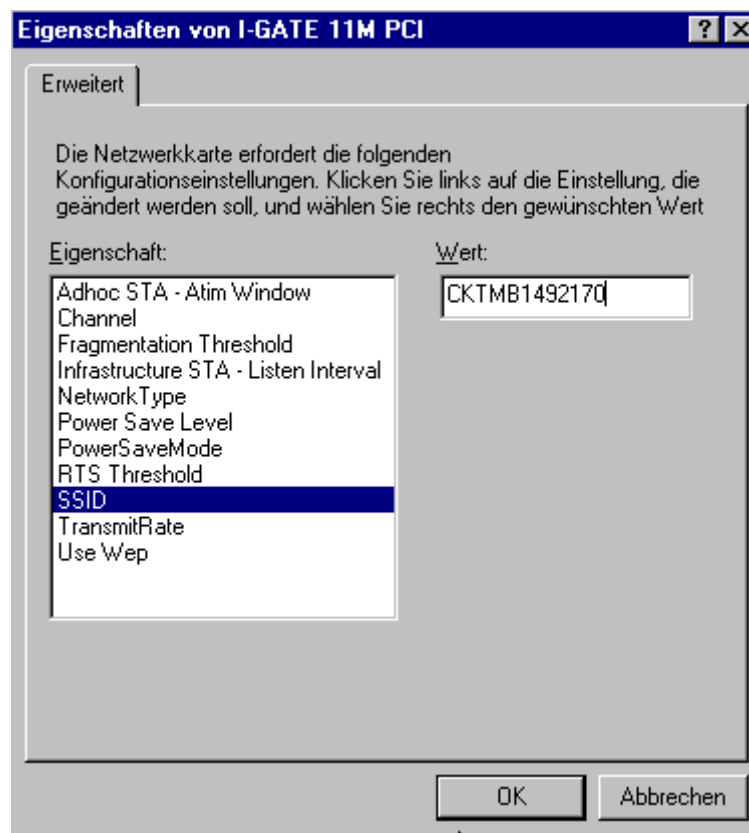


Bild 3.4 SSID eingeben unter Windows 95/98

5 Bestätigen Sie Ihre Eingabe mit **OK**.



Sicherheit nach der Erstinstallation

Die SSID dient lediglich der Zuordnung zu einem AccessPoint und entspricht damit noch keiner Sicherheitsvorkehrung. Wir empfehlen Ihnen trotzdem die SSID nach der Erstinstallation zu ändern (siehe Kapitel "9.5 SSID (= WLAN Domain) ändern").

Nach der Erstinstallation empfehlen wir Ihnen die Kapitel "12.1 Sicherheit für Ihre Konfiguration" bis und mit Kapitel "12.3.3 WEP - Sicherheit für Ihr WLAN" zu lesen und Sicherheitsmerkmale entsprechend Ihren Bedürfnissen einzurichten. Einige in den vorgenannten Kapiteln beschriebenen Sicherheitseinrichtungen:

Aus Sicherheitsgründen empfehlen wir Ihnen nach der Erstinstallation die Erstellung einer Liste der MobilePorts, die über den AccessPoint Zutritt (oder keinen Zutritt) zum WAN haben sollen. Sehen Sie dazu Kapitel "9.6 Access Control mittels MAC-Adressenliste".

Eine weitere Sicherheitsvorkehrung nach der Erstinstallation ist WEP (Wired Equivalent Privacy). Für die AccessPoint Einstellungen sehen Sie Kapitel "9.7 AccessPoint WEP Verschlüsselung", für die Einstellungen am MobilePort, Kapitel "6.1.2.2 MobilePort WEP Verschlüsselung".

6 CD-ROM wechseln

Legen Sie die Windows 98 CD-ROM ein und bestätigen Sie mit **OK**. Die Dateien werden kopiert. Beenden Sie die Installation mit **Fertigstellen**. Beantworten Sie die Fragen ob ein Neustart durchgeführt werden soll, jeweils mit **Nein**.

7 IP-Adresse automatisch beziehen (I-GATE 11M AccessPoint als DHCP-Server)

Doppelklicken Sie in der 'Systemsteuerung' (**Start -> Einstellungen -> Systemsteuerung**) das Icon **Netzwerk**. Das Fenster Netzwerk öffnet sich. Wählen Sie das Register **Konfiguration**. Markieren Sie den Eintrag **TCP/IP -> I-GATE 11M PCI** und klicken Sie auf **Eigenschaften**. Wählen Sie das Register 'IP-Adresse' und aktivieren Sie die Option **IP-Adresse automatisch beziehen**. Schliessen Sie das Fenster 'Eigenschaften von TCP/IP' mit **OK**. Schliessen Sie ebenfalls das Fenster 'Netzwerk' mit **OK**. Starten Sie Ihren Computer neu.

Wenn Sie mit fixen IP-Adressen arbeiten wollen, verfahren Sie gemäss Punkt 8. Sonst gehen Sie zu Punkt 9.

8 Fixe IP-Adresse

Doppelklicken Sie in der 'Systemsteuerung' (**Start -> Einstellungen -> Systemsteuerung**) das Icon **Netzwerk**. Das Fenster 'Netzwerk' öffnet sich.

Im Register 'Konfiguration' markieren Sie den Eintrag **TCP/IP -> I-GATE 11M PCI MobilePort** und klicken Sie auf **Eigenschaften**. Das Fenster 'Eigenschaften von TCP/IP' öffnet sich.

Wählen Sie das Register 'IP-Adresse' und aktivieren Sie die Option **IP-Adresse festlegen**. Geben Sie in den nun freigegebenen Eingabefeldern die gewünschten fixen Daten (IP-Adresse, Subnet-Mask und Gateway) des TCP/IP -Stacks des Rechners ein. Vergessen Sie nicht den DNS-Server anzugeben; dieser wird für den Internet-Zugang unbedingt benötigt. In der Betriebsart nach [Bild 1.2](#) oder [Bild 1.8](#) (I-GATE 11M AccessPoint als Internet-Zugangsrouten für ein WLAN) muss das Gateway und der DNS-Server auf die IP-Adresse des AccessPoints konfiguriert werden.

Sie haben nun alle erforderlichen Einstellungen für fixe IP-Adressen vorgenommen und können deshalb den Netzwerkdialog mit **OK** beenden. Auf die Frage, ob der Computer neu gestartet werden soll, antworten Sie mit **Ja**.

9 Betriebsanzeigen (LEDs)



Der I-GATE 11M PCI ist mit einer LED versehen. Bei einem erfolgreich installierten Treiber muss diese permanent grün blinken.

grün blinken = MobilePort sucht AccessPoint (Scanning)

grün leuchten = MobilePort hat AccessPoint gefunden (Associated)

Wie Sie Probleme beheben können, lesen Sie im Kapitel "[13.1 Ist der MobilePort Treiber erfolgreich geladen?](#)" nach.

- 10 Zurück zu Kapitel "[2 MobilePort Hardware installieren](#)" wenn Sie weitere MobilePorts zu installieren haben, sonst weiter zu Kapitel "[3.2 MobilePort Manager installieren](#)".

3.1.3 Treiber für I-GATE 11M PCI unter Windows NT



Die I-GATE 11M PC Card und die I-GATE 11M PC Card plus dürfen bei eingeschaltetem PC weder in die PCI-Adapterkarte eingeschoben noch herausgezogen werden. Nichtbeachtung kann die Beschädigung der PC Cards zur Folge haben.

Sie haben Ihre I-GATE 11M PCI gemäss Kapitel "[2.1 I-GATE 11M PCI in den PC einbauen](#)" installiert und haben Ihren PC wieder hochgefahren.

Wenn Sie nicht mindestens Service Pack 6 installiert haben, spielen Sie dieses jetzt auf. Service Pack 6 resp. 6a finden Sie auf der I-GATE 11M CD-ROM unter **CD durchsuchen -> misc -> nt4spx** in Ihrer Sprache.

3.1.3.1 NT-Netzwerkunterstützung installieren

In diesem Kapitel installieren Sie den Loopback-Adapter, damit die für den Netzwerkbetrieb notwendigen Dateien auf die Festplatte Ihres PCs geschrieben werden. Der Loopback-Adapter selbst wird nicht benötigt und anschliessend wieder gelöscht. (Falls der TCP/IP-Protokollstack bereits vollständig vorhanden ist, kann auf die Installation des Loopback-Adapters verzichtet werden. Fahren Sie dann weiter mit "[3.1.3.2 BIOS Einstellungen](#)". Sollte der TCP/IP-Protokollstack noch nicht vollständig vorhanden sein, fahren Sie bei Punkt 1 weiter.

- 1 Doppelklicken Sie unter **Start -> Einstellungen -> Systemsteuerung** das Icon **Netzwerk**. Sie werden gefragt, ob Sie die Windows NT-Netzwerkunterstützung jetzt installieren möchten. Bestätigen Sie mit **Ja**.

Das Fenster 'Assistent für die Netzwerkinstallation' öffnet sich. Wählen Sie **Direkt am Netzwerk anschliessen** und **Weiter**. Klicken Sie danach auf **Aus Liste auswählen....**

- 2 **Loopback-Adapter wählen**

In dem sich öffnenden Auswahlfenster wählen Sie den Eintrag **MS Loopback-Adapter**, klicken auf **OK** und anschliessend auf **Weiter**.

3 Protokoll wählen

Im Fenster 'Assistent für die Netzwerkinstallation' sehen Sie jetzt die Liste der Netzwerkprotokolle. Wählen Sie **TCP/IP-Protokoll**.

4 Netzwerkdienste wählen

Mit **Weiter** gelangen Sie ins Verzeichnis der Netzwerkdienste. Wir empfehlen, alle aufgeführten Dienste auszuwählen. Klicken Sie zweimal auf **Weiter**. Es erscheint das Fenster 'Windows NT-Setup'.

Legen Sie die Windows NT CD-ROM ein. Falls sich das NT- Einstiegsbild öffnet, schliessen Sie es.

5 Installation Netzwerkunterstützung starten

Geben Sie im Fenster 'Windows NT-Setup' den Laufwerksbuchstaben des CD-ROM Laufwerks ein (z.B. F:\) und klicken Sie nach dem Hochlaufen des Laufwerks in den folgenden Fenstern zweimal auf **Fortsetzen**. Sie werden nun gefragt, ob Sie DHCP verwenden wollen. Antworten Sie mit **Ja**.



Die Daten für die Netzwerkunterstützung und das TCP/IP-Protokoll werden nun kopiert. Dies kann einige Minuten dauern.

6 Installation Netzwerkunterstützung beenden

Nach abgeschlossener Installation werden die Netzwerkbindungen angezeigt. Klicken Sie zweimal auf **Weiter** und warten Sie, bis die Konfiguration gesichert wurde. Das kann einige Minuten dauern. Beantworten Sie allfällige weitere Fragen ob DHCP Meldungen angezeigt werden sollen mit **JA**. Sie erhalten die Meldung, dass der DHCP-Client keine IP-Adresse erhalten konnte. Beantworten Sie die Frage, ob DHCP-Meldungen weiterhin angezeigt werden sollen, mit **JA**.

Im folgenden Fenster werden die Daten (Computername, Arbeitsgruppe etc.) abgefragt, die beim Einsatz mehrerer MobilePorts benötigt werden (siehe auch Kap. "9.5 SSID (= WLAN Domain ändern)"). Klicken Sie bei der Erstinstallation auf **Weiter** und anschliessend auf **Fertigstellen**. Eventuell werden Sie gefragt, ob der Computername so geändert werden soll, dass er auch im Internet gültig ist. Antworten Sie mit **Nein**.

Beantworten Sie die Frage, ob der Computer neu gestartet werden soll, mit **Nein**. Doppelklicken Sie in der 'Systemsteuerung' das Icon **Netzwerk**. Wählen Sie das Register 'Netzwerkkarte' und selektieren Sie **MS Loopback-Adapter**. Löschen Sie diesen mit **Entfernen** und bestätigen Sie die Rückfrage mit **Ja**. Schliessen Sie das Fenster 'Netzwerk' mit **Schliessen**. Beantworten Sie die Frage, ob der Computer neu gestartet werden soll, mit **Nein**. Entfernen Sie die Windows NT CD-ROM. Fahren Sie den PC herunter mit **Start -> Beenden - Computer herunterfahren** und schalten Sie ihn aus.

3.1.3.2 BIOS Einstellungen

7 Starten sie Ihr PC neu und drücken Sie die Tasten gemäss dem Handbuch Ihres PCs, um ins BIOS Setup zu gelangen. Kontrollieren bzw. aktivieren Sie folgende Einstellungen:

8 Die Einstellung 'Plug & Play OS' (PnP OS) sollte auf 'Nein' stehen, da Sie ein nicht Plug&Play-fähiges Betriebssystem (Windows NT4) verwenden.

Als PCI-Gerät ist das MobilePort dazu fähig ein Interrupt zu teilen und so muss dafür keinen eigenen Interrupt reserviert werden. Jedoch setzen Sie die Einstellung 'Reset Configuration Data' (je nach Rechner auch 'Reset PCI Configuration' genannt) auf 'JA'.

Speichern Sie die Einstellungen und starten Sie Ihren PC neu. Je nach Version Ihrer Betriebssystem CD-ROM erscheinen ev. Fehlermeldungen während des Aufstartens, welche Sie zum jetzigen Zeitpunkt ignorieren können.

3.1.3.3 MobilePort Treiber-Installation

9 Legen Sie jetzt die I-GATE 11M CD-ROM mit den Treibern in das Laufwerk. Sollte sich das I-GATE 11M CD-Einstiegsbild öffnen, schliessen Sie es.

Doppelklicken Sie in der 'Systemsteuerung' das Icon **Netzwerk**. Das Fenster 'Netzwerk' öffnet sich. Wählen Sie das Register 'Netzwerkkarte' und klicken Sie auf **Hinzufügen....**

10 Pfad eingeben und OEM-Option auswählen

In dem sich öffnenden Fenster 'Auswahl: Netzwerkkarte' klicken Sie auf **Diskette...**. Geben Sie nun den Laufwerksbuchstaben Ihres CD-ROM Laufwerkes (z.B. F:\) ein. Bestätigen Sie mit **OK**. Im Fenster 'OEM-Option auswählen' selektieren Sie 'I-GATE 11M PCI' und klicken auf 'OK'.

11 SSID (= WLAN-Domain) eingeben

Markieren Sie im sich automatisch öffnenden Fenster 'I-GATE 11M PCI Setup' die Zeile **SSID** (Service Set Identifier) und geben Sie in das Feld 'Wert' die Seriennummer des AccessPoints ein. Diese finden Sie auf dem Typenschild auf der Rückseite des AccessPoints. Die ersten 5 Stellen sind Buchstaben wobei der Buchstabe 'O' nicht verwendet wird. Beachten Sie die Gross-/Kleinschreibung! Die folgenden 7 Stellen sind Zahlen. (Bild 3.5)

Die Eingabe der SSID ist bei der Erstinstallation zwingend. Falls die SSID bereits geändert wurde, müssen Sie den aktuellen Wert eingeben.



Sicherheit nach der Erstinstallation

Die SSID dient lediglich der Zuordnung zu einem AccessPoint und entspricht damit noch keiner Sicherheitsvorkehrung. Wir empfehlen Ihnen trotzdem die SSID nach der Erstinstallation zu ändern (siehe Kapitel "9.5 SSID (= WLAN Domain) ändern").

Nach der Erstinstallation empfehlen wir Ihnen die Kapitel "12.1 Sicherheit für Ihre Konfiguration" bis und mit Kapitel "12.3.3 WEP - Sicherheit für Ihr WLAN" zu lesen und Sicherheitsmerkmale entsprechend Ihren Bedürfnissen einzurichten. Einige in den vorgenannten Kapiteln beschriebenen Sicherheitseinrichtungen:

Aus Sicherheitsgründen empfehlen wir Ihnen nach der Erstinstallation die Erstellung einer Liste der MobilePorts, die über den AccessPoint Zutritt (oder keinen Zutritt) zum WAN haben sollen. Sehen Sie dazu Kapitel "9.6 Access Control mittels MAC-Adressenliste".

Eine weitere Sicherheitsvorkehrung nach der Erstinstallation ist WEP (Wired Equivalent Privacy). Für die Einstellungen am AccessPoint sehen Sie Kapitel "9.7 AccessPoint WEP Verschlüsselung", für die Einstellungen am MobilePort, Kapitel "6.1.2.2 MobilePort WEP Verschlüsselung".

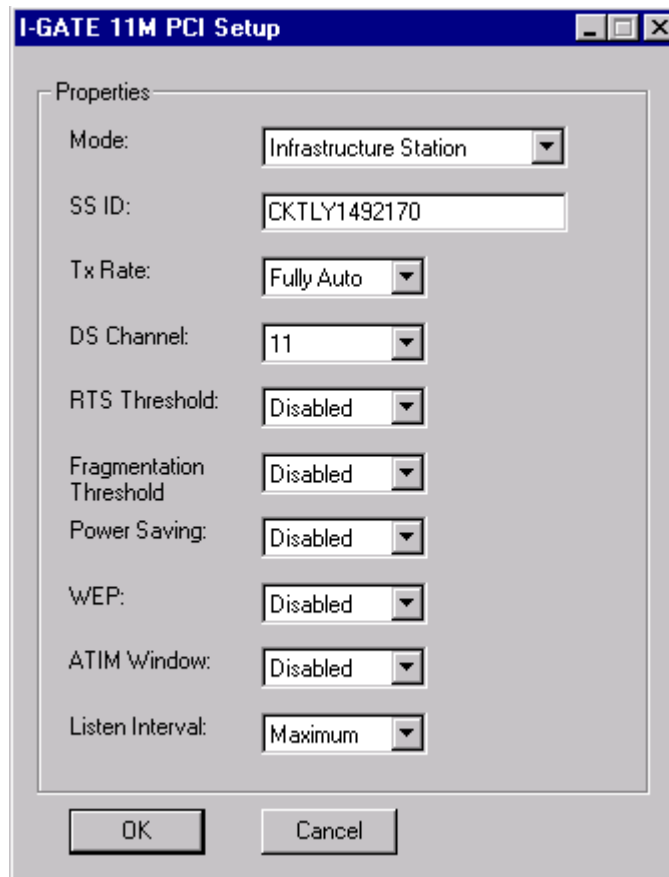


Bild 3.5 SSID eingeben unter Windows NT4

12

Schliessen Sie Ihre Eingabe mit **OK** ab.

13

Netzwerkbindungen kontrollieren (Bild 3.6)

Im Fenster 'Netzwerk' erscheint jetzt neu der Eintrag 'I-GATE 11M PCI'. Wechseln Sie auf die Registerkarte 'Bindungen' und kontrollieren Sie durch Klick auf die Plus-Zeichen im Verzeichnisbaum, ob 'I-GATE 11M PCI' bei allen Diensten aufgeführt wird (siehe Bild 3.6).

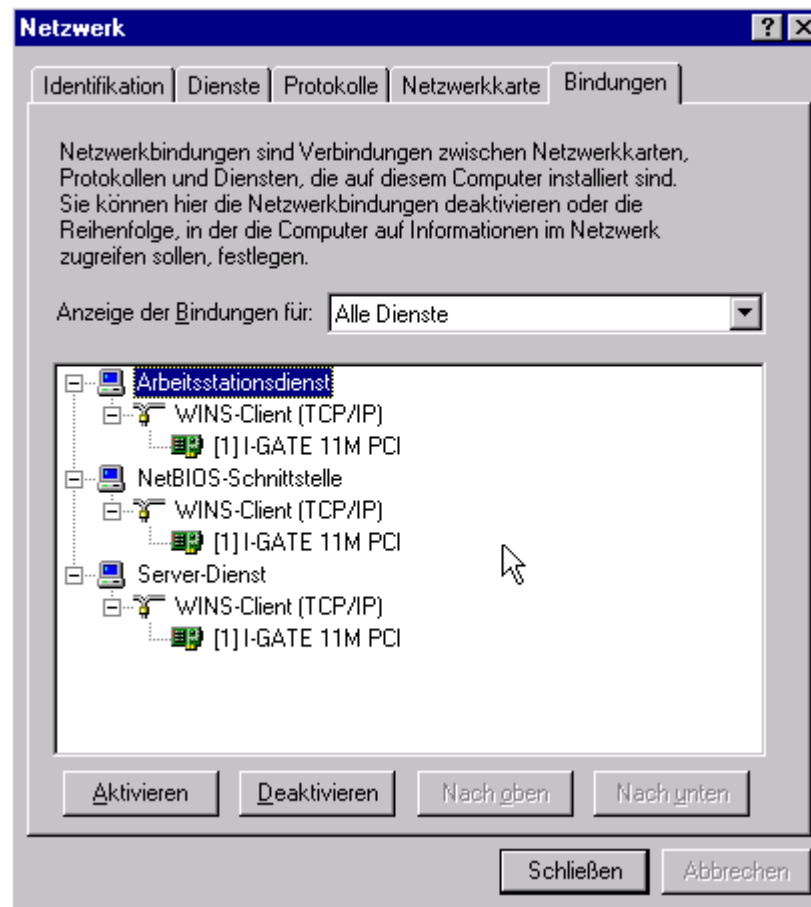


Bild 3.6 Netzwerkbindungen kontrollieren

14

IP-Adresse automatisch beziehen (I-GATE 11M AccessPoint als DHCP-Server)

Wählen Sie das Register **Protokolle**. Markieren Sie den Eintrag **TCP/IP Protokoll** und klicken Sie auf **Eigenschaften**. Wählen Sie im Fenster 'Eigenschaften von Microsoft TCP/IP' unter 'Netzwerkwerkarte' den Eintrag **I-GATE 11M PCI** und aktivieren Sie die Option **IP-Adresse von einem TCP/IP-Server beziehen**. Beantworten Sie die Frage, ob Sie DHCP aktivieren möchten mit **Ja**. Fahren Sie mit **OK** und **Schliessen** weiter, bis die Frage erscheint, ob der Computer neu gestartet werden soll. Beantworten Sie die Frage mit **Ja**. Beantworten Sie allfällige Fehlermeldungen mit **OK**.

Wenn Sie mit fixen IP-Adressen arbeiten wollen, verfahren Sie gemäss Punkt 15 und 16. Sonst gehen Sie zu Punkt 17.

15**Fixe IP-Adresse**

Wählen Sie das Register 'Protokolle', markieren Sie den Eintrag **TCP/IP-Protokoll** und klicken Sie auf **Eigenschaften**. Das Fenster 'Eigenschaften von Microsoft TCP/IP' öffnet sich.

Im Register 'IP-Adresse' aktivieren Sie die Option **IP-Adresse angeben**. Geben Sie in den nun freigegebenen Eingabefeldern die gewünschten fixen Daten (IP-Adresse, Subnet-Mask und Gateway) des TCP/IP -Stacks des Rechners ein. Vergessen Sie nicht den DNS-Server anzugeben; dieser wird für den Internet-Zugang unbedingt benötigt. In der Betriebsart nach **Bild 1.2** oder **Bild 1.8** (I-GATE 11M AccessPoint als Internet-Zugangsrouten für ein WLAN) muss das Gateway und der DNS-Server auf die IP-Adresse des AccessPoints konfiguriert werden.

Um die Werte zu aktualisieren, wählen Sie als nächstes das Register 'Bindungen'. Sie haben nun alle erforderlichen Einstellungen für fixe IP-Adressen vorgenommen und können deshalb den Netzwerkdialog mit **Schliessen** beenden. Auf die Frage, ob der Computer neu gestartet werden soll, antworten Sie mit **Ja**.

16**Computer neu starten**

Nach dem Neustart erscheint der Hinweis, dass der DHCP-Client keine IP-Adresse erhalten konnte. Das ist normal, solange noch keine Verbindung mit dem AccessPoint besteht. Beantworten Sie die Frage, ob DHCP-Meldungen weiterhin angezeigt werden sollen, mit **Nein**.

Eventuell weist Sie der 'Dienstkontroll-Manager' darauf hin, dass der Start mindestens eines Dienstes fehlgeschlagen ist. Klicken Sie auf **OK**.

17**Betriebsanzeigen (LEDs).**

Der I-GATE 11M PCI ist mit einer LED versehen. Bei einem erfolgreich installierten Treiber muss diese permanent grün blinken.

grün blinken = MobilePort sucht AccessPoint (Scanning)

grün leuchten = MobilePort hat AccessPoint gefunden (Associated)

Wie Sie Probleme beheben können, lesen Sie im Kapitel "[13.1 Ist der MobilePort Treiber erfolgreich geladen?](#)" nach.

Wenn Sie trotzdem noch Probleme haben, können diese mit dem aufspielen von Ihrem Service Pack (mindestens Service Pack 6 - Service Packs 6 resp. 6a finden Sie auf der I-GATE 11M CD-ROM unter **CD durchsuchen -> misc -> nt4spx** in Ihrer Sprache) behoben werden. Führen Sie jedoch zuerst Punkt 18 aus.

18

Zurück zu Kapitel "[2 MobilePort Hardware installieren](#)" wenn Sie weitere MobilePorts zu installieren haben, sonst weiter zu Kapitel "[3.2 MobilePort Manager installieren](#)".

3.1.4 Treiber für I-GATE 11M PCI unter Windows 2000



Die I-GATE 11M PC Card und die I-GATE 11M PC Card plus dürfen bei eingeschaltetem PC weder in die PCI-Adapterkarte eingeschoben noch herausgezogen werden. Nichtbeachtung kann die Beschädigung der PC Cards zur Folge haben.

1

Treiber suchen - automatische Kennung

Nachdem Sie Ihre I-GATE 11M PCI gemäss Kapitel "2.1 I-GATE 11M PCI in den PC einbauen" installiert haben und nachdem Ihr PC wieder hochgefahren ist öffnet sich der Assistent für das Suchen neuer Hardware mit der Meldung, dass er einen Treiber für ein neues Gerät installiert. Klicken Sie auf **Weiter**. Der Assistent für das Suchen neuer Hardware fragt nun, wie Sie vorgehen möchten. Gehen Sie zu Punkt 2.

Treiber suchen - manuelle Kennung

Sollte sich der Assistent für das Suchen neuer Hardware nicht öffnen, starten Sie die Installation mit **Start -> Einstellungen -> Systemsteuerung -> Hardware** und klicken Sie dreimal auf **Weiter**. Markieren Sie den Eintrag 'Netzwerkcontroller' und klicken Sie auf **Weiter** und dann auf **Fertig stellen**. Im Assistent zum Aktualisieren von Gerätetreibern klicken Sie auf **Weiter**. Der Assistent zum Aktualisieren von Gerätetreibern fragt nun, wie Sie vorgehen möchten. Stellen Sie sicher, dass 'Nach einem passenden Treiber für das Gerät suchen' angewählt ist und gehen Sie zu Punkt 2.

2

I-GATE 11M CD-ROM einlegen

Legen Sie die I-GATE 11M CD-ROM ein. Sollte sich das I-GATE 11M CD-Einstiegsbild öffnen, so schliessen Sie es mit **Beenden**. Klicken Sie auf **Weiter**.

Im folgenden Fenster selektieren Sie auf die Frage, wo die Treiber gesucht werden sollen, nur die Option 'CD-ROM Laufwerk' und bestätigen mit **Weiter**.

3 Treiberdatei gefunden

Ein Treiber für das Gerät 'Netzwerkcontroller' wird gefunden. Klicken Sie auf **Weiter**. Das Fenster mit der Meldung, dass Windows 2000 keine Microsoft digitale Signatur für 'I-GATE 11M PCI' findet, öffnet sich. Beantworten Sie die Frage, ob die Installation fortgesetzt werden soll, mit **Ja**. Klicken Sie auf 'Fertig stellen'.

4 SSID (= WLAN-Domain) eingeben

Markieren Sie unter **Start -> Eigenschaften -> Systemsteuerung -> Netzwerk- und DFU-Verbindungen -> LAN Verbindung 2 -> Eigenschaften -> Konfigurieren -> Erweiterte Einstellungen** im Fenster 'Eigenschaften von I-GATE 11M PCI' die Zeile **SSID** (Service Set Identifier) und geben Sie in das Feld 'Wert' die Seriennummer des AccessPoints ein. Diese finden Sie auf dem Typenschild auf der Rückseite des AccessPoints. Die ersten 5 Stellen sind Buchstaben wobei der Buchstabe 'O' nicht verwendet wird. Beachten Sie die Gross-/Kleinschreibung! Die folgenden 7 Stellen sind Zahlen. (Bild 3.7)

Die Eingabe der SSID ist bei der Erstinstallation zwingend. Falls die SSID bereits geändert wurde, müssen Sie den aktuellen Wert eingeben.



Sicherheit nach der Erstinstallation

Die SSID dient lediglich der Zuordnung zu einem AccessPoint und entspricht damit noch keiner Sicherheitsvorkehrung. Wir empfehlen Ihnen trotzdem die SSID nach der Erstinstallation zu ändern (siehe Kapitel "9.5 SSID (= WLAN Domain) ändern").

Nach der Erstinstallation empfehlen wir Ihnen die Kapitel "12.1 Sicherheit für Ihre Konfiguration" bis und mit Kapitel "12.3.3 WEP - Sicherheit für Ihr WLAN" zu lesen und Sicherheitsmerkmale entsprechend Ihren Bedürfnissen einzurichten. Einige in den vorgenannten Kapiteln beschriebenen Sicherheitseinrichtungen:

Aus Sicherheitsgründen empfehlen wir Ihnen nach der Erstinstallation die Erstellung einer Liste der MobilePorts, die über den AccessPoint Zutritt (oder keinen Zutritt) zum WAN haben sollen. Sehen Sie dazu Kapitel "9.6 Access Control mittels MAC-Adressenliste".

Eine weitere Sicherheitsvorkehrung nach der Erstinstallation ist WEP (Wired Equivalent Privacy). Für die Einstellungen am AccessPoint sehen Sie Kapitel "9.7 AccessPoint WEP Verschlüsselung", für die Einstellungen am MobilePort, Kapitel "6.1.2.2 MobilePort WEP Verschlüsselung".

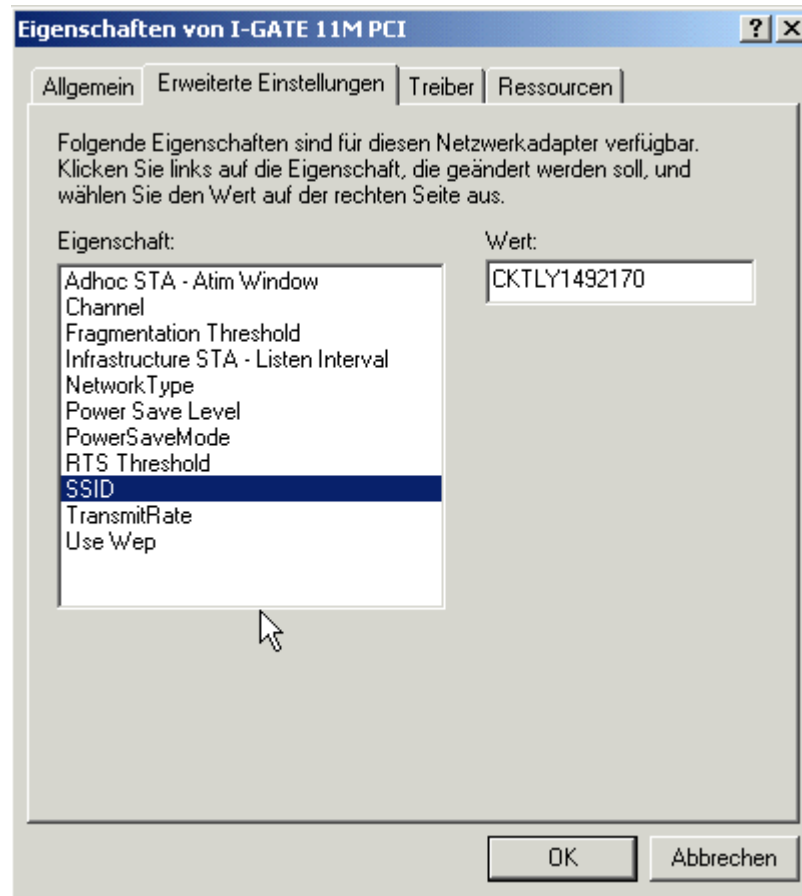


Bild 3.7 SSID eingeben unter Windows 2000

- 5** Bestätigen Sie Ihre Eingabe mit **OK**.
- 6** **IP-Adresse automatisch beziehen (I-GATE 11M AccessPoint als DHCP-Server)**

Das Fenster 'Eigenschaften von LAN-Verbindung 2' öffnet sich. Markieren Sie den Eintrag **Internetprotokoll (TCP/IP)** und klicken Sie auf **Eigenschaften**. Aktivieren Sie die Option **IP-Adresse automatisch beziehen** und die Option **DNS-Serveradresse automatisch beziehen**. Schliessen Sie das Fenster 'Eigenschaften von Internetprotokoll (TCP/IP)' mit **OK**. Schliessen alle weitere Fenster, entfernen Sie die I-GATE 11M CD und starten Sie Ihren Computer neu.

Wenn Sie mit fixen IP-Adressen arbeiten wollen, verfahren Sie gemäss Punkt 7. Sonst gehen Sie zu Punkt 8.

7 Fixe IP-Adresse

Klicken Sie auf **Start -> Einstellungen -> Systemsteuerung -> Netzwerk- und DFÜ-Verbindungen -> LAN-Verbindung -> Eigenschaften**.

Markieren Sie den Eintrag **Internetprotokoll (TCP/IP)** und klicken Sie auf **Eigenschaften**. Das Fenster 'Eigenschaften von Internetprotokoll (TCP/IP)' öffnet sich.

Aktivieren Sie die Option **Folgende IP-Adresse verwenden**. Geben Sie in den nun freigegebenen Eingabefeldern die gewünschten fixen Daten (IP-Adresse, Subnet-Mask und Gateway) des TCP/IP - Stacks des Rechners ein. Vergessen Sie nicht den DNS-Server anzugeben; dieser wird für den Internet-Zugang unbedingt benötigt. In der Betriebsart nach [Bild 1.2](#) oder [Bild 1.8](#) (I-GATE 11M AccessPoint als Internet-Zugangsrouten für ein WLAN) muss das Gateway und der DNS-Server auf die IP-Adresse des AccessPoints konfiguriert werden.

Sie haben nun alle erforderlichen Einstellungen für fixe IP-Adressen vorgenommen und können deshalb den Netzwerkdialog mit **OK** beenden. Auf die Frage, ob der Computer neu gestartet werden soll, antworten Sie mit **Ja**.

8 Betriebsanzeigen (LEDs)



Der I-GATE 11M PCI ist mit einer LED versehen. Bei einem erfolgreich installierten Treiber muss diese permanent grün blinken.

grün blinken = MobilePort sucht AccessPoint (Scanning)

grün leuchten = MobilePort hat AccessPoint gefunden (Associated)

Wie Sie Probleme beheben können, lesen Sie im Kapitel "[13.1 Ist der MobilePort Treiber erfolgreich geladen?](#)" nach.

9 Zurück zu Kapitel "[2 MobilePort Hardware installieren](#)", wenn Sie weitere MobilePorts zu installieren haben, sonst weiter zu Kapitel "[3.2 MobilePort Manager installieren](#)".

3.2 MobilePort Manager installieren

- 1 Entfernen Sie die Windows CD-ROM (Ausnahme: W2000, wo keine Windows CD-ROM eingelegt werden musste), legen Sie die I-GATE 11M CD-ROM ein und klicken Sie auf **I-GATE MobilePort Manager installieren**. Je nachdem welchen MobilePort Manager Sie installieren wollen, klicken Sie auf **PC Card MobilePort installieren**, **PCI Card MobilePort installieren** oder **USB MobilePort installieren**. Um den MobilePort Manager für PC Card plus zu installieren klicken Sie ebenfalls auf **PC Card MobilePort installieren**.

Sollte sich das I-GATE 11M CD-Einstiegsbild nicht automatisch öffnen, klicken Sie mit der rechten Maus Taste auf Ihr CD-ROM Laufwerk und dann auf **AutoPlay -> I-GATE MobilePort Manager installieren**. Je nachdem welchen MobilePort Manager Sie installieren wollen, klicken Sie dann auf **PC Card MobilePort installieren**, **PCI Card MobilePort installieren** oder **USB MobilePort installieren**.

- 2 Der 'I-GATE MobilePort Manager Setup' öffnet sich. Klicken Sie auf **Next**. Als Destination Folder erscheint 'C:\Programme\Siemens I-Gate\MobilePort Manager'. Klicken Sie zweimal auf **Next**. Bestätigen Sie die Meldung 'Setup is Complete.' mit **OK**.

- 3 Das Fenster 'I-GATE MobilePort Manager' öffnet sich. Doppelklicken Sie das 'MobilePort Manager' Verknüpfungssicon (grüner PC). Der MobilePort Manager erscheint nun als rotes PC Icon im Windows Taskbar Ihres Rechners. Schliessen Sie das Fenster 'I-GATE MobilePort Manager' und alle anderen Fenstern. Klicken Sie auf das rote PC Icon. Das Register 'Link Info' öffnet sich und im Feld 'State' erscheint 'Scanning'. Klicken Sie auf **OK**. Nach der Erstinstallation empfehlen wir Ihnen Kapitel **"6 MobilePort Management"** zu lesen.

4 Service Pack aufspielen



Wenn Sie den MobilePort Manager auf NT4 installiert haben und keinen AccessPoint installieren werden, spielen Sie Ihr Service Pack (mindestens Service Pack 6) jetzt neu auf.

Wenn Sie den MobilePort Manager auf NT4 installiert haben, Probleme beim installieren des MobilePorts hatten (z.B. nicht ständig blinkende LED oder DHCP resp. Dienst Fehlermeldungen) und einen AccessPoint installieren werden, spielen Sie Ihr Service Pack (mindestens Service Pack 6) jetzt neu auf.

Die Service Packs 6 resp. 6a finden Sie auf der I-GATE 11M CD-ROM unter **CD durchsuchen -> misc -> nt4spx** in Ihrer Sprache.

Nach dem Aufspielen des Service Packs muss die MobilePort LED permanent grün blinken.

grün blinken = MobilePort sucht AccessPoint (Scanning)

grün leuchten = MobilePort hat AccessPoint gefunden (Associated)

5 Weiter zu "8 I-GATE 11M AccessPoint Hardware anschliessen"

4 I-GATE 11M PC Card und I-GATE 11M PC-Card plus Software installieren

In diesem Kapitel wird die Installation einer I-GATE 11M PC Card auf den jeweiligen Betriebssystemen beschrieben. Verwenden Sie die selben Beschreibungen für die Installation einer I-GATE 11M PC-Card plus.

In dieser **Standard Installation** gehen wir davon aus, dass Sie ein TCP/IP-Netzwerk betreiben und dass Sie Ihre IP-Adressen über die DHCP-Server Funktion des AccessPoints automatisch (dynamisch) beziehen. Für den Fall, dass Sie fixe IP-Adressen verwenden möchten, haben wir diesen jeweils alternativ beschrieben.

Bevor Sie mit der Installation weiterfahren sollten Sie also wissen, ob Sie Ihr TCP/IP-Netzwerk mit dynamischen oder fixen IP-Adressen betreiben wollen und ob Sie die DHCP-Server Funktion des AccessPoints nutzen wollen.

Wenn Sie mit Netzwerken und IP-Adressen vertraut sind, gehen Sie zu Punkt 1 auf der folgenden Seite.

Wenn Sie nicht mit Netzwerken und IP-Adressen vertraut sind und dazu Entscheidungshilfen möchten, lesen Sie in diesem Handbuch die Kapitel "[9.2.1 AccessPoint Grundeinstellung über Siemens AccessPoint Manager](#)" und "[12.10 Automatische Adreßverwaltung mit DHCP](#)". Lesen Sie auch im Kapitel Technische Grundlagen des Referenzhandbuchs die Abschnitte 'Netzwerk-Arten' und 'IP-Adressierung'. Gehen Sie dann zu Punkt 1 auf der folgenden Seite.

Wenn Sie nicht mit Netzwerken und IP-Adressen vertraut sind und jetzt keine Zeit haben dies zu werden, empfehlen wir Ihnen die DHCP-Server Funktion des AccessPoints zu nutzen und die IP-Adresse aller Netzteilnehmer vom AccessPoint automatisch zu beziehen. So wählen Sie den Punkt 'IP-Adresse automatisch beziehen' wenn Sie zum Auswahl des Punkts 'IP-Adresse automatisch beziehen' oder des Punkts 'Fixe IP-Adresse' in diesem Kapitel kommen. Gehen Sie jetzt zu Punkt 1 auf der folgenden Seite.

4.1 Treiber für I-GATE 11M PC Card installieren

4.1.1 Treiber für I-GATE 11M PC Card unter Windows 95

1 Treiber suchen

Nachdem Sie Ihre I-GATE 11M PC Card gemäss Kapitel "2.2 I-GATE 11M PC Card oder I-GATE 11M PC Card plus in das Notebook einschieben" installiert haben, öffnet sich der Assistent für Gerätetreiber-Updates mit der Meldung, dass er nach Treibern für 'PCI Network Controller' sucht. Überspringen Sie in diesem Falle den Punkt 2, manuelle Hardware-Erkennung und fahren Sie weiter mit Punkt 3, Automatische Hardware-Erkennung.

2 Manuelle Hardware-Erkennung

Sollte sich der Assistent für Gerätetreiber-Updates nicht öffnen, starten Sie die Installation mit **Start -> Einstellungen -> Systemsteuerung -> Hardware** und bestätigen Sie mit **Weiter**.

Beantworten Sie die Frage nach der Hardware-Suche mit **Nein** und **Weiter**.

Selektieren Sie in der Liste der 'Hardware-Typen' den Eintrag **Netzwerkarten** und klicken Sie auf **Weiter**. Im nächsten Fenster klicken Sie auf den Button **Diskette** und geben im Feld 'Herstellerdateien kopieren von' den Laufwerksbuchstaben für Ihr CD-ROM Laufwerk (z.B. F:\) ein (**Bild 4.1**).

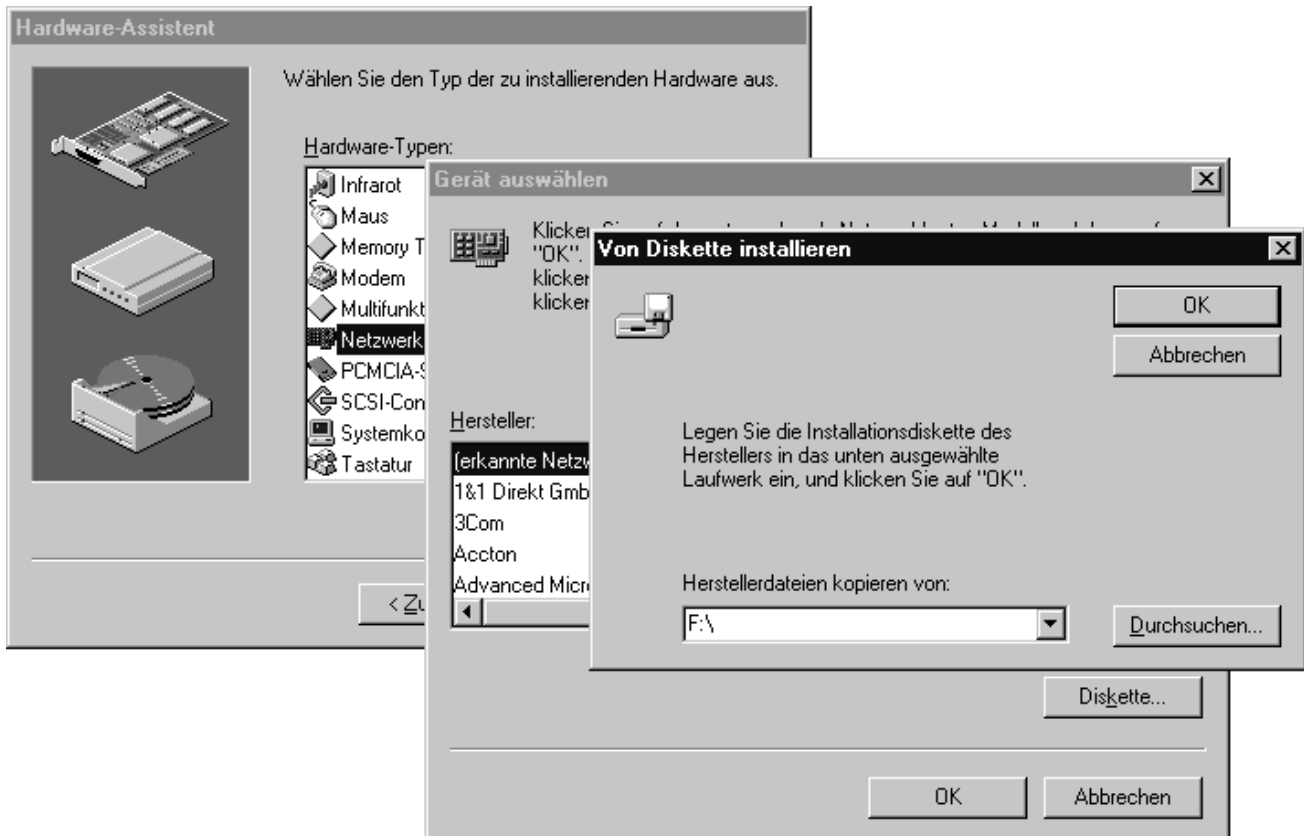


Bild 4.1 Pfad eingabe MobilePort-Treiber bei manueller Hardware-Erkennung

Legen Sie die I-GATE 11M CD-ROM ein und bestätigen Sie nach dem Hochlaufen des CD-ROM Laufwerks mit **OK**.

Sollte sich das I-GATE 11M CD-Einstiegsbild öffnen, so schließen Sie es. Selektieren Sie im Fenster 'Gerät auswählen' den Eintrag 'I-GATE 11M PC Card/PC Card plus'. Bestätigen Sie mit **OK** und anschließend mit **Weiter**.

Fahren Sie nun weiter mit Punkt 4, Namen des Computers und der Arbeitsgruppe eingeben.

3 Automatische Hardware-Erkennung

Legen Sie die I-GATE 11M CD-ROM ein und klicken Sie nach dem Hochlaufen des CD-ROM Laufwerks auf **Weiter**. Sollte sich die I-GATE 11M CD-Einstiegsbild öffnen, schließen Sie dieses mit **Beenden**.

Der Treiber für I-GATE 11M PC Card wird gefunden. Bestätigen Sie erneut mit **Weiter**. Sie werden daraufhin vom System nochmals

aufgefordert, die CD-ROM einzulegen. Da sie bereits eingelegt wurde, können Sie mit **OK** bestätigen. Sollte anschliessend eine Datei nicht gefunden werden, geben Sie im Feld 'Quelle' den Laufwerksbuchstaben für Ihr CD-ROM Laufwerk (z.B. F : \) ein und bestätigen Sie mit **OK**.

4

Namen des Computers und der Arbeitsgruppe eingeben

Sie werden vom System aufgefordert, Computer- und Arbeitsgruppennamen anzugeben. Schliessen Sie die Meldung mit **OK**. Falls Sie nicht aufgefordert wurden, Computernamen und Arbeitsgruppennamen einzugeben, öffnen Sie die Netzwerkeinstellungen mit **Start -> Einstellungen -> Systemsteuerung -> Netzwerk**, klicken Sie auf das Register Identifikation und überprüfen Sie den Computer- und Arbeitsgruppennamen. Sie können Computernamen und Arbeitsgruppennamen frei wählen. Beachten Sie dabei, dass alle Computer, die miteinander Daten austauschen, der gleichen Arbeitsgruppe angehören. Sie müssen den gleichen Arbeitsgruppennamen aber verschiedene Computernamen aufweisen.

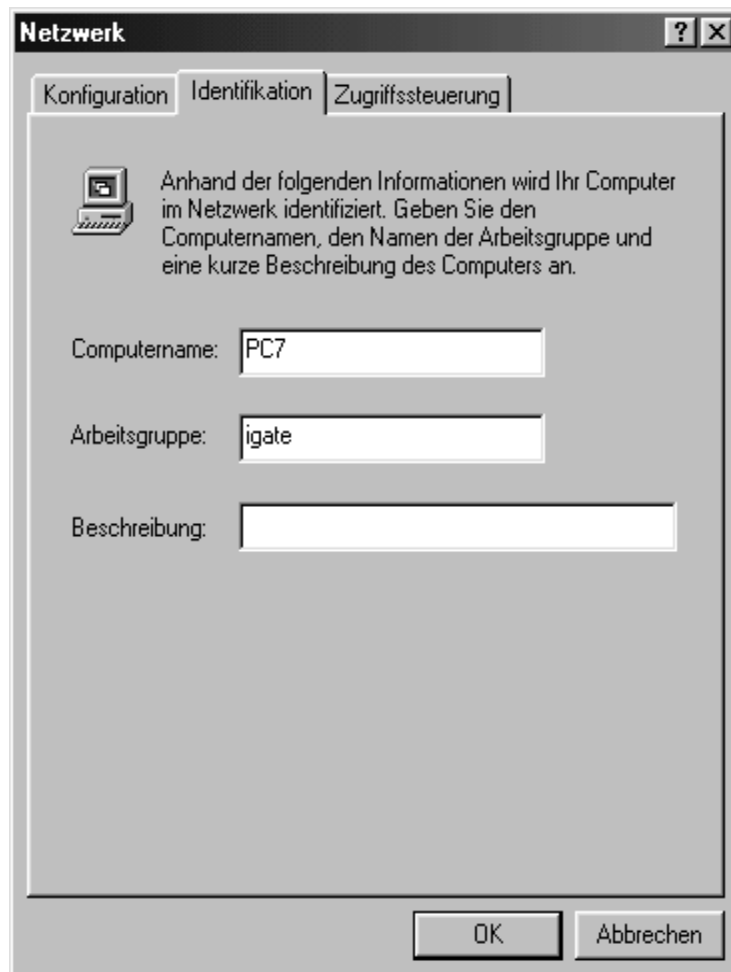


Bild 4.2 Eingabe Computer- und Arbeitsgruppennamen

Geben Sie im Fenster 'Netzwerk' in der Registerkarte 'Identifikation' den Computer- und Arbeitsgruppennamen ein. **Schliessen** Sie das Fenster.

5 SSID (= WLAN-Domain) eingeben

Markieren Sie im sich automatisch öffnenden Fenster 'Eigenschaften von I-GATE 11M PC Card / PC Card plus' die Zeile **SSID** (Service Set Identifier) und geben Sie in das Feld 'Wert' die Seriennummer des AccessPoints ein. Diese finden Sie auf dem Typenschild auf der Rückseite des AccessPoints. Die ersten 5 Stellen sind Buchstaben wobei der Buchstabe 'O' nicht verwendet wird. Beachten Sie die Gross-/Kleinschreibung! Die folgenden 7 Stellen sind Zahlen. (Bild 4.3)

Die Eingabe der SSID ist bei der Erstinstallation zwingend. Falls die SSID bereits geändert wurde, müssen Sie den aktuellen Wert eingeben.



Sicherheit nach der Erstinstallation

Die SSID dient lediglich der Zuordnung zu einem AccessPoint und entspricht damit noch keiner Sicherheitsvorkehrung. Wir empfehlen Ihnen trotzdem die SSID nach der Erstinstallation zu ändern (siehe Kapitel "9.5 SSID (= WLAN Domain) ändern").

Nach der Erstinstallation empfehlen wir Ihnen die Kapitel "12.1 Sicherheit für Ihre Konfiguration" bis und mit Kapitel "12.3.3 WEP - Sicherheit für Ihr WLAN" zu lesen und Sicherheitsmerkmale entsprechend Ihren Bedürfnissen einzurichten. Einige in den vorgenannten Kapiteln beschriebenen Sicherheitseinrichtungen:

Aus Sicherheitsgründen empfehlen wir Ihnen nach der Erstinstallation die Erstellung einer Liste der MobilePorts, die über den AccessPoint Zutritt (oder keinen Zutritt) zum WAN haben sollen. Sehen Sie dazu Kapitel "9.6 Access Control mittels MAC-Adressenliste".

Eine weitere Sicherheitsvorkehrung nach der Erstinstallation ist WEP (Wired Equivalent Privacy). Für die Einstellungen am AccessPoint sehen Sie Kapitel "9.7 AccessPoint WEP Verschlüsselung", für die Einstellungen am MobilePort, Kapitel "6.1.2.2 MobilePort WEP Verschlüsselung".

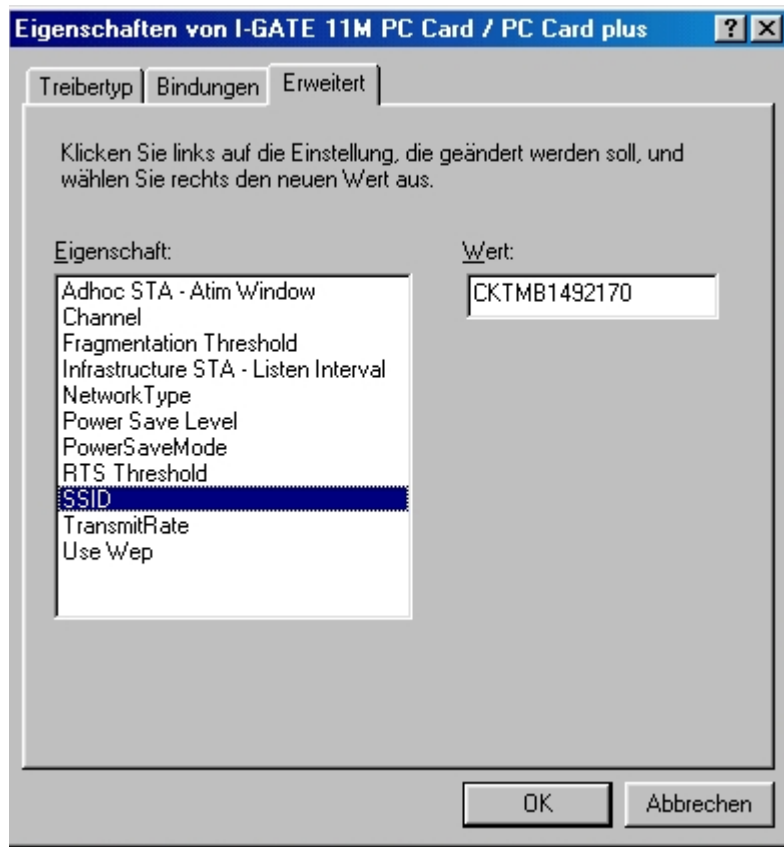


Bild 4.3 SSID eingeben unter Windows 95/98

- 6** Bestätigen Sie Ihre Eingabe mit **OK**.
- 7** **CD-ROM wechseln und Fehlermeldung 'Datei nicht gefunden'**
 Legen Sie nun wie aufgefordert, die Windows 95 CD-ROM ein. Starten Sie nach dem Hochlaufen den Kopiervorgang durch Klick auf **OK**. Es erscheint die Fehlermeldung, dass eine Datei nicht gefunden wurde. Geben Sie in diesem Fall unter 'Quelle' den Buchstaben Ihres CD-ROM Laufwerks ein (z.B. F), gefolgt vom Pfad : \WIN95 und bestätigen Sie mit **OK**. Die Dateien werden fertig kopiert. Beantworten Sie die Fragen, ob der Computer neu gestartet werden soll mit **Nein**.

8 TCP/IP-Protokoll installieren & IP-Adresse automatisch beziehen (I-GATE 11M AccessPoint als DHCP-Server)

Doppelklicken Sie in der 'Systemsteuerung' (**Start -> Einstellungen -> Systemsteuerung**) das Icon **Netzwerk**. Das Fenster Netzwerk öffnet sich. Wählen Sie das Register **Konfiguration**. Klicken Sie auf **Hinzufügen**, sofern im Register 'Konfiguration' TCP/IP fehlen sollte. Das Fenster 'Netzwerkkomponententyp auswählen' öffnet sich. Markieren Sie **Protokoll** und bestätigen Sie mit **Hinzufügen**. Das Fenster 'Netzwerkprotokoll auswählen' öffnet sich. Markieren Sie unter 'Hersteller' **Microsoft** und unter 'Netzwerkprotokolle' **TCP/IP**. Bestätigen Sie mit **OK**. Im Fenster 'Netzwerk' sehen Sie neu den Eintrag 'TCP/IP'. Markieren Sie den Eintrag **TCP/IP** und klicken Sie auf **Eigenschaften**. Das Fenster 'Eigenschaften für TCP/IP' öffnet sich. Wählen Sie das Register 'IP-Adresse' und aktivieren Sie die Option **IP-Adresse automatisch beziehen**. Schliessen Sie das Fenster 'Eigenschaften für TCP/IP' mit **OK**. Schliessen Sie ebenfalls das Fenster 'Netzwerk' mit **OK**.

Wenn Sie mit fixen IP-Adressen arbeiten wollen, verfahren Sie gemäss Punkt 9. Sonst gehen Sie zu Punkt 10.

9 Fixe IP-Adresse

Doppelklicken Sie in der 'Systemsteuerung' (**Start -> Einstellungen -> Systemsteuerung**) das Icon **Netzwerk**. Das Fenster 'Netzwerk' öffnet sich.

Im Register 'Konfiguration' markieren Sie den Eintrag **TCP/IP -> I-GATE 11M PC Card/PC Card plus** und klicken Sie auf **Eigenschaften**. Das Fenster 'Eigenschaften von TCP/IP' öffnet sich.

Wählen Sie das Register 'IP-Adresse' und aktivieren Sie die Option **IP-Adresse festlegen**. Geben Sie in den nun freigegebenen Eingabefeldern die gewünschten fixen Daten (IP-Adresse, Subnet-Mask und Gateway) des TCP/IP -Stacks des Rechners ein. Vergessen Sie nicht den DNS-Server anzugeben; dieser wird für den Internet-Zugang unbedingt benötigt. In der Betriebsart nach **Bild 1.2** oder **Bild 1.8** (I-GATE 11M AccessPoint als Internet-Zugangsrouten für ein WLAN) muss das Gateway und der DNS-Server auf die IP-Adresse des AccessPoints konfiguriert werden.

Sie haben nun alle erforderlichen Einstellungen für fixe IP-Adressen vorgenommen und können deshalb den Netzwerkdialog mit **OK** beenden.

10 Windows 95 CD-ROM einlegen

Sie werden jetzt aufgefordert, die Windows 95 CD-ROM einzulegen. Da diese bereits eingelegt ist, bestätigen Sie mit **OK**. Eventuell müssen Sie den Pfad analog Punkt 7 anpassen. Die Dateien werden nun kopiert.

11 Computer neu starten

Das System fragt, ob der Computer neu gestartet werden soll. Entfernen Sie die Window 95 CD-ROM und antworten Sie mit **Ja**.



Möglicherweise erscheint nach dem Neustart der Hinweis, dass der DHCP-Client keine IP-Adresse erhalten konnte. Das ist normal, so lange keine Verbindung zum AccessPoint besteht. Schliessen Sie das Fenster 'DHCP Client' durch Drücken des Buttons **Nein**. Sollte der Hinweis nicht erscheinen, fahren Sie weiter bei Punkt 12.

12 Betriebsanzeigen (LEDs)



Der I-GATE 11M PCI ist mit einer LED versehen. Bei einem erfolgreich installierten Treiber muss diese permanent grün blinken.

grün blinken = MobilePort sucht AccessPoint (Scanning)

grün leuchten = MobilePort hat AccessPoint gefunden (Associated)

Wie Sie Probleme beheben können, lesen Sie im Kapitel "[13.1 Ist der MobilePort Treiber erfolgreich geladen?](#)" nach.

13 Benutzernamen und Kennwort eingeben

Das System fordert Sie eventuell auf, einen Benutzernamen und ein Kennwort einzugeben. Beide Werte sind frei wählbar.



Beachten Sie, dass Sie in Zukunft nach jedem Neustart nach den von Ihnen festgelegten Benutzernamen und Kennwort gefragt werden.

Sie können das Feld 'Kennwort' leer lassen. In diesem Fall müssen Sie auch in Zukunft dieses Wort nicht eingeben.

Wiederholen Sie Ihre erste Eingabe und bestätigen Sie anschließend mit **OK**.

14

Zurück zu Kapitel "[2 MobilePort Hardware installieren](#)" wenn Sie weitere MobilePorts zu installieren haben, sonst weiter zu Kapitel "[4.2 MobilePort Manager installieren](#)".

4.1.2 Treiber für I-GATE 11M PC Card unter Windows 98

1 Treiber suchen - automatische Kennung

Nachdem Sie Ihre I-GATE 11M PC Card gemäss Kapitel "2.2 I-GATE 11M PC Card oder I-GATE 11M PC Card plus in das Notebook einschieben" installiert haben öffnet sich der Hardware-Assistent mit der Meldung, dass er nach neuen Treibern für 'PC Network Controller' sucht. Klicken Sie auf **Weiter**. Der Hardware-Assistent fragt nun wie Sie vorgehen möchten. Stellen Sie sicher, dass 'Nach einem passenden Treiber für das Gerät suchen' angewählt ist und gehen Sie zu Punkt 2.

Treiber suchen - manuelle Kennung

Sollte sich der Hardware-Assistent nicht öffnen, starten Sie die Installation mit **Start** -> **Einstellungen** -> **Systemsteuerung** -> **Hardware** und klicken Sie viermal auf **Weiter**. Gehen sie zu Punkt 2.

2 I-GATE 11M CD-ROM einlegen

Legen Sie die I-GATE 11M CD-ROM ein. Sollte sich das I-GATE 11M CD-Einstiegsbild öffnen, so schliessen Sie es. Klicken Sie einmal auf **Weiter**.

Im folgenden Fenster selektieren Sie auf die Frage, wo die Treiber gesucht werden sollen, nur die Option 'CD-ROM Laufwerk' und bestätigen mit **Weiter**.

3 Treiberdatei gefunden

Der Treiber Datei 'I-GATE 11M PC Card MobilePort / PC Card plus' für I-GATE 11M wird gefunden. Klicken Sie auf **Weiter**.

4 SSID (= WLAN-Domain) eingeben

Markieren Sie im sich automatisch öffnenden Fenster 'Eigenschaften von I-GATE 11M PC Card / PC Card plus' die Zeile **SSID** (Service Set Identifier) und geben Sie in das Feld 'Wert' die Seriennummer des AccessPoints ein. Diese finden Sie auf dem Typenschild auf der Rückseite des AccessPoints. Die ersten 5 Stellen sind Buchstaben wobei der Buchstabe 'O' nicht verwendet wird. Beachten Sie die Gross-/Kleinschreibung! Die folgenden 7 Stellen sind Zahlen. (Bild 4.4)

Die Eingabe der SSID ist bei der Erstinstallation zwingend. Falls die SSID bereits geändert wurde, müssen Sie den aktuellen Wert eingeben.



Sicherheit nach der Erstinstallation

Die SSID dient lediglich der Zuordnung zu einem AccessPoint und entspricht damit noch keiner Sicherheitsvorkehrung. Wir empfehlen Ihnen trotzdem die SSID nach der Erstinstallation zu ändern (siehe Kapitel "9.5 SSID (= WLAN Domain) ändern").

Nach der Erstinstallation empfehlen wir Ihnen die Kapitel "12.1 Sicherheit für Ihre Konfiguration" bis und mit Kapitel "12.3.3 WEP - Sicherheit für Ihr WLAN" zu lesen und Sicherheitsmerkmale entsprechend Ihren Bedürfnissen einzurichten. Einige in den vorgenannten Kapiteln beschriebenen Sicherheitseinrichtungen:

Aus Sicherheitsgründen empfehlen wir Ihnen nach der Erstinstallation die Erstellung einer Liste der MobilePorts, die über den AccessPoint Zutritt (oder keinen Zutritt) zum WAN haben sollen. Sehen Sie dazu Kapitel "9.6 Access Control mittels MAC-Adressenliste".

Eine weitere Sicherheitsvorkehrung nach der Erstinstallation ist WEP (Wired Equivalent Privacy). Für die Einstellungen am AccessPoint sehen Sie Kapitel "9.7 AccessPoint WEP Verschlüsselung", für die Einstellungen am MobilePort, Kapitel "6.1.2.2 MobilePort WEP Verschlüsselung".

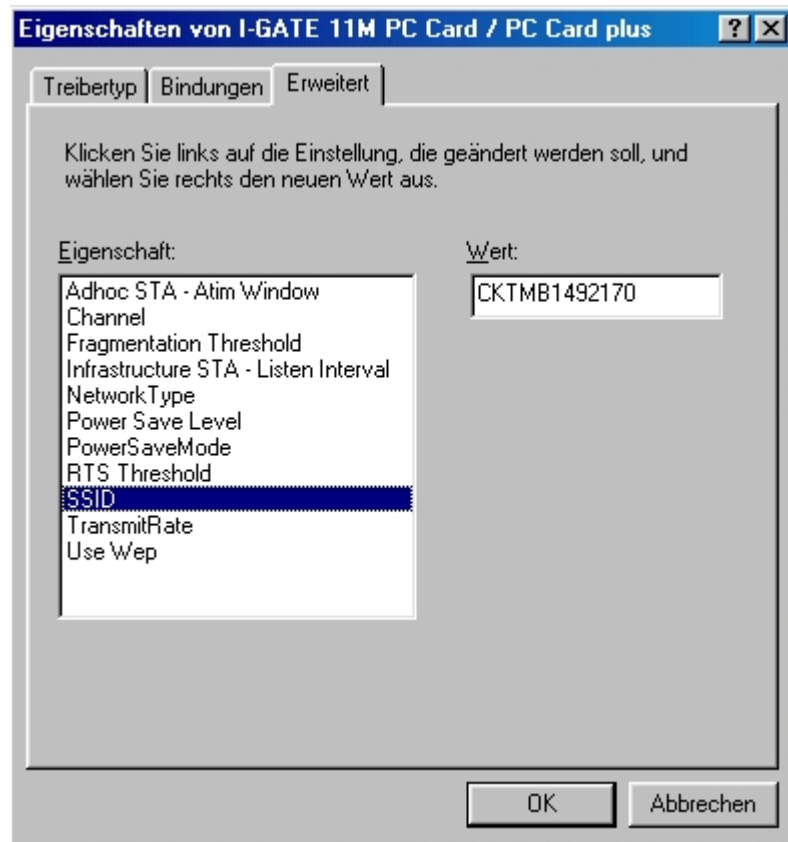


Bild 4.4 SSID eingeben unter Windows 95/98

- 5** Bestätigen Sie Ihre Eingabe mit **OK**.
- 6** **CD-ROM wechseln**
Legen Sie die Windows 98 CD-ROM ein und bestätigen Sie mit **OK**. Die Dateien werden kopiert. Beenden Sie die Installation mit **Fertigstellen**. Beantworten Sie die Fragen, ob ein Neustart durchgeführt werden soll, zweimal mit **Nein**.

7 TCP/IP-Protokoll installieren & IP-Adresse automatisch beziehen (I-GATE 11M AccessPoint als DHCP-Server)

Doppelklicken Sie in der 'Systemsteuerung' (**Start -> Einstellungen -> Systemsteuerung**) das Icon **Netzwerk**. Das Fenster Netzwerk öffnet sich. Wählen Sie das Register **Konfiguration**. Markieren Sie den Eintrag **TCP/IP -> I-GATE 11M PC Card / PC Card plus** und klicken Sie auf **Eigenschaften**. Wählen Sie das Register 'IP-Adresse' und aktivieren Sie die Option **IP-Adresse automatisch beziehen**. Schliessen Sie das Fenster 'Eigenschaften für TCP/IP' mit **OK**. Schliessen Sie ebenfalls das Fenster 'Netzwerk' mit **OK**. Starten Sie Ihren Computer neu.

Wenn Sie mit fixen IP-Adressen arbeiten wollen, verfahren Sie gemäss Punkt 8. Sonst gehen Sie zu Punkt 9.

8 Fixe IP-Adresse

Doppelklicken Sie in der 'Systemsteuerung' (**Start -> Einstellungen -> Systemsteuerung**) das Icon **Netzwerk**. Das Fenster 'Netzwerk' öffnet sich.

Im Register 'Konfiguration' markieren Sie den Eintrag **TCP/IP -> I-GATE 11M PC Card** und klicken Sie auf **Eigenschaften**. Das Fenster 'Eigenschaften von TCP/IP' öffnet sich.

Wählen Sie das Register 'IP-Adresse' und aktivieren Sie die Option **IP-Adresse festlegen**. Geben Sie in den nun freigegebenen Eingabefeldern die gewünschten fixen Daten (IP-Adresse, Subnet-Mask und Gateway) des TCP/IP -Stacks des Rechners ein. Vergessen Sie nicht den DNS-Server anzugeben; dieser wird für den Internet-Zugang unbedingt benötigt. In der Betriebsart nach **Bild 1.2** oder **Bild 1.8** (I-GATE 11M AccessPoint als Internet-Zugangsrouten für ein WLAN) muss das Gateway und der DNS-Server auf die IP-Adresse des AccessPoints konfiguriert werden.

Sie haben nun alle erforderlichen Einstellungen für fixe IP-Adressen vorgenommen und können deshalb den Netzwerkdialog mit **OK** beenden. Auf die Frage, ob der Computer neu gestartet werden soll, antworten Sie mit **Ja**.

9 Betriebsanzeigen (LEDs)

Wie Sie Probleme beheben können, lesen Sie im Kapitel "[13.1 Ist der MobilePort Treiber erfolgreich geladen?](#)" nach.



Die I-GATE 11M PC Card ist mit einer LED versehen. Bei einem erfolgreich installierten Treiber muss diese permanent grün blinken.

grün blinken = MobilePort sucht AccessPoint (Scanning)

grün leuchten = MobilePort hat AccessPoint gefunden (Associated)

10 Zurück zu Kapitel "[2 MobilePort Hardware installieren](#)" wenn Sie weitere MobilePorts zu installieren haben, sonst weiter zu Kapitel "[4.2 MobilePort Manager installieren](#)".

4.1.3 Treiber für I-GATE 11M PC Card unter Windows NT

Sie haben Ihre I-GATE 11M PC Card MobilePort gemäss Kapitel "2.2 I-GATE 11M PC Card oder I-GATE 11M PC Card plus in das Notebook einschieben" installiert. Haben Sie auch die PC Card Spannungsumschaltungs-Software und mindestens Service Pack 6 installiert? Wenn nicht, entfernen Sie die PC Card und tun Sie dies jetzt.

4.1.3.1 NT-Netzwerkunterstützung installieren

In diesem Kapitel installieren Sie den Loopback-Adapter, damit die für den Netzwerkbetrieb notwendigen Dateien auf die Festplatte Ihres Notebooks geschrieben werden. Der Loopback-Adapter selbst wird nicht benötigt und anschliessend wieder gelöscht. Falls der TCP/IP-Protokollstack bereits vollständig vorhanden ist, kann auf die Installation des Loopback-Adapters verzichtet werden. Fahren Sie dann weiter mit "4.1.3.2 BIOS Einstellungen". Sollte der TCP/IP-Protokollstack noch nicht vollständig vorhanden sein, fahren Sie bei Punkt 1 weiter.

- 1 Doppelklicken Sie unter **Start -> Einstellungen -> Systemsteuerung** das Icon **Netzwerk**. Sie werden gefragt, ob Sie die Windows NT-Netzwerkunterstützung jetzt installieren möchten. Bestätigen Sie mit **Ja**.

Das Fenster 'Assistent für die Netzwerkinstallation' öffnet sich. Wählen Sie **Direkt am Netzwerk anschliessen** und **Weiter**. Klicken Sie danach auf **Aus Liste auswählen....**

- 2 **Loopback-Adapter wählen**

In dem sich öffnenden Auswahlfenster wählen Sie den Eintrag **MS Loopback-Adapter**, klicken auf **OK** und anschliessend auf **Weiter**.

- 3 **Protokoll wählen**

Im Fenster 'Assistent für die Netzwerkinstallation' sehen Sie jetzt die Liste der Netzwerkprotokolle. Wählen Sie **TCP/IP-Protokoll**.

4 Netzwerkdienste wählen

Mit **Weiter** gelangen Sie ins Verzeichnis der Netzwerkdienste. Wir empfehlen, alle aufgeführten Dienste auszuwählen. Klicken Sie zweimal auf **Weiter**, bis Sie ins Fenster 'Windows NT-Setup' kommen.

Legen Sie die Windows NT CD-ROM ein. Falls sich das NT-Einstiegsbild öffnet, schliessen Sie es.

5 Installation Netzwerkunterstützung starten

Geben Sie im Fenster 'Windows NT-Setup' den Laufwerksbuchstaben Ihres CD-ROM Laufwerkes ein (z.B. F:\) und klicken Sie nach dem Hochlaufen des Laufwerks in den folgenden Fenstern zweimal auf **Fortsetzen**, bis Sie gefragt werden, ob Sie DHCP verwenden wollen. Antworten Sie mit **Ja**.



Die Daten für die Netzwerkunterstützung und das TCP/IP-Protokoll werden nun kopiert. Dieser Vorgang kann einige Minuten in Anspruch nehmen.

6 Installation Netzwerkunterstützung beenden

Nach abgeschlossener Installation werden die Netzwerkbindungen angezeigt. Klicken Sie zweimal auf **Weiter** und warten Sie, bis die Konfiguration gesichert wurde. Dies kann einige Minuten dauern. Beantworten Sie allfällige weitere Fragen ob DHCP Meldungen angezeigt werden sollen mit **JA**. Sie erhalten die Meldung, dass der DHCP-Client keine IP-Adresse erhalten konnte. Beantworten Sie die Frage, ob DHCP-Meldungen weiterhin angezeigt werden sollen, mit **JA**.

Im folgenden Fenster werden die Daten (Computername, Arbeitsgruppe etc.) abgefragt, die beim Einsatz mehrerer MobilePorts benötigt werden (siehe auch Kap. "9.5 SSID (= WLAN Domain) ändern"). Klicken Sie bei der Erstinstallation auf **Weiter** und anschliessend auf **Fertigstellen**. Eventuell werden Sie gefragt, ob der Computername so geändert werden soll, dass er auch im Internet gültig ist. Antworten Sie mit **Nein**.

Beantworten Sie die Frage, ob der Computer neu gestartet werden soll, mit **Nein**. Doppelklicken Sie in der 'Systemsteuerung' erneut das Icon **Netzwerk**. Wählen Sie das Register 'Netzwerkkarte' und

selektieren Sie **MS Loopback-Adapter**. Löschen Sie diesen mit **Entfernen** und bestätigen Sie die Rückfrage mit **Ja**. Schliessen Sie das Fenster 'Netzwerk'. Beantworten Sie die Frage, ob der Computer neu gestartet werden soll, mit **Nein**. Entfernen Sie die Windows NT CD-ROM. Fahren Sie das Notebook herunter mit **Start -> Beenden - Computer herunterfahren** und schalten Sie es aus.

4.1.3.2 BIOS Einstellungen

7 Für den Betrieb des MobilePorts wird ein Interrupt benötigt. Starten Sie Ihr Notebook neu und drücken Sie die Tasten gemäss dem Handbuch Ihres Notebooks, um ins BIOS Setup zu gelangen. Kontrollieren bzw. aktivieren Sie folgende Einstellungen:

8 Die Einstellung 'Plug & Play OS' (PnP OS) sollte auf 'Nein' stehen, da Sie ein nicht Plug&Play-fähiges Betriebssystem (Windows NT4) verwenden.

Wenn Ihr BIOS die Möglichkeit bietet, ISA Interrupts zu reservieren (Reserved ISA IRQ oder Legacy ISA IRQ), reservieren Sie einen noch freien Interrupt. Reservieren Sie 10, 9, 11 oder 5 wenn einer dieser Interrupts noch frei ist. Sie können aber auch einen anderen noch freien Interrupt verwenden.

Speichern Sie die Einstellungen und starten Sie Ihr Notebook neu. Je nach Version Ihrer Betriebssystem CD-ROM erscheinen ev. Fehlermeldungen während des Aufstartens, welche Sie zum jetzigen Zeitpunkt ignorieren können.

4.1.3.3 MobilePort Treiber-Installation

9 Legen Sie jetzt die I-GATE 11M CD-ROM ein. Sollte sich das I-GATE 11M CD-Einstiegsbild öffnen, schliessen Sie es.

Doppelklicken Sie in der 'Systemsteuerung' das Icon **Netzwerk**. Das Fenster 'Netzwerk' öffnet sich. Wählen Sie das Register 'Netzwerkkarte' und klicken Sie auf **Hinzufügen....**

10 Pfad eingeben und OEM-Option auswählen

In dem sich öffnenden Fenster 'Auswahl: Netzwerkkarte' klicken Sie auf **Diskette...**. Geben Sie nun den Laufwerksbuchstaben Ihres CD-ROM Laufwerkes (z.B. F:\) ein. Bestätigen Sie mit **OK**. Im Fenster 'OEM-Option auswählen' selektieren Sie "I-GATE 11M PC Card / PC Card plus" und klicken auf 'OK'.

11 SSID (= WLAN-Domain) eingeben

Markieren Sie im sich automatisch öffnenden Fenster 'I-GATE 11M PC Card / PC Card plus Setup' die Zeile **SSID** (Service Set Identifier) und geben Sie in das Feld 'Wert' die Seriennummer des AccessPoints ein. Diese finden Sie auf dem Typenschild auf der Rückseite des AccessPoints. Die ersten 5 Stellen sind Buchstaben wobei der Buchstabe 'O' nicht verwendet wird. Beachten Sie die Gross-/Kleinschreibung! Die folgenden 7 Stellen sind Zahlen. (Bild 4.5)

Die Eingabe der SSID ist bei der Erstinstallation zwingend. Falls die SSID bereits geändert wurde, müssen Sie den aktuellen Wert eingeben.



Sicherheit nach der Erstinstallation

Die SSID dient lediglich der Zuordnung zu einem AccessPoint und entspricht damit noch keiner Sicherheitsvorkehrung. Wir empfehlen Ihnen trotzdem die SSID nach der Erstinstallation zu ändern (siehe Kapitel "9.5 SSID (= WLAN Domain) ändern").

Nach der Erstinstallation empfehlen wir Ihnen die Kapitel "12.1 Sicherheit für Ihre Konfiguration" bis und mit Kapitel "12.3.3 WEP - Sicherheit für Ihr WLAN" zu lesen und Sicherheitsmerkmale entsprechend Ihren Bedürfnissen einzurichten. Einige in den vorgenannten Kapiteln beschriebenen Sicherheitseinrichtungen:

Aus Sicherheitsgründen empfehlen wir Ihnen nach der Erstinstallation die Erstellung einer Liste der MobilePorts, die über den AccessPoint Zutritt (oder keinen Zutritt) zum WAN haben sollen. Sehen Sie dazu Kapitel "9.6 Access Control mittels MAC-Adressenliste".

Eine weitere Sicherheitsvorkehrung nach der Erstinstallation ist WEP (Wired Equivalent Privacy). Für die Einstellungen am AccessPoint sehen Sie Kapitel "9.7 AccessPoint WEP Verschlüsselung", für die Einstellungen am MobilePort, Kapitel "6.1.2.2 MobilePort WEP Verschlüsselung".

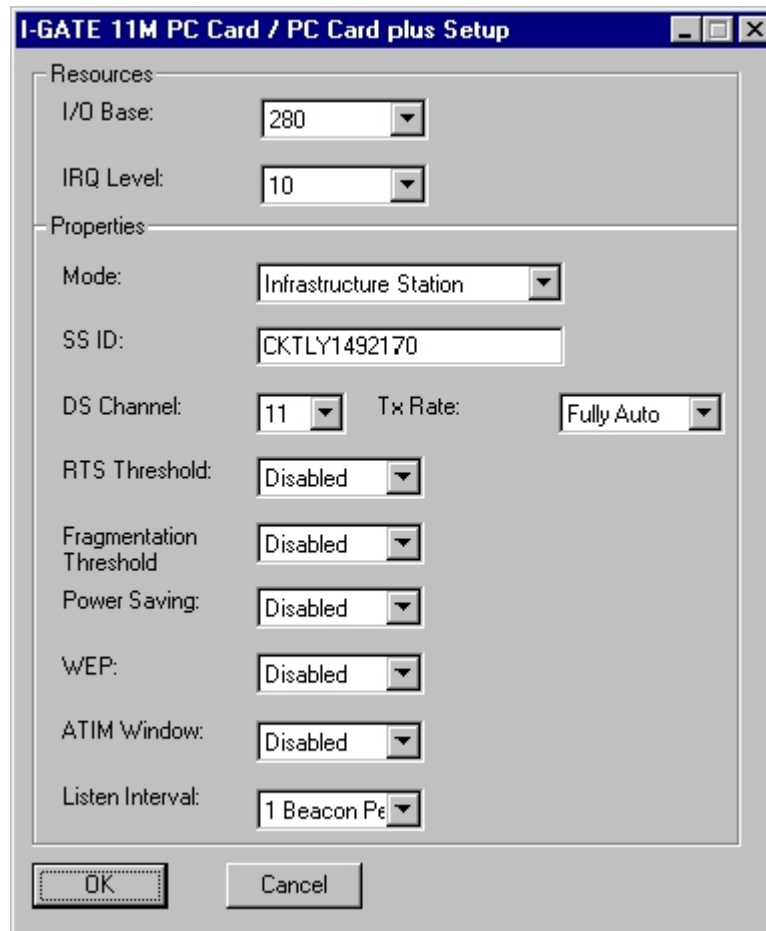


Bild 4.5 SSID eingeben unter Windows NT4

12

Tragen Sie im Feld 'IRQ Level' den IRQ ein, den Sie unter Kapitel **"4.1.3.2 BIOS Einstellungen"** als frei ermittelt und reserviert haben.

Als 'I/O Base' sollte nach Möglichkeit '0280' verwendet werden. Kontrollieren Sie mit **Start -> Programme -> Verwaltung -> Windows NT-Diagnose** in der Registerkarte 'Ressourcen' unter dem Button **I/O-Port**, ob diese frei ist. Ist sie belegt, wählen Sie im Feld 'I/O Base' solange alternativ angebotene Einträge aus, bis Sie eine freie Adresse gefunden haben.

Schliessen Sie Ihre Eingabe mit **OK** ab.

13**Netzwerkbindungen kontrollieren (Bild 4.6)**

Im Fenster 'Netzwerk' erscheint jetzt neu der Eintrag 'I-GATE 11M PC Card / PC Card plus'. Wechseln Sie auf die Registerkarte 'Bindungen' und kontrollieren Sie durch Klick auf die Plus-Zeichen im Verzeichnisbaum, ob 'I-GATE 11M PC Card / PC Card plus' bei allen Diensten aufgeführt wird.

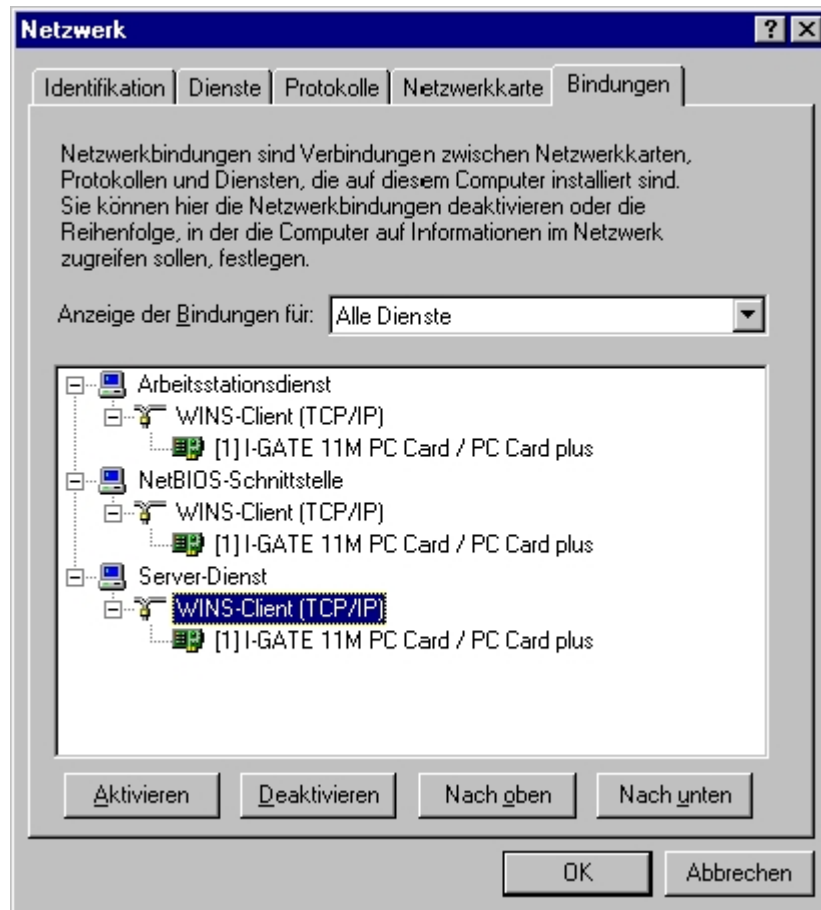


Bild 4.6 Netzwerkbindungen kontrollieren

14 TCP/IP-Protokoll installieren & IP-Adresse automatisch beziehen (I-GATE 11M AccessPoint als DHCP-Server)

Wählen Sie das Register **Protokolle**. Markieren Sie den Eintrag **TCP/IP Protokoll** und klicken Sie auf **Eigenschaften**. Wählen Sie im Fenster 'Eigenschaften von Microsoft TCP/IP' unter 'Netzwerkwerkarte' den Eintrag 'I-GATE 11M PC Card / PC Card plus' und aktivieren Sie die Option **IP-Adresse von einem DHCP-Server beziehen**. Beantworten Sie die Frage, ob Sie DHCP aktivieren möchten mit **Ja**. Fahren Sie mit **OK** und **Schliessen** weiter, bis die Frage erscheint, ob der Computer neu gestartet werden soll. Beantworten Sie die Frage mit **Ja**. Beantworten Sie allfällige Fehlermeldungen mit **OK**.

Wenn Sie mit fixen IP-Adressen arbeiten wollen, verfahren Sie gemäss Punkt 15 und 16. Sonst gehen Sie zu Punkt 17.

15 Fixe IP-Adresse

Wählen Sie das Register 'Protokolle', markieren Sie den Eintrag **TCP/IP-Protokoll** und klicken Sie auf **Eigenschaften**. Das Fenster 'Eigenschaften von Microsoft TCP/IP' öffnet sich.

Im Register 'IP-Adresse' aktivieren Sie die Option **IP-Adresse angeben**. Geben Sie in den nun freigegebenen Eingabefeldern die gewünschten fixen Daten (IP-Adresse, Subnet-Mask und Gateway) des TCP/IP -Stacks des Rechners ein. Vergessen Sie nicht den DNS-Server anzugeben; dieser wird für den Internet-Zugang unbedingt benötigt. In der Betriebsart nach [Bild 1.2](#) oder [Bild 1.8](#) (I-GATE 11M AccessPoint als Internet-Zugangsrouten für ein WLAN) muss das Gateway und der DNS-Server auf die IP-Adresse des AccessPoints konfiguriert werden.

Um die Werte zu aktualisieren, wählen Sie als nächstes das Register 'Bindungen'. Sie haben nun alle erforderlichen Einstellungen für fixe IP-Adressen vorgenommen und können deshalb den Netzwerkdialog mit **Schliessen** beenden. Auf die Frage, ob der Computer neu gestartet werden soll, antworten Sie mit **Ja**.

16 Computer neu starten

Nach dem Neustart erscheint der Hinweis, dass der DHCP-Client keine IP-Adresse erhalten konnte. Das ist normal, so lange noch keine Verbindung mit dem AccessPoint besteht. Beantworten Sie die Frage, ob DHCP-Meldungen weiterhin angezeigt werden sollen, mit **Nein**.

Eventuell weist Sie der 'Dienstkontroll-Manager' darauf hin, dass der Start mindestens eines Dienstes fehlgeschlagen ist. Klicken Sie auf **OK**.

17 Betriebsanzeigen (LEDs).



Der I-GATE 11M PCI ist mit einer LED versehen. Bei einem erfolgreich installierten Treiber muss diese permanent grün blinken.

grün blinken = MobilePort sucht AccessPoint (Scanning)

grün leuchten = MobilePort hat AccessPoint gefunden (Associated)

Wie Sie Probleme beheben können, lesen Sie im Kapitel "[13.1 Ist der MobilePort Treiber erfolgreich geladen?](#)" nach.

Wenn Sie trotzdem noch Probleme haben können diese mit dem aufspielen von Ihrem Service Pack (mindestens Service Pack 6 - Service Packs 6 resp. 6a finden Sie auf der I-GATE 11M CD-ROM unter **CD durchsuchen -> misc -> nt4spx** in Ihrer Sprache) behoben werden. Führen Sie jedoch zuerst Punkt 18 aus.

18 Zurück zu Kapitel "[2 MobilePort Hardware installieren](#)" wenn Sie weitere MobilePorts zu installieren haben, sonst weiter zu Kapitel "[4.2 MobilePort Manager installieren](#)".

4.1.4 Treiber für I-GATE 11M PC Card unter Windows 2000

1 Treiber suchen - automatische Kennung

Nachdem Sie Ihre I-GATE 11M PC Card gemäss Kapitel "2.2 I-GATE 11M PC Card oder I-GATE 11M PC Card plus in das Notebook einschieben" installiert haben öffnet sich der Hardware-Assistent mit der Meldung, dass er die neue Hardware 'Intersil_I-Gate_11M_PC_Card plus' gefunden hat. Warten Sie bis sich der 'Assistent für das Suchen neuer Hardware' öffnet. Klicken Sie auf **Weiter**. Der 'Assistent für das Suchen neuer Hardware' fragt nun, wie Sie vorgehen möchten. Gehen Sie zu Punkt 2.

Treiber suchen - manuelle Kennung

Sollte sich der 'Assistent für das Suchen neuer Hardware' nicht öffnen, starten Sie die Installation mit **Start -> Einstellungen -> Systemsteuerung -> Hardware** und klicken Sie dreimal auf **Weiter**. Markieren Sie den Eintrag "Intersil_I-Gate_11M_PC_Card plus" und klicken Sie auf **Weiter** und dann auf **Fertig stellen**. Im 'Assistent zum Aktualisieren von Gerätetreibern' klicken Sie auf **Weiter**. Der Assistent zum Aktualisieren von Gerätetreibern fragt nun, wie Sie vorgehen möchten. Stellen Sie sicher, dass 'Nach einem passenden Treiber für das Gerät suchen' angewählt ist und gehen Sie zu Punkt 2.

2 I-GATE 11M CD-ROM einlegen

Legen Sie die I-GATE 11M CD-ROM ein. Sollte sich das I-GATE 11M CD-Einstiegsbild öffnen, so schliessen Sie es mit **Beenden**. Klicken Sie auf **Weiter**.

Im folgenden Fenster selektieren Sie auf die Frage, wo die Treiber gesucht werden sollen, nur die Option 'CD-ROM Laufwerk' und bestätigen mit **Weiter**.

3 Treiberdatei gefunden

Der Treiber für 'Intersil_I-Gate_11M_PC_Card plus' wird gefunden. Klicken Sie auf **Weiter**. Das Fenster mit der Meldung, dass Windows 2000 keine Microsoft digitale Signatur für 'I-GATE 11M PC Card / PC Card plus' findet, öffnet sich. Beantworten Sie die Frage, ob die Installation fortgesetzt soll, mit **Ja**. Klicken Sie auf 'Fertig stellen'.

4 SSID (= WLAN-Domain) eingeben

Markieren Sie unter **Start -> Eigenschaften -> Systemsteuerung -> Netzwerk- und DFU-Verbindungen -> LAN Verbindung -> Eigenschaften -> Konfigurieren -> Erweiterte Einstellungen** im Fenster 'Eigenschaften von I-GATE 11M PC Card / PC Card plus' die Zeile **SSID** (Service Set Identifier) und geben Sie in das Feld 'Wert' die Seriennummer des AccessPoints ein. Diese finden Sie auf dem Typenschild auf der Rückseite des AccessPoints. Die ersten 5 Stellen sind Buchstaben wobei der Buchstabe 'O' nicht verwendet wird. Beachten Sie die Gross-/Kleinschreibung! Die folgenden 7 Stellen sind Zahlen. (Bild 4.7)

Die Eingabe der SSID ist bei der Erstinstallation zwingend. Falls die SSID bereits geändert wurde, müssen Sie den aktuellen Wert eingeben.



Sicherheit nach der Erstinstallation

Die SSID dient lediglich der Zuordnung zu einem AccessPoint und entspricht damit noch keiner Sicherheitsvorkehrung. Wir empfehlen Ihnen trotzdem die SSID nach der Erstinstallation zu ändern (siehe Kapitel "9.5 SSID (= WLAN Domain) ändern").

Nach der Erstinstallation empfehlen wir Ihnen die Kapitel "12.1 Sicherheit für Ihre Konfiguration" bis und mit Kapitel "12.3.3 WEP - Sicherheit für Ihr WLAN" zu lesen und Sicherheitsmerkmale entsprechend Ihren Bedürfnissen einzurichten. Einige in den vorgenannten Kapiteln beschriebenen Sicherheitseinrichtungen:

Aus Sicherheitsgründen empfehlen wir Ihnen nach der Erstinstallation die Erstellung einer Liste der MobilePorts, die über den AccessPoint Zutritt (oder keinen Zutritt) zum WAN haben sollen. Sehen Sie dazu Kapitel "9.6 Access Control mittels MAC-Adressenliste".

Eine weitere Sicherheitsvorkehrung nach der Erstinstallation ist WEP (Wired Equivalent Privacy). Für die Einstellungen am AccessPoint sehen Sie Kapitel "9.7 AccessPoint WEP Verschlüsselung", für die Einstellungen am MobilePort, Kapitel "6.1.2.2 MobilePort WEP Verschlüsselung".

5 Bestätigen Sie Ihre Eingabe mit **OK**.

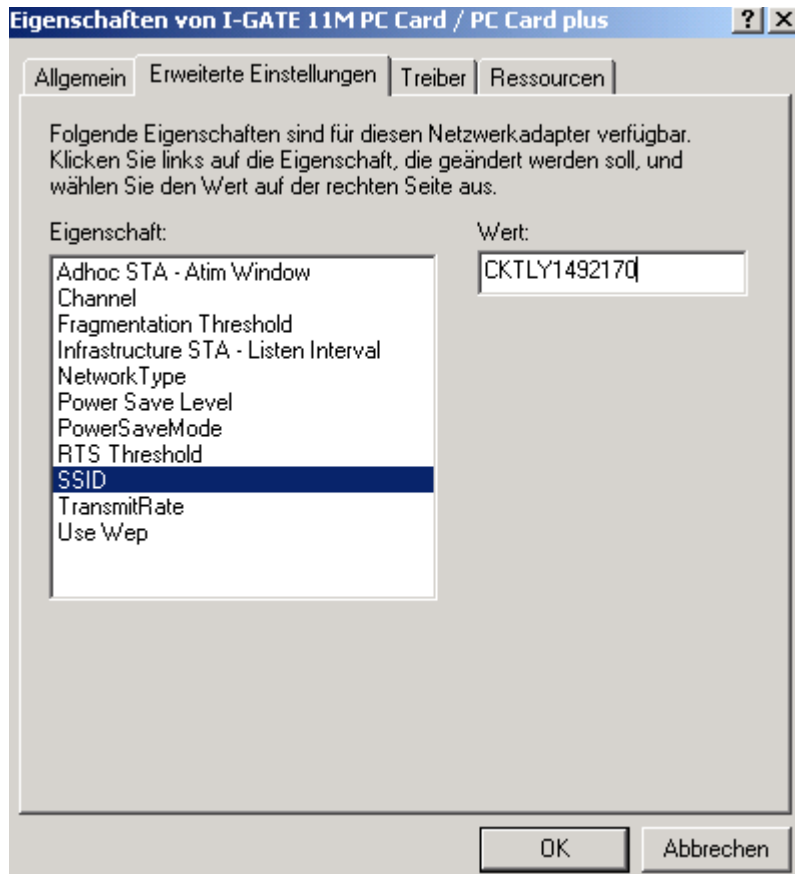


Bild 4.7 SSID eingeben unter Windows 2000

6 **IP-Adresse automatisch beziehen (I-GATE 11M AccessPoint als DHCP-Server)**

Das Fenster 'Eigenschaften von LAN-Verbindung' öffnet sich. Markieren Sie den Eintrag **Internetprotokoll (TCP/IP)** und klicken Sie auf **Eigenschaften**. Aktivieren Sie die Option **IP-Adresse automatisch beziehen** und die Option **DNS-Serveradresse automatisch beziehen**. Schliessen Sie das Fenster 'Eigenschaften von Internetprotokoll (TCP/IP)' mit **OK**. Schliessen alle weiteren Fenster und starten Sie Ihren Computer neu.

Wenn Sie mit fixen IP-Adressen arbeiten wollen, verfahren Sie gemäss Punkt 7. Sonst gehen Sie zu Punkt 8.

7 Fixe IP-Adresse

Klicken Sie auf **Start -> Einstellungen -> Systemsteuerung -> Netzwerk- und DFÜ-Verbindungen -> LAN-Verbindung -> Eigenschaften**.

Markieren Sie den Eintrag **Internetprotokoll (TCP/IP)** und klicken Sie auf **Eigenschaften**. Das Fenster 'Eigenschaften von Internetprotokoll (TCP/IP)' öffnet sich.

Aktivieren Sie die Option **Folgende IP-Adresse verwenden**. Geben Sie in den nun freigegebenen Eingabefeldern die gewünschten fixen Daten (IP-Adresse, Subnet-Mask und Gateway) des TCP/IP - Stacks des Rechners ein. Vergessen Sie nicht den DNS-Server anzugeben; dieser wird für den Internet-Zugang unbedingt benötigt. In der Betriebsart nach [Bild 1.2](#) oder [Bild 1.8](#) (I-GATE 11M AccessPoint als Internet-Zugangsrouten für ein WLAN) muss das Gateway und der DNS-Server auf die IP-Adresse des AccessPoints konfiguriert werden.

Sie haben nun alle erforderlichen Einstellungen für fixe IP-Adressen vorgenommen und können deshalb den Netzwerkdialog mit **OK** beenden. Auf die Frage, ob der Computer neu gestartet werden soll, antworten Sie mit **Ja**.

8 Betriebsanzeigen (LEDs)



Der I-GATE 11M PC Card ist mit einer LED versehen. Bei einem erfolgreich installierten Treiber muss diese permanent grün blinken.

grün blinken = MobilePort sucht AccessPoint (Scanning)

grün leuchten = MobilePort hat AccessPoint gefunden (Associated)

Wie Sie Probleme beheben können, lesen Sie im Kapitel "[13.1 Ist der MobilePort Treiber erfolgreich geladen?](#)" nach.

9 Zurück zu Kapitel "[2 MobilePort Hardware installieren](#)", wenn Sie weitere MobilePorts zu installieren haben, sonst weiter zu Kapitel "[4.2 MobilePort Manager installieren](#)".

4.2 MobilePort Manager installieren

- 1 Entfernen Sie die Windows CD-ROM (Ausnahme: W2000, wo keine Windows CD-ROM eingelegt werden musste). Legen Sie die I-GATE 11M CD-ROM ein und klicken Sie auf **I-GATE MobilePort Manager installieren**. Je nachdem welchen MobilePort Manager Sie installieren wollen, klicken Sie auf **PC Card MobilePort installieren**, **PCI Card MobilePort installieren** oder **USB MobilePort installieren**. Um den MobilePort Manager für PC Card plus zu installieren klicken Sie ebenfalls auf **PC Card MobilePort installieren**.

Sollte sich das I-GATE 11M CD-Einstiegsbild nicht automatisch öffnen, klicken Sie mit der rechten Maustaste auf Ihr CD-ROM Laufwerk und dann auf **AutoPlay -> I-GATE MobilePort Manager installieren**. Je nachdem welchen MobilePort Manager Sie installieren wollen, klicken Sie dann auf **PC Card MobilePort installieren**, **PCI Card MobilePort installieren** oder **USB MobilePort installieren**.

- 2 Der 'I-GATE MobilePort Manager Setup' öffnet sich. Klicken Sie auf **Next**. Als Destination Folder erscheint 'C:\Programme\Siemens I-Gate\MobilePort Manager'. Klicken Sie zweimal auf **Next**. Bestätigen Sie die Meldung 'Setup is Complete.' mit **OK**.

- 3 Das Fenster 'I-GATE MobilePort Manager' öffnet sich. Doppelklicken Sie das 'MobilePort Manager' Verknüpfungssicon (grüner PC). Der MobilePort Manager erscheint nun als rotes PC Icon im Windows Taskbar Ihres Rechners. Schliessen Sie das Fenster 'I-GATE MobilePort Manager' und alle anderen Fenstern. Klicken Sie auf das rote PC Icon. Das Register 'Link Info' öffnet sich und im Feld 'State' erscheint 'Scanning'. Nach der Erstinstallation empfehlen wir Ihnen Kapitel "[6 MobilePort Management](#)" zu lesen.

4 Service Pack aufspielen



Wenn Sie den MobilePort Manager auf NT4 installiert haben und keinen AccessPoint installieren werden, spielen Sie Ihr Service Pack (mindestens Service Pack 6) jetzt neu auf.

Wenn Sie den MobilePort Manager auf NT4 installiert haben, Probleme beim installieren des MobilePorts hatten (z.B. nicht ständig blinkende LED oder DHCP resp. Dienst Fehlermeldungen) und einen AccessPoint installieren werden, spielen Sie Ihr Service Pack (mindestens Service Pack 6) jetzt neu auf.

Die Service Packs 6 resp. 6a finden Sie auf der I-GATE 11M CD-ROM unter **CD durchsuchen -> misc -> nt4spx** in Ihrer Sprache.

Nach dem Aufspielen des Service Packs muss die MobilePort LED permanent grün blinken.

grün blinken = MobilePort sucht AccessPoint (Scanning)

grün leuchten = MobilePort hat AccessPoint gefunden (Associated)

5 Weiter zu Kapitel "8 I-GATE 11M AccessPoint Hardware anschliessen".

5 I-GATE 11M USB Software installieren

In dieser **Standard Installation** gehen wir davon aus, dass Sie ein TCP/IP-Netzwerk betreiben und dass Sie Ihre IP-Adressen über die DHCP-Server Funktion des AccessPoints automatisch (dynamisch) beziehen. Für den Fall, dass Sie fixe IP-Adressen verwenden möchten, haben wir diesen jeweils alternativ beschrieben.

Bevor Sie mit der Installation weiterfahren sollten Sie also wissen, ob Sie Ihr TCP/IP-Netzwerk mit dynamischen oder fixen IP-Adressen betreiben wollen und ob Sie die DHCP-Server Funktion des AccessPoints nutzen wollen.

Wenn Sie mit Netzwerken und IP-Adressen vertraut sind, gehen Sie zu Punkt 1 auf der folgenden Seite.

Wenn Sie nicht mit Netzwerken und IP-Adressen vertraut sind und dazu Entscheidungshilfen möchten, lesen Sie in diesem Handbuch die Kapitel "**9.2.1 AccessPoint Grundeinstellung über Siemens AccessPoint Manager**" und "**12.10 Automatische Adreßverwaltung mit DHCP**". Lesen Sie auch im Kapitel Technische Grundlagen des Referenzhandbuchs die Abschnitte 'Netzwerk-Arten' und 'IP-Adressierung'. Gehen Sie dann zu Punkt 1 auf der folgenden Seite.

Wenn Sie nicht mit Netzwerken und IP-Adressen vertraut sind und jetzt keine Zeit haben dies zu werden, empfehlen wir Ihnen die DHCP-Server Funktion des AccessPoints zu nutzen und die IP-Adresse aller Netzteilnehmer vom AccessPoint automatisch zu beziehen. So wählen Sie den Punkt 'IP-Adresse automatisch beziehen' wenn Sie zum Auswahl des Punkts 'IP-Adresse automatisch beziehen' oder des Punkts 'Fixe IP-Adresse' in diesem Kapitel kommen. Gehen Sie jetzt zu Punkt 1 auf der folgenden Seite.

5.1 Treiber für I-GATE 11M USB installieren

5.1.1 Treiber für I-GATE 11M USB unter Windows 98

1

Treiber suchen - automatische Kennung

Nachdem Sie Ihre I-GATE 11M USB gemäss Kapitel "2.3 I-GATE 11M USB anschliessen" installiert haben öffnet sich der Hardware-Assistent mit der Meldung, dass er nach neuen Treibern für 'USB Network Controller' sucht. Klicken Sie auf **Weiter**. Der Hardware-Assistent fragt nun wie Sie vorgehen möchten. Stellen Sie sicher, dass 'Nach einem passenden Treiber für das Gerät suchen' ausgewählt ist und gehen Sie zu Punkt 2.

Treiber suchen - manuelle Kennung

Sollte sich der Hardware-Assistent nicht öffnen, starten Sie die Installation mit **Start -> Einstellungen -> Systemsteuerung -> Hardware** und klicken Sie viermal auf **Weiter**. Gehen sie zu Punkt 2.

2

I-GATE 11M CD-ROM einlegen

Legen Sie die I-GATE 11M CD-ROM ein. Sollte sich das I-GATE 11M CD-Einstiegsbild öffnen, so schliessen Sie es. Klicken Sie einmal auf **Weiter**.

Im folgenden Fenster selektieren Sie nur die Option 'CD-ROM Laufwerk' und bestätigen mit **Weiter**.

3

Treiberdatei gefunden

Der Treiber Datei 'I-GATE 11M PC Card MobilePort / PC Card plus' für I-GATE 11M wird gefunden. Klicken Sie auf **Weiter**.

4**SSID (= WLAN-Domain) eingeben**

Markieren Sie im sich automatisch öffnenden Fenster 'Eigenschaften von I-GATE 11M USB MobilePort' die Zeile **SSID** (Service Set Identifier) und geben Sie in das Feld 'Wert' die Seriennummer des AccessPoints ein. Beachten Sie die Gross-/Kleinschreibung!

Diese finden Sie auf dem Typenschild unter Serien Nr. auf der Rückseite des AccessPoints.

Die Eingabe der SSID ist bei der Erstinstallation zwingend. Falls die SSID bereits geändert wurde, müssen Sie den aktuellen Wert eingeben.

**Sicherheit nach der Erstinstallation**

Die SSID dient lediglich der Zuordnung zu einem AccessPoint und entspricht damit noch keiner Sicherheitsvorkehrung. Wir empfehlen Ihnen trotzdem die SSID nach der Erstinstallation zu ändern (siehe Kapitel "9.5 SSID (= WLAN Domain) ändern").

Nach der Erstinstallation empfehlen wir Ihnen die Kapitel "12.1 Sicherheit für Ihre Konfiguration" bis und mit Kapitel "12.3.3 WEP - Sicherheit für Ihr WLAN" zu lesen und Sicherheitsmerkmale entsprechend Ihren Bedürfnissen einzurichten. Einige in den vorgenannten Kapiteln beschriebenen Sicherheitseinrichtungen:

Aus Sicherheitsgründen empfehlen wir Ihnen nach der Erstinstallation die Erstellung einer Liste der MobilePorts, die über den AccessPoint Zutritt (oder keinen Zutritt) zum WAN haben sollen. Sehen Sie dazu Kapitel "9.6 Access Control mittels MAC-Adressenliste".

Eine weitere Sicherheitsvorkehrung nach der Erstinstallation ist WEP (Wired Equivalent Privacy). Für die Einstellungen am AccessPoint sehen Sie Kapitel "9.7 AccessPoint WEP Verschlüsselung", für die Einstellungen am MobilePort, Kapitel "6.1.2.2 MobilePort WEP Verschlüsselung".

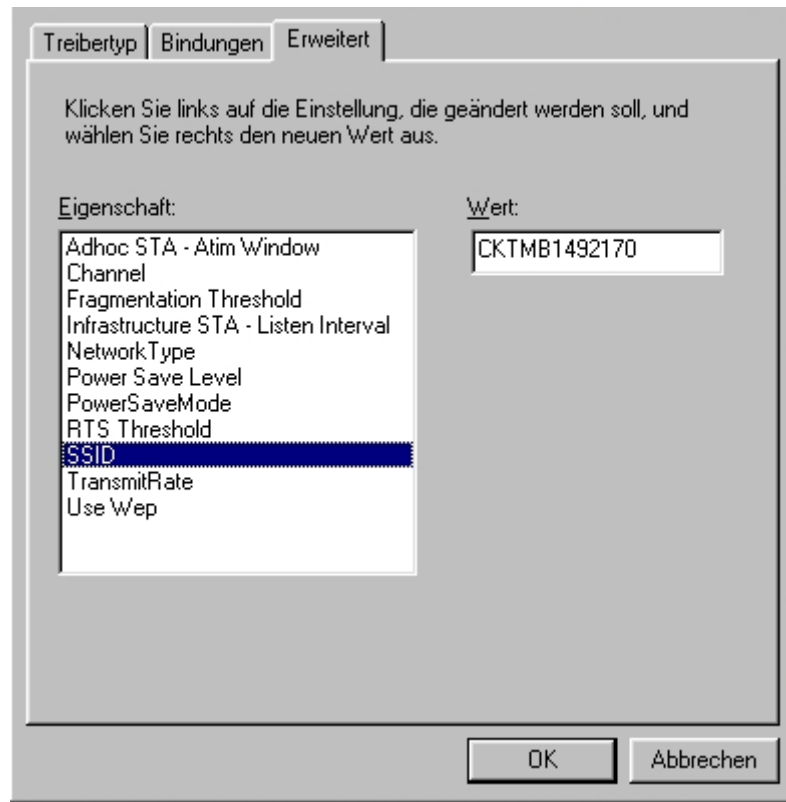


Bild 5.1 SSID eingeben unter Windows 95/98

5

Bestätigen Sie Ihre Eingabe mit **OK**.

6

CD-ROM wechseln

Legen Sie die Windows 98 CD-ROM ein und bestätigen Sie mit **OK**. Die Dateien werden kopiert. Beenden Sie die Installation mit **Fertigstellen**. Beantworten Sie die Fragen, ob ein Neustart durchgeführt werden soll, zweimal mit **Nein**.

7 TCP/IP-Protokoll installieren & IP-Adresse automatisch beziehen (I-GATE 11M AccessPoint als DHCP-Server)

Doppelklicken Sie in der 'Systemsteuerung' (**Start -> Einstellungen -> Systemsteuerung**) das Icon **Netzwerk**. Das Fenster Netzwerk öffnet sich. Wählen Sie das Register **Konfiguration**. Markieren Sie den Eintrag **TCP/IP -> I-GATE 11M USB MobilePort** und klicken Sie auf **Eigenschaften**. Wählen Sie das Register 'IP-Adresse' und aktivieren Sie die Option **IP-Adresse automatisch beziehen**. Schliessen Sie das Fenster 'Eigenschaften für TCP/IP' mit **OK**. Schliessen Sie ebenfalls das Fenster 'Netzwerk' mit **OK**. Starten Sie Ihren Computer neu.

Wenn Sie mit fixen IP-Adressen arbeiten wollen, verfahren Sie gemäss Punkt 8. Sonst gehen Sie zu Punkt 9.

8 Fixe IP-Adresse

Doppelklicken Sie in der 'Systemsteuerung' (**Start -> Einstellungen -> Systemsteuerung**) das Icon **Netzwerk**. Das Fenster 'Netzwerk' öffnet sich.

Im Register 'Konfiguration' markieren Sie den Eintrag **TCP/IP -> I-GATE 11M USB MobilePort** und klicken Sie auf **Eigenschaften**. Das Fenster 'Eigenschaften von TCP/IP' öffnet sich.

Wählen Sie das Register 'IP-Adresse' und aktivieren Sie die Option **IP-Adresse festlegen**. Geben Sie in den nun freigegebenen Eingabefeldern die gewünschten fixen Daten (IP-Adresse, Subnet-Mask und Gateway) des TCP/IP -Stacks des Rechners ein. Vergessen Sie nicht den DNS-Server anzugeben; dieser wird für den Internet-Zugang unbedingt benötigt. In der Betriebsart nach **Bild 1.2** oder **Bild 1.8** (I-GATE 11M AccessPoint als Internet-Zugangsrouten für ein WLAN) muss das Gateway und der DNS-Server auf die IP-Adresse des AccessPoints konfiguriert werden.

Sie haben nun alle erforderlichen Einstellungen für fixe IP-Adressen vorgenommen und können deshalb den Netzwerkdialog mit **OK** beenden. Auf die Frage, ob der Computer neu gestartet werden soll, antworten Sie mit **Ja**.

9 Betriebsanzeigen (LEDs)



Der I-GATE 11M USB ist mit einer LED versehen. Bei einem erfolgreich installierten Treiber muss diese permanent grün blinken.

grün blinken = MobilePort sucht AccessPoint (Scanning)

grün leuchten = MobilePort hat AccessPoint gefunden (Associated)

Wie Sie Probleme beheben können, lesen Sie im Kapitel "[13.1 Ist der MobilePort Treiber erfolgreich geladen?](#)" nach.

- 10 Zurück zu Kapitel "[2 MobilePort Hardware installieren](#)", wenn Sie weitere MobilePorts zu installieren haben, sonst weiter zu Kapitel "[5.2 MobilePort Manager installieren](#)".

5.1.2 Treiber für I-GATE 11M USB unter Windows 2000

1

Treiber suchen - automatische Kennung

Nachdem Sie Ihre I-GATE 11M USB gemäss Kapitel "2.3 I-GATE 11M USB anschliessen" installiert haben öffnet sich der Hardware-Assistent mit der Meldung, dass er die neue Hardware 'I-GATE 11M USB MobilePort' gefunden hat. Warten Sie bis sich der 'Assistent für das Suchen neuer Hardware' öffnet. Klicken Sie auf **Weiter**. Der Assistent für das Suchen neuer Hardware fragt nun, wie Sie vorgehen möchten. Gehen Sie zu Punkt 2.

Treiber suchen - manuelle Kennung

Sollte sich der Assistent für das Suchen neuer Hardware nicht öffnen, starten Sie die Installation mit **Start -> Einstellungen -> Systemsteuerung -> Hardware** und klicken Sie dreimal auf **Weiter**. Markieren Sie den Eintrag 'I-GATE 11M USB MobilePort' und klicken Sie auf **Weiter** und dann auf **Fertig stellen**. Im Assistent zum Aktualisieren von Gerätetreibern klicken Sie auf **Weiter**. Der Assistent zum Aktualisieren von Gerätetreibern fragt nun, wie Sie vorgehen möchten. Stellen Sie sicher, dass 'Nach einem passenden Treiber für das Gerät suchen' angewählt ist und gehen Sie zu Punkt 2.

2

I-GATE 11M CD-ROM einlegen

Legen Sie die I-GATE 11M CD-ROM ein. Sollte sich das I-GATE 11M CD-Einstiegsbild öffnen, so schliessen Sie es mit **Beenden**. Klicken Sie auf **Weiter**.

Im folgenden Fenster selektieren Sie auf die Frage, wo die Treiber gesucht werden sollen, nur die Option 'CD-ROM Laufwerk' und bestätigen mit **Weiter**.

3

Treiberdatei gefunden

Der Treiber für 'I-GATE 11M USB MobilePort' wird gefunden. Klicken Sie auf **Weiter**. Das Fenster mit der Meldung, dass Windows 2000 keine Microsoft digitale Signatur für 'I-GATE 11M USB MobilePort' findet, öffnet sich. Beantworten Sie die Frage ob die Installation fortgesetzt soll, mit **Ja**. Klicken Sie auf 'Fertigstellen'.

4**SSID (= WLAN-Domain) eingeben**

Markieren Sie unter **Start -> Eigenschaften -> Systemsteuerung -> Netzwerk- und DFU-Verbindungen -> LAN Verbindung -> Eigenschaften -> Konfigurieren -> Erweiterte Einstellungen** im Fenster 'Eigenschaften von I-GATE 11M USB MobilePort' die Zeile **SSID** (Service Set Identifier) und geben Sie in das Feld 'Wert' die Seriennummer des AccessPoints ein. Beachten Sie die Gross-/Kleinschreibung!

Diese finden Sie auf dem Typenschild unter Serien Nr. auf der Rückseite des AccessPoints.

Die Eingabe der SSID ist bei der Erstinstallation zwingend. Falls die SSID bereits geändert wurde, müssen Sie den aktuellen Wert eingeben.

**Sicherheit nach der Erstinstallation**

Die SSID dient lediglich der Zuordnung zu einem AccessPoint und entspricht damit noch keiner Sicherheitsvorkehrung. Wir empfehlen Ihnen trotzdem die SSID nach der Erstinstallation zu ändern (siehe Kapitel "9.5 SSID (= WLAN Domain) ändern").

Nach der Erstinstallation empfehlen wir Ihnen die Kapitel "12.1 Sicherheit für Ihre Konfiguration" bis und mit Kapitel "12.3.3 WEP - Sicherheit für Ihr WLAN" zu lesen und Sicherheitsmerkmale entsprechend Ihren Bedürfnissen einzurichten. Einige in den vorgenannten Kapiteln beschriebenen Sicherheitseinrichtungen:

Aus Sicherheitsgründen empfehlen wir Ihnen nach der Erstinstallation die Erstellung einer Liste der MobilePorts, die über den AccessPoint Zutritt (oder keinen Zutritt) zum WAN haben sollen. Sehen Sie dazu Kapitel "9.6 Access Control mittels MAC-Adressenliste".

Eine weitere Sicherheitsvorkehrung nach der Erstinstallation ist WEP (Wired Equivalent Privacy). Für die Einstellungen am AccessPoint sehen Sie Kapitel "9.7 AccessPoint WEP Verschlüsselung", für die Einstellungen am MobilePort, Kapitel "6.1.2.2 MobilePort WEP Verschlüsselung".

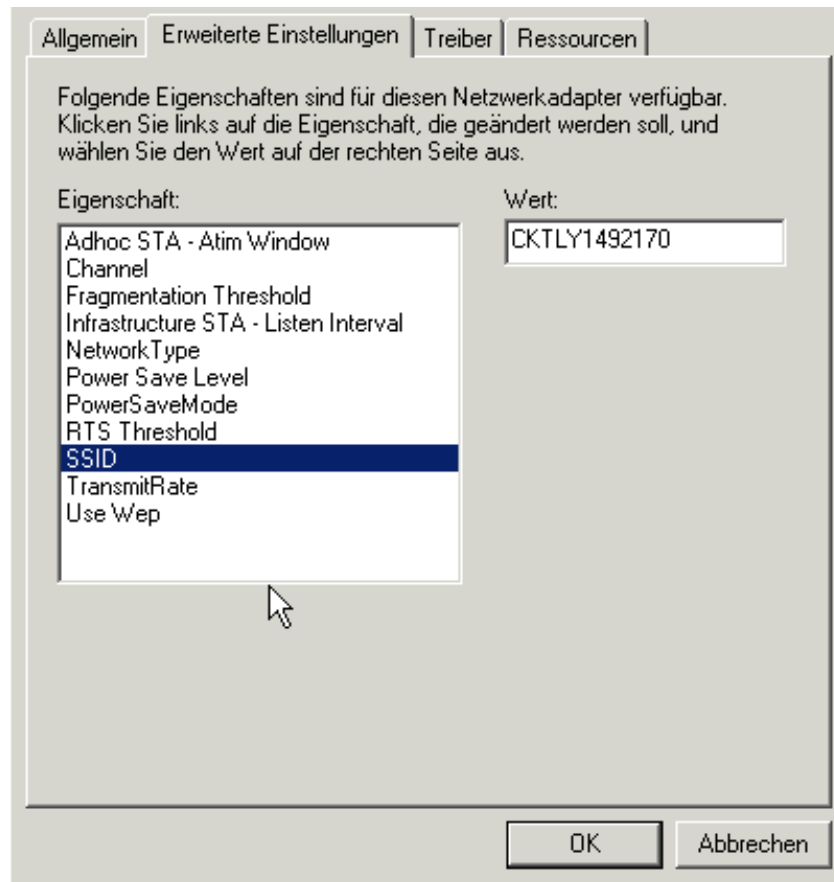


Bild 5.2 SSID eingeben unter Windows 2000

- 5** Bestätigen Sie Ihre Eingabe mit **OK**.
- 6** **IP-Adresse automatisch beziehen (I-GATE 11M AccessPoint als DHCP-Server)**

Das Fenster 'Eigenschaften von LAN-Verbindung' öffnet sich. Markieren Sie den Eintrag **Internetprotokoll (TCP/IP)** und klicken Sie auf **Eigenschaften**. Aktivieren Sie die Option **IP-Adresse automatisch beziehen** und die Option **DNS-Serveradresse automatisch beziehen**. Schliessen Sie das Fenster 'Eigenschaften von Internetprotokoll (TCP/IP)' mit **OK**. Schliessen alle weitere Fenster und starten Sie Ihren Computer neu.

Wenn Sie mit fixen IP-Adressen arbeiten wollen, verfahren Sie gemäss Punkt 7. Sonst gehen Sie zu Punkt 8.

7**Fixe IP-Adresse**

Klicken Sie auf **Start -> Einstellungen -> Systemsteuerung -> Netzwerk- und DFÜ-Verbindungen -> LAN-Verbindung -> Eigenschaften**.

Markieren Sie den Eintrag **Internetprotokoll (TCP/IP)** und klicken Sie auf **Eigenschaften**. Das Fenster 'Eigenschaften von Internetprotokoll (TCP/IP)' öffnet sich.

Aktivieren Sie die Option **Folgende IP-Adresse verwenden**. Geben Sie in den nun freigegebenen Eingabefeldern die gewünschten fixen Daten (IP-Adresse, Subnet-Mask und Gateway) des TCP/IP - Stacks des Rechners ein. Vergessen Sie nicht den DNS-Server anzugeben; dieser wird für den Internet-Zugang unbedingt benötigt. In der Betriebsart nach [Bild 1.2](#) oder [Bild 1.8](#) (I-GATE 11M AccessPoint als Internet-Zugangsrouten für ein WLAN) muss das Gateway und der DNS-Server auf die IP-Adresse des AccessPoints konfiguriert werden.

Sie haben nun alle erforderlichen Einstellungen für fixe IP-Adressen vorgenommen und können deshalb den Netzwerkdialog mit **OK** beenden. Auf die Frage, ob der Computer neu gestartet werden soll, antworten Sie mit **Ja**.

8**Betriebsanzeigen (LEDs)**

Der I-GATE 11M USB ist mit einer LED versehen. Bei einem erfolgreich installierten Treiber muss diese permanent grün blinken.

grün blinken = MobilePort sucht AccessPoint (Scanning)

grün leuchten = MobilePort hat AccessPoint gefunden (Associated)

Wie Sie Probleme beheben können, lesen Sie im Kapitel "[13.1 Ist der MobilePort Treiber erfolgreich geladen?](#)" nach.]

9

Zurück zu Kapitel "[2 MobilePort Hardware installieren](#)" wenn Sie weitere MobilePorts zu installieren haben, sonst weiter zu Kapitel "[5.2 MobilePort Manager installieren](#)".

5.2 MobilePort Manager installieren

- 1 Entfernen Sie die Windows CD-ROM (Ausnahme: W2000, wo keine Windows CD-ROM eingelegt werden musste), legen Sie die I-GATE 11M CD-ROM ein und klicken Sie auf **I-GATE MobilePort Manager installieren**. Je nachdem welchen MobilePort Manager Sie installieren wollen klicken Sie auf **PC Card MobilePort installieren** oder **PCI Card MobilePort installieren** oder **USB MobilePort installieren**. Um den MobilePort Manager für PC Card plus zu installieren klicken Sie ebenfalls auf **PC Card MobilePort installieren**.

Sollte sich das I-GATE 11M CD-Einstiegsbild nicht automatisch öffnen, klicken Sie mit der rechten Maus Taste auf Ihr CD-ROM Laufwerk und dann auf **AutoPlay -> I-GATE MobilePort Manager installieren**. Je nachdem welchen MobilePort Manager Sie installieren wollen klicken Sie dann auf **PC Card MobilePort installieren** oder **PCI Card MobilePort installieren** oder **USB MobilePort installieren**.

- 2 'I-GATE MobilePort Manager Setup' öffnet sich. Klicken Sie auf **Next**. Als Destination Folder erscheint 'C:\Programme\Siemens I-Gate\MobilePort Manager'. Klicken Sie zweimal auf **Next**. Bestätigen Sie die Meldung 'Setup is Complete.' mit **OK**.

- 3 Das Fenster 'I-GATE MobilePort Manager' öffnet sich. Doppelklicken Sie das 'MobilePort Manager' Verknüpfungssicon (grüner PC). Der MobilePort Manager erscheint nun als rotes PC Icon im Windows Taskbar Ihres Rechners. Schliessen Sie das Fenster 'I-GATE MobilePort Manager' und alle anderen Fenstern. Klicken Sie auf das rote PC Icon. Der Register 'Link Info' öffnet sich und im Feld 'State' erscheint 'Scanning'. Klicken Sie auf **OK**. Nach der Erstinstallation empfehlen wir Ihnen Kapitel "[6 MobilePort Management](#)" zu lesen.

4 Service Pack aufspielen



Wenn Sie den MobilePort Manager auf NT4 installiert haben und keinen AccessPoint installieren werden, spielen Sie Ihr Service Pack (mindestens Service Pack 6) jetzt neu auf.

Wenn Sie den MobilePort Manager auf NT4 installiert haben, Probleme beim installieren des MobilePorts hatten (z.B. nicht ständig blinkende LED oder DHCP resp. Dienst Fehlermeldungen) und einen AccessPoint installieren werden, spielen Sie Ihr Service Pack (mindestens Service Pack 6) jetzt neu auf.

Die Service Packs 6 resp. 6a finden Sie auf der I-GATE 11M CD-ROM unter **CD durchsuchen -> misc -> nt4spx** in Ihrer Sprache.

Nach dem Aufspielen des Service Packs muss die MobilePort LED permanent grün blinken.

grün blinken = MobilePort sucht AccessPoint (Scanning)

grün leuchten = MobilePort hat AccessPoint gefunden (Associated)

5 Weiter zu Kapitel "8 I-GATE 11M AccessPoint Hardware anschliessen"

6 MobilePort Management

Monitoring - Für das Monitoring Ihres MobilePorts verwenden Sie den I-GATE 11M MobilePort Manager.

Konfiguration - Am einfachsten konfigurieren Sie Ihr MobilePort über den I-GATE MobilePort Manager. Sie können aber auch die erweiterten Einstellungen des MobilePort Treibers verwenden, müssen aber über diesen Weg nach jeder Konfigurationsänderung einen Neustart durchführen. Bestimmte Konfigurationsparameter können Sie allerdings nur über den erweiterten Einstellungen des MobilePort Treibers ändern.

6.1 Monitoring und Konfiguration mit dem MobilePort Manager

Der installierte und gestartete MobilePort Manager erscheint als PC Icon auf Ihrem Windows Taskbar ([Bild 6.1](#)).



Bild 6.1 MobilePort Manager PC Icon

6.1.1 Monitoring mit dem MobilePort Manager

Je nach Farbe des PC Icons, wissen Sie ohne den MobilePort Manager zu öffnen, bereits etwas über die Qualität Ihrer Verbindung zu einem WLAN AccessPoint. Das Icon leuchtet permanent rot, wenn Ihr MobilePort keine Verbindung findet, gelb wenn die Verbindung ungenügend ist und grün, wenn sie gut ist ([Bild 6.1](#)).

Öffnen Sie den MobilePort Manager indem Sie auf das PC Icon im Windows Taskbar auf Ihrem Desktop klicken.

Das Register **Link Info** ([Bild 6.2](#)) gibt Ihnen weitere Auskünfte über die Verbindung:

State - Das Feld 'Zustand' kann im normalen Betriebszustand 3 Einträge anzeigen: leer = Sie haben keine Verbindung, 'Scanning' = am Suchen oder 'Associated' = verbunden. Im Betriebsart Infrastructure erscheint neben 'Associated' die MAC-Adresse des AccessPoint MobilePorts mit dem Sie verbunden sind.

Current Channel - Im Feld 'Aktueller Kanal' erscheint der default-mässige Kanal für Ihr Land.

Current Tx Rate - die im Register 'Configuration' vorgegebene Senderate erscheint hier.

Rescan - Einen Klick auf diesen Knopf führt zum erneuten 'Scanning' d.h. zum erneuten Suchen nach einer Verbindung auf allen für Ihr Land zugelassenen Kanälen (diese sind in der Firmware ihres MobilePorts einprogrammiert) durch.

Throughput [Bytes/sec] - die aktuellen Datendurchsatzraten. 'Tx' = Senderate und 'Rx' = Empfangsrate.

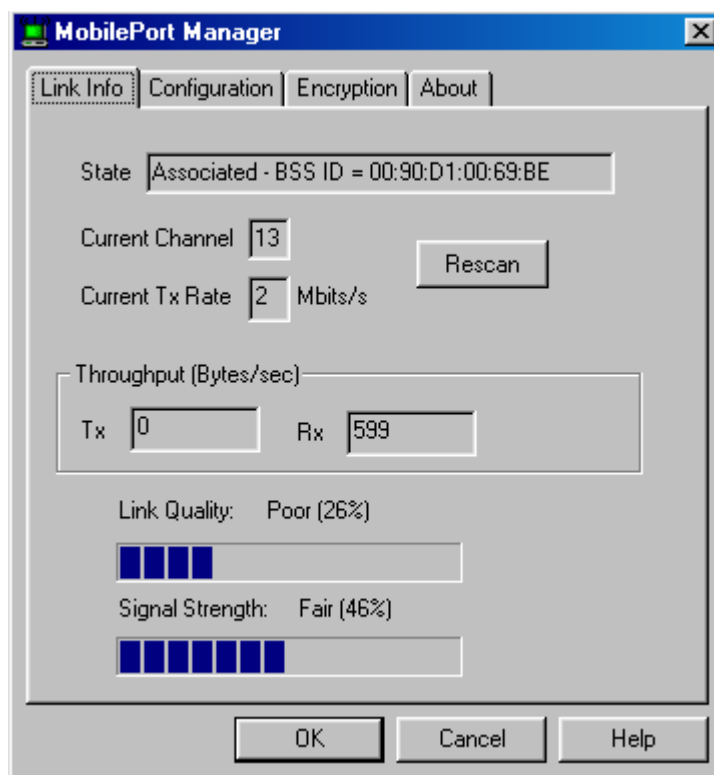


Bild 6.2 MobilePort Manager Link Info

Link Quality - die Verbindungsqualität, wobei Qualität auf Prozent der fehlerlosen Pakete bezogen wird. Je mehr fehlerlose Pakete, desto bessere Verbindungsqualität. Je mehr fehlerlose Pakete, desto besser sind auch die Datendurchsatzraten (siehe 'Throughput' oben). Vier Zustände sind möglich: leer = keine Verbindung, fair = akzeptabel, good = gut, excellent = ausgezeichnet.

Signal Strength - die Feldstärke. Je höher die Feldstärke, desto besser die Verbindung.

6.1.2 Konfiguration mit dem MobilePort Manager

6.1.2.1 Configuration

Das Register **Configuration** (Bild 6.3) zeigt die aktive Konfigurationswerte an. Defaultmässige Konfigurationswerte erscheinen in rot und nicht defaultmässige in schwarz.



Änderungen der Konfigurationswerte sollten nur von erfahrenen Anwendern durchgeführt werden. Generell gilt:

Ändern Sie nie Parameter, von denen Sie nicht genau wissen, was sie bedeuten.

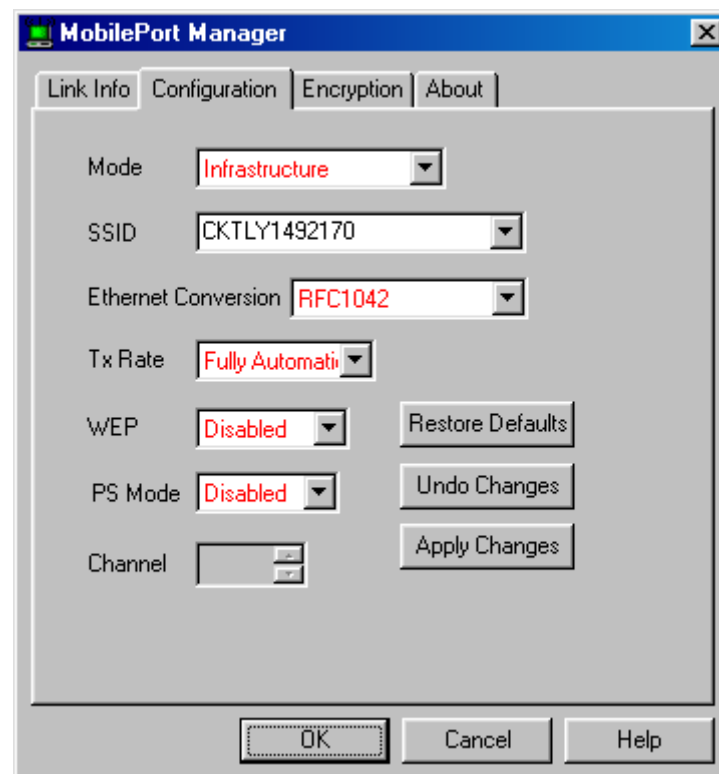


Bild 6.3 MobilePort Manager Configuration

Mode - Der Defaultwert ist 'Infrastructure'. Weiter kann Adhoc gewählt werden. Sehen Sie dazu Kapitel "1.6 Betriebsarten" oder den Kapitel technischen Grundlagen im Referenzhandbuch.

SSID (=WLAN Domain) - Die von Ihnen bei der Treiber Installation angegebene SSID erscheint in schwarz.



Die SSID dient lediglich der Zuordnung zu einem AccessPoint und entspricht damit noch keiner Sicherheitsvorkehrung. Wir empfehlen Ihnen trotzdem, die SSID nach der Erstinstallation zu ändern (siehe Kapitel "9.5 SSID (= WLAN Domain) ändern").

Ethernet Conversion - Der Defaultwert ist 'RFC1042'. Weiter kann 'Encapsulated' oder '802.1h' gewählt werden.

Tx Rate - Der Defaultwert ist 'Fully Automatic'. Weiter kann '1 Mb', '2 Mb', 'Auto 1 or 2Mb', '5.5 Mb' oder '11 Mb' gewählt werden.

WEP - (Wired Equivalent Privacy) Verschlüsselung ist defaultmässig deaktiviert ('Disabled'). Sie können WEP hier (nachdem Sie die Anweisungen im Kapitel "6.1.2.2 MobilePort WEP Verschlüsselung" befolgt haben) für Ihren MobilePort Rechner mit 'Mandatory' aktivieren. Um WEP auf einem AccessPoint einzurichten, befolgen Sie die Anweisungen in Kapitel "9.7 AccessPoint WEP Verschlüsselung".

PS Mode - Power Save Mode ist defaultmässig deaktiviert ('Disabled'). Sie können ihn nachdem Sie den den 'Power Save Level' über den erweiterten Einstellungen des MobilePort Treibers eingestellt haben, hier mit 'Enabled' aktivieren.

6.1.2.2 MobilePort WEP Verschlüsselung

Erst durch WEP Verschlüsselung bestimmen Sie eindeutig wer in Ihrem WLAN teilnimmt. Die 11-Mbit-Funk-Netzwerkkarten (MobilePorts) unterstützen eine Datenverschlüsselung nach dem WEP-Verfahren.

WEP können Sie

- für MobilePorts (d.h. MobilePort Rechner) ohne AccessPoint in einem Ad-hoc Netzwerk und
- für MobilePorts mit AccessPoint in einem Infrastruktur Netzwerk verwenden.



Das WEP-Verfahren funktioniert nur innerhalb eines WLANs, das über die 11-Mbit MobilePorts kommuniziert. Wenn Sie andere Karten verwenden, sollten Sie diese Sicherheitsoption nicht aktivieren.

WEP ist zum Zeitpunkt des Versands dieser Produkte wie folgt verfügbar:

- 11 Mbit Datendurchsatz in einem Ad-hoc Netzwerk mit MobilePorts (d.h. MobilePort Rechner) ohne AccessPoint: Die 11 Mbit WEP Funktionalität ist in den MobilePorts implementiert.
- 2 Mbit oder 5,5 Mbit Datendurchsatz in einem Infrastruktur Netzwerk mit MobilePorts und AccessPoint: Eine 5,5 Mbit WEP Funktionalität ist in den AccessPoints implementiert.
- Besuchen Sie **www.siemens.com/i-gate**. Dort können Sie AccessPoint Firmware für WEP mit 11Mbit Datendurchsatz in einem Infrastruktur Netzwerk demnächst herunterladen.

Wenn Sie WEP auf MobilePorts ohne AccessPoint in einem Ad-hoc Netzwerk verwenden wollen, nehmen Sie jetzt WEP Einstellungen an die MobilePorts im MobilePort Manager unter 'Encryption' vor.



Wenn Sie WEP auf MobilePorts mit AccessPoint in einem Infrastruktur Netzwerk verwenden wollen, gehen Sie jetzt zu Kapitel "[9.7 AccessPoint WEP Verschlüsselung](#)" und nehmen Sie zuerst die AccessPoint WEP Einstellungen vor.

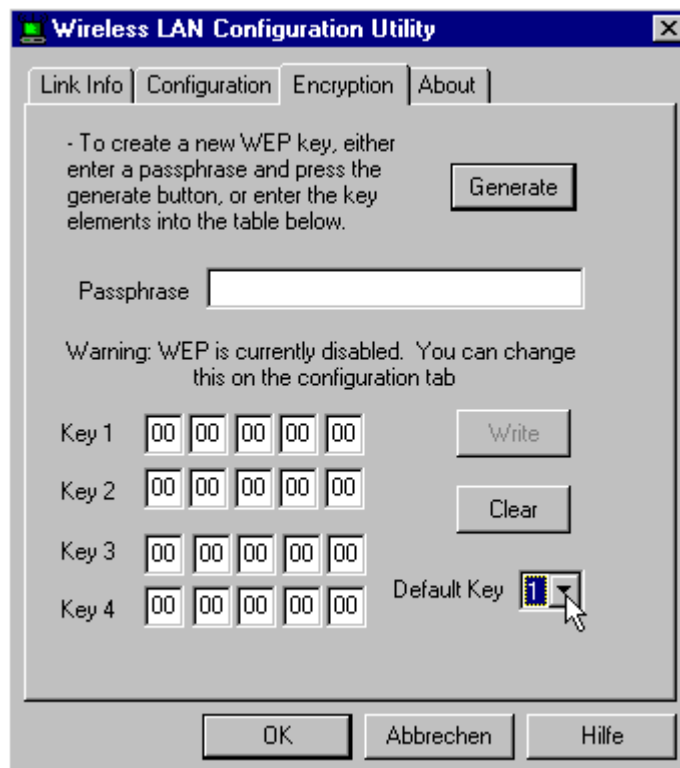


Bild 6.4 MobilePort WEP Verschlüsselung

WEP Schlüssel definieren

Mit WEP haben Sie die Möglichkeit vier unterschiedliche Schlüssel zu definieren, nach denen

- die über die MobilePorts empfangenen Daten entschlüsselt und
- die über die MobilePorts gesendeten Daten verschlüsselt werden.

Definieren Sie die vier Schlüssel über Passphraseeingabe oder über hexadezimale Schlüsseleingabe.



Um eine verschlüsselte Datenkommunikation zu ermöglichen, müssen für alle MobilePort Rechner und AccessPoints die gleiche Passphrase oder die gleiche hexadezimale Schlüssel verwendet werden. Notieren Sie sich die vergebenen Passphrase resp. Schlüssel und bewahren Sie diese an einem sicheren Ort auf.

Über Passphrase

1. Geben Sie im Feld 'Passphrase' einen beliebigen Text ein.
2. Klicken Sie auf 'Generate'. Die Schlüssel 1 bis 4 werden generiert.
3. Klicken Sie auf 'Write'. Der Treiber und das Registry werden mit dem neuen WEP Schlüssel aufdatiert.
4. Klicken Sie auf 'OK'.
5. Wenn Sie WEP auf MobilePorts mit AccessPoint (Infrastruktur Netzwerk) verwenden, öffnen Sie das Register 'Configuration' im MobilePort Manager und stellen Sie 'Tx Rate' auf 'Auto 1 or 2Mb' oder auf '5,5 Mb'.
6. Aktivieren Sie WEP indem Sie im Register 'Configuration' des MobilePort Managers 'WEP' auf 'Mandatory' setzen.
7. Öffnen Sie das Register 'Encryption' des MobilePort Managers und wählen Sie den zu verwendenden Schlüssel im Fenster 'Default Key'. Dabei spielt es keine Rolle welchen Sie wählen.
8. Schliessen Sie das Fenster mit 'OK'.

Über hexadezimale Schlüsseleingabe

1. Geben Sie in jedem der 4 'Key' Felder einen 10-stelligen hexadezimalen Wert ein. Beispiel: 'AB CD 12 34 FE'.
2. Klicken Sie auf 'Clear' um bereits eingetragene Werte zu löschen und neue Einträge zu machen.
3. Klicken Sie auf 'Write'. Der Treiber und das Registry werden mit dem neuen WEP Schlüssel aufdatiert.
4. Klicken Sie auf 'OK'.
5. Wenn Sie WEP auf MobilePorts mit AccessPoint (Infrastruktur Netzwerk) verwenden, öffnen Sie das Register 'Configuration' im MobilePort Manager und stellen Sie 'Tx Rate' auf 'Auto 1 or 2Mb' oder auf '5,5 Mb'.
6. Aktivieren Sie WEP indem Sie im Register 'Configuration' des MobilePort Managers 'WEP' auf 'Mandatory' setzen.
7. Öffnen Sie das Register 'Encryption' im MobilePort Manager und wählen Sie den zu verwendenden Schlüssel im Fenster 'Default Key'. Dabei spielt es keine Rolle welchen Sie wählen.
8. Schliessen Sie das Fenster mit 'OK'.

Neues Passphrase resp. neue hexadezimale Schlüssel definieren

Die in den Dialogfenster eingetragenen Passphrase resp. Schlüssel sind nur bei der ersten Eingabe sichtbar. Nachdem Sie die Eingabe abgeschlossen haben, ist das Feld 'Passphrase' leer und die Schlusselfelder enthalten '00'. Neue WEP Schlüssel definieren Sie durch Überschreiben der Felder und Wiederholung der Punkte 1. bis 8. oben.



Wenn Sie WEP auf MobilePorts mit AccessPoint in einem Infrastruktur Netzwerk verwenden, definieren Sie die AccessPoint WEP Schlüssel neu gemäss Kapitel "[9.7 AccessPoint WEP Verschlüsselung](#)" bevor Sie die MobilePort WEP Schlüssel neu definieren.

6.2 Konfiguration über den erweiterten Einstellungen des MobilePort Treibers

Es ist auch möglich, das MobilePort über die erweiterten Einstellungen des MobilePort Treibers zu konfigurieren. Wir empfehlen Ihnen jedoch die Konfiguration über den MobilePort Manager vorzunehmen.

In den erweiterten Einstellungen sind die Parameter

- 'Mode' resp. 'Network Type'
- 'SSID'
- 'Tx Rate'
- 'Channel' resp. 'DS Channel'
- 'WEP'
- 'PS Mode'

wie im MobilePort Manager Register 'Configuration' konfigurierbar.

Weiter sind die folgenden Parameter konfigurierbar:

- 'Adhoc STA - Atim Window'
- 'RTS Threshold'
- 'Fragmentation Threshold'
- 'Infrastructure STA - Listen Interval'
- 'Power Save Level'

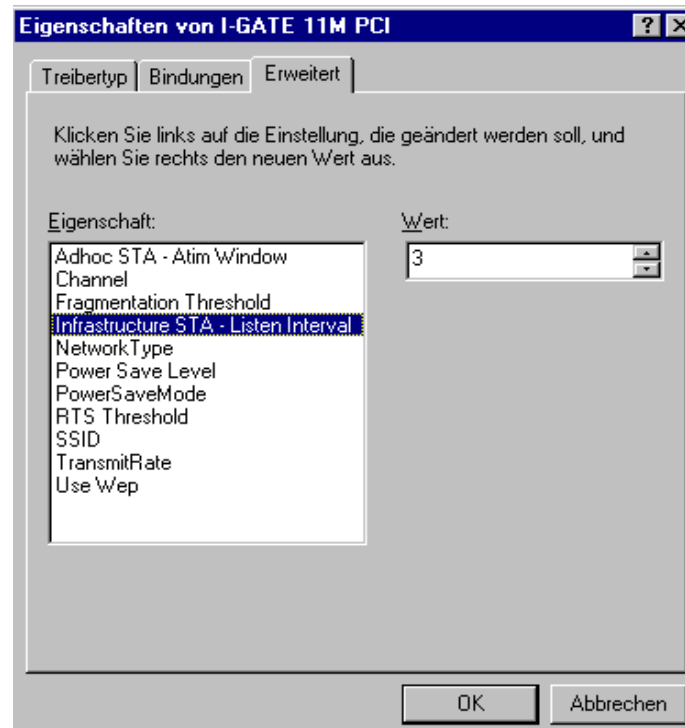


Bild 6.5 Erweiterte Einstellungen des MobilePort Treibers

6.2.1 Power Management

Die Einstellungen

- 'Adhoc STA - Atim Window' (Defaultwert '0')
- 'Infrastructure STA -Listen Interval' (Defaultwert '3')
- 'Power Save Level' (Defaultwert 'Normal') und
- 'Power Save Mode' (Defaultwert 'Disabled')

betreffen Power Management.

Power Management ist zum Zeitpunkt des Versands dieser Produkte noch nicht verfügbar. Belassen Sie diese Einstellungen mit den Defaultwerten und besuchen Sie www.siemens.com/i-gate. Dort können Sie Power Management Software demnächst herunterladen.

Die Power Management Einstellungen der I-GATE 11M MobilePorts dienen zur Schonung der Batterie Ihres Notebooks. Wenn Sie Power Management aktivieren, geht Ihr MobilePort so oft wie möglich in einen 'Schlaf' Modus um Strom zu sparen.

In einem **Infrastruktur** Netzwerk werden im 'Schlaf' Modus an Ihren MobilePort adressierten Daten im AccessPoint gepuffert. Ihr MobilePort wacht in regelmässigen Abständen auf und prüft nach, ob im AccessPoint gepufferten Daten vorhanden sind.

In einem **Ad-hoc** Netzwerk werden im 'Schlaf' Modus an Ihren MobilePort adressierten Daten in den jeweils im Netzwerk beteiligten MobilePorts gepuffert. Ihr MobilePort wacht in regelmässigen Abständen auf und prüft nach, ob in anderen MobilePorts gepufferte Daten vorhanden sind.

Sind keine Daten vorhanden, geht Ihr MobilePort zurück auf 'Schlaf' Modus. Sind gepufferte Daten vorhanden, holt sich das MobilePort diese und geht dann auf 'Schlaf' Modus zurück.

Den 'Power Save Level' stellen Sie für ein Infrastruktur sowohl als auch für ein Ad-hoc Netzwerk entweder auf 'Normal' oder 'Enhanced' Modus ein.

- 'Normal' Modus ist der reguläre IEEE 802.11 Power Save Modus.
- 'Enhanced' Modus ist der Modus in dem das MobilePort auf den regulären Modus schaltet bis alle Nachrichten erhalten wurden und dann auf Power Save Modus zurück geht. Dies erlaubt erhöhten Durchsatz.

Power Management Einstellungen nehmen Sie unter **Start -> Einstellungen -> Systemsteuerung -> System -> Geräte-Manager -> Netzwerkkadpter -> I-GATE 11M PC Card / PC Card plus -> Erweiterte Einstellungen** im Fenster 'Eigenschaften von I-GATE 11M PC Card / PC Card plus' vor.

Für ein **Infrastruktur** Netzwerk:

1. 'Network Type' (Defaultwert 'Infrastructure') stellen Sie auf 'Infrastructure'.
2. 'Infrastructure STA - Listen Interval' (Defaultwert '3'): Dies ist der Listen Interval in Beacon Intervals. Lassen Sie den Defaultwert stehen, da dieser auf den AccessPoint abgestimmt ist.
3. 'Power Save Level' (Defaultwert 'Normal') stellen Sie auf 'Normal' oder 'Enhanced'.
4. 'Power Save Mode' (Defaultwert 'Disabled') stellen Sie auf 'Enabled'.
5. Bestätigen Sie Ihre Eingabe mit OK und führen Sie einen Neustart durch.

Für ein **Ad-hoc** Netzwerk:

1. 'Network Type' (Defaultwert 'Infrastructure') stellen Sie auf 'Ad-hoc'.
2. 'Ad-hoc STA - Atim Window' (Defaultwert zum Zeitpunkt des Versands dieser Produkte noch nicht verfügbar): Dies ist die Zeit nach einem TBTT während dem nur Beacon oder Atim Frames übermittelt werden. Lassen Sie den Defaultwert stehen, da dieser auf den AccessPoint abgestimmt ist.
3. 'Power Save Level' (Defaultwert 'Normal') stellen Sie auf 'Normal' oder 'Enhanced'.
4. 'Power Save Mode' (Defaultwert 'Disabled') stellen Sie auf 'Enabled'.
5. Bestätigen Sie Ihre Eingabe mit OK und führen Sie einen Neustart durch.

7 Anwendung ohne AccessPoint (nur im Ad-hoc-Modus)

7.1 Grundlagen

Netzwerk-Funktionalität

I-GATE 11M erlaubt eine drahtlose Vernetzung von PCs und Notebooks, die mit einem MobilePort bestückt sind. Für das Betriebssystem besteht kein Unterschied zwischen einer konventionellen Ethernet Netzwerkkarte und einem I-GATE 11M MobilePort. Alle mit einem MobilePort ausgerüsteten Geräte bilden ein "wireless" LAN (WLAN).

7.2 Windows "Peer-to-Peer" Netzwerke ohne AccessPoint



Kleine Netzwerke können als sogenanntes "Peer-to-Peer" Netzwerk betrieben werden. Alle Microsoft Betriebssysteme (Windows 95/98/NT/2000) bieten diese Möglichkeit. Jeder Rechner im Netz kann Laufwerke, Verzeichnisse und lokal angeschlossene Drucker unter einem frei wählbaren Namen freigeben und so Benutzern auf anderen Rechnern im Netzwerk den Zugriff auf diese Ressourcen ermöglichen.

Mit I-GATE 11M MobilePorts vernetzte Rechner bieten alle Möglichkeiten von Windows "Peer-to-Peer" Netzwerken. Wichtig ist, dass auf allen beteiligten Rechnern die gleiche Arbeitsgruppe eingestellt ist.

Nach der erfolgreichen Installation der MobilePort Treiber auf mehreren Rechnern sind weitere Einstellungen vorzunehmen, um in einem "Peer-to-Peer" Netzwerk Ressourcen gemeinsam zu verwenden. Bei einem erfolgreich eingerichteten Windows "Peer-to-Peer" Netzwerk sind im Fenster 'Netzwerkumgebung' (klicken Sie hierzu zweimal auf dem Desktop das Icon **Netzwerkumge-**

bung) alle am Netzwerk beteiligten Rechner mit ihrem Namen sichtbar. Durch doppelklicken auf das Rechnersymbol werden die auf diesem Rechner freigegebenen Ressourcen (Laufwerke, Drucker) angezeigt.



Voraussetzung für das Aufsetzen eines "Peer-to-Peer" Netzes ist ein funktionsfähiges TCP/IP-Protokoll auf den I-GATE 11M Mobile-Ports. Die Rechner müssen untereinander über IP kommunizieren können. Ein sehr gutes Diagnosetool hierzu ist der `ping` Befehl (siehe Kapitel 13.4).

7.2.1 "Peer-to-Peer" Netzwerke unter Windows 98

Der folgende Ablauf gibt Ihnen einen Überblick, wie Sie die erforderlichen Einstellungen für ein "Peer-to-Peer" Netzwerk unter Windows 98 vornehmen. Die Punkte 1 und 2 erfolgen im Netzwerk-Setup, den Sie über **Start -> Einstellungen -> Systemsteuerung -> Netzwerk** aufrufen (**Bild 7.1**)

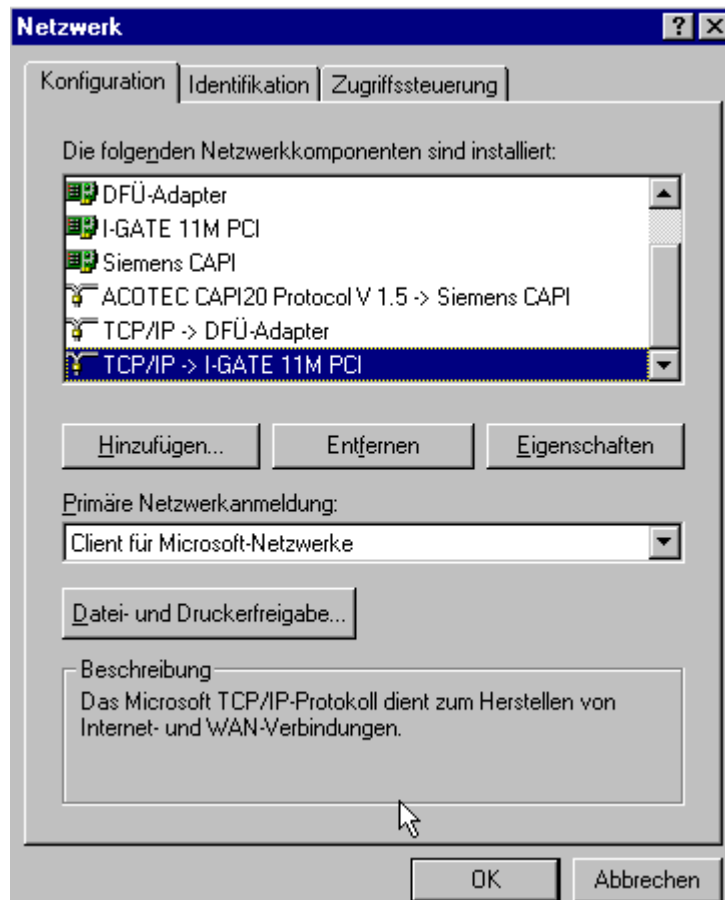


Bild 7.1 Netzwerk-Setup unter Windows 98

- 1 Vergewissern Sie sich im Register 'Konfiguration' dass der Dienst 'Client für Microsoft-Netzwerke' installiert ist und aktivieren Sie die **Datei- und Druckerfreigabe**, sofern dieser Rechner Ressourcen bereitstellen soll. (Dies gilt für alle Rechner.)
- 2 Vergewissern Sie sich, dass auf allen Rechnern im Register 'Identifikation' die gleiche **Arbeitsgruppe** eingetragen ist und unter **Computernamen** jeder Rechner einen eindeutigen Namen hat. Die Arbeitsgruppe wird dazu benutzt, um Rechner an einem LAN in verschiedene "Peer-to-Peer" Netze aufzuteilen.

- ③ Geben Sie bereitzustellenden Ressourcen (Verzeichnisse, Drucker) auf den jeweiligen Rechnern frei. Hierzu markieren Sie im 'Arbeitsplatz' oder Explorer die jeweilige Ressource, klicken auf die rechte Maustaste und wählen den Punkt **Freigabe**. Sollte der Punkt 'Freigabe' fehlen, sind die Punkte 1 und 2 nicht richtig eingerichtet.
- ④ Um einen Drucker, der lokal an einem Rechner im Netzwerk angeschlossen und freigegeben ist, von anderen Rechnern aus zu nutzen, müssen Sie auf allen anderen Rechnern einen 'Remote Printer' einrichten. Wählen Sie hierzu im 'Arbeitsplatz' **Drucker -> Neuer Drucker** und folgen Sie den Anweisungen des Windows Drucker-Setup Assistenten.

7.2.2 Automatische Konfiguration des TCP/IP-Stacks eines "Peer-to-Peer" Netzwerks (ohne AccessPoint) nur bei Windows 98 und 2000

Ein Windows "Peer-to-Peer" Netzwerk benötigt ein funktionsfähiges Transportprotokoll (TCP/IP, NetBEUI oder IPX/ISX). Wenn Sie TCP/IP verwenden wollen müssen die Rechner TCP/IP-mässig richtig konfiguriert sein. In I-GATE 11M Netzwerken mit AccessPoint erfolgt die Konfiguration des WLAN IP-Protokollstacks der am Netz angeschlossenen Rechner durch die DHCP-Server Funktion des I-GATE 11M AccessPoints, d.h. Sie werden überhaupt nicht mit der Konfiguration von TCP/IP-Parametern wie IP-Adressen, Netzmasken, Gateways und DNS-Server konfrontiert. Die Rechner müssen im Netzwerk-Setup für das TCP/IP-Protokoll auf DHCP-Betrieb ('IP-Adresse automatisch beziehen') eingestellt sein und automatisch entsteht ein funktionsfähiges Netzwerk. Bei Windows 98 ist 'IP-Adresse automatisch beziehen' die Standard-einstellung von Microsoft. Dies ist möglich, weil Windows 98 und 2000 einen eingebauten internen DHCP-Server besitzt, der benutzt wird, wenn der Rechner beim Hochfahren keinen externen DHCP-Server im Netz findet. Der interne DHCP-Server vergibt IP-Adressen der Form 169.254.x.x und der Netzmaske 255.255.0.0.

7.2.3 Konfiguration des TCP/IP-Stacks mit festen Werten bei Windows 95 und Windows NT

Da die interne DHCP-Server Funktionalität nur bei Windows 98 und 2000 vorhanden ist, gilt es beim Betrieb von I-GATE 11M Netzwerken ohne AccessPoint mit Rechnern unter Windows 95 oder Windows NT einiges zu beachten. Bei der Einstellung 'IP-Adresse automatisch beziehen' kommt es zu DHCP-Fehlermeldungen und der TCP/IP-Protokollstack ist nicht funktionstüchtig.

Für eine feste IP-Konfiguration Ihres Netzwerks verwenden Sie am besten die für private Zwecke reservierten IP-Adressbereiche. **Tab. 7.1** zeigt die reservierten Adressbereiche mit den zugehörigen Netzmasken. Vermeiden Sie die Werte 254 und 255 auf der letzten Stelle der IP-Adresse. Die 254 ist die Node-Adresse, auf die ein AccessPoint im Auslieferungszustand belegt. Die 255 ist für Broadcasts reserviert.

Adressbereich	Netzmaske	Klasse
10.0.0.0 - 10.255.255.255	255.0.0.0	A
172.16.0.0 - 172.31.255.255	255.255.0.0	B
192.168.0.0 - 192.168.255.255	255.255.255.0	C

Tab. 7.1 Reservierte Adressbereiche

Sie können den Rechnern z.B. folgende IP-Adressen/Netzmasken zuteilen:

Rechner 1: 192.168.10.1/255.255.255.0

Rechner 2: 192.168.10.2/255.255.255.0

usw.



Wichtig ist, dass bei einer Netzmaske von 255.255.255.0 die ersten drei Zahlen in der IP-Adresse bei allen Rechnern unbedingt gleich sind.

Die Einstellung dieser Werte nehmen Sie im Netzwerk-Setup von Windows 95 / Windows NT über die Eigenschaften des TCP/IP-Protokolls vor (siehe **Bild 7.1**).



Für weitergehende Informationen zu den Möglichkeiten von Windows "Peer-to-Peer" Netzwerken ziehen Sie bitte die Online-Help oder die entsprechende Dokumentation von Microsoft zu Rate.

8 I-GATE 11M AccessPoint Hardware anschliessen

8.1 I-GATE 11M ISDN AccessPoint Hardware anschliessen

- 1 Vergewissern Sie sich, dass der MobilePort im AccessPoint steckt.
- 2 Verbinden Sie den AccessPoint mit einem ISDN-S₀-Anschluss (Bild 8.1).
- 3 Schliessen Sie den AccessPoint mit dem mitgelieferten Stecker-netzgerät am Stromnetz an (Bild 8.1).

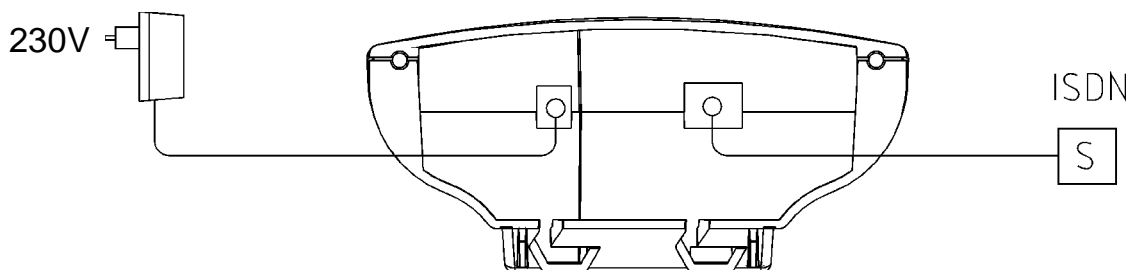


Bild 8.1 I-GATE 11M ISDN AccessPoint von unten

4 Betriebsanzeigen (LEDs)

AccessPoint:

Nach einem kurzen Selbsttest leuchtet die LED 'Power' an der Frontseite permanent.



Die LED 'S-State' leuchtet auf und zeigt an, dass Ihr ISDN-Anschluss aktiv ist.

Ob die LED 'S-State' nur einmal kurz aufleuchtet oder immer leuchtet, ist von Land zu Land verschieden. Sie können jedoch ein Aufleuchten provozieren, indem Sie z.B. ein Telefon am gleichen ISDN-Anschluss aktivieren.

Am MobilePort PC Card in dem AccessPoint muss die grüne LED permanent leuchten.

Rechner mit MobilePort:

An den MobilePorts PCI, PC Card und USB von Rechnern in Reichweite des AccessPoints muss die grüne LED nun ständig leuchten und nicht mehr ständig blinken:

Grün blinken = MobilePort sucht AccessPoint (Scanning)

Grün leuchten = MobilePort hat AccessPoint gefunden (Associated)

Im Windows Taskbar auf dem Destop Ihres Rechners sollte das PC Icon des MobilePort Managers nun gelb oder grün leuchten.

- 5 Genauere Angaben über die Bedeutung Ihrer LEDs finden Sie in ["Tab. 8.1 I-GATE 11M ISDN AccessPoint LEDs"](#).
- 6 Zurück zu Punkt 1 wenn Sie weitere I-GATE 11M ISDN AccessPoints zu installieren haben oder weiter zu ["8.2 I-GATE 11M I/LAN AccessPoint Hardware anschliessen"](#) oder weiter zu Kapitel ["9 I-GATE 11M AccessPoint Software und Grundeinstellungen"](#).

Bezeichnung	Farbe/Zustand	Bedeutung
Power	Aus	Keine Speisung
	Grün	Betriebsbereit
	Grün blinkend	Bootfehler
	Grün unterbrechend	Fehlermeldung oder Gebührensperre verhindert abgehende Rufe
S-State	Aus	S0-Bus nicht angeschlossen
	Grün blinkend	Initalisierung (Kontaktaufnahme mit Verbindungsstelle)
	Grün	Betriebsbereit (S0-Bus aktiviert, D-Kanalprotokoll geprüft)
	Grün kurz aus	Ankommender digitaler Ruf
	Grün	Power-LED aus: Gerät im Bootmonitor

Tab. 8.1 I-GATE 11M ISDN AccessPoint LEDs

Bezeichnung	Farbe/Zustand	Bedeutung
Channel 1 (B-Kanal 1)	Aus	Kanal in Ruhe
	Orange blinkend	Ankommender Ruf liegt an
	Orange	Kanal ist physikalisch hergestellt
	Grün blinkend	Abgehender Ruf wird durchgeführt
	Grün	Zugehörige Protokollverhandlung (z.B. PPP) ist abgeschlossen, Kanal ist logisch online
Channel 2 (B-Kanal 2)	Orange / Grün	Wie Channel 1
Channel 1+2	Aus	Keine Bündelverbindung aktiv
	Grün	Statische bzw. dynamische Bündelverbindung aktiv
Sechste LED	LED nicht bestückt	keine

Tab. 8.1 I-GATE 11M ISDN AccessPoint LEDs

8.2 I-GATE 11M I/LAN AccessPoint Hardware anschliessen

- 1 Vergewissern Sie sich, dass der MobilePort im AccessPoint steckt.
- 2 Über 3 (= ISDN) schliessen Sie den AccessPoint mit einem ISDN-S₀-Anschluss und über 2 (= LAN/ADSL) mit einem Ethernet Hub bzw. Switch oder einem ADSL Modem an (Bild 8.2).
- 3 Schliessen Sie den AccessPoint über 1 (= Strom) mit dem mitgelieferten Steckernetzgerät am Stromnetz an (Bild 8.2).

Prüfen Sie je nach Anschluss (Punkte 4-6 jeweils für ISDN, LAN und ADSL Betriebsanzeigen) das Verhalten Ihrer LEDs:

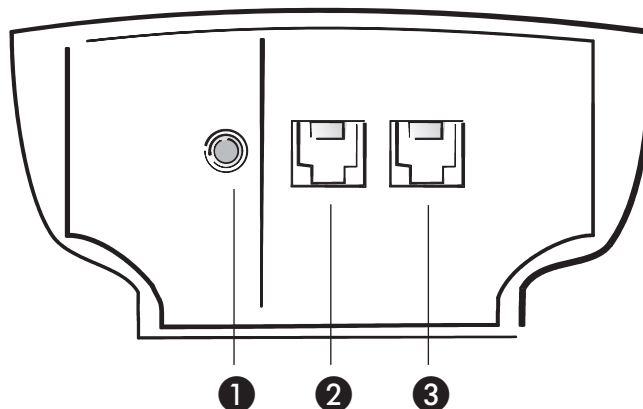


Bild 8.2 I-GATE 11M I/LAN AccessPoint von unten: 1 = Stromversorgung, 2 = LAN/ADSL, 3 = ISDN

ISDN Betriebsanzeigen (LEDs)

- 4 ISDN Betriebsanzeigen (LEDs) in ISDN/LAN Mode (Auslieferungsmode ab Fabrik) oder in ISDN/DSL Mode (DSL erst nach Ausführung Kapitel 9.1 und Umsschaltung von LAN auf DSL Firmware gemäss Kapitel "11.7 Siemens I-GATE 11M I/LAN AccessPoint DSL-Firmware")

AccessPoint:

Nach einem kurzen Selbsttest leuchtet die LED 'Power/Msg' an der Frontseite permanent.



Die LED 'S₀-Status' leuchtet auf und zeigt an, dass Ihr ISDN-Anschluss aktiv ist.

Ob die LED 'S₀-Status' nur eine Weile aufleuchtet oder immer leuchtet, ist von Land zu Land verschieden. Sie können jedoch ein Aufleuchten provozieren, indem Sie z.B. ein Telefon am gleichen ISDN-Anschluss aktivieren.

Am MobilePort PC Card in dem AccessPoint muss die grüne LED permanent leuchten.

Rechner mit MobilePort:

An den MobilePorts PCI, PC Card und USB von Rechnern in Reichweite des AccessPoints muss die grüne LED nun ständig leuchten und nicht mehr ständig blinken.

Grün blinken = MobilePort sucht AccessPoint (Scanning)

Grün leuchten = MobilePort hat AccessPoint gefunden (Associated)

Im Windows Taskbar auf dem Desktop Ihres Rechners sollte das PC Icon des MobilePort Managers nun gelb oder grün leuchten.

- 5 Genauere Angaben über die Bedeutung Ihrer ISDN LEDs finden Sie in ["Tab. 8.2 I-GATE 11M I/LAN AccessPoint LEDs in ISDN/LAN Mode"](#) und ["Tab. 8.3 I-GATE 11M I/LAN AccessPoint LEDs in ISDN/DSL Mode"](#).
- 6 Weiter zu Punkt 4 LAN Betriebsanzeigen oder Punkt 4 DSL Betriebsanzeigen oder zu Kapitel ["9 I-GATE 11M AccessPoint Software und Grundeinstellungen"](#).

LAN Betriebsanzeigen (LEDs)

- 4 **LAN Betriebsanzeigen (LEDs) in ISDN/LAN Mode (Auslieferungsmode ab Fabrik)**

AccessPoint:

Nach einem kurzen Selbsttest leuchtet die LED 'Power/Msg' an der Frontseite permanent.

Die LED 'LAN-Link' leuchtet auf und zeigt an, dass Ihr LAN-Anschluss aktiv ist.

Am MobilePort PC Card in dem AccessPoint muss die grüne LED permanent leuchten.

Rechner mit MobilePort:

An den MobilePorts PCI, PC Card und USB von Rechnern in Reichweite des AccessPoints muss die grüne LED nun ständig leuchten und nicht mehr ständig blinken.

Grün blinken = MobilePort sucht AccessPoint (Scanning)

Grün leuchten = MobilePort hat AccessPoint gefunden (Associated)

Im Windows Taskbar auf dem Desktop Ihres Rechners sollte das PC Icon des MobilePort Managers nun gelb oder grün leuchten.

- 5 Genauere Angaben über die Bedeutung Ihrer LAN LEDs finden Sie in ["Tab. 8.2 I-GATE 11M I/LAN AccessPoint LEDs in ISDN/LAN Mode"](#)
- 6 Weiter zu Kapitel ["9 I-GATE 11M AccessPoint Software und Grundeinstellungen"](#).

DSL Betriebsanzeigen (LEDs)

- 4 **DSL Betriebsanzeigen (LEDs) in ISDN/DSL Mode (DSL erst nach Ausführung Kapitel 9.1 und Umsschaltung von LAN auf DSL Firmware gemäss Kapitel ["11.7 Siemens I-GATE 11M I/LAN AccessPoint DSL-Firmware"](#))**

AccessPoint:

Nach einem kurzen Selbsttest leuchtet die LED 'Power/Msg' an der Frontseite permanent.

Die LED 'LAN-Link' leuchtet auf und zeigt an, dass Ihr DSL-Anschluss aktiv ist.

Am MobilePort PC-Card in dem AccessPoint muss die grüne LED permanent leuchten.

Rechner mit MobilePort:

An den MobilePorts PCI, PC-Card und USB von Rechnern in Reichweite des AccessPoints muss die grüne LED nun ständig leuchten und nicht mehr ständig blinken.

Grün blinken = MobilePort sucht AccessPoint (Scanning)

Grün leuchten = MobilePort hat AccessPoint gefunden (Associated)

Im Windows Taskbar auf dem Desktop Ihres Rechners sollte das PC Icon des MobilePort Managers nun gelb oder grün leuchten.

- 5** Genauere Angaben über die Bedeutung Ihrer DSL LEDs finden Sie in "[Tab. 8.3 I-GATE 11M I/LAN AccessPoint LEDs in ISDN/DSL Mode](#)".
- 6** Weiter zu Kapitel "[9 I-GATE 11M AccessPoint Software und Grundeinstellungen](#)".

Bezeichnung	Farbe/ Funktion	Bedeutung
Power/Msg	grün	Anzeige für Betriebsstatus, Fehlermeldungen, Warnungen, Selbsttest
	aus	Gerät abgeschaltet
	1 x kurz	Bootvorgang (test und laden) begonnen
	blinkend	Anzeige eines Bootfehlers (im Blinkcode kodiert)
	an	Gerät betriebsbereit
	unterbrochen	Wichtige Meldung vorhanden (=> AccessPoint Manager aufrufen !)
S ₀ -Status	grün	Zustand des S ₀ -Anschlusses
	aus	nicht angeschlossen oder S ₀ -Bus im Ruhezustand
	blinkend	Initialisierung (Kontaktaufnahme mit Verbindungsstelle)
	an	betriebsbereit (aktiviert und TEI vorhanden und D-Kanal Protokoll geprüft) (bei Wählverbindungen) Wenn gleichzeitig die Power-LED aus ist, befindet sich das Gerät im Boot-Monitor.

Tab. 8.2 I-GATE 11M I/LAN AccessPoint LEDs in ISDN/LAN Mode

Bezeichnung	Farbe/ Funktion	Bedeutung
WAN-Channel 1	rot/grün	zeigt den Zustand des 1. logischen (!) ISDN-B-Kanals an (sowohl für Router- als auch CAPI-Betrieb)
	aus	Kanal in Ruhe
	rot blinkend	ankommender Ruf liegt an
	grün blinkend	abgehender Ruf wird durchgeführt
	rot	Kanal ist physikalisch hergestellt
	grün	zugehörige Protokollverhandlung (X.75, PPP, etc.) ist abgeschlossen => Kanal ist logisch „online“
	grün mit roten Blitzen (ca. 1/10s)	zeigt ein gesendetes oder empfangenes Daten-Paket an (bei CAPI auch: Layer 2 B-Kanal Pakete. Bei bit-transparenten Protokollen: Dauer-Blitzen, 1 Hz)
WAN-Channel 2	rot/grün	zeigt den Zustand des 2. logischen (!) ISDN-B-Kanals an (sowohl für Router- als auch CAPI-Betrieb)
	aus	Kanal in Ruhe
	rot blinkend	ankommender Ruf liegt an
	grün blinkend	abgehender Ruf wird durchgeführt
	rot	Kanal ist physikalisch hergestellt
	grün	zugehörige Protokollverhandlung (X.75, PPP, etc.) ist abgeschlossen => Kanal ist logisch „online“
	grün mit roten Blitzen (ca. 1/10s)	zeigt ein gesendetes oder empfangenes Daten-Paket an (bei CAPI auch: Layer 2 B-Kanal Pakete. Bei bit-transparenten Protokollen: Dauer-Blitzen, 1 Hz)
LAN-Tx/Rx	grün	zeigt das Senden und Empfangen von Datenpaketen des Netzwerk-Controllers an
	aus	Ruhezustand (keine Pakete)
	an	Datenpaket Empfang oder gesendet

Tab. 8.2 I-GATE 11M I/LAN AccessPoint LEDs in ISDN/LAN Mode

Bezeichnung	Farbe/ Funktion	Bedeutung
LAN-Link	rot/grün	zeigt den Link-Zustand des Netzwerk-Controllers an
	aus	10Base-T not OK (kein Link)
	grün	10Base-T OK (Link)
	rot	Kollision

Tab. 8.2 I-GATE 11M I/LAN AccessPoint LEDs in ISDN/LAN Mode

LED-Be- schriftung	Farbe/Funk- tion	Bedeutung
Power/Msg	grün	Anzeige für Betriebsstatus, Fehlermeldungen, Warnungen, Selbsttest
	aus	Gerät abgeschaltet
	1 x kurz	Bootvorgang (test und laden) begonnen
	blinkend	Anzeige eines Bootfehlers (im Blinkcode kodiert)
	an	Gerät betriebsbereit
	unterbrochen	Wichtige Meldung vorhanden (=> AccessPoint Manager aufrufen !)
S ₀ -Status	grün	Zustand des S ₀ -Anschlusses
	aus	nicht angeschlossen oder S ₀ -Bus im Ruhezustand
	blinkend	Initialisierung (Kontaktaufnahme mit Verbindungsstelle)
	an	betriebsbereit (aktiviert und TEI vorhanden und D-Kanal Protokoll geprüft) (bei Wählverbindungen) Wenn gleichzeitig die Power-LED aus ist, befindet sich das Gerät im Boot-Monitor.

Tab. 8.3 I-GATE 11M I/LAN AccessPoint LEDs in ISDN/DSL Mode

LED-Beschriftung	Farbe/Funktion	Bedeutung
WAN-Channel 1	rot/grün	zeigt den Zustand des 1. logischen (!) ISDN-B-Kanals an (sowohl für Router- als auch CAPI-Betrieb)
	aus	Kanal in Ruhe
	rot blinkend	ankommender Ruf liegt an
	grün blinkend	abgehender Ruf wird durchgeführt
	rot	Kanal ist physikalisch hergestellt
	grün	zugehörige Protokollverhandlung (X.75, PPP, etc.) ist abgeschlossen => Kanal ist logisch „online“
	grün mit roten Blitzen (ca. 1/10s)	zeigt ein gesendetes oder empfangenes Daten-Paket an (bei CAPI auch: Layer 2 B-Kanal Pakete. Bei bittransparenten Protokollen: Dauer-Blitzen, 1 Hz)
WAN-Channel 2	rot/grün	zeigt den Zustand des 2. logischen (!) ISDN-B-Kanals an (sowohl für Router- als auch CAPI-Betrieb)
	aus	Kanal in Ruhe
	rot blinkend	ankommender Ruf liegt an
	grün blinkend	abgehender Ruf wird durchgeführt
	rot	Kanal ist physikalisch hergestellt
	grün	zugehörige Protokollverhandlung (X.75, PPP, etc.) ist abgeschlossen => Kanal ist logisch „online“
	grün mit roten Blitzen (ca. 1/10s)	zeigt ein gesendetes oder empfangenes Daten-Paket an (bei CAPI auch: Layer 2 B-Kanal Pakete. Bei bittransparenten Protokollen: Dauer-Blitzen, 1 Hz)
DSL-Tx/Rx	grün	zeigt das Senden und Empfangen von Datenpaketen des Netzwerk-Controllers an
	aus	Ruhezustand (keine Pakete)
	an	Datenpaket Empfang oder gesendet

Tab. 8.3 I-GATE 11M I/LAN AccessPoint LEDs in ISDN/DSL Mode

LED-Be- schriftung	Farbe/Funk- tion	Bedeutung
DSL-Link	rot/grün	zeigt den Link-Zustand des Netzwerk-Controllers an
	aus	10Base-T not OK (kein Link)
	grün	10Base-T OK (Link)
	rot	Kollision

Tab. 8.3 I-GATE 11M I/LAN AccessPoint LEDs in ISDN/DSL Mode

9 I-GATE 11M AccessPoint Software und Grundeinstellungen

Sie können die Grundeinstellungen für die I-GATE 11M AccessPoints über den Siemens AccessPoint Manager aber auch über Siemens WEBConfig oder Telnet vornehmen. In unserer **Standard Installation** beschreiben wir die Grundeinstellungen über den Siemens AccessPoint Manager für den Betrieb auf Windows 95, 98, NT4 oder 2000.

Stellen Sie sicher, dass das Netzwerk Protokoll TCP/IP auf dem Rechner von dem aus Sie Ihren AccessPoint einstellen möchten installiert ist.

Gehen Sie jetzt zu "[9.1 I-GATE AccessPoint Tools installieren](#)".

9.1 I-GATE AccessPoint Tools installieren

Die AccessPoint Tools verwenden Sie für den I-GATE 11M ISDN AccessPoint sowie auch für den I-GATE 11M I/LAN AccessPoint.

- 1 Stellen Sie sicher, dass der AccessPoint eingeschaltet ist.
- 2 Im I-GATE 11M CD-Einstiegsbild klicken Sie auf **I-GATE AccessPoint Tools installieren** und anschliessend auf **Weiter**. Wählen Sie die zu installierende Software aus. Sollte sich das I-GATE 11M CD-Einstiegsbild nicht automatisch öffnen, klicken Sie mit der rechten Maus Taste auf Ihr CD-ROM Laufwerk und dann auf **AutoPlay**.
 - **Siemens AccessPoint Manager (Standard)**
Die Installation des AccessPoint Managers auf mindestens einem Rechner ist zwingend. Bei einem I-GATE 11M I/LAN AccessPoint der mit einem kabelgebundenen LAN verbunden ist können Sie die AccessPoint Tools auch auf einem Rechner im kabelgebundenen LAN installieren.
 - **Siemens AccessPoint Monitor (Standard)**
Die Installation dieses Monitoring-Tools wird empfohlen.

- **Siemens CAPI**

Diesen ISDN-CAPI-Interface werden Sie brauchen, wenn Sie CAPI-basierte Bürokommunikationsprogramme wie RVS-Com oder z.B. PC-Fax-Programme mit Fax Modem einsetzen wollen. Wenn Sie bereits einen ISDN-CAPI-Interface installiert haben, deinstallieren Sie diesen, bevor Sie Siemens CAPI installieren.



Folgen Sie den weiteren Anweisungen des Setup-Assistenten.

3

Wenn Sie Siemens CAPI installiert haben, werden Sie gefragt, ob der PC neu gestartet werden soll. Entfernen Sie die I-GATE 11M CD-ROM und beantworten Sie mit **JA**.

Wenn Sie Siemens CAPI nicht installiert haben, werden Sie nicht gefragt, ob der PC neu gestartet werden soll. Entfernen Sie die I-GATE 11M CD-ROM und führen Sie trotzdem einen Neustart durch.

4

Im Windows Taskbar auf dem Desktop Ihres Rechners sollte neben dem gelb oder grün leuchtenden PC Icon des MobilePort Managers nun auch das AccessPoint Manager Icon erscheinen. Wenn Sie Siemens CAPI installiert haben, steht 'CAPI' auf dem Icon (**Bild 9.1**).



Bild 9.1 AccessPoint Manager & MobilePort Manager Icons

5

Service Pack aufspielen



Wenn Sie die AccessPoint Tools auf NT4 installiert haben und keinen Internet Zugang einrichten werden, spielen Sie den Service Pack (mindestens Service Pack 6) jetzt neu auf.

Die Service Packs 6 resp. 6a finden Sie auf der I-GATE 11M CD-ROM unter **CD durchsuchen -> misc -> nt4spx** in Ihrer Sprache.

9.2 AccessPoint Grundeinstellungen

Für die im folgenden beschriebene Konfiguration eines I-GATE 11M AccessPoints mit dem Siemens AccessPoint Manager ist eine funktionierende Verbindung auf Ethernet- oder WLAN-Ebene zwischen Konfigurationsrechner und AccessPoint notwendig. Wenn Sie den AccessPoint Manager auf einem Rechner mit MobilePort installiert haben muss die grüne LED dieses MobilePorts permanent leuchten. Ist dies nicht der Fall ist der Start des AccessPoint Managers zwecklos. Versuchen Sie in diesem Fall über den MobilePort Manager und das Kapitel "13 Fehlersuche" das Verbindungsproblem zu lösen.

9.2.1 AccessPoint Grundeinstellung über Siemens AccessPoint Manager

- 1 Starten Sie den installierten AccessPoint Manager mit **Start -> Programme -> Siemens I-Gate -> Siemens AccessPoint Manager**. Dieser erkennt nun den vorhandenen AccessPoint und startet bei einem noch gänzlich unkonfiguriertem AccessPoint (IP-Adresse '10.0.0.254') automatisch den Setup-Assistent für die Grundkonfiguration. (Sollte dies nicht der Fall sein, starten Sie ihn manuell: Im Fenster 'Siemens AccessPoint Manager' klicken Sie auf den AccessPoint Icon unter 'Name' und dann auf **Extras -> Setup Assistent..**) Das Fenster 'I-GATE 11M ISDN - Grundeinstellungen' (Bild 9.2) öffnet sich wenn ein I-GATE 11M ISDN AccessPoint vorhanden ist. Wenn ein I-GATE 11M I/LAN AccessPoint vorhanden ist, heisst das sich öffnende Fenster 'I-GATE 11M I/LAN - Grundeinstellungen'. Ansonsten sind die Fenster identisch.

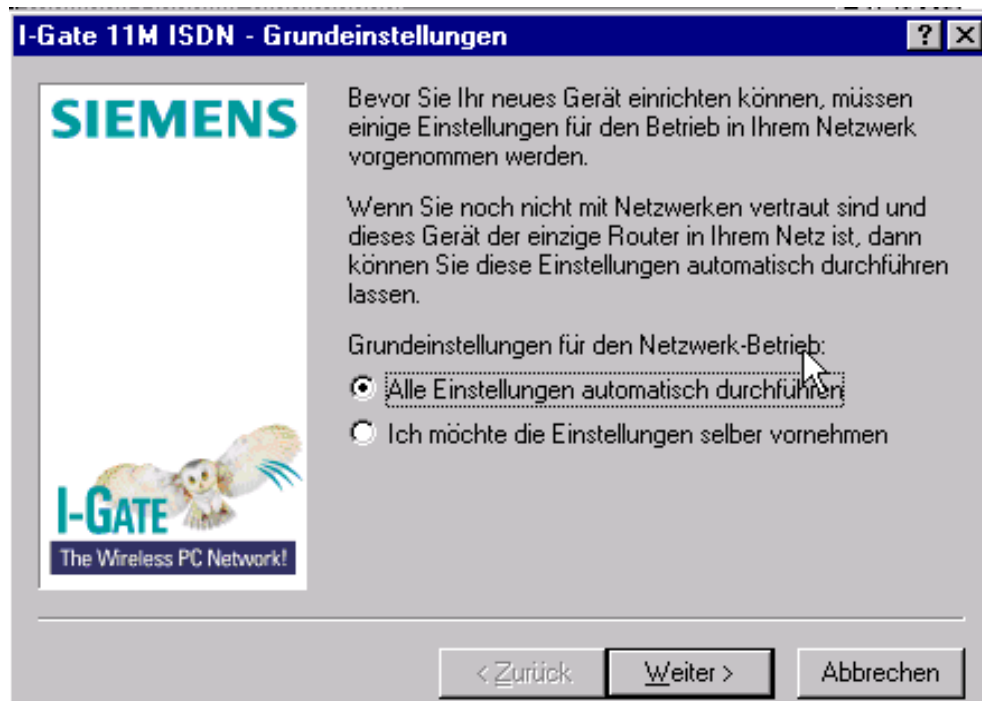


Bild 9.2 AccessPoint Grundeinstellungen für Netzwerk Betrieb

- 2** Wenn Sie mit Netzwerken und IP-Adressen vertraut sind, gehen Sie zu Punkt 3 oder 4.

Wenn Sie nicht mit Netzwerken und IP-Adressen vertraut sind und dazu Entscheidungshilfen möchten, lesen Sie in diesem Handbuch den Kapitel "[12.10 Automatische Adreßverwaltung mit DHCP](#)". Lesen Sie auch im Kapitel Technische Grundlagen des Referenzhandbuchs die Abschnitte 'Netzwerk-Arten' und 'IP-Adressierung'. Gehen Sie dann zu Punkt 3 oder 4.

Wenn Sie nicht mit Netzwerken und IP-Adressen vertraut sind und jetzt keine Zeit haben dies zu werden, empfehlen wir Ihnen die DHCP-Server Funktion des AccessPoints zu nutzen und die IP-Adresse aller Netzteilnehmer vom AccessPoint automatisch zu beziehen. In diesem Fall gehen Sie jetzt zu Punkt 3, die Option 'Alle Einstellungen automatisch durchführen'.

- 3** Wählen Sie die Option 'Alle Einstellungen automatisch durchführen', wenn Sie **NICHT** mit Netzwerken und IP-Adressen vertraut sind und eine der folgenden Annahmen zutrifft. Sonst gehen Sie zu Punkt 4.

Sie haben bisher in Ihrem Netzwerk noch keine IP-Adressen verwendet, möchten das ab jetzt aber gerne tun. Welche IP-Adressen dabei verwendet werden, ist Ihnen egal. Der AccessPoint wird dann als DHCP-Server die IP-Adressen für alle Geräte im Netzwerk (LAN und WLAN) automatisch festlegen und zuweisen.

oder:

Sie möchten überhaupt keine IP-Adressen verwenden, weil Sie z.B. ein reines Windows-Netzwerk betreiben.

(Mit der Option 'Alle Einstellungen automatisch durchführen' macht sich Ihren neuen AccessPoint im lokalen Netz selber unter der IP-Adresse '10.0.0.1' bekannt. Nach einem Neustart beziehen alle Geräte im lokalen Netz ihre IP-Adresse vom DHCP-Server im AccessPoint. Dabei wird automatisch der IP-Adress-Pool von '10.0.0.2' bis '10.0.0.253' verwendet.)

Klicken Sie auf **Weiter** und gehen Sie zu Punkt 5.

4 Wählen Sie die Option 'Ich möchte die Einstellungen selber vornehmen', wenn Sie mit Netzwerken und IP-Adressen vertraut sind und eine der folgenden Annahmen zutrifft:

Sie haben bisher in Ihrem Netzwerk noch keine IP-Adressen verwendet, möchten das ab jetzt aber gerne tun. Sie möchten die IP-Adresse für den AccessPoint jedoch selbst festlegen und geben ihm eine beliebige Adresse aus einem der für private Zwecke reservierten Adressbereiche, z.B. '192.168.10.1' mit der Netzmaske '255.255.255.0'. (In diesem Beispiel macht sich Ihr AccessPoint im lokalen Netz selber unter der IP-Adresse '192.168.10.1' bekannt. Nach einem Neustart beziehen alle Geräte im lokalen Netz ihre IP-Adresse vom DHCP-Server im AccessPoint - sofern Sie den DHCP-Server nicht ausgeschaltet haben. Dabei wird automatisch der IP-Adress-Pool von '192.168.10.2' bis '192.168.10.253' verwendet.

oder:

Sie haben auch bisher schon IP-Adressen auf den Rechnern im LAN verwendet. Geben Sie dem AccessPoint eine freie Adresse aus dem bisher verwendeten Adreßbereich, und wählen Sie aus, ob der AccessPoint als DHCP-Server arbeiten soll oder nicht.

Klicken Sie auf **Weiter** und gehen Sie zu Punkt 5.

- 5** Tragen Sie im Fenster 'I-GATE 11M ISDN - Grundeinstellungen' (bei einem vorhandenen I-GATE 11M I/LAN AccessPoint heisst das Fenster wiederum 'I-GATE 11M I/LAN - Grundeinstellungen') wie in **Bild 9.3** Ihren WLAN-Domain (=SSID) und einen in Ihrem Land gültigen Kanal gemäss Kapitel "14.1 Funkkanäle" ein. In Europa können Sie einfach den bei der Installation defaultmässig vorgeschlagenen Kanal 11 übernehmen. Die vorhandenen Mobile-Ports stellen sich automatisch auf dem im AccessPoint gewählten Kanal ein. Klicken Sie zweimal auf **Weiter**. Auch beim ISDN-Setup ('Rufnummer:' und 'Amtsziffer') brauchen Sie keine Eingaben zu machen; klicken Sie auf **Weiter** und **Fertigstellen**.

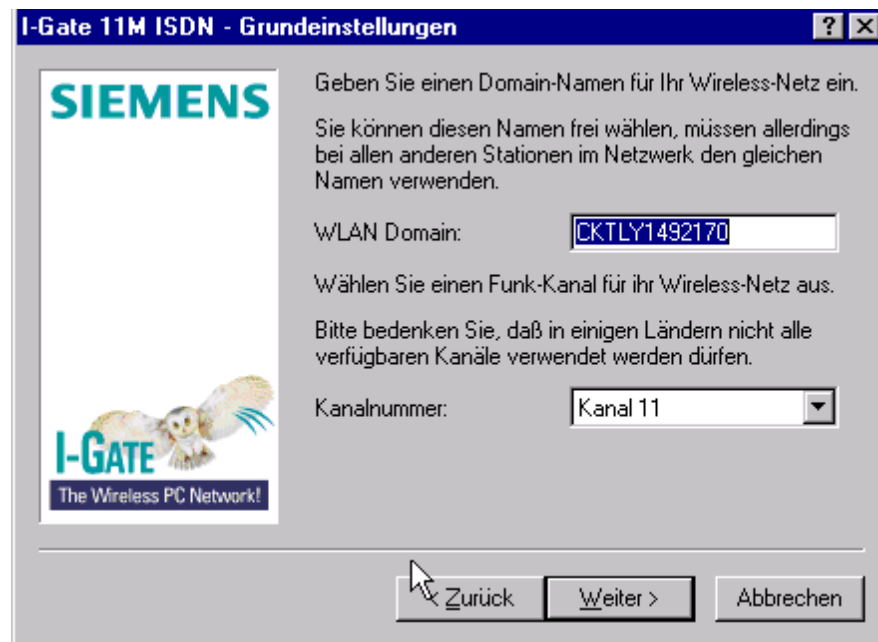


Bild 9.3 AccessPoint Grundeinstellungen für Wireless Netz

Für einen reinen LAN Betrieb mit dem I-GATE 11M I/LAN AccessPoint haben Sie nun die **Standard Installation** gemäss Kapitel 1.8.1 abgeschlossen. Wählen Sie also im sich automatisch öffnenden Setup-Assistent für die Konfiguration von bestimmten Anwendungen **Abbrechen**. Wir empfehlen Ihnen nun Ihre SSID gemäss Kapitel 9.5 zu ändern. Danach empfehlen wir Ihnen die Kapitel "12.1 Sicherheit für Ihre Konfiguration" bis und mit Kapitel "12.3.3 WEP - Sicherheit für Ihr WLAN" zu lesen und Sicherheitsmerkmale entsprechend Ihren Bedürfnissen einzurichten. Details zur Einrichtung einer MAC-Adressenliste finden Sie in Kapitel 9.6

und zur Einrichtung von WEP in Kapitel "9.7 AccessPoint WEP Verschlüsselung".

Wenn Sie ISDN Internet-Zugang über Ihr I-GATE 11M ISDN AccessPoint oder Ihr I-GATE 11M I/LAN AccessPoint einrichten möchten gehen Sie zu Kapitel "9.3 AccessPoint Setup-Assistent für Anwendungen".

9.3 AccessPoint Setup-Assistent für Anwendungen

- 1 Wenn die Grundeinstellungen erledigt sind, wird automatisch der Setup-Assistent für die Konfiguration von bestimmten Anwendungen gestartet. Die Liste mit den verfügbaren Setup-Assistenten wird angezeigt (siehe Bild 9.4).
- 2 Wählen Sie **Internet-Zugang einrichten** wenn Sie einen ISDN Internetzugang einrichten wollen und klicken Sie auf **Weiter**.

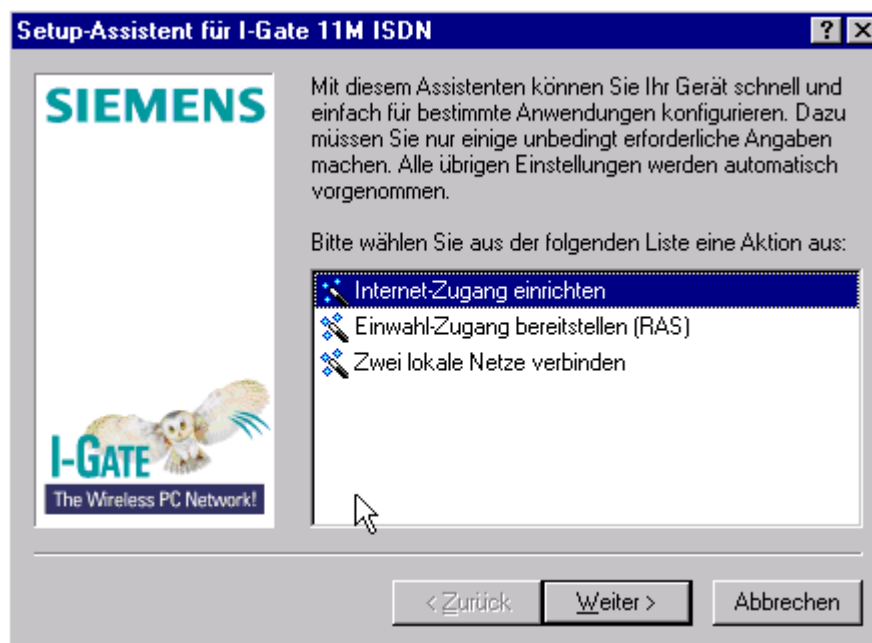


Bild 9.4 AccessPoint Setup Assistent für Anwendungen

9.4 ISDN Internet-Zugang einrichten

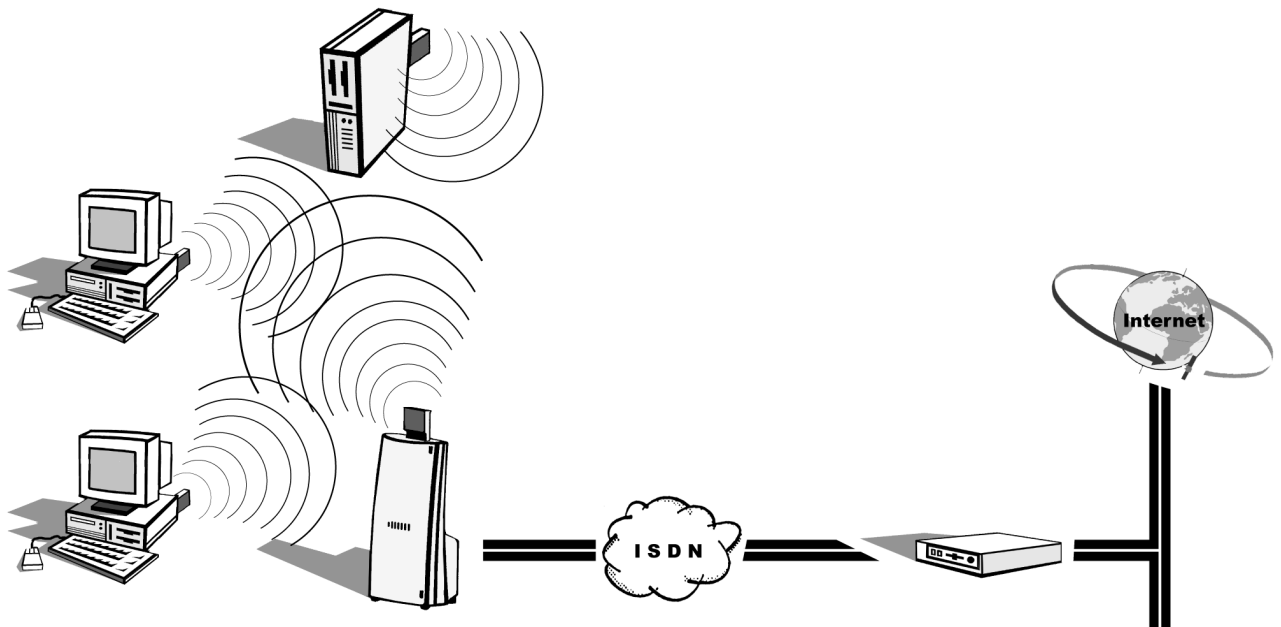


Bild 9.5 ISDN Internet-Zugang mit I-GATE 11M AccessPoint

- 3** Sie werden nun aufgefordert, ein Land auszuwählen. Selektieren Sie das Land, in dem Sie sich befinden.
- 4** Nun erscheint eine Liste mit vorkonfigurierten Providern. Wählen Sie Ihren Internet Provider aus oder 'Standardzugang über PPP'. Folgen Sie den Anweisungen des Setup-Assistenten.



Dazu benötigen Sie folgende Daten Ihres Internet Providers:

- die Einwahltelefonnummer
- die Benutzerkennung
- das Passwort

Diese können Sie der Dokumentation Ihres Internet Providers entnehmen oder kontaktieren Sie gegebenenfalls dessen Hotline.

Verwenden Sie keine vom Internet Provider abgegebene Starter CD-ROM, da diese auf die Einwahl mittels Modem abstützt und deshalb mit der LAN-basierten Funktionsweise des I-GATE 11M nicht kompatibel ist.

Obige Einstellungen müssen nur einmal (auch bei Verwendung mehrerer PCs in Ihrem I-GATE 11M Netz) vorgenommen werden, da diese im AccessPoint gespeichert werden.



Gebührensperre Einstellung anpassen!

Um Ihre Telefonrechnung nicht zu sehr zu strapazieren, verfügt der AccessPoint über eine Gebührensperre, welche im Auslieferungszustand eingeschaltet ist und Ihre Verbindungszeit auf 210 Minuten limitiert. Wird der eingestellte Betrag überschritten, sind keine weiteren Internet-Zugriffe mehr möglich. Die Einstellungen der Gebührensperre können Sie im AccessPoint Manager (siehe "[Bild 9.13 Gebührensperre](#)") ändern.

5

Internet Browsers auf der I-GATE 11M CD-ROM

Falls Sie noch keinen Internet Browser installiert haben, finden Sie Netscape Communicator und MS Internet Explorer auf der I-GATE 11M CD-ROM. Wenn es ganz schnell gehen soll, installieren Sie z.B. den Netscape Communicator 4.7 indem Sie auf **CD durchsuchen -> nscom -> Ihre Sprache -> setup.exe** klicken. Bestätigen Sie alle Anweisungen des Assistenten mit **Weiter** und starten Sie den Computer neu wenn Sie danach gefragt werden. So haben Sie einen aktuellen Browser in weniger als 5 Minuten installiert.

6

Browser einrichten

Bevor Sie sich nun auf eine Internet-Kommunikation mit einem Internet Browser stürzen, nehmen Sie folgende Einstellung in Ihrem Browser vor, zum Beispiel im Netscape Communicator 4.7 unter Windows 95/98/NT4/2000:

Klicken Sie auf **Bearbeiten -> Einstellungen -> Erweitert -> Proxies -> direkte Verbindung zum Internet**.



Sollte diese Option in Ihrem Browser nicht vorhanden sein, installieren Sie ab I-GATE 11M CD-ROM eine aktuelle Version des von Ihnen gewünschten Internet Browsers.

Für weitere Information über die Einstellungen Ihrer Browser Software, sehen Sie die dazugehörige Dokumentation.



Wenn Sie einen Internet Browser, resp. den Internet Zugang auf NT4 installiert haben, spielen Sie Ihr Service Pack (mindestens Service Pack 6) jetzt neu auf. Die Service Packs 6 resp. 6a finden Sie auf der I-GATE 11M CD-ROM unter **CD durchsuchen -> misc -> nt4spx** in Ihrer Sprache.

7

Sie haben die ISDN **Standard Installation mit einem I-GATE 11M ISDN AccessPoint resp. einen I-GATE 11M I/LAN AccessPoint gemäss Kapitel 1.8.1 fertiggestellt.** Wir empfehlen Ihnen nun Ihre SSID gemäss Kapitel 9.5 zu ändern. Danach empfehlen wir Ihnen die Kapitel "**12.1 Sicherheit für Ihre Konfiguration**" bis und mit Kapitel "**12.3.3 WEP - Sicherheit für Ihr WLAN**" zu lesen und Sicherheitsmerkmale entsprechend Ihren Bedürfnissen einzurichten. Details zur Einrichtung einer MAC-Adressenliste finden Sie in Kapitel 9.6 und zur Einrichtung von WEP in Kapitel "**9.7 AccessPoint WEP Verschlüsselung**".

9.5 SSID (= WLAN Domain) ändern

Nach der Erstinstallation ist in den MobilePorts und im AccessPoint die Seriennummer des AccessPoints als SSID eingetragen. Wir empfehlen Ihnen diese nach der Erstinstallation wie folgt zu ändern:

1

Zuerst über den AccessPoint Manager

Doppelklicken Sie im AccessPoint Manager auf das I-GATE 11M AccessPoint Icon. Es erscheint der Konfigurationsdialog. Klicken Sie auf die Registerkarte 'Interfaces'. Das Fenster 'I-GATE 11M Konfiguration' (**Bild 9.6**) mit den einstellbaren Parametern des Funk-LANs öffnet sich. Um die erweiterte Ansicht mit 6 anstatt 3 Register wie in **Bild 9.6** zu erhalten wählen Sie **Ansicht -> Optionen... -> Vollständige Darstellung der Konfiguration**. Geben Sie im Feld 'WLAN Domain' Ihre neue SSID ein. Schliessen Sie das Fenster mit **OK**



Mit dieser Aktion verlieren Sie die Verbindung zum MobilePort Rechner.

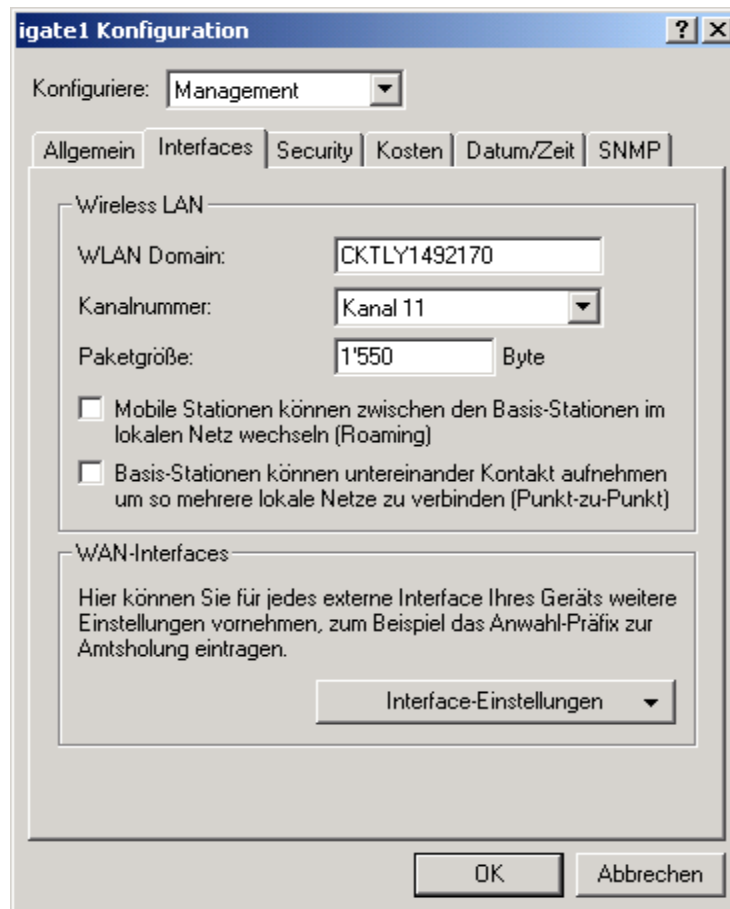


Bild 9.6 I-GATE 11M Konfiguration - WLAN Domain (=SSID) im AccessPoint ändern

2 Dann über den MobilePort Manager...

Passen Sie die SSID Ihres MobilePorts an die SSID Ihres AccessPoints an indem Sie den MobilePort Manager öffnen und dort im Register 'Configuration' den selben Wert im Feld 'SSID' eingetragen.

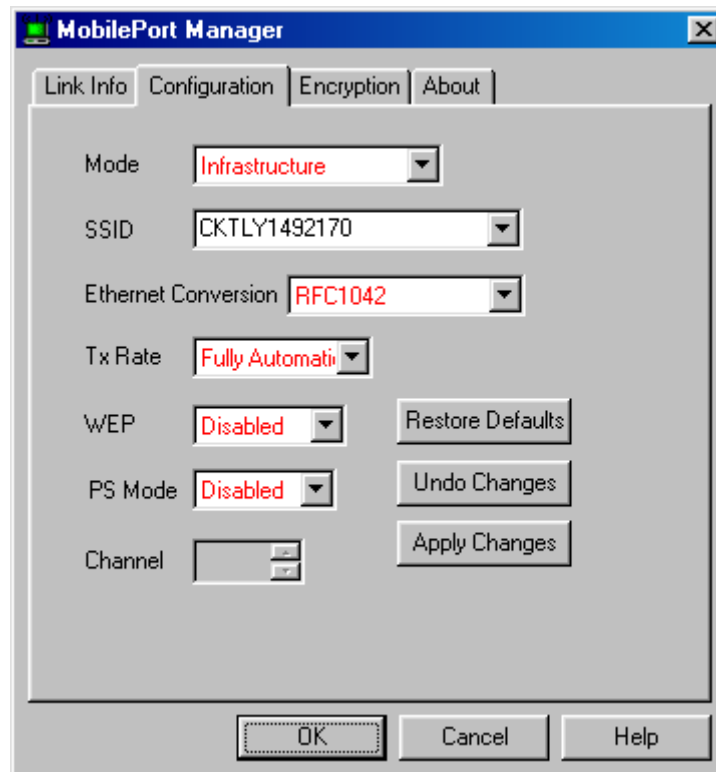


Bild 9.7 MobilePort Manager Configuration - SSID (=WLAN Domain) im MobilePort ändern



Der Wert für die SSID muss auf allen MobilePort Rechnern identisch sein mit der SSID des I-GATE 11M AccessPoints.

9.6 Access Control mittels MAC-Adressenliste

Im Infrastruktur- oder Ad-hoc-Modus können Sie mit dieser Liste spezifischen WLAN MobilePorts den Zugriff auf das WAN über den I-GATE 11M ISDN AccessPoint Router verweigern oder zulassen.

Einstellungen für Access Control nehmen Sie nur im AccessPoint vor. Klicken Sie dazu im AccessPoint Manager auf **Gerät -> Konfigurieren -> WLAN-Zugriff -> Stationsfilter**. Wählen Sie die Arbeitsweise des Filters, d.h. Daten der aufgelisteten Stationen ausfiltern oder übertragen und klicken Sie auf **Stationen...-> Hinzufügen**.

Tragen Sie die MAC-Adressen ein. Diese sind 12-stelligen Zahlen auf der Rückseite Ihres MobilePorts, z.B. 00-60-B3-1F-02-11, wobei Sie die Trennzeichen weglassen. So würde der Listeneintrag '0060B31F0211' lauten (Bild 9.8).

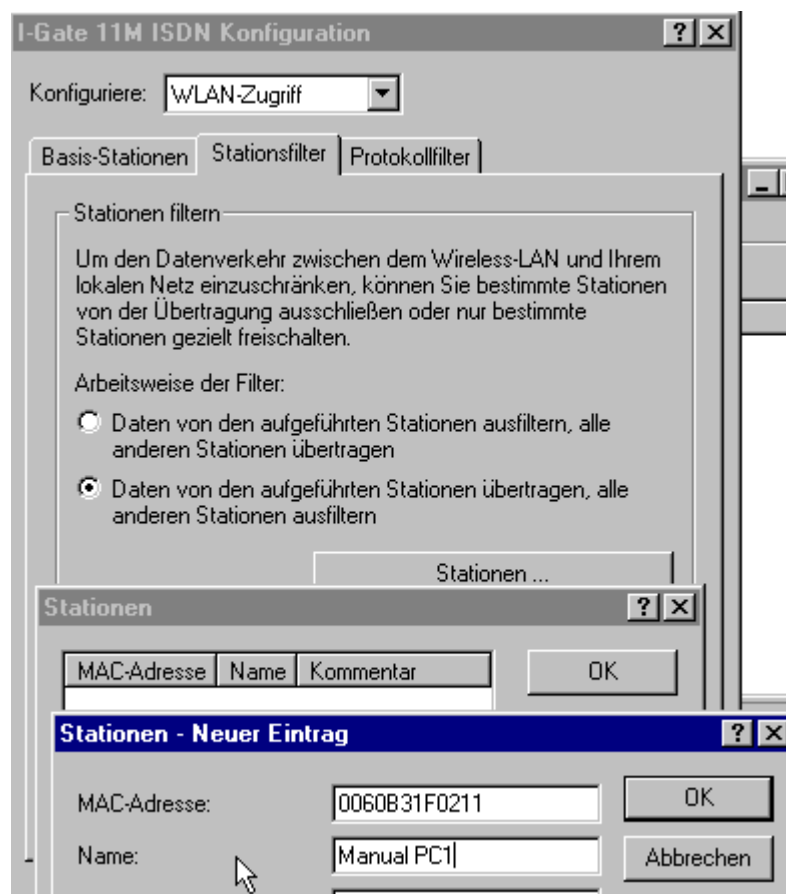


Bild 9.8 MAC-Adressenliste

Daten können trotzdem von und nach MobilePorts (denen der Zugang zum WAN über den I-GATE 11M ISDN mit der MAC-Adressenliste verweigert wurde), übermittelt werden.

Die MAC-Adressenliste limitiert den Zugang zum Router Teil des AccessPoints und somit den Zugang zum WAN oder Ethernet aber nicht den Zugang zum WLAN-Funknetz. Dies entspricht auch dem IEEE 802.11 Standard, wonach es möglich sein muss, sich mit dem Eintrag 'ANY' im Feld 'SSID' resp. im Feld 'WLAN-Domain' an beliebigen innerhalb der Funkweite bestehenden WLAN-Funknetzen anzuschliessen.

Wenn Sie als Netzbetreiber Ihr WLAN-Funknetz schliessen möchten, so verwenden Sie dazu WEP (Wired Equivalent Privacy) Verschlüsselung.

9.7 AccessPoint WEP Verschlüsselung

Erst durch WEP Verschlüsselung bestimmen Sie eindeutig wer in Ihrem WLAN teilnimmt. Die 11-Mbit-Funk-Netzwerkkarten (MobilePorts) unterstützen eine Datenverschlüsselung nach dem WEP-Verfahren.

WEP können Sie

- für MobilePorts (d.h. MobilePort Rechner) ohne AccessPoint in einem Ad-hoc Netzwerk und
- für MobilePorts mit AccessPoint in einem Infrastruktur Netzwerk verwenden.



Das WEP-Verfahren funktioniert nur innerhalb eines WLANs, das über die 11-Mbit MobilePorts kommuniziert. Wenn Sie andere Karten verwenden, sollten Sie diese Sicherheitsoption nicht aktivieren.

WEP ist zum Zeitpunkt des Versands dieser Produkte wie folgt verfügbar:

- 11 Mbit Datendurchsatz in einem Ad-hoc Netzwerk mit MobilePorts (d.h. MobilePort Rechner) ohne AccessPoint: Die 11 Mbit WEP Funktionalität ist in den MobilePorts implementiert.
- 2 Mbit und 5,5 Mbit Datendurchsatz in einem Infrastruktur Netzwerk mit MobilePorts und AccessPoint: Eine 5,5 Mbit WEP Funktionalität ist in den AccessPoints implementiert.
- Besuchen Sie **www.siemens.com/i-gate**. Dort können Sie AccessPoint Firmware für WEP mit 11Mbit Datendurchsatz in einem Infrastruktur Netzwerk demnächst herunterladen.



Wenn Sie WEP auf MobilePorts mit AccessPoint in einem Infrastruktur Netzwerk verwenden wollen, nehmen Sie zuerst die WEP Einstellungen für das AccessPoint im AccessPoint Manager unter **Gerät - Konfigurieren -> Konfiguriere: WLAN-Zugriff -> WEP** wie folgt beschrieben vor. Dann gehen Sie für MobilePort WEP Einstellungen zu "**6.1.2.2 MobilePort WEP Verschlüsselung**".

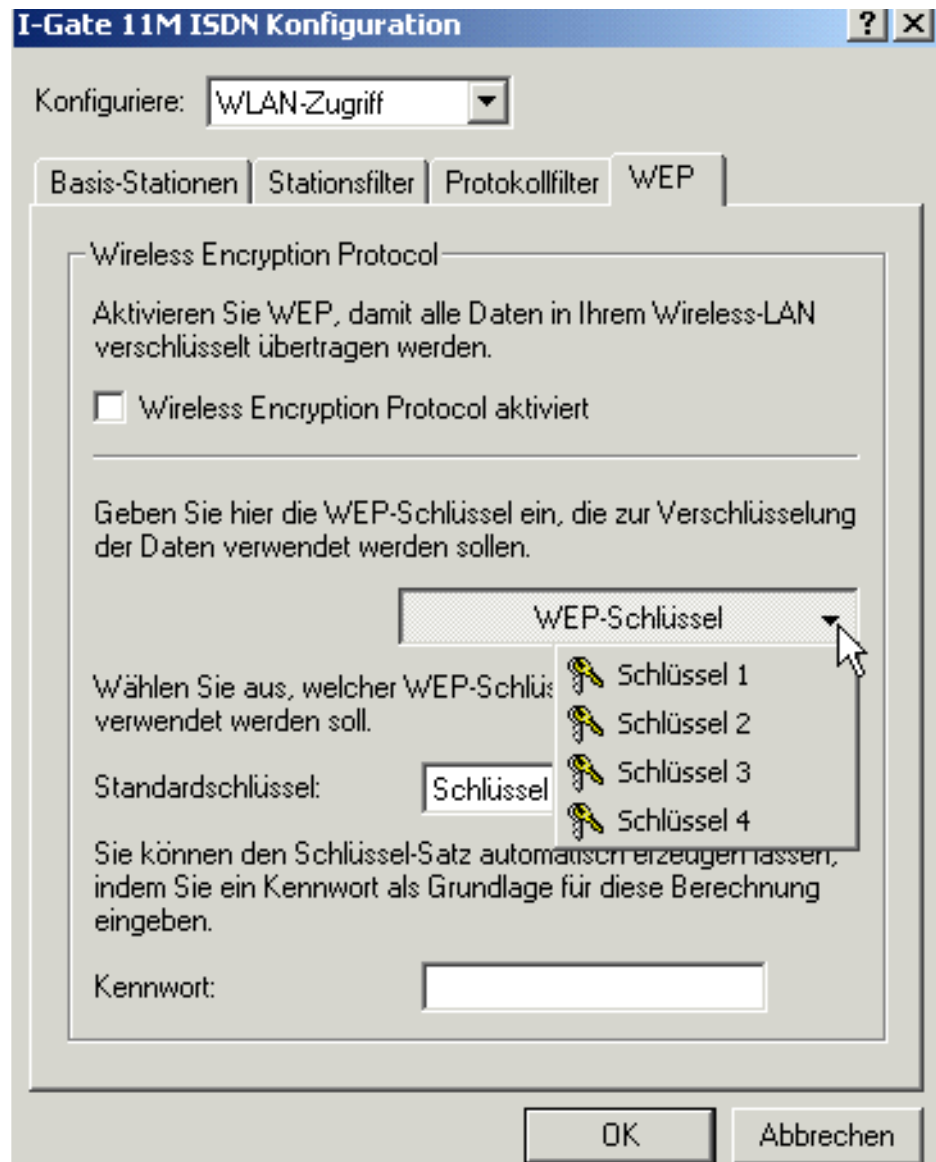


Bild 9.9 AccessPoint WEP Verschlüsselung

WEP Schlüssel definieren

Mit WEP haben Sie die Möglichkeit vier unterschiedliche Schlüssel zu definieren, nach denen

- die über die MobilePorts empfangenen Daten entschlüsselt und
- die über die MobilePorts gesendeten Daten verschlüsselt werden.

Definieren Sie die vier Schlüssel über Kennworteingabe oder über hexadezimale Schlüsseleingabe.



Um eine verschlüsselte Datenkommunikation zu ermöglichen, müssen für alle MobilePort Rechner und AccessPoints die gleichen Kennworte oder die gleichen hexadezimalen Schlüssel verwendet werden. Notieren Sie sich die vergebenen Kennworte resp. Schlüssel und bewahren Sie diese an einem sicheren Ort auf.

Über Kennwort

1. Geben Sie im Feld 'Kennwort' einen beliebigen Text ein.
2. Klicken Sie auf 'OK'.
3. Wenn Sie das nicht bereits gemäss Kapitel "6.1.2.2 MobilePort WEP Verschlüsselung" für Ihr MobilePort Rechner getan haben, öffnen Sie das Register 'Configuration' im MobilePort Manager und stellen Sie 'Tx Rate' auf 'Auto 1 or 2Mb' oder auf '5,5 Mb'.
4. Öffnen Sie das Fenster WEP im AccessPoint Manager wieder und aktivieren Sie WEP indem Sie im 'Wireless Encryption Protocol aktiviert' ankreuzen.
5. Wählen Sie den zu verwendenden Schlüssel im Fenster 'Standardschlüssel'. Dabei spielt es keine Rolle welchen Sie wählen.
6. Schliessen Sie das Fenster mit 'OK'.
7. Nehmen Sie WEP Einstellungen an Ihren MobilePorts gemäss Kapitel "6.1.2.2 MobilePort WEP Verschlüsselung" vor.

Über hexadezimale Schlüsseingabe

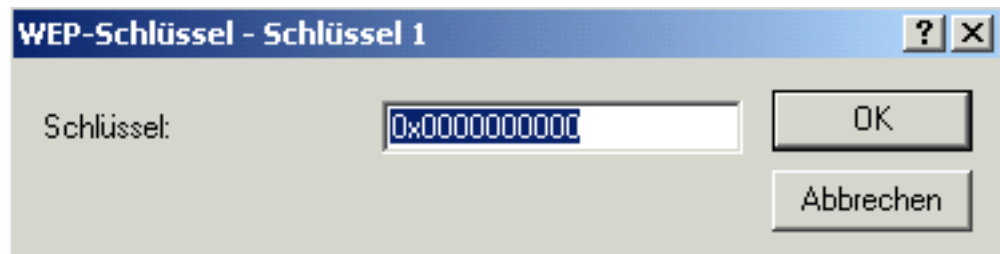


Bild 9.10 AccessPoint WEP Verschlüsselung - Schlüssel 1

1. Geben Sie in jedem der 4 'Schlüssel' Felder einen 10-stelligen hexadezimalen Wert und Beispiel: 'ABCD1234FE'
2. Bestätigen Sie jede der 4 Eingaben mit 'OK'.
3. Wenn Sie das nicht bereits gemäss Kapitel "6.1.2.2 MobilePort WEP Verschlüsselung" für Ihr MobilePort Rechner getan haben, öffnen Sie das Register 'Configuration' im MobilePort Manager und stellen Sie 'Tx Rate' auf 'Auto 1 or 2Mb' oder auf '5,5 Mb'.
4. Öffnen Sie das Fenster WEP wieder und aktivieren Sie WEP indem Sie im 'Wireless Encryption Protocol aktiviert' ankreuzen.
5. Wählen den zu verwendenden Schlüssel im Fenster 'Standard-schlüssel'. Dabei spielt es keine Rolle welchen Sie wählen.
6. Schliessen Sie das Fenster mit 'OK'.
7. Nehmen Sie WEP Einstellungen an Ihren MobilePorts gemäss Kapitel "6.1.2.2 MobilePort WEP Verschlüsselung" vor.

Neues Passphrase resp. neue hexadezimale Schlüssel definieren

Die in den Dialogfenster eingetragenen Kennworte resp. Schlüssel bleiben nach der ersten Eingabe sichtbar. Neue WEP Schlüssel definieren Sie durch Überschreiben der Werte und Wiederholung der Punkte 1. bis 7. oben.



Wenn Sie WEP auf MobilePorts mit AccessPoint in einem Infrastruktur Netzwerk verwenden, definieren Sie die AccessPoint WEP Schlüssel neu gemäss Kapitel "9.7 AccessPoint WEP Verschlüsselung" bevor Sie die MobilePort WEP Schlüssel neu definieren.

9.8 Konfiguration mit dem AccessPoint Manager

Bevor Sie aufgrund dieses Kapitels Änderungen an der Konfiguration vornehmen, empfehlen wir Ihnen den Kapitel 'Technische Grundlagen' im Referenzhandbuch auf der I-GATE 11M CD-ROM zu lesen. Danach empfehlen wir, den Abschnitt **Konfiguration sichern/wiederherstellen** zu beachten. Ausführlichere Information zu Konfiguration, Funktionen und Betriebsarten finden Sie in Kapitel "11 AccessPoint - Konfigurationsmöglichkeiten" und Kapitel "12 AccessPoint - Funktionen und Betriebsarten".

Mit dem Siemens AccessPoint Manager steht Ihnen ein komfortables Programm zur Verwaltung Ihres I-GATE 11M AccessPoints zur Verfügung. Folgende Funktionen können Sie damit ausführen:

- Ändern der Konfiguration des AccessPoints.
- Speichern bzw. Laden von kompletten Konfigurationen in bzw. aus Dateien.
- Laden einer neuen Firmware.
- Aufruf von Setup-Assistenten für die Konfiguration typischer Anwendungen.

Bild 9.11 zeigt das Hauptfenster des Siemens AccessPoint Managers.

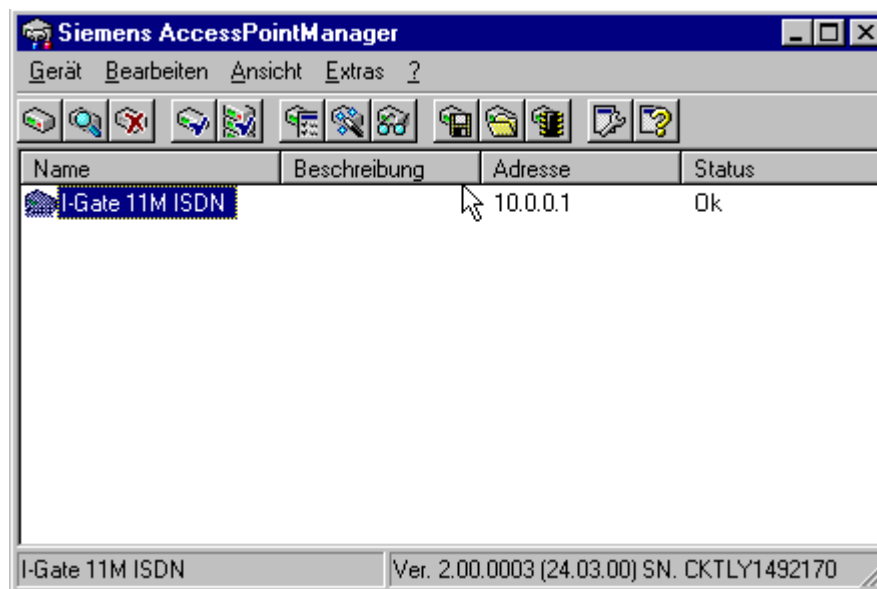


Bild 9.11 AccessPoint Manager Hauptfenster

Erkennen von AccessPoints

Beim Aufstarten sucht der AccessPoint Manager das Netz nach vorhandenen AccessPoints ab und vergleicht die Daten der gefun-

denen AccessPoints mit seinen internen Daten. Falls ein in den internen Daten vorhandener AccessPoint nicht mehr gefunden wird (z.B. wenn er ausgeschaltet ist), wird dies durch ein gelbes Ausrufezeichen im Hauptfenster angezeigt. Wenn ein in der internen Datenbank vorhandener AccessPoint wirklich nicht mehr erreichbar ist (z.B. wenn Sie seine IP-Adresse umkonfiguriert haben), sollten Sie ihn löschen (Menü **Gerät** -> **Löschen**). Andernfalls wird beim Aufstarten des AccessPoint Managers unnötig viel Zeit durch Kommunikationsversuche mit dem nicht mehr vorhandenen Gerät benötigt.

Falls der AccessPoint Manager beim Aufstarten einen noch nicht konfigurierten AccessPoint (Auslieferungszustand) findet, startet er automatisch einen Assistenten zur Grundkonfiguration und anschließend den Setup-Assistenten (siehe Kapitel 9.2).

Der Konfigurationsdialog

Den allgemeinen Konfigurationsdialog (Bild 9.12) erreichen Sie durch Doppelklicken des AccessPoint Icons im Hauptfenster des AccessPoint Managers oder durch das Menü **Gerät** -> **Konfigurieren**, wenn Sie ein AccessPoint ausgewählt haben.

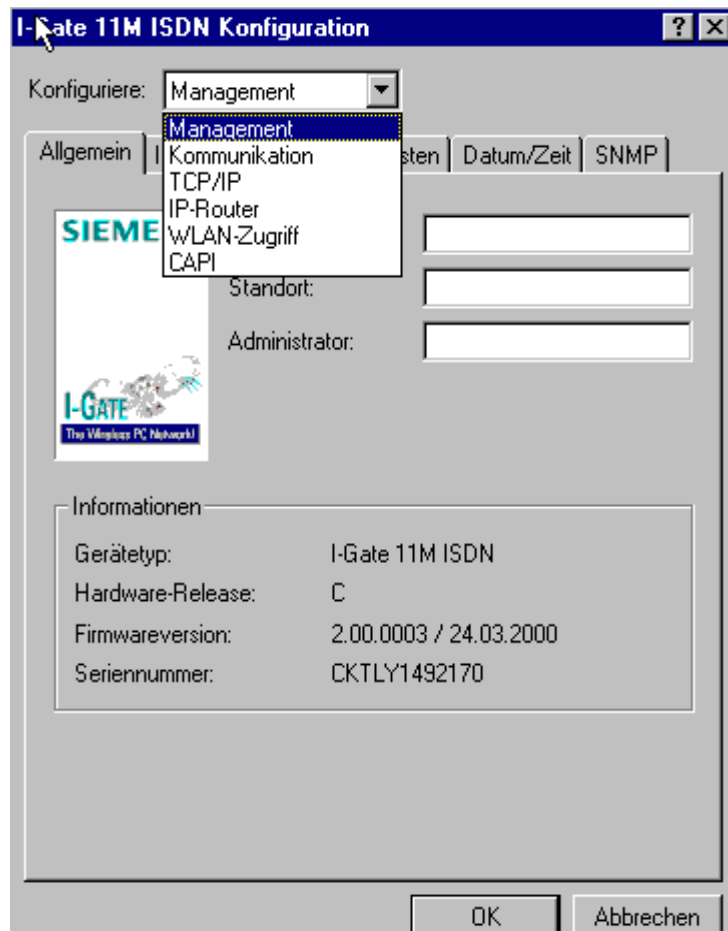


Bild 9.12 Konfigurationsdialog

Die änderbaren Parameter sind in mehrere Bereiche (Feld 'Konfiguriere') aufgeteilt. Für jedes Eingabefeld können Sie mit der <F1> Taste eine Hilfefunktion zur genauen Erläuterung des Parameters aufrufen.



Änderungen in den 'Konfiguriere' Bereichen des Konfigurationsdialogs sollten nur von erfahrenen Anwendern durchgeführt werden. Für diese sollten die angebotenen Einstellmöglichkeiten zusammen mit der Hilfefunktion selbsterklärend sein. Generell gilt:
Ändern Sie nie Parameter, von denen Sie nicht genau wissen, was sie bedeuten.

Konfiguration sichern/wiederherstellen

Unter dem Menü **Bearbeiten** finden Sie im AccessPoint Manager die Funktionen zur Verwaltung von kompletten Konfigurationen des AccessPoints. Sie können die aktuelle AccessPoint Konfiguration in einer Datei speichern, eine gesicherte Konfiguration wiederherstellen oder eine bereits gespeicherte editieren.



Wenn Sie umfangreiche Änderungen vornehmen oder nur ein wenig experimentieren wollen, empfehlen wir Ihnen, die funktionierende Konfiguration zu speichern, um sie gegebenenfalls schnell wiederherstellen zu können. Die nicht funktionierende Konfigurationsdatei kann auch als Basis für telefonisches oder elektronisches (Internet, E-Mail) Troubleshooting verwendet werden.

Firmware Update

Ebenfalls unter dem Menü **Bearbeiten** befindet sich der Punkt **Firmware Verwaltung**. Hier können Sie sich die aktuell geladenen Firmwareversionen anzeigen lassen. Der AccessPoint ist generell in der Lage, zwei verschiedene Firmwareversionen in seinem Speicher zu halten. Von denen ist jeweils eine aktiv geschaltet (Kennzeichnung mit schwarzem Punkt).

Wichtigster Punkt ist die Funktion **Neue Firmware hochladen**. Damit können Sie den AccessPoint mit einer neuen Firmware, die als Datei vorliegen muss, laden. Falls neue AccessPoint Firmware verfügbar ist, können Sie diese von der I-GATE 11M Support Seite über das Internet (www.siemens.com/i-gate) herunterladen und anschliessend Ihren AccessPoint selber mit der neuen Firmware hochrüsten. Mehr über das Hochladen von Firmware erfahren Sie in Kapitel "[11.4 Neue Firmware mit FirmSafe](#)".

Setup-Assistent

Unter dem Menü **Extras** befindet sich der Setup-Assistent für die drei typischen Anwendungen des AccessPoints. Mit diesen Assistenten ist es auch einem unerfahrenen Anwender in Kombination mit dem DHCP-Server Betrieb des AccessPoints möglich, zumindest den Betrieb als Internet Access Router für mehrere Rechner in einem Netzwerk erfolgreich einzurichten.

Gebührensperre

Um die Einstellungen der Gebührensperre zu ändern, gehen Sie wie folgt vor. Wählen Sie im allgemeinen Konfigurationsdialog (Bild 9.13) den Managementbereich Management -> Kosten. Um die Gebührensperre auszuschalten, geben Sie in den Feldern 'Gebühren-Limit' (in Einheiten) und 'Zeit-Limit' (in Minuten) den Wert 0 ein.

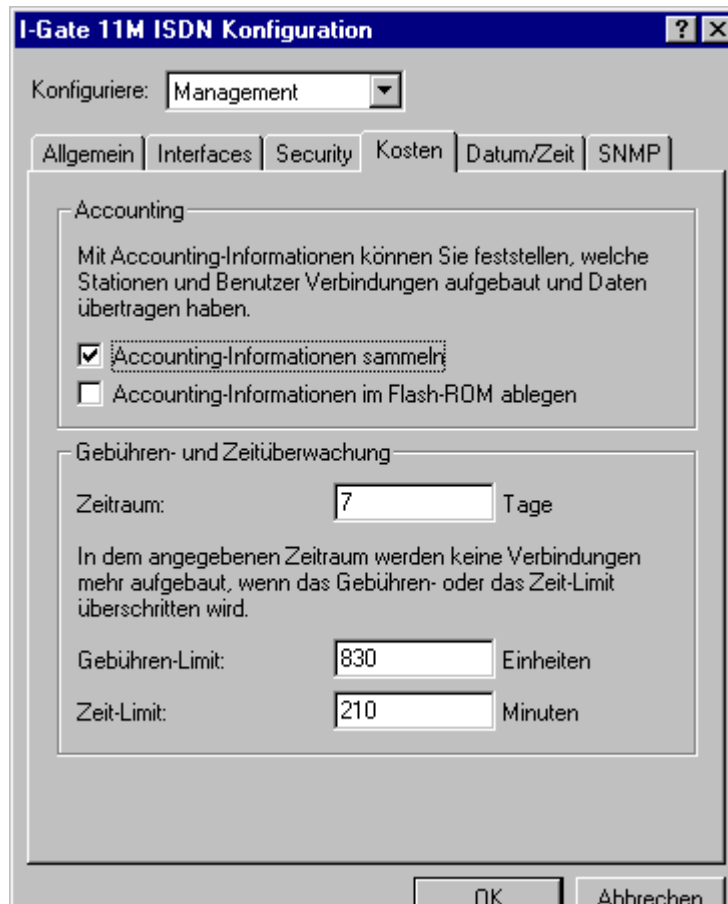


Bild 9.13 Gebührensperre

Providerwechsel

Auf dem AccessPoint können die Zugangsdaten zu mehreren Internet Providern eingerichtet werden, aktiv ist jedoch immer nur einer. Welcher Provider vom AccessPoint gewählt wird, hängt von der Einstellung der Default Route in der Routing-Tabelle des AccessPoints ab.

Wenn Sie einen weiteren Provider über den Setup-Assistenten einrichten, werden Sie gefragt, ob Sie die bestehende Default Route überschreiben möchten. Wenn Sie diese Frage positiv quittieren,

gehen Sie ab jetzt über den neuen Provider ins Netz. Der erste Provider ist zwar noch eingerichtet, aber nicht mehr als Default Route eingetragen.

Eine manuelle Umschaltung können Sie über die Änderung der Default Route des AccessPoints mit dem AccessPoint Manager durchführen. Wählen Sie hierzu im Konfigurationsdialog (Bild 9.12) den Managementbereich **IP-Router -> Routing** und öffnen Sie die Routing-Tabelle mit dem dort vorhandenen Button. Das Fenster 'Routing-Tabelle' öffnet sich.

Die Default Route ist gekennzeichnet durch die IP-Adresse '255.255.255.255' und die Netzmaske '0.0.0.0'. Selektieren Sie diesen Eintrag und wählen Sie **Bearbeiten**. Das Fenster 'Routing-Tabelle - Eintrag bearbeiten' (Bild 9.14) öffnet sich. Im Feld 'Router' können Sie nun den gewünschten Provider auswählen (sofern Sie mit dem Setup-Assistenten mehrere Provider mit unterschiedlichen Namen eingerichtet haben).

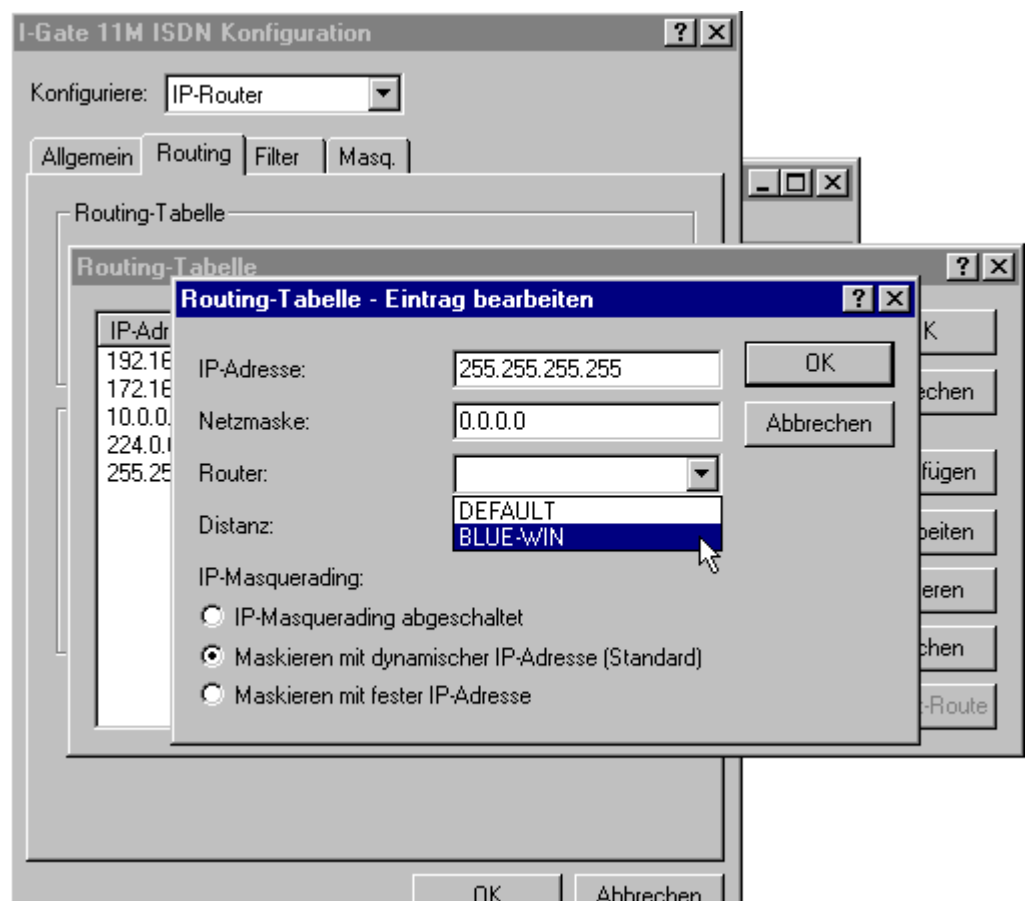


Bild 9.14 Manueller Providerwechsel

Provider löschen

Sollten Sie einmal in die Lage geraten, einen bereits eingerichteten Provider löschen zu wollen, müssen Sie wie folgt vorgehen. Wählen Sie im allgemeinen Konfigurationsdialog (**Bild 9.12**) den Managementbereich **Kommunikation -> Gegenstellen**. Entfernen Sie den gewünschten Providereintrag in der 'Namensliste' und auch im Register 'Protokolle' in der 'PPP-Liste'. Selbstverständlich können Sie mit dem Setup-Assistenten einen bereits eingerichteten Provider jederzeit korrigieren, indem Sie den Provider unter dem selben Namen erneut einrichten.

Telnet Sitzung

Für gewisse spezielle Anwendungen (z.B. Fehlersuche mit trace, Anschauen von Statistikdaten) können Sie unter dem Menü **Extras** eine Telnet Sitzung zu dem gerade selektierten AccessPoint starten. Weiterführende Informationen zu Telnet finden Sie im Referenzhandbuch auf der I-GATE 11M CD-ROM.

9.9 Monitoring mit dem AccessPoint Monitor

Mit dem Siemens AccessPoint Monitor steht Ihnen ein komfortables Monitoringprogramm für die Aktivitäten Ihres AccessPoints zur Verfügung. Auch wenn der AccessPoint nicht direkt sichtbar ist, haben Sie mit dem AccessPoint Monitor jederzeit einen Überblick über den aktuellen Verbindungszustand Ihres AccessPoints.

Am einfachsten starten Sie den AccessPoint Monitor aus dem Siemens AccessPoint Manager heraus mit dem Menü **Extras -> Gerät überwachen**. Wenn Sie ihn direkt starten, müssen Sie beim erstmaligen Start im Menü **Gerät** unter **Neu** die IP-Adresse des AccessPoints eingeben.

Bild 9.15 zeigt Ihnen das AccessPoint Monitor Monitoring Fenster mit der eingeschalteten Anzeigeoption 'System-Informationen' bei einer aktiven PPP-Internetverbindung über 'Line 1'.

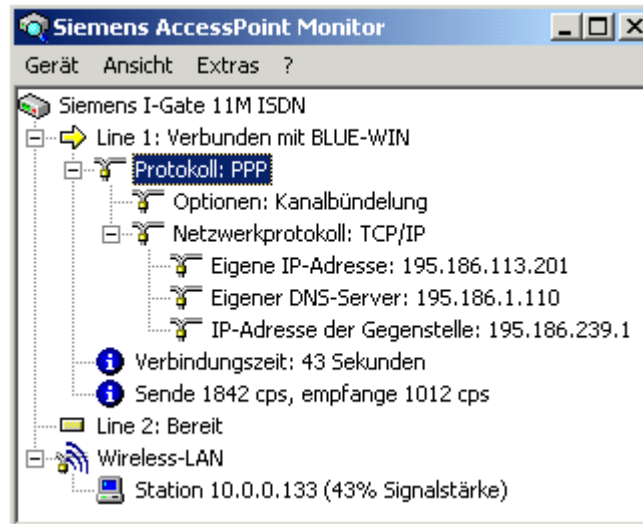


Bild 9.15 Siemens AccessPoint Monitor

Unter 'Line 1' finden Sie z.B. die aktuelle IP-Adresse Ihres AccessPoints, die ihm beim Verbindungsaufbau zum Provider Internet-seitig zugeteilt wurde. Weitere wichtige Informationen sind:

- Dauer der aktuellen Verbindung (Zeile 'Verbindungszeit')
- Gesamtverbindungszeit (Zeile 'Verbindungszeit gesamt')
- Aufgelaufene Gebühreneinheiten (nur bei eingeschaltetem Gebührenimpuls) (Zeile 'Gebühren gesamt')
- Aktuelle Sende- und Empfangsdatenrate (Zeile 'Sende..empfangen') (cps = characters per second = bytes per second)

Verbindung trennen / Fehler rücksetzen

Wenn ein Kanal Ihres ISDN-Anschlusses ('Line 1' oder 'Line 2') verbunden oder mit einer Fehlermeldung versehen ist, können Sie diese selektieren. Mit der rechten Maustaste können Sie nun die Verbindung trennen bzw. die Fehlermeldung löschen.

Kanalanzeige

Wie in [Bild 9.16](#) gezeigt, können Sie im Kontextmenü (rechte Maustaste) des Gerätesymbols (Zeile 'Siemens I-Gate 11M') ein separates Kanalanzeige Fenster öffnen ([Bild 9.17](#)), um den Verbindungszustand des AccessPoints in konzentrierter Form anzuzeigen.

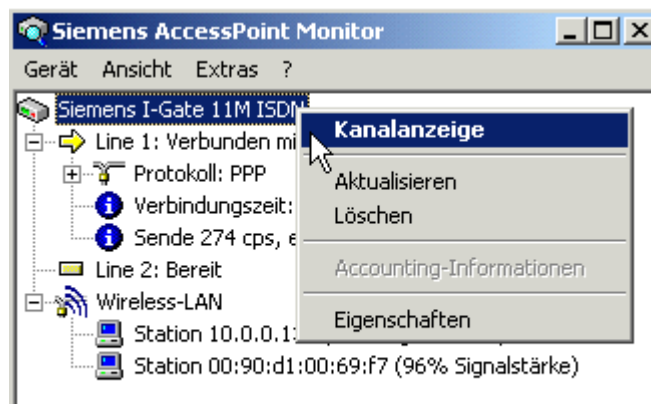


Bild 9.16 Kanalanzeige aktivieren



Bild 9.17 Kanalanzeige

Protokolldateien

Der AccessPoint Monitor bietet Ihnen auch die Möglichkeit, alle Verbindungen des AccessPoints in Dateien zu protokollieren. Wählen Sie hierzu **Gerät -> Eigenschaften -> Protokoll**. Das Fenster 'Optionen' (Bild 9.18) öffnet sich.

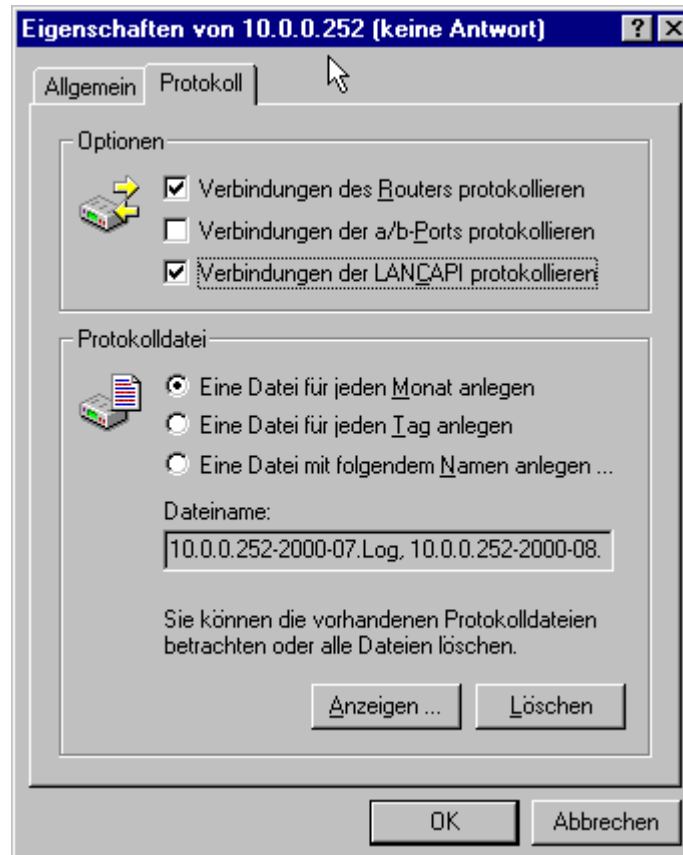


Bild 9.18 Protokolldateien

Hier können Sie nun auswählen, welche Verbindungen in welchen Zeiträumen in welchen Dateien mitprotokolliert werden sollen. (Die Protokolldateien sind reine Textdateien.)

10 Anwendungen mit AccessPoint - Überblick

10.1 Grundlagen

- Netzwerk-Funktionalität** I-GATE 11M erlaubt eine drahtlose Vernetzung von PCs und Notebooks, die mit einem MobilePort bestückt sind. Für das Betriebssystem besteht kein Unterschied zwischen einer konventionellen Ethernet Netzwerkkarte und einem I-GATE 11M MobilePort. Alle mit einem MobilePort ausgerüsteten Geräte bilden ein "wireless" LAN (WLAN). Netzwerk Grundlagen finden Sie im Kapitel Technische Grundlagen des Referenzhandbuchs auf der I-GATE CD.
- Internet-Zugriff** Die AccessPoints I-GATE 11M ISDN und I-GATE 11M I/LAN beinhalten ein ISDN-Router mit integriertem WLAN-Interface (MobilePort). Sie ermöglichen es, WLANs über ISDN als WAN-Verbindung zu koppeln bzw. an das Internet anzubinden. Damit ein WLAN mit mehreren Rechnern über einen einzigen Account bei einem Internet Service Provider an das Internet angebunden werden kann, beherrschen die I-GATE 11M AccessPoints das sogenannte IP-Masquerading. Mit dieser Funktion werden bei der Kommunikation mit dem Internet die im allgemeinen "privaten" IP-Adressen der Rechner innerhalb des WLANs auf die einzige vom Internet Provider zugeteilte "Live" IP-Adresse umgesetzt.
- Peer-to-LAN** Der I-GATE 11M I/LAN AccessPoint hat neben der ISDN-Schnittstelle noch eine Ethernet-Schnittstelle. Wenn Sie diese Schnittstelle über einen Hub oder Switch mit einem bestehenden kabelgebundenen LAN verbinden funktioniert er als Bridge zwischen dem 'wired' und dem 'wireless' LAN.
- DHCP-Server** Die I-GATE 11M AccessPoints beinhalten einen DHCP-Server zur automatischen Konfiguration der TCP/IP-Parameter der Rechner im Netz. Wenn Sie Ihre Rechner mit 'IP-Adresse automatisch beziehen' betreiben entsteht so automatisch ein funktionsfähiges TCP/IP-Netzwerk. Im Auslieferungszustand steht der DHCP-Server Betrieb des AccessPoints auf 'Auto', d.h. nur wenn der AccessPoint einen anderen DHCP-Server im Netz findet schaltet er seinen eigenen ab sonst fungiert er selber als DHCP-Server. Weitere Details hierzu finden Sie in Kapitel [12.10](#).

10.2 Windows "Peer-to-Peer" Netzwerke mit AccessPoint

Kleine Netzwerke können als sogenanntes "Peer-to-Peer" Netzwerk betrieben werden. Alle Microsoft Betriebssysteme (Windows 95/98/NT/2000) bieten diese Möglichkeit. Jeder Rechner im Netz kann Laufwerke, Verzeichnisse und lokal angeschlossene Drucker unter einem frei wählbaren Namen freigeben und so Benutzern auf anderen Rechnern im Netzwerk den Zugriff auf diese Ressourcen ermöglichen.

Mit I-GATE 11M MobilePorts vernetzte Rechner bieten alle Möglichkeiten von Windows "Peer-to-Peer" Netzwerken. Wichtig ist, dass auf allen beteiligten Rechnern die gleiche Arbeitsgruppe eingestellt ist.

Nach der erfolgreichen Installation der MobilePort Treiber auf mehreren Rechnern sind weitere Einstellungen vorzunehmen, um in einem "Peer-to-Peer" Netzwerk Ressourcen gemeinsam zu verwenden. Bei einem erfolgreich eingerichteten Windows "Peer-to-Peer" Netzwerk sind im Fenster 'Netzwerkumgebung' (klicken Sie hierzu zweimal auf dem Desktop das Icon **Netzwerkumgebung**) alle am Netzwerk beteiligten Rechner mit ihrem Namen sichtbar. Durch doppelklicken auf das Rechnersymbol werden die auf diesem Rechner freigegebenen Ressourcen (Laufwerke, Drucker) angezeigt.



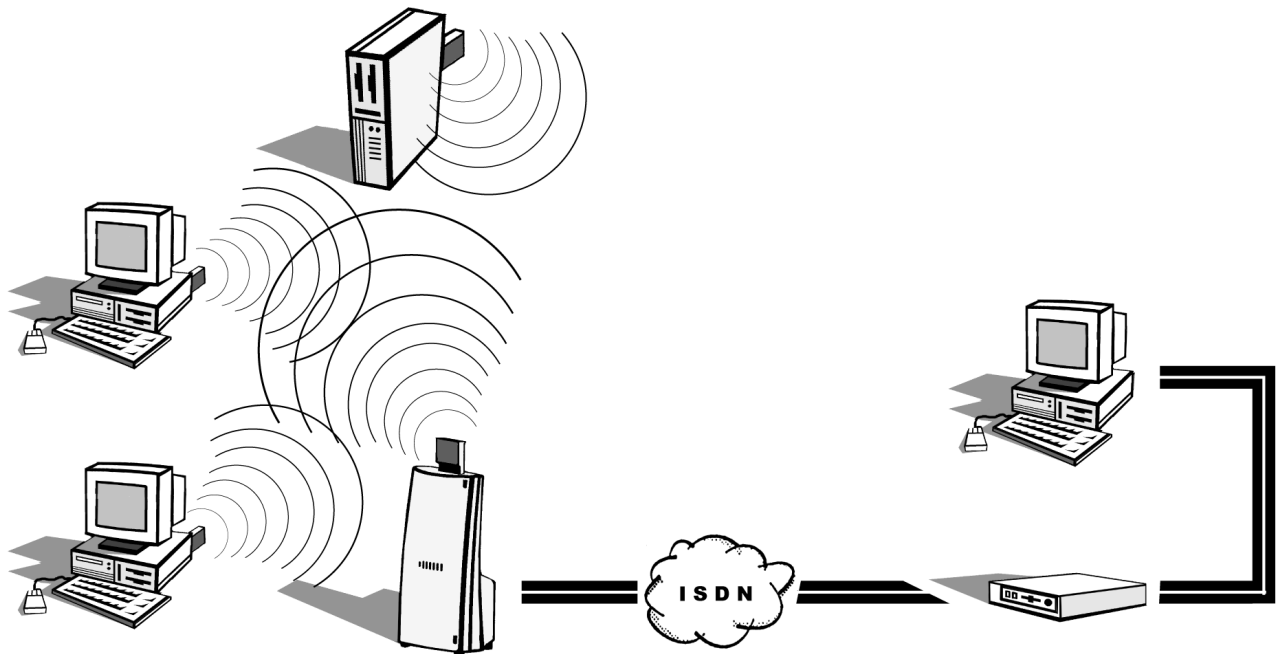
Voraussetzung für das Aufsetzen eines "Peer-to-Peer" Netzes ist ein funktionsfähiges TCP/IP-Protokoll auf den I-GATE 11M MobilePorts. Die Rechner müssen untereinander über IP kommunizieren können. Ein sehr gutes Diagnosetool hierzu ist der `ping` Befehl (siehe Kapitel [13.4](#)).

“Peer-to-Peer” Netzwerk unter Windows 98

Der folgende Ablauf gibt Ihnen einen Überblick, wie Sie die erforderlichen Einstellungen für ein “Peer-to-Peer” Netzwerk unter Windows 98 vornehmen. Die Punkte 1 und 2 erfolgen im Netzwerk-Setup, den Sie über **Start -> Einstellungen -> Systemsteuerung -> Netzwerk** aufrufen.

- 1** Vergewissern Sie sich im Register 'Konfiguration' dass der Dienst 'Client für Microsoft-Netzwerke' installiert ist und aktivieren Sie die **Datei- und Druckerfreigabe**, sofern dieser Rechner Ressourcen bereitstellen soll. (Dies gilt für alle Rechner.)
- 2** Vergewissern Sie sich, dass auf allen Rechnern im Register 'Identifikation' die gleiche **Arbeitsgruppe** eingetragen ist und unter **Computernamen** jeder Rechner einen eindeutigen Namen hat. Die Arbeitsgruppe wird dazu benutzt, um Rechner an einem LAN in verschiedene “Peer-to-Peer” Netze aufzuteilen.
- 3** Geben Sie bereitzustellenden Ressourcen (Verzeichnisse, Drucker) auf den jeweiligen Rechnern frei. Hierzu markieren Sie im 'Arbeitsplatz' oder Explorer die jeweilige Ressource, klicken auf die rechte Maustaste und wählen den Punkt **Freigabe**. Sollte der Punkt 'Freigabe' fehlen, sind die Punkte 1 und 2 nicht richtig eingerichtet.
- 4** Um einen Drucker, der lokal an einem Rechner im Netzwerk angeschlossen und freigegeben ist, von anderen Rechnern aus zu nutzen, müssen Sie auf allen anderen Rechnern einen 'Remote Printer' einrichten. Wählen Sie hierzu im 'Arbeitsplatz' **Drucker -> Neuer Drucker** und folgen Sie den Anweisungen des Windows Drucker-Setup Assistenten.

10.3 Remote Access mit I-GATE 11M

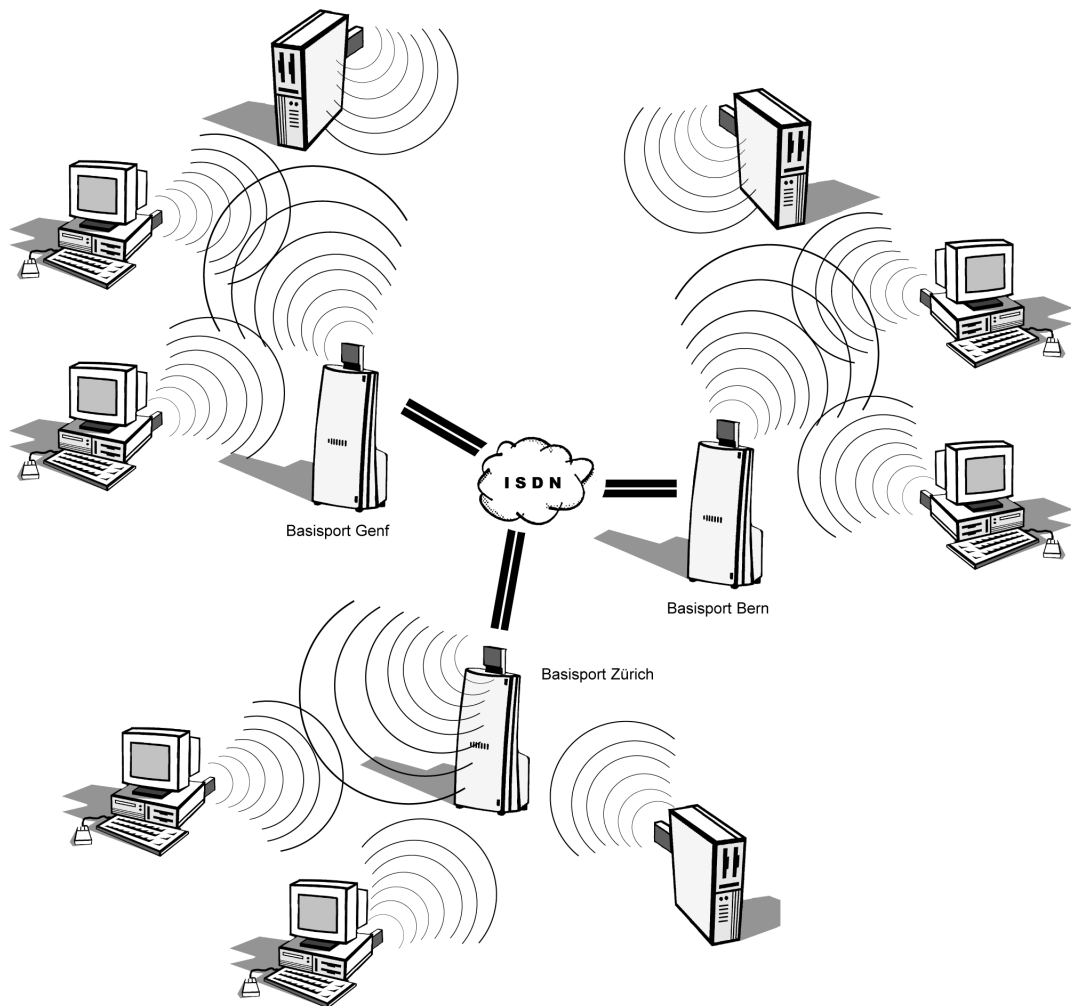


Wenn Sie ein WLAN mit einem I-GATE 11M AccessPoint betreiben, können Sie z.B. einem Aussendienstmitarbeiter oder einem Teleworker Zugriff auf ihr WLAN geben.

Hierzu verwenden Sie das Remote Access Leistungsmerkmal ihres AccessPoints. Konfigurieren Sie auf dem AccessPoint einen PPP Login Account, über den sich nun ein abgesetzter PC mit ISDN-Karte oder ISDN-Modem über das DFÜ-Netzwerk von Windows in ihr Netzwerk einwählen und auf die dort freigegebenen Ressourcen wie Verzeichnisse und Drucker zugreifen kann. Ebenfalls können mit Client-Applikationen auf entsprechende Server-Dienste im Netz zugegriffen werden (z.B. Datenbankserver, E-Mail Postfach, etc.).

Zur Einrichtung eines Remote Access Zuganges finden Sie im AccessPoint Manager unter 'Extras' einen entsprechenden Setup-Assistenten.

10.4 Wireless LAN-LAN-Kopplung mit I-GATE 11M



Neben dem bevorzugten Einsatz als Internet Access Router für ein I-GATE 11M WLAN können Sie die I-GATE 11M AccessPoints auch als normalen ISDN-Router zur LAN-Kopplung einsetzen. Wenn Sie an zwei oder mehr Standorten ein I-GATE 11M WLAN betreiben, können Sie durch entsprechende Konfiguration der an den Standorten vorhandenen I-GATE 11M AccessPoints eine standortübergreifende Rechnerkommunikation ermöglichen.

Jeder Rechner in einem WLAN kann mit jedem Rechner aus einem WLAN an einem anderen Standort mit ISDN-Bandbreite (max. 128 Kbit/s) kommunizieren. Zur Konfiguration der LAN-Kopplung bietet der Siemens AccessPoint Manager unter 'Extras' einen Setup-Assistenten an.

10.5 Die I-GATE 11M AccessPoints als CAPI-Server

Die mit der I-GATE 11M AccessPoint Tools mitgelieferte Siemens CAPI gestattet, die I-GATE 11M AccessPoints wie ein externes ISDN-Modem zu betreiben. Auf allen Rechnern, auf denen Sie die Siemens CAPI installieren, steht eine CAPI konforme Treiberschnittstelle zu Verfügung, die es erlaubt, alle CAPI-basierten ISDN-Applikationsprogramme (z.B. Bürokommunikation) auch über die I-GATE 11M AccessPoints zu betreiben.

Um mit der CAPI auch eingehende Anrufe entgegenzunehmen, müssen Sie mit dem Siemens AccessPoint Manager diese Funktion auf dem AccessPoint explizit freischalten. Weitere Information über die Installation und Konfiguration finden Sie in Kapitel ["12.15.1 Die Siemens CAPI"](#).

11 AccessPoint - Konfigurationsmöglichkeiten

AccessPoints von Siemens werden mit einer aktuellen Software ausgeliefert, in der schon einige Einstellungen für Sie vorbereitet sind.

Trotzdem ist noch eine Ergänzung der Angaben und eine Anpassung an Ihre spezielle Aufgabe nötig. Diese Einstellungen werden während der Konfiguration vorgenommen.

In diesem Kapitel zeigen wir Ihnen, mit welchen Programmen und über welche Wege Sie auf das Gerät zugreifen können, um die Einstellungen vorzunehmen.

Und wenn das Entwickler-Team eine neue Firmware mit neuen Features für Sie fertiggestellt hat, finden Sie unter **www.siemens.ch/i-gate** Hinweise zum Laden der neuen Software.

11.1 Funk oder Kabel: Wege für die Konfiguration

Mit der Inband-Konfiguration (Konfiguration über das Netzwerk) haben Sie von jedem Rechner aus dem WLAN, LAN oder WAN (ISDN) aus Zugriff auf den AccessPoint. Den Zugang können Sie über die IP-Zugangsliste eingeschränken oder ganz sperren.

Um die Inband-Konfiguration des Siemens AccessPoint vorzunehmen, verwenden Sie entweder Telnet (gehört zum Lieferumfang der meisten Betriebssysteme) oder Siemens AccessPoint Manager für Windows. Siemens AccessPoint Manager ist im Lieferumfang Ihres Geräts enthalten. Aktuelle Versionen stehen immer in unseren Online-Medien für Sie bereit.

Voraussetzungen

Die Konfiguration mit Telnet oder Siemens AccessPoint Manager läuft über TCP/IP bzw. TFTP ab. Dazu muß also auf dem verwendeten Rechner das TCP/IP installiert sein, und Ihr AccessPoint benötigt eine IP-Adresse, mit der Sie sie ansprechen können.

Ein noch nicht konfiguriertes Gerät hört auf die IP-Adresse XXX.XXX.XXX.254. Die vielen X stehen dabei für die Netzwerk-Adresse in Ihrem LAN. Haben die Rechner in Ihrem Netz also z.B. Adressen wie 192.168.130.1, dann können Sie Ihr Gerät mit der Adresse 192.168.130.254 erreichen.

Haben Sie bereits einen Rechner mit der Adresse XXX.XXX.XXX.254 in Ihrem Netz stehen, schalten sie zunächst den Rechner mit dieser IP-Adresse aus. Sobald Sie mit Siemens AccessPoint Manager oder Telnet Verbindung zum AccessPoint aufgenommen haben, geben Sie ihr eine andere, freie IP-Adresse.

11.2 Alternativ: Adreßverwaltung mit dem DHCP-Server

Wenn die Konfiguration der korrekten IP-Adressen „von Hand“ keine absolute Notwendigkeit für Sie ist, erledigt der DHCP-Server diese Arbeit auch gerne selbständig für Sie. Bei der Verwendung des DHCP-Servers können Sie die IP-Adressen für alle Rechner im Netz automatisch einstellen lassen (siehe auch Kapitel 'Automatische Adreßzuweisung mit DHCP')

11.2.1 Konfiguration über Siemens AccessPoint Manager

Rufen Sie Siemens AccessPoint Manager z.B. aus der Windows-Startleiste auf mit **Start -> Programme -> Siemens I-Gate -> Siemens AccessPoint Manager**. Siemens AccessPoint Manager sucht nun automatisch im lokalen Netz nach Geräten. Wird dabei ein noch nicht konfiguriertes Gerät im lokalen Netz gefunden, startet Siemens AccessPoint Manager selbständig den Setup-Assistenten.



Um die Suche eines neuen Geräts manuell einzuleiten, klicken Sie auf die Schaltfläche Suchen oder rufen den Befehl über **Gerät -> Suchen** auf. SiemensSiemens AccessPoint Manager erkundigt sich dann, wo es suchen soll. Bei der Inband-Lösung reicht hier die Auswahl des lokalen Netzes, und los geht's.

Sobald Siemens AccessPoint Manager mit der Suche fertig ist, zeigt es in der Liste alle gefundenen Geräte mit Namen, evtl. einer Beschreibung, der IP-Adresse und dem Status an.

Für die Konfiguration der Geräte mit Siemens AccessPoint Manager stehen zwei verschiedene Darstellungsmöglichkeiten zur Auswahl:

- In der 'einfachen Darstellung' werden nur die Einstellungen angezeigt, die für übliche Anwendungsfälle benötigt werden.

- In der 'vollständigen Darstellung' werden alle verfügbaren Einstellungen angezeigt. Einige davon sollten nur von erfahrenen Benutzern verändert werden.



Ein Doppelklick auf den Eintrag für das markierte Gerät, der Klick auf die Schaltfläche Konfigurieren oder den Menüeintrag **Bearbeiten** -> **Konfiguration** bearbeiten liest die aktuellen Einstellungen aus dem Gerät aus und zeigt die allgemeinen Geräteinformationen an.

Die weitere Bedienung des Programms erklärt sich im Prinzip selbst bzw. über die Online-Hilfe. Mit einem Klick auf das Fragezeichen oben rechts in jedem Fenster bzw. mit einem rechten Mausklick auf einen unklaren Begriff können Sie jederzeit die kontextsensitive Hilfe aufrufen.

11.2.2 Konfiguration mit Siemens WEBconfig

Über einen Web-Browser können Sie die Grundeinstellungen des Siemens AccessPoint vornehmen und Assistenten zum Einrichten des Netzwerks oder des Internet-Zugangs starten.

Voraussetzungen

Um eine Verbindung zum Siemens AccessPoint herzustellen, muss eine TCP/IP-Verbindung über das Ethernet-LAN (nur bei I-GATE 11M I/LAN) oder über das WLAN bestehen.

11.2.3 Konfiguration über Telnet

Über Telnet starten Sie die Konfiguration z.B. aus einer DOS-Box mit dem Kommando:

```
telnet 10.1.80.125
```

Telnet baut dann eine Verbindung zum Gerät mit der eingegebenen IP-Adresse auf.

Nach der Eingabe des Paßworts (sofern Sie eines zum Schutz der Konfiguration vereinbart haben) stehen Ihnen alle Befehle aus dem Abschnitt 'Befehle für die Konfiguration' zur Verfügung.

11.3 Der Fernzugang: Konfiguration über DFÜ-Netzwerk

Besonders einfach wird die Einstellung von AccessPoints an entfernten Standorten mit der Fernkonfiguration über das DFÜ-Netzwerk. Das Gerät ist nach dem Einschalten und der Verbindung mit dem WAN-Anschluß ohne eine einzige Einstellung sofort vom Administrator zu erreichen. Damit sparen Sie beim Anschluß von anderen Netzwerken an Ihr eigenes LAN viel Zeit und Geld für die Reise zum anderen Netzwerk oder für die Einweisung der Mitarbeiter vor Ort in die Konfiguration der AccessPoint.

Außerdem können Sie eine spezielle Rufnummer für die Fernkonfiguration reservieren. Damit kann ein Service-Techniker immer auf den AccessPoint zugreifen, auch wenn das Gerät durch fehlerhafte Einstellungen eigentlich nicht mehr ansprechbar ist.

11.3.1 Das brauchen Sie für die Fernkonfiguration

- einen Rechner mit PPP-Client, z.B. Windows DFÜ-Netzwerk
- ein Programm für die Inband-Konfiguration, z.B. Siemens AccessPoint Manager oder Telnet

11.3.2 So bereiten Sie die Fernkonfiguration vor

1. Versorgen Sie den AccessPoint mit der nötigen Spannung.
2. Verbinden Sie das Gerät mit einem WAN-Anschluß.

11.3.3 Die erste Fernverbindung mit DFÜ-Netzwerk (Siemens AccessPoint Manager)

1. Wählen Sie im Siemens AccessPoint Manager Gerät -> Neu, aktivieren Sie die 'DFÜ-Verbindung' als Anschlußtyp und geben Sie die Rufnummer des WAN-Anschlusses ein, an dem der AccessPoint angeschlossen ist. Stellen Sie dazu ggf. die Zeit ein, nach der eine Verbindung ohne Datentransfer automatisch getrennt werden soll
2. Siemens AccessPoint Manager legt nun automatisch einen neuen Eintrag im DFÜ-Netzwerk an. Wählen Sie ein PPP-fähiges Gerät (z.B. einen NDIS-WAN-Treiber - nicht im Lieferumfang) für die Verbindung aus, und bestätigen Sie mit **OK**.

3. Anschließend zeigt Siemens AccessPoint Manager in der Geräteliste ein neues Gerät mit dem Namen 'Unbekannt' und der Rufnummer über DFÜ als Adresse an



Mit dem Eintrag in der Geräteliste wird die Verbindung im DFÜ-Netzwerk gelöscht.

4. Sie können das Gerät über die Fernverbindung nun genauso einstellen wie alle anderen Geräte. Zum Auslesen der Konfiguration baut Siemens AccessPoint Manager eine Verbindung über das DFÜ-Netzwerk auf.

11.3.4 Die erste Fernverbindung mit PPP-Client und Telnet

1. Stellen Sie mit Ihrem PPP-Client eine Verbindung zum AccessPoint her, verwenden Sie dabei folgende Angaben:
 - Benutzername 'ADMIN'
 - Paßwort wie beim AccessPoint eingestellt, im Auslieferungszustand kein Paßwort
 - eine IP-Adresse für die Verbindung, nur wenn erforderlich
2. Starten Sie eine Telnet-Verbindung zum AccessPoint. Verwenden Sie dazu die folgende IP-Adresse:
 - '172.17.17.18', wenn Sie keine IP-Adresse für den PPP-Client festgelegt haben. Diese Adresse verwendet der AccessPoint automatisch, falls nichts anderes vereinbart ist. Der anrufende PC reagiert dann auf die IP '172.17.17.17'.
 - Erhöhen Sie die IP-Adresse des PCs um eins, wenn Sie eine Adresse festgelegt haben. Beispiel: Sie haben für den PPP-Client die IP '10.0.200.123' festgelegt, dann hört der AccessPoint auf die '10.0.200.124'. Ausnahme: Bei einer '254' am Ende der IP reagiert der AccessPoint auf die 'x.x.x.1'.
3. Sie können den AccessPoint über die Fernverbindung nun genauso einstellen wie alle anderen Geräte.

11.3.5 Fernkonfiguration einschränken

Die PPP-Verbindung von einer beliebigen Gegenstelle zum AccessPoint gelingt natürlich nur dann, wenn das Gerät jeden Ruf mit den entsprechenden Einstellungen für den PPP-Betrieb annimmt. Im Auslieferungszustand geht das auch, da das Standard-Protokoll (Default-Layer) auf PPP eingestellt ist.

Aber vielleicht möchten Sie ja nach der ersten Konfiguration den Default-Layer z.B. für LAN-LAN-Verbindungen auf ein anderes Protokoll einstellen. Dann nimmt das Gerät die Rufe über die DFÜ-Verbindung nicht mehr mit den PPP-Einstellungen an. Abhilfe schafft hier die Vereinbarung einer speziellen Rufnummer für den Konfigurationszugriff. Empfängt das Gerät einen Ruf auf dieser Nummer, wird immer die Einstellung für PPP verwendet, unabhängig von der weiteren Konfiguration des AccessPoints. Dabei wird nur ein spezieller Benutzername während der PPP-Verhandlung akzeptiert, der beim Verbindungsaufbau über Siemens AccessPoint Manager automatisch eingetragen wird.

1. Wechseln Sie im Konfigurationsbereich 'Management' auf die Registerkarte 'Security'.
2. Wählen Sie im Feld 'Konfigurationszugriff' aus, ob die Einstellung aus entfernten Netzen vollständig, nur zum Lesen oder nicht erlaubt ist.
Geben Sie bei einer Telnet- oder Terminalverbindung alternativ den folgenden Befehl ein:

```
set /setup/config-modul/wan-config
[ein][read][aus]
```



Wenn Sie den Zugriff auf den AccessPoint über das WAN ganz sperren wollen, stellen Sie den Konfigurationszugriff von entfernten Netzen auf 'nicht erlaubt'.

3. Geben Sie als Rufnummer im Bereich 'Konfigurationszugriff' eine Rufnummer Ihres Anschlusses ein, die nicht für andere Zwecke verwendet wird.
Geben Sie alternativ den folgenden Befehl ein:

```
set /setup/config-modul/Fernconfig 123456
```

4. Schützen Sie die Einstellungen des Geräts ggf. zusätzlich durch die Vergabe eines Paßworts.
Geben Sie bei einer Telnet- oder Terminalverbindung alternativ den folgenden Befehl ein:

```
passwd
```

Damit werden Sie zur Eingabe eines neuen Paßworts mit Bestätigung aufgefordert.

11.4 Neue Firmware mit FirmSafe

Die Software für die Geräte von Siemens wird ständig weiterentwickelt. Damit Sie auch in den Genuß von neuen Features und Funktionen kommen, haben wir die Geräte mit einem Flash-ROM-Speicher ausgerüstet, der das nachträgliche Ändern der Betriebssoftware zum Kinderspiel macht. Kein EPROM tauschen, kein Gehäuse öffnen: Einfach die neue Version einspielen und fertig!

11.4.1 So funktioniert FirmSafe

FirmSafe macht das Einspielen der neuen Software zur sicheren Sache: Die gerade verwendete Firmware wird dabei nicht einfach überschrieben, sondern es wird eine zweite Firmware zusätzlich im Gerät gespeichert.

Von den beiden im Gerät gespeicherten Firmware-Versionen kann immer nur eine aktiv sein. Beim Laden einer neuen Firmware wird die nicht aktive Firmware überschrieben. Sie können selbst entscheiden, welche Firmware nach dem Upload aktiviert werden soll:

- 'Unmittelbar': Als erste Möglichkeit können Sie die neue Firmware laden und sofort aktivieren. Folgende Situationen können dann entstehen:
 - Die neue Firmware wird erfolgreich geladen und arbeitet anschließend wie gewünscht. Dann ist alles in Ordnung.
 - Das Gerät ist nach dem Ladevorgang der neuen Firmware nicht mehr ansprechbar. Falls schon während des Uploads ein Fehler auftritt, aktiviert das Gerät automatisch wieder die bisherige Firmware und startet damit neu.
- 'Login': Um den Problemen eines fehlerhaften Uploads zu begegnen, gibt es die zweite Möglichkeit, bei der die Firmware geladen und ebenfalls sofort gestartet wird.
 - Im Unterschied zur ersten Variante wartet das Gerät anschließend fünf Minuten lang auf einen erfolgreichen Login. Nur wenn dieser Login erfolgt, wird die neue Firmware auch dauerhaft aktiviert.
 - Wenn das Gerät nicht mehr ansprechbar ist und ein Login somit unmöglich ist, aktiviert es automatisch wieder die bisherige Firmware und startet damit neu.
- 'Manuell': Bei der dritten Möglichkeit können Sie vorher selbst eine Zeit bestimmen, in der Sie die neue Firmware testen wollen. Das Gerät startet mit der neuen Firmware und wartet in der

eingestellten Zeit darauf, daß die geladene Firmware von Hand aktiviert und damit dauerhaft wirksam gemacht wird.

11.4.2 So spielen Sie eine neue Firmware ein

Beim Firmware-Upload (so heißt das Einspielen der Software) gibt es verschiedene Wege zum Ziel:

- Siemens AccessPoint Manager (empfohlen)
- Terminal-Programme
- TFTP



Beim Firmware-Upload bleiben alle Einstellungen erhalten! Trotzdem sollten Sie sicherheitshalber die Konfiguration vorher speichern (bei Siemens AccessPoint Manager z.B. mit **Bearbeiten** -> **Konfiguration** sichern).

Enthält die neu eingespielte Version Parameter, die in der aktuellen Firmware des Gerätes nicht vorhanden sind, werden die fehlenden Werte mit den Default-Einstellungen ergänzt.

Siemens AccessPoint Manager



Beim Siemens AccessPoint Manager markieren Sie das gewünschte Gerät in der Auswahlliste und klicken auf **Bearbeiten** -> **Firmware-Verwaltung** -> **Neue Firmware** hochladen oder direkt auf die Schaltfläche **Firmware-Upload**. Dann wählen Sie das Verzeichnis, in dem sich die neue Version befindet, und markieren die entsprechende Datei.

Siemens AccessPoint Manager informiert Sie dann in der Beschreibung über Versions-Nr. und Datum der Firmware und bietet den Upload an. Mit **Öffnen** ersetzen Sie die vorhandene Firmware durch die ausgewählte Version.

Wählen Sie außerdem aus, ob die Firmware sofort nach dem Laden dauerhaft aktiviert werden soll, oder stellen Sie eine Testzeit ein, in der Sie die Firmware selbst freischalten. Um anschließend die Firmware während der eingestellten Testzeit zu aktivieren, klicken Sie auf **Bearbeiten** -> **Firmware-Verwaltung** -> **Firmware im Test freischalten**.

TFTP

Über TFTP kann eine neue Firmware mit dem Befehl **writelflash** eingespielt werden. Um eine neue Firmware in ein Gerät mit der IP-

Adresse 194.162.200.17 zu übertragen, geben Sie z.B. unter Windows NT folgenden Befehl ein:

```
tftp -i 194.162.200.17 put lc_1000u.130 writeflash
```



Durch diesen Befehl wird die entsprechende Datei mit dem Kommando **writeflash** an die angegebene IP-Adresse gesendet. Dabei muß für TFTP die binäre Dateiübertragung eingestellt werden. Auf vielen Systemen ist jedoch das ASCII-Format voreingestellt. In diesem Beispiel für Windows NT erreichen Sie das durch den Parameter '-i'.

Nach einem erfolgreichen Firmware-Upload bootet das Gerät und aktiviert so direkt die neue Firmware. Tritt während des Uploads ein Fehler auf (Schreibfehler im Flash-ROM, TFTP-Übertragungsfehler o.ä.), aktiviert FirmSafe die vorherige Firmware. Die Konfiguration bleibt dabei erhalten.

Mit TFTP können auch andere Konfigurations-Befehle ausgeführt werden. Die Syntax ist am einfachsten den folgenden Beispielen zu entnehmen:

- `tftp 10.0.0.1 get readconfig file1`: Liest die Konfiguration aus dem Gerät mit der Adresse 10.0.0.1 und speichert diese unter file1 im aktuellen Verzeichnis ab.
- `tftp 10.0.0.1 put file1 writeconfig`: schreibt die Konfiguration aus file1 in das Gerät mit der Adresse 10.0.0.1.
- `tftp 10.0.0.1 get dir/status/verb file2`: Speichert die aktuellen Verbindungsinformationen in file2.

11.5 Was ist los auf der Leitung?

Nach der Grundkonfiguration der Geräte erhält man weitere wichtige Hinweise über die noch zu ändernden Parameter vor allem durch die Beobachtung des Datenverkehrs auf den verschiedenen Schnittstellen der AccessPoint.

Neben den Statistiken des Geräts, die Sie zum Beispiel in einer Telnet- oder Terminalsitzung auslesen können, stehen Ihnen dazu noch weitere Möglichkeiten zur Verfügung.

11.5.1 Siemens AccessPoint Monitor

Mit dem Überwachungstool Siemens AccessPoint Monitor können Sie sich unter Windows-Betriebssystemen die wichtigsten Informationen über den Status Ihres AccessPoints immer auf dem Bild-

schirm anzeigen lassen. Viele der internen Meldungen des Gerätes werden dabei in Klartext umgewandelt, zeigen Ihnen den aktuellen Zustand des Gerätes und helfen Ihnen so bei der Fehlersuche.

Siemens AccessPoint Monitor installieren

Siemens AccessPoint Monitor wird in der Regel automatisch mit Siemens AccessPoint Manager installiert, und zwar auf dem Rechner, von dem aus Sie Ihren AccessPoint einstellen möchten.

Falls Siemens AccessPoint Monitor noch nicht auf Ihrem Rechner installiert ist, legen Sie die Siemens I-GATE 11M-CD ein. Wenn das Setup-Programm beim Einlegen der CD nicht automatisch startet, klicken Sie im Explorer von Windows einfach auf die 'autorun.exe' auf der Siemens I-GATE 11M-CD und folgen den weiteren Hinweisen der Installationsroutine.

Aktivieren Sie bei der Installation die Option für 'AccessPoint Monitor'.

Sie können mit Siemens AccessPoint Monitor nur solche Geräte überwachen, die Sie Inband über das lokale Netzwerk erreichen. Dazu muß auf Ihrem Rechner das Netzwerkprotokoll TCP/IP installiert sein. Über die serielle Schnittstelle angeschlossene AccessPoints können Sie mit diesem Programm nicht ansprechen.

11.6 Konfiguration über SNMP

Das Simple Network Management Protocol (SNMP V.1 nach RFC 1157) ermöglicht die Überwachung und Konfiguration von Geräten in einem Netz von einer zentralen Instanz aus.

Detaillierte Informationen über die Konfiguration von Siemens-Geräten mit SNMP finden Sie im Referenzhandbuch auf der CD.

11.7 Siemens I-GATE 11M I/LAN AccessPoint DSL-Firmware

Mit der xDSL-Firmware des I-GATE 11M I/LAN AccessPoint können Sie diesen für einen Breitband Internet-Zugang über xDSL einsetzen.



Beachten Sie, dass nach dem Hochladen der Firmware keine Netzanbindung über Ethernet mehr zur Verfügung steht. Sie sollten sicherheitshalber die Verbindung zum AccessPoint über das WLAN aufbauen. Die Funkverbindung zum AccessPoint besteht auch nach dem Firmware-Upgrade.

Vorgehensweise

1. Trennen Sie den AccessPoint vom Netzwerk, und stellen Sie eine Verbindung über die Funk-Netzwerkkarte her (WLAN-Verbindung).
2. Legen Sie die beiliegende CD in den Rechner ein, der mit dem AccessPoint über WLAN verbunden ist ein.
3. Starten Sie Siemens AccessPoint Manager, und wählen Sie **Bearbeiten -> Firmware-Verwaltung -> Neue Firmware hochladen**

Öffnen Sie auf der CD das Firmware-Verzeichnis, und markieren Sie die Datei:

`ILDSL2xx.upx`

Die zwei 'x' entsprechen den Firmware Stand. Nach dem Kopiervorgang der Firmware können Sie die DSL-Verbindung einrichten.



Wenn Sie den Vorgang wieder rückgängig machen wollen und Ihr AccessPoint für den LAN-Betrieb innerhalb eines Ethernet-Netzwerkes einsetzen möchten, gehen Sie genauso wie oben vor, jedoch mit der LAN Firmware Datei `IL2xx.upx`.

Mehr über das Hochladen von Firmware erfahren Sie in Kapitel ["11.4 Neue Firmware mit FirmSafe"](#).

12 AccessPoint - Funktionen und Betriebsarten

Dieses Kapitel stellt Ihnen die Funktionen und Betriebsarten Ihres Gerätes vor. Dabei finden Sie u.a. Informationen zu den folgenden Punkten:

- Funk-Verbindungen
- Sicherheit für die Konfiguration
- Sicherheit für das LAN
- Gebührenmanagement
- ISDN-Verbindungen
- PPP-Unterstützung
- IPX-Routing
- IP-Routing
- Automatische Adreßverwaltung mit DHCP
- DHCP-Server
- DHCP-Relay-Agent
- DNS-Server
- NetBIOS-Proxy
- Least-Cost-Router
- Siemens CAPI
- Zeitkontrolle

Neben der Beschreibung der einzelnen Punkte geben wir Ihnen hier auch Hinweise, die Sie bei der Konfiguration unterstützen.

Eine detaillierte Beschreibung aller Parameter und Menüs finden Sie im Referenzhandbuch.

12.1 Sicherheit für Ihre Konfiguration

Mit der Konfiguration des Gerätes legen Sie eine Reihe von wichtigen Parametern für den Datenaustausch fest: Die Sicherheit des eigenen Netzes, die Kontrolle der Kosten und die Berechtigung einzelner Netzteilnehmer gehören z.B. dazu.

Die von Ihnen einmal eingestellten Parameter sollen natürlich nicht durch Unbefugte verändert werden. Daher bietet ein Siemens I-GATE 11M AccessPoint die Möglichkeit, die Konfiguration mit verschiedenen Mitteln zu schützen.

12.1.1 **Paßwortschutz**

Die einfachste Möglichkeit zum Schutz der Konfiguration ist die Vereinbarung eines Paßworts. Solange Sie kein Paßwort vereinbart haben, kann jeder die Konfiguration des Gerätes verändern.

Das Feld zur Eingabe des Paßworts finden Sie in Siemens AccessPoint Manager im Konfigurationsbereich 'Management' auf der Registerkarte 'Security'. Bei einer Terminal- oder Telnetsitzung schalten Sie die Paßwortabfrage im Menü /Setup/Config-Modul/Passw.Zwang ein. Das Paßwort selbst wird in diesem Fall mit dem Befehl passwd gesetzt.

12.1.2 **Die Login-Sperre**

Die Konfiguration im Siemens I-GATE 11M AccessPoint ist durch eine Login-Sperre gegen „Brute-Force-Angriffe“ geschützt. Bei einem Brute-Force-Angriff versucht ein unberechtigter Benutzer ein Paßwort zu „knacken“ und so Zugang zu einem Netzwerk, einem Rechner oder einem anderen Gerät zu erlangen. Dazu spielt z.B. ein Rechner automatisch alle möglichen Kombinationen aus Buchstaben und Zahlen durch, bis das richtige Paßwort gefunden wurde.

Zum Schutz gegen solche Versuche kann die maximal zulässige Anzahl von fehlerhaften Login-Versuchen eingegeben werden. Wird dieser Grenze erreicht, wird der Zugang für eine bestimmte Zeit gesperrt.

Diese Parameter gelten global für alle Konfigurationsmöglichkeiten (Telnet, TFTP/Siemens AccessPoint Manager und SNMP). Tritt auf einem Zugang die Sperre in Kraft, so sind auch alle anderen Zugänge automatisch gesperrt.

Zur Konfiguration der Login-Sperre stehen in Siemens AccessPoint Manager im Konfigurationsbereich 'Management' auf der Registerkarte 'Security' bzw. im Menü /Setup/Config-Modul die folgenden Einträge zur Verfügung:

- 'Sperre aktivieren nach' (Login-Fehler)
- 'Dauer der Sperre' (Sperr-Minuten)

12.1.3 Zugangskontrolle über TCP/IP

Mit einer speziellen Filterliste kann der Zugriff auf die internen Funktionen der Geräte über TCP/IP eingeschränkt werden. Mit den internen Funktionen werden hierbei Konfiguration-Sitzungen über Telnet oder TFTP (Siemens AccessPoint Manager) bezeichnet.

Standardmäßig enthält diese Tabelle keine Einträge, damit kann also von Rechnern mit beliebigen IP-Adressen aus über TCP/IP mit Telnet oder TFTP ein Zugriff auf den über xDSL gestartet werden. Mit dem ersten Eintrag einer IP-Adresse sowie der zugehörigen Netzmaske wird der Filter aktiviert, und nur noch die in diesem Eintrag enthaltenen IP-Adressen werden berechtigt, die internen Funktionen zu nutzen. Mit weiteren Einträgen kann der Kreis der Berechtigten erweitert werden. Die Filter-Einträge können sowohl einzelne Rechner als auch ganze Netze bezeichnen.

Die Zugangsliste finden Sie in Siemens AccessPoint Manager im Konfigurationsbereich 'TCP/IP' auf der Registerkarte 'Allgemein' bzw. im Menü /Setup/TCP-IP-Modul/Zugangsliste.

12.2 Sicherheit für Ihr LAN

Sie mögen es sicher nicht, wenn jeder Außenstehende einfach die Daten auf Ihren Rechnern einsehen oder verändern kann. Ein Siemens I-GATE 11M AccessPoint bietet verschiedene Möglichkeiten, den Zugriff von außen einzuschränken:

- Verschlüsselung des Datenstroms
- Zugangsschutz mit Name, Paßwort und Rufnummer
- Rückruf an festgelegte Rufnummern
- Filterung von Datenpaketen
- IP-Masquerading (auch NAT/PAT genannt)

12.3 Die Kontrolle

Welcher „Identifizier“ zur Erkennung des Anrufers verwendet werden soll, wird im Konfigurationsbereich 'Kommunikation' auf der Registerkarte 'Rufannahme' bzw. im Menü /Setup/WAN-Modul/Schutz eingestellt. Zur Auswahl stehen die folgenden Möglichkeiten:

- alle: Anrufe aller Gegenstellen werden angenommen.
- Name: Es werden nur Anrufe von solchen Gegenstellen angenommen, die in der Namenliste eingetragen sind.

- Nummer: Es werden nur Anrufe von solchen Gegenstellen angenommen, die in der Nummernliste eingetragen sind.
- Name oder Nummer: Es werden nur Anrufe von solchen Gegenstellen angenommen, die in der Nummernliste oder in der Namenliste eingetragen sind.

Die Identifizierung setzt natürlich voraus, daß die entsprechende Information vom Anrufer auch übermittelt wird.

Überprüfung des Namens

Bei Verbindungen über PPP kann auch der Name der Gegenstelle übertragen werden.

Dazu muß allerdings zunächst eine Verbindung aufgebaut werden, weil der Name nicht über den D-Kanal ausgetauscht werden kann.

Die Reaktion des Routers ist klar: Wenn ein Schutz über den Namen vereinbart ist, werden nur Anrufe mit bekannten Namen angenommen, die anderen abgelehnt.

Beim PPP-Protokoll wird überprüft, ob der Name der Gegenstelle in der PPP-Liste als Benutzername vorhanden ist. Fehlt der Benutzername, wird der Gerätenamenname als Name der Gegenstelle angenommen und geprüft. Die PPP-Liste finden Sie in Siemens AccessPoint Manager im Konfigurationsbereich 'Kommunikation' auf der Registerkarte 'Protokolle' bzw. im Menü /Setup/WAN-Modul/PPP-Liste.

Kein Paßwort? Doch, diese besondere Möglichkeit gibt es beim PPP: Hier kann zusätzlich ein speziell für dieses Protokoll gültiger Schutz nach PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol) oder MS-CHAP (Microsoft-Variante des CHAP) verlangt werden. Dabei handelt es sich um den Schutz, den das eigene Gerät von der Gegenstelle verlangt.



Die Sicherungsverfahren PAP, CHAP oder MS-CHAP wenden Sie natürlich nicht an, wenn Sie selber mit dem I-GATE 11M AccessPoint z.B. einen Internet-Service-Provider anwählen. Sie werden den ISP wahrscheinlich nicht dazu bewegen können, eine Anfrage an ihn nach einem Paßwort zu beantworten ...

Und woher kommen Name und Paßwort des Anrufers?

Bei PPP werden Name und Paßwort beim Verbindungsaufbau mit der Gegenstelle eingegeben, z.B. im entsprechenden Fenster einer Verbindung im DFÜ-Netzwerk. Wenn der Router selbst eine Verbin-

ung aufbaut, werden Geräte-Name, Paßwort und Benutzername aus der PPP-Liste verwendet.

Überprüfung der Nummer

Wenn die Rufnummer in der Nummernliste vorhanden ist, kann der Zugang zum eigenen Netz gewährt werden, oder der Anrufer wird bei eingeschalteter Rückrufoption zurückgerufen. Ist ein Schutz im I-GATE 11M AccessPoint über die Nummer vereinbart, werden alle Anrufe von Gegenstellen mit unbekanntem Rufnummern abgelehnt.

12.3.1 Der Rückruf

Eine besondere Variante des Zugriffsschutzes wird mit der Rückruffunktion erreicht: Dazu wird in der Namenliste für den gewünschten Anrufer die Option 'Rückruf' aktiviert und ggf. die Rufnummer angegeben.

Mit den Einstellungen in Namen- und Nummernliste und der Auswahl des Protokolls können Sie das Rückrufverhalten Ihres Routers steuern:

- Der Router kann den Rückruf ablehnen.
- Es kann eine voreingestellte Rufnummer zurückrufen.
- Die Rufnummer für den Rückruf kann vom Anrufer frei eingegeben werden.

Und ganz nebenbei steuern Sie über die Einstellungen die Verteilung der Kosten für die Verbindung. Ist in der Namenliste ein Rückruf 'Nach Name' vereinbart, übernimmt der rückrufende Router alle Gebühren bis auf eine, die für die Namensübermittlung benötigt wird. Ebenfalls eine Einheit fällt für den Router an, wenn der Anrufer nicht über CLIP identifiziert wird. Ist dagegen eine Identifizierung über die Rufnummer des Anrufers erlaubt und möglich, kommt der Anrufer sogar ganz ohne Kosten weg.

Wenn der Router selbst zurückrufen soll, dann kann für viele Gegenstellen auch das Fast-Call-Back-Verfahren (zum Patent angemeldet) verwendet werden. Dies beschleunigt die Rückrufprozedur um ein beträchtliches.

12.3.2 Das Versteck – IP-Masquerading (NAT, PAT)

Aber da gibt es Einwände der Netzwerkbetreuer, die sich um die Sicherheit der Daten im firmeneigenen Netz sorgen: Jeder Arbeitsplatzrechner im WWW? Da kann doch dann auch jeder von außen dran! – Kann er nicht!

IP-Masquerading heißt das Versteck für alle Rechner im Internet. Dabei wird nur das Routermodul des Geräts mit seiner IP-Adresse im Internet bekannt gemacht. Die Rechner im LAN nutzen den Router dann als Gateway und können selbst nicht erkannt werden. Der Router trennt dabei Internet und Intranet wie eine Wand. IP-Masquerading wird daher auch als „Firewall-Technik“ bezeichnet.

Weitere Informationen finden Sie im Abschnitt 'IP-Routing: IP-Masquerading'.

12.3.3 WEP - Sicherheit für Ihr WLAN

Die 11-Mbit-Funk-Netzwerkkarten (MobilePorts) unterstützen eine Datenverschlüsselung nach dem WEP-Verfahren (Wired Equivalent Privacy).

Mit WEP haben Sie die Möglichkeit vier unterschiedliche Schlüssel zu definieren, nach denen

- die über die MobilePorts empfangenen Daten entschlüsselt und
- die über die MobilePorts gesendeten Daten verschlüsselt werden.



Das WEP-Verfahren funktioniert nur innerhalb eines WLANs, das über die 11-Mbit MobilePorts kommuniziert. Wenn Sie andere Karten verwenden, sollten Sie diese Sicherheitsoption nicht aktivieren.



Um eine verschlüsselte Datenkommunikation zu ermöglichen, müssen für alle MobilePort Rechner und AccessPoints der gleiche Schlüssel verwendet werden. Notieren Sie sich die vergebenen Schlüssel, und bewahren Sie diese an einem sicheren Ort auf.

Mehr über WEP erfahren Sie in Kapitel ["6.1.2.2 MobilePort WEP Verschlüsselung"](#) und ["9.7 AccessPoint WEP Verschlüsselung"](#).

12.4 Gebührenmanagement

Die Eigenschaft des Routers, Verbindungen selbständig zu allen gewünschten Gegenstellen aufzubauen und sie mit dem Ende der Übertragung wieder zu beenden, ermöglicht dem Benutzer sehr komfortablen Zugriff z.B. auf das Internet. Bei der Datenübertragung über kostenpflichtige Leitungen können jedoch durch Fehlkonfiguration des Routers (z.B. bei der Filterkonfiguration) oder durch übermäßigen Gebrauch des Angebots (z.B. andauerndes Surfen im Internet) recht hohe Kosten entstehen.

12.4.1 Einstellungen im Gebührenmodul

Sie finden die Interface-Einstellungen in Siemens AccessPoint Manager im Konfigurationsbereich 'Management' auf der Registerkarte 'Gebühren' oder bei Telnet- oder Terminalsitzungen unter /Setup/Gebuehren-Modul.



Die Informationen über die Gebühren und Verbindungszeiten werden über einen Bootvorgang hinaus gesichert (z.B. beim Einspielen einer neuen Firmware) und gehen erst verloren, wenn das Gerät ausgeschaltet wird. Alle hier erwähnten Zeitangaben werden in Minuten gemacht.

12.5 ISDN-Verbindungen

Die Datenkommunikation zwischen zwei ISDN-Endgeräten läuft über ISDN-Verbindungen ab. Bei diesen Verbindungen kann es sich prinzipiell um Wählverbindungen oder Festverbindungen handeln.

Die Routermodule ermitteln zunächst nur, zu welcher Gegenstelle ein Datenpaket übertragen werden soll. Damit die entsprechende Verbindung ausgewählt und ggf. aufgebaut werden kann, müssen verschiedene Parameter für alle notwendigen ISDN-Verbindungen vereinbart werden. Diese Parameter sind in unterschiedlichen Listen abgelegt, deren Zusammenspiel die richtigen Verbindungen erlaubt.

Wir wollen diesen Ablauf an einem vereinfachten Beispiel verdeutlichen.

Ein Datenpaket aus einem Rechner findet den Weg ins Internet in erster Linie über die IP-Adresse des Empfängers. Mit dieser Adres-

se schickt der Rechner das Paket los über das LAN zum Router. Der Router schaut mit der IP-Adresse zunächst in der IP-Routing-Tabelle nach und findet die Gegenstelle, die zu dieser Adresse gehört, z.B. 'Provider_A'. Mit diesem Namen prüft der Router dann die ISDN-Namenliste und findet die Rufnummer der zugehörigen Gegenstelle, die über ISDN erreicht werden kann, inkl. des Kommunikations-Layers, der verwendet werden soll. Außerdem erhält der Router aus der PPP-Liste Benutzernamen und Paßwort, die für die Anmeldung beim Provider A notwendig sind.

Der Router kann dann eine Verbindung auf der ISDN-Leitung zum Router des Providers aufbauen. Sobald die Verbindung hergestellt ist, kann der Router das Datenpaket über die ISDN-Leitung ins Internet weitergeben.



Weitere Informationen zu IP-Netzwerken etc. finden Sie in den technischen Grundlagen im Referenzhandbuch auf der CD.

Die folgenden Abschnitte stellen Ihnen die ISDN-Namenliste und die darin enthaltenen Parameter kurz vor, zeigen den Zusammenhang zu anderen Listen und Parametern und wie sie in der Software konfiguriert werden.

Informationen zur IP-Routing-Tabelle finden Sie im Abschnitt 'IP-Routing'.

12.5.1 ISDN-Namenliste

Sie finden die Namenliste in Siemens AccessPoint Manager im Konfigurationsbereich 'Kommunikation' auf der Registerkarte 'Gegenstellen' oder bei Telnet- oder Terminalsitzungen unter /Setup/WAN-Modul/ISDN-Namenliste.

Um die verfügbaren Gegenstellen zu definieren, werden sie in der Namenliste mit einem geeigneten Namen und zusätzlichen Parametern angelegt:

- Name
Mit diesem Namen wird die Gegenstelle in den Routermodulen identifiziert.

- Rufnummer
Diese Rufnummer soll angerufen werden, wenn der Router selbst aktiv eine Verbindung zur Gegenstelle aufbauen soll. Wenn die Gegenstelle unter verschiedenen Rufnummern erreicht werden kann, tragen Sie die weiteren Rufnummern in der Round-Robin-Liste ein.
Wird diese Gegenstelle über eine Festverbindung erreicht, kann hier die Rufnummer für eine Backup-Leitung über Wählverbindung angegeben werden.
- Haltezeiten
Diese Zeiten geben an, wie lange die B-Kanäle aktiv bleiben, nachdem
 - bei statisch aufgebauten Kanälen für die Haltezeit B1 keine Daten mehr übertragen wurden.
 - bei dynamisch aufgebauten Kanälen für die Haltezeit B2 der Datendurchsatz unter einem fest definierten Schwellwert liegt.
- Layername
Der Layer steht für eine Sammlung von Protokollen, die für diese Verbindung verwendet werden sollen. Der Layer muß auf beiden Seiten der Verbindung gleich eingestellt sein.
- Rückruf
Wenn der Router einen Anruf von dieser Gegenstelle erhält, können Sie hier optional einstellen, daß der Anruf nicht angenommen wird. Stattdessen wird die Gegenstelle zurückgerufen mit den folgenden Optionen:
 - normaler Rückruf
 - Rückruf nach dem schnellen Siemens-Verfahren
 - Rückruf nach Überprüfung des Namens
 - selbst den Rückruf der Gegenstelle nach dem schnellen Siemens-Verfahren erwarten

12.5.2 Interface-Einstellungen

Sie finden die Interface-Einstellungen in Siemens AccessPoint Manager im Konfigurationsbereich 'Management' auf der Registerkarte 'Interfaces' oder bei Telnet- oder Terminalsitzungen unter /Setup/WAN-Modul/Interface-Liste.

In den Interface-Einstellungen legen Sie für jedes Interface (also jeden S₀-Anschluß) die allgemeinen Parameter fest. Diese Parameter gelten für alle Betriebsarten der Geräte. Es sind im einzelnen:

- Das D-Kanal-Protokoll, das an diesem S₀-Anschluß verwendet wird.
Automatische Erkennung: DSS1 (Euro-ISDN), DSS1 Punkt-zu-Punkt, 1TR6, Festverbindung Gruppe 0
- Festverbindungsoption
B-Kanal, der ggf. für die Festverbindung verwendet werden soll
- Anwahlpräfix
Nummer, die bei abgehenden Rufen der Rufnummer vorangestellt wird, z.B. die Amtskennziffer beim Betrieb an TK-Anlagen

12.5.3 Router-Interface-Einstellungen

Sie finden die Router-Interface-Einstellungen in Siemens AccessPoint Manager im Konfigurationsbereich 'Kommunikation' auf der Registerkarte 'Allgemein' oder bei Telnet- oder Terminalsitzen unter /Setup/WAN-Modul/Router-Interface-Liste.

In den Router-Interface-Einstellungen legen Sie für jedes Interface (also jeden S₀-Anschluß) die Parameter fest, die in der Betriebsart als Router verwendet werden. Diese Parameter gelten nicht für die anderen Betriebsarten der Geräte. Es sind im einzelnen:

- Rufnummern (MSN/EAZ)
Auf diese Rufnummern reagiert der Router bei eingehenden Anrufen. Mehrere Rufnummern werden durch Semikolon getrennt. Ohne Eingabe der Rufnummer reagiert der Router auf alle anliegenden Rufnummern.
Die erste der eingetragenen Rufnummern wird bei aktivem Verbindungsaufbau an die Gegenstelle übertragen. Ohne Eingabe der Rufnummer wird die Haupt-MSN des Anschlusses übertragen.
- Option für Y-Verbindung
Schalten Sie diese Option ein, wenn die beiden B-Kanäle des Anschlusses parallel Verbindungen zu unterschiedlichen Gegenstellen aufbauen können sollen.
- Unterdrückung der eigenen Rufnummer
Schalten Sie diese Option ein, wenn die eigene Rufnummer bei aktivem Verbindungsaufbau des Routers nicht bei der Gegenstelle angezeigt werden soll.
Diese Funktion muß vom Netzbetreiber unterstützt werden.

12.5.4 CAPI-Interface-Einstellungen

Sie finden die CAPI-Interface-Einstellungen in Siemens AccessPoint Manager im Konfigurationsbereich 'CAPI' auf der Registerkarte 'Allgemein' oder bei Telnet- oder Terminalsitzungen unter /Setup/CAPI-Modul/Interface-Liste.

In den Router-Interface-Einstellungen legen Sie für jedes Interface (also jeden S0-Anschluß) die Parameter fest, die für die CAPI verwendet werden. Diese Parameter gelten nicht für die anderen Betriebsarten der Geräte. Es sind im einzelnen:

- Rufnummern (MSN/EAZ)
Auf diese Rufnummern reagiert die CAPI bei eingehenden Anrufen. Mehrere Rufnummern werden durch Semikolon getrennt. Ohne Eingabe der Rufnummer reagiert der Router auf alle anliegenden Rufnummern.
- Zugriff auf die CAPI
Hier können Sie die Funktion der CAPI für das Interface ganz ausschalten, nur für ausgehende Rufe oder für ein- und ausgehende Rufe zulassen.
- Übertragung der eigenen Rufnummer
Normalerweise wird beim aktiven Verbindungsaufbau über die CAPI die Rufnummer übermittelt, die in der CAPI-Applikation eingestellt wurde. Falls diese Rufnummer fehlt oder nicht gültig ist, überträgt die CAPI keine Rufnummer. Mit dieser Option können Sie festlegen, daß bei fehlender Rufnummer der CAPI-Applikation stattdessen die erste im Feld 'Rufnummer' eingetragene Nummer übertragen wird.

12.5.5 Layer-Liste

Sie finden die Liste der Kommunikationslayer in Siemens AccessPoint Manager im Konfigurationsbereich 'Kommunikation' auf der Registerkarte 'Allgemein' oder bei Telnet- oder Terminalsitzungen unter /Setup/WAN-Modul/Layer-Liste.

In einem Layer definieren Sie eine bestimmte Kombination von Protokoll-Einstellungen, die für die Übertragung zu anderen Geräten verwendet werden sollen. Es sind im einzelnen:

- Layername
Unter diesem Namen werden die Protokoll-Einstellungen gespeichert. In der Namenliste wählen Sie die Einstellungen mit dem Layernamen für die entsprechende Verbindung aus.

- Encapsulation
Stellen Sie hier ein, ob den Datenpaketen ein Ethernet-Header hinzugefügt werden soll. Normalerweise reicht die Einstellung 'Transparent', nur bei HDLC-Verbindungen zu Fremdgeräten kann diese Einstellung notwendig sein.
- Layer-3
Layer-3-Protokoll für die Verbindung. Wird bei ankommenden Rufen teilweise automatisch erkannt.
Bei Verwendung von PPP ist ein zusätzlicher Eintrag in der PPP-Liste erforderlich.
Bei Verwendung von Scripts ist ein zusätzlicher Eintrag in der Script-Liste erforderlich.
- Layer-2
Layer-2-Protokoll für die Verbindung.
- Optionen
Aktiviert optional die Kompression der Daten und die Kanalbündelung. Diese Optionen werden nur wirksam, wenn sie von den Protokollen auf Layer 2 und Layer 3 unterstützt werden.
- Layer-1
Layer-1-Protokoll für die Verbindung. Wird bei ankommenden Rufen teilweise automatisch erkannt.

12.5.6 Round-Robin-Liste

Sie finden die Round-Robin-Liste in Siemens AccessPoint Manager im Konfigurationsbereich 'Kommunikation' auf der Registerkarte 'Gegenstellen' oder bei Telnet- oder Terminalsitzungen unter /Setup/WAN-Modul/RoundRobin-Liste.

Wenn eine Gegenstelle unter mehreren Rufnummern zu erreichen ist, tragen Sie zunächst die erste Rufnummer in der Namenliste und alle weiteren in der Round-Robin-Liste ein.

- Gegenstelle
Name der Gegenstelle, wie sie vorher in der Namenliste definiert wurde.
- Round-Robin
Weitere Rufnummern für diese Gegenstelle. Mehrere Nummern werden durch Bindestriche getrennt.
- Anfangen mit:
Geben Sie an, ob ein neuer Verbindungsaufbau mit der zuletzt erfolgreichen Nummer gestartet werden soll oder immer mit der ersten Nummer der Liste.

12.5.7 Script

Sie finden die Script-Liste in Siemens AccessPoint Manager im Konfigurationsbereich 'Kommunikation' auf der Registerkarte 'Protokolle' oder bei Telnet- oder Terminalsitzungen unter /Setup/WAN-Modul/Script-Liste.

Wenn für die Anwahl der Gegenstelle die Abarbeitung eines Scripts erforderlich ist, können Sie hier das Script eintragen und der Gegenstelle zuordnen.

Das in der Layerliste für diese Verbindung ausgewählte Layer-3-Protokoll muß die Scriptverarbeitung unterstützen.

- Gegenstelle
Name der Gegenstelle, wie sie vorher in der Namenliste definiert wurde.
- Script
Tragen Sie hier das Script ein, wie im Referenzteil der Dokumentation beschrieben.

12.5.8 Rufannahme

Sie finden die Einstellungen für die Rufannahme in Siemens AccessPoint Manager im Konfigurationsbereich 'Kommunikation' auf der Registerkarte 'Rufannahme' oder bei Telnet- oder Terminalsitzungen unter /Setup/WAN-Modul/Schutz.

Mit den Einstellungen für die Rufannahme legen Sie fest, unter welchen Umständen das Gerät ankommende Rufe annimmt. Diese Einstellungen gelten nur für die Routerfunktionen des Geräts.

- Alle
Alle Rufe werden angenommen.
- Name
Alle Rufe werden zunächst angenommen. In der Protokollverhandlung wird der Name ermittelt und geprüft, ob dieser Name in der Namenliste vorhanden ist. Nur dann bleibt die Verbindung bestehen, ansonsten wird sie wieder abgebaut.
- Nummer
Der Anruf wird nur angenommen, wenn die Gegenstelle in der Nummernliste eingetragen ist und die Rufnummer der Gegenstelle übermittelt wird.
- Name oder Nummer
Der Anruf wird angenommen, wenn eine der beiden Überprüfungen erfolgreich ist.

12.5.9 Nummernliste

Sie finden die Nummernliste in Siemens AccessPoint Manager im Konfigurationsbereich 'Kommunikation' auf der Registerkarte 'Rufannahme' oder bei Telnet- oder Terminalsitzungen unter /Setup/WAN-Modul/Nummernliste.

Die Nummernliste wird für den passiven Verbindungsaufbau zum Schutz bei der Rufannahme und für den Start eines Rückrufs verwendet.

- **Rufnummer**
Rufnummer, die von der anrufenden Gegenstelle übermittelt wird (ggf. inkl. Landes- und Orts-Kennzahlen).
- **Gegenstelle**
Name der Gegenstelle, wie sie in der Namenliste definiert wurde. Ist in der Namenliste ein Rückruf definiert, wird diese Gegenstelle zurückgerufen.

12.6 Point-to-Point Protocol

Router von Siemens unterstützen auch das Point-to-Point Protocol (PPP). PPP ist ein Sammelbegriff für eine ganze Reihe von WAN-Protokollen, die das Zusammenspiel von Routern verschiedener Hersteller erleichtern, denn dieses Protokoll wird von fast allen Herstellern unterstützt.

Und gerade weil das PPP nicht einer bestimmten Betriebsart der Router zugeordnet werden kann und natürlich auch wegen der großen und in Zukunft noch weiter steigenden Bedeutung dieser Protokoll-Familie, möchten wir Ihnen die Funktionen der Geräte im Zusammenhang mit dem PPP hier in einem eigenen Abschnitt vorstellen.

12.7 Das Protokoll

Was ist PPP?

Das Point-to-Point Protocol (PPP) wurde speziell für Netzwerkverbindungen über serielle Kanäle entwickelt und hat sich als Standard für Verbindungen zwischen Routern behauptet. Es realisiert folgende Funktionen:

- Paßwortschutz nach PAP, CHAP oder MS-CHAP
- Aushandlung der über die aufgebaute Verbindung zu benutzenden Netzwerkprotokolle (z.B. IP). Dazu gehören auch für diese Protokolle notwendige Parameter wie z.B. IP-Adressen. Diese Verhandlung läuft über das Protokoll IPCP (IP Control Protocol) ab.
- Überprüfung der Verbindung mit dem LCP (Link Control Protocol)

Für Router-Verbindungen ist PPP der Standard für die Kommunikation zwischen Geräten bzw. der WAN-Verbindungssoftware unterschiedlicher Hersteller. Um eine erfolgreiche Datenübertragung nach Möglichkeit sicherzustellen, erfolgt die Verhandlung der Verbindungsparameter und eine Einigung auf einen gemeinsamen Nenner über standardisierte Steuerungsprotokolle (z.B. LCP, IPCP, CCP), die im PPP enthalten sind.

Wozu wird PPP verwendet?

Das Point-to-Point Protocol wird bei folgenden Anwendungen sinnvoll eingesetzt:

- aus Kompatibilitätsgründen z.B. bei Kommunikation mit Fremdroutern
- Internet-Access (mit der Übermittlung von Adressen)

Die Phasen einer PPP-Verhandlung

Der Verbindungsaufbau über PPP startet immer mit einer Verhandlung der Parameter, die für die Verbindung verwendet werden sollen. Diese Verhandlung läuft in vier Phasen ab, deren Kenntnis für die Konfiguration und Fehlersuche wichtig sind.

- **Establish-Phase**
Nach einem Verbindungsaufbau über den Datenkommunikationsteil startet die Aushandlung der Verbindungsparameter über das LCP.
Es wird festgestellt, ob die Gegenstelle auch bereit ist, PPP zu benutzen, die Paketgrößen und das Authentifizierungsprotokoll (PAP, CHAP, MS-CHAP oder keines) werden festgelegt. Danach wechselt das LCP in den Opened-Zustand.
- **Authenticate-Phase**
Falls notwendig, werden danach die Paßworte ausgetauscht. Bei Authentifizierung nach PAP wird das Paßwort nur einmalig übertragen. Bei Benutzung von CHAP oder MS-CHAP wird ein verschlüsseltes Paßwort periodisch in einstellbaren Abständen gesendet.
- **Network-Phase**
Ist die Verhandlung der Parameter erfolgreich verlaufen, können von den Router-Modulen IP-Pakete auf der geöffneten (logischen) Leitung übertragen werden.
- **Terminate-Phase**
In der letzten Phase wird die Leitung geschlossen, wenn die logischen Verbindungen für alle Protokolle abgebaut sind.

Die PPP-Verhandlung im I-GATE 11M Wireless

Der Verlauf einer PPP-Verhandlung wird in der PPP-Statistik der Geräte protokolliert und kann im Fehlerfall mit Hilfe der dort detailliert gezählten Protokoll-Pakete überprüft werden.

Eine weitere Analyse-Möglichkeit bieten die PPP-Trace-Ausgaben. Mit dem Befehl

```
trace + ppp
```

kann die Ausgabe der ausgetauschten PPP-Protokoll-Frames innerhalb einer Terminal-Sitzung gestartet werden. Wird diese Terminal-Sitzung in einem Log-File protokolliert, kann nach Abbruch der Verbindung eine detaillierte Analyse erfolgen.

12.7.1 Die PPP-Liste

In der PPP-Liste können Sie für jede Gegenstelle, die mit Ihrem Netz Kontakt aufnimmt, eine eigene Definition der PPP-Verhandlung festlegen. Die PPP-Liste finden Sie in Siemens AccessPoint Manager im Konfigurationsbereich 'Kommunikation' auf der Registerkarte 'Protokolle' bzw. im Menü /Setup/WAN-Modul/PPP-Liste.

Die PPP-Liste kann 64 Einträge aufnehmen, die folgende Werte enthalten:

In dieser Spalte der PPP-Liste tragen Sie folgende Werte ein:
Gerätename	Name der Gegenstelle, mit dem sie sich bei Ihrem Router anmeldet
Username	Name, mit dem sich Ihr Router bei der Gegenstelle anmeldet. Ist hier kein Eintrag vorhanden, wird der Gerätename Ihres Routers verwendet.

Tab. 12.1 PPP-Liste

In dieser Spalte der PPP-Liste tragen Sie folgende Werte ein:
Sicherheit	<p>Verfahren zur Sicherung der PPP-Verbindung ('PAP', 'CHAP', 'MS-CHAP' oder 'keine'). Ihr eigener Router verlangt von der Gegenstelle die Einhaltung dieses Verfahrens! Nicht etwa umgekehrt.</p> <p>Daher bietet sich die Sicherung nach 'PAP', 'CHAP' oder 'MS-CHAP' nicht an bei Verbindungen zu Internet-Service-Providern, die uns vielleicht kein Paßwort übermitteln wollen. Für solche Verbindungen wählen Sie 'keine' Sicherung.</p>
Paßwort	<p>Paßwort, das von Ihrem Router an die Gegenstelle übertragen wird (falls gefordert).</p> <p>* in der Liste zeigen an, daß ein Eintrag vorhanden ist.</p>
Zeit	<p>Zeit zwischen zwei Überprüfungen der Verbindung mit LCP. Diese Zeit geben Sie in Vielfachen von 10 Sekunden ein (also z.B. 2 für 20 Sek.).</p> <p>Gleichzeitig die Zeit zwischen zwei Überprüfungen der Verbindung nach CHAP. Diese Zeit geben Sie in Minuten ein.</p> <p>Für Gegenstellen mit Windows 95, Windows 98 oder Windows NT muß die Zeit auf '0' gesetzt werden!</p>

Tab. 12.1 PPP-Liste

In dieser Spalte der PPP-Liste tragen Sie folgende Werte ein:
Wdh	<p>Anzahl der Wiederholungen für den Überprüfungsversuch. Mit mehreren Wiederholungen schalten Sie den Einfluß kurzfristiger Leitungsstörungen aus. Erst wenn alle Versuche erfolglos bleiben, wird die Verbindung abgebaut. Der zeitliche Abstand zwischen zwei Wiederholungen beträgt 1/10 der Zeit zwischen zwei Überprüfungen.</p> <p>Gleichzeitig die Anzahl der „Configure Requests“, die der Router maximal aussendet, bevor es von einer Leitungsstörung ausgeht und selber die Verbindung abbaut.</p>
Conf, Fail, Term	<p>Mit diesen Parametern wird die Arbeitsweise des PPPs beeinflusst. Die Parameter sind in der RFC 1661 definiert und werden hier nicht näher beschrieben. Falls Sie keine PPP-Verbindungen aufbauen können, finden Sie in dieser RFC im Zusammenhang mit der PPP-Statistik des Routers Hinweise zur Behebung der Störung.</p> <p>Im allgemeinen sind die Default-Einstellungen ausreichend.</p> <p>Diese Parameter können nur über SNMP oder TFTP (mit Siemens AccessPoint Manager) verändert werden!</p>

Tab. 12.1 PPP-Liste

12.7.2 Alles o.k.? Leitungsüberprüfung mit LCP

Beim Verbindungsaufbau über PPP handeln die beteiligten Geräte ein gemeinsames Verhalten während der Datenübertragung aus. Sie entscheiden z.B. zunächst, ob mit den Einstellungen der Sicherungsverfahren, Namen und Paßwörter überhaupt eine Verbindung zustande kommen darf.

Wenn die Verbindung einmal steht, kann mit Hilfe des LCPs die Zuverlässigkeit der Leitung ständig überprüft werden. Innerhalb des

Protokolls geschieht dies mit dem LCP-Echo-Request und dem zugehörigen LCP-Echo-Reply. Der LCP-Echo-Request ist eine Anfrage in Form eines Datenpakets, das neben den reinen Nutzdaten zur Gegenstelle übertragen wird. Wenn auf diese Anfrage eine gültige Antwort (LCP-Echo-Reply) zurückgeschickt wird, ist die Verbindung zuverlässig und stabil. Zur dauerhaften Überprüfung der Verbindung wird dieser Request in bestimmten Abständen wiederholt.

Was passiert nun, wenn der Reply ausbleibt? Zuerst werden einige Wiederholungen der Anfrage gestartet, um kurzfristige Störungen der Leitung auszuschließen. Wenn alle diese Wiederholungen unbeantwortet bleiben, wird die Leitung abgebaut und ein Ersatzweg gesucht.

Das Verhalten der LCP-Anfragen stellen Sie in der PPP-Liste für jede Verbindung einzeln ein. Mit dem Eintrag in die Felder 'Zeit' und 'Wdh.' legen Sie fest, in welchen Abständen die LCP-Anfrage gestellt werden soll und wie viele Wiederholungen beim Ausbleiben der Antwort gestartet werden, bis die Leitung als gestört bezeichnet werden darf. Mit einer Zeit von '0' und '0' Wiederholungen stellen Sie die LCP-Requests ganz ab.

12.8 IPX-Routing

Der IPX-Router überträgt Daten aus Netzwerken, die IPX/SPX als Netzwerkprotokoll verwenden (z.B. Novell-Netze). Mit dem Eintrag in der IPX-Routing-Tabelle wird ein entferntes Netz für die Rechner im lokalen Netz bekannt gemacht. In der Routing-Tabelle können bis zu 16 verschiedene Netze eingetragen werden.

12.8.1 IPX-Adressierung

Eine vollständige Adresse in einem IPX-Netzwerk besteht aus drei Teilen: einer Netzwerknummer, der MAC-Adresse der Netzwerkkarte und der Socket-Nummer:

- Die Netzwerknummer kann frei gewählt werden. Sie muß allerdings über alle erreichbaren IPX-Netze hinweg eindeutig sein, um eine richtige Zuordnung zu gewährleisten.
- Die MAC-Adresse ist fest in jede Netzwerkkomponente eingebrannt. Nur in Sonderfällen wird netzintern auch eine andere Adresse verwendet.
- Um nicht nur einen Rechner, sondern auch einen ganz besonderen Dienst auf diesem Rechner anzusprechen, verwendet

ein IPX-Netz die Socket-Nummern. Damit werden die verschiedenen Dienste eindeutig identifiziert.

12.8.2 Informationen über das LAN

Wenn an einem Standort mehrere getrennte LANs benötigt werden, so müssen diese nicht unbedingt auch eigene Verkabelungen haben. Verschiedene logische Netze können sich ein Kabel teilen. Damit die Daten der verschiedenen Netzwerke sich nicht stören und ein Netz für die anderen unsichtbar bleibt, verwenden sie unterschiedliche Formate für die Ethernet-Pakete. Diese Formate werden durch das Binding bestimmt, das zu einer eindeutigen Netzwerknummer auf diesem Kabel gehört.

Damit der Router nun auch weiß, zu welchem Netz er gehört, müssen Sie ihm die Netzwerknummer und das zugehörige Binding angeben. Lassen Sie die Netzwerkadresse auf der Standard-Einstellung '00000000', ermittelt der Router die Adresse und das Binding selbst. Dazu sucht er sich auf dem angeschlossenen Kabel das Netz aus, auf dem er die meisten SAP-Replies erhält.

12.8.3 IPX-Routing-Tabelle

In der IPX-Routing-Tabelle legen Sie fest, welche Gegenstellen (also welche anderen Router oder Rechner) für das lokale Netzwerk erreichbar sind, und geben ihm einige Parameter für die Verbindung an. Die Tabelle mit maximal 16 Einträgen hat folgenden Aufbau:

Gegenstelle	Netzwerk	Binding	Propagate	Backoff
FILIALE01	00000245	802.3	Route	Ein
FILIALE02	00000320	SNAP	Filt.	Ein
ZENTRALE	00000420	802.2	Filt.	Aus

Tab. 12.2 IPX-Routing Tabelle

- Gegenstelle
Der Name der Gegenstelle, wie er als Geräte-Name in dem entsprechenden Router auf der Gegenseite eingetragen ist.

- **Netzwerk**
Adresse des WANs. Das ist nicht die Adresse des Ziel-Netzwerks, sondern eine dritte Adresse, die das Netz zwischen den beiden zu verbindenden Netzen darstellt. Hier gilt also:
LAN-Adresse 1 \neq WAN-Adresse 1 = WAN-Adresse 2
 \neq LAN-Adresse 2 \neq LAN-Adr. 1
- **Binding**
Hier wird eingestellt, welches Ethernet-Binding auf dem WAN verwendet werden soll. Dieser Eintrag ist nur wirksam, wenn der Layer für diese Verbindung Ethernet-Encapsulation unterstützt. Fehlt der Eintrag, wird 802.3 angenommen.
- **Propagate**
Filter für IPX-Pakete vom Typ 20 (NetBIOS Propagated Frames). Das Network Basic Input/Output System wurde ursprünglich für IBM entwickelt und wird mittlerweile in abgewandelter Form auch von Microsoft verwendet. Dieses Protokoll stellt in Layer 3 und 4 des OSI-Modells Dienste wie Namensauflösung, Datensicherung und korrekte Paketreihenfolge zur Verfügung (gesichertes Protokoll). NetBIOS-Pakete besitzen einen speziellen Pakettyp und Socket (Propagated Pakets). NetBIOS wird in erster Linie für den Datenaustausch zwischen Stationen in einem lokalen Netz (LAN) verwendet.
Diese IPX-Pakete können mit der Einstellung 'Filter' von der Übertragung ausgeschlossen oder geroutet werden. Bei der Einstellung 'Route' werden die Pakete übertragen, wenn eine Verbindung zur entsprechenden Gegenstelle besteht oder noch ein freier Kanal für den Aufbau einer weiteren Verbindung verfügbar ist. Sind alle Leitungen mit anderen Gegenstellen beschäftigt, werden die Propagated Frames verworfen.
- **Backoff**
Der IPX-Router benutzt einen speziellen Algorithmus (Exponential-Backoff), um bei Fehlkonfigurationen die anfallenden Verbindungskosten so gering wie möglich zu halten.
Wenn im Netz der Gegenstelle kein Server vorhanden ist (z.B. bei Remote-Access von einer Workstation), dann sollte die Backoff-Funktion ausgeschaltet sein (siehe auch 'Exponential-Backoff').
Die Default-Einstellung ist 'Ein'.

12.8.4 Was passiert bei der Datenübertragung im IPX-Netz?

Wenn sich ein Gerät in einem IPX-Netz anmeldet, sendet es zunächst eine Anfrage nach dem Service Advertising Protocol (SAP) aus und erkundigt sich nach dem nächsten erreichbaren Server (Get Nearest Server Request) im Netz mit der Nr. '00000000'. Befindet sich in diesem Netz ein Router oder Server, antwortet dieser auf diese Anfrage und teilt dabei die korrekte Netzwerknummer mit.

Die Server versenden außerdem regelmäßig Informationen darüber, welche Dienste sie anbieten und welche anderen Netzwerke sie erreichen können. Dazu verwenden sie spezielle Datenpakete nach dem Service Advertising Protocol bzw. Routing Information Protocol (RIP).

Wenn der IPX-Router fertig konfiguriert ist und eingeschaltet wird, baut er zunächst einmal zu allen über die Routing-Tabellen erreichbaren Gegenstellen Verbindungen auf und tauscht dann mit diesen Netzen SAP- und RIP-Informationen aus. Der Router speichert diese Daten in seinen internen SAP- und RIP-Tabellen.

12.8.5 RIP- und SAP-Tabellen

Die RIP- und SAP-Informationen erscheinen in den entsprechenden Tabellen alphabetisch sortiert. RIPs sind dabei nur nach dem Netzwerk geordnet, SAPs zuerst nach dem Service-Typ, dann nach dem Servernamen.

Mit jedem neuen RIP- bzw. SAP-Paket werden die RIP- und SAP-Tabellen angepaßt. Damit dabei nur solche Dienste angeboten werden (SAP), die auch erreichbar sind (RIP), nimmt der Router nur diese SAP-Informationen in die eigene Tabelle auf, für die es auch den entsprechenden RIP-Eintrag gibt. Neben den Informationen über erreichbare Routen und Dienste verraten die Einträge der Tabellen z.B. auch, wie viele Router auf dem Weg dorthin zu passieren sind (Hops) oder welche Zeit ein Datenpaket ins Zielnetz braucht (Tics = ca. 1/18 Sekunde). Werden über die RIP-Informationen z.B. mehrere Routen in ein Zielnetz angeboten, wählt der Router anhand der Tabellen den Weg mit den wenigsten Tics und dem kleinsten Hopcount aus und speichert nur diese Route.

RIP-Tabellen können 64, SAP-Tabellen 128 Einträge aufnehmen. Wenn jedes neue Paket die Tabellen aktualisiert, müssen natürlich irgendwann auch die alten Einträge verschwinden. Dazu bekommen die Einträge ein künstliche Alterung. Für alle Einträge in den

RIP/SAP-Tabellen, die durch lokalen Datenaustausch gelernt wurden, wird das Alter alle 60 Sekunden um eins erhöht. Ein neues RIP- bzw. SAP-Paket für einen Eintrag setzt das Alter auf Null zurück. Nach einem einstellbaren Alter von 1 bis 60 wird die Route oder der Service als unerreichbar (Down) bezeichnet. Ist das Doppelte dieser Zeit abgelaufen, wird der Eintrag entfernt. Außerdem werden bei einem Verbindungsaufbau alle RIP- und SAP-Informationen, die diese Gegenstelle betreffen, aus den Tabellen gelöscht und durch neue Informationen ersetzt.

12.8.6 So viele Router hier ...

Ist in einem Netz der Aufbau zu mehr Gegenstellen gleichzeitig erwünscht, als ein Router realisieren kann, dann wird es Zeit für einen zweiten (dritten ...) Router. Damit das Zusammenspiel der Brüder reibungslos funktioniert und das Netz wirklich immer einen Ansprechpartner findet, werden in allen Routern die gleichen Einträge in der Routing-Tabelle vorgenommen. Durch die RIP-Pakete werden jedem Router dann auch die gleichen Routing-Informationen übermittelt, allerdings mit höherem Tic- und Hopcount (Setup/IPX-Modul/LAN-Einstellung/RIP-SAP-Skal. einschalten).

Dadurch werden diese Routen quasi als Reserve markiert, wenn auf dem angesprochenen Gerät alle Kanäle besetzt sind.

12.8.7 Redundante Routen

Empfängt ein Router mit einem RIP-Paket Informationen über Routen mit gleichem Tic- und Hopcount wie die eigenen Routen (redundante Routen), muß er dem Absender diese Routen natürlich nicht selbst wieder bekanntgeben. Er sendet diese Routen also nur an die Router, die die Route nicht propagiert haben. Dieses Verfahren nennt man Split Horizon.

Sollte es trotzdem einmal nötig sein, redundante Routen im lokalen Netz bekanntzugeben, kann die Funktion 'Loop-Propagieren' verwendet werden (SETUP/IPX-MODUL/LAN-EINSTELLUNG/LOOP-PROPAGIEREN). Die so gelernten Routen werden in der RIP-Tabelle dann als 'LOOP' gekennzeichnet. Da die Verbreitung von redundanten Routen nach den Novell-Spezifikationen zwar nicht verboten ist, aber trotzdem möglichst unterlassen werden sollte, ist die Default-Einstellung 'Aus'.

12.8.8 Exponential-Backoff

Um die für den Betrieb notwendigen Routing-Informationen (RIP- und SAP-Informationen) der IPX-Gegenstellen zu erhalten, versucht der IPX-Router des Gerätes nach dem Einschalten entsprechende Verbindungen aufzubauen. Falls dies nicht möglich ist, etwa durch eine Fehlkonfiguration des IPX-Routers, vermeidet der Exponential-Backoff-Algorithmus, daß laufend Verbindungsaufbau gestartet wird und spart damit Gebühren.

Gelingt der erste Verbindungsversuch zu einer Gegenstelle nicht, versucht der Router nach einer ständig wachsenden Wartezeit erneut die Gegenstelle zu erreichen. Die Wartezeit wird dabei folgendermaßen bestimmt:

- Die erste Anwahl erfolgt nach $10 + x$ Sekunden. x ist dabei ein Zahl zwischen 0 und 10.
- Der zweite Versuch wird um $10 + x$ Sekunden nach dem Scheitern des ersten Versuchs gestartet. x steht jetzt für eine Zahl zwischen 0 und 20 Sekunden.
- Der obere Wert für x wird nun bei jedem neuen Versuch verdoppelt. Nach dem 16. erfolglosen Versuch gibt der Router schließlich auf. Durch das ständige Anwachsen der Wartezeit ist nach 16 Versuchen maximal ein Tag vergangen.

Bleiben alle Versuche zur Anwahl der Gegenstelle erfolglos, wird die Route gesperrt. Nur eine Änderung des Eintrags in der Routing-Tabelle kann dann zu erneuten Verbindungsversuchen führen.



Die Zeit bis zur nächsten Anwahl und die Zahl der Aufbauversuche können der Netzwerkstatistik entnommen werden (Status/IPX-Statistik/Router-Statistik/Netzwerke).

12.8.9 Filter für die IPX-Pakete

Mit den Einträgen in der Routing-Tabelle legen Sie fest, welche anderen Netze erreichbar sind. Diese Netze sind damit allerdings auch erreichbar für solche Datenpakete, die im Netz der Gegenstelle eigentlich nicht benötigt werden. Diese Pakete führen auch zum Aufbau unerwünschter Verbindungen und kosten Geld.

Also müssen geeignete Filter her. Damit können Sie z.B. Datenpakete, die nur zur internen Kommunikation der Netze verwendet werden, von der Übertragung über das WAN ausschließen oder sie zumindest einschränken:

- **Propagated Frames**
Diese speziellen Datenpakete verwenden Protokolle, die eigentlich nicht geroutet werden können. Um trotzdem am gemeinsamen Routing teilnehmen zu können, werden diese Daten in normale IPX-Pakete gekapselt und als Broadcast verschickt.
Manchmal sind diese Pakete beim Routing nicht erwünscht. Daher können Sie für diesen Paket-Typ explizit einstellen, ob er geroutet oder gefiltert werden soll.
- **Socket-Filter**
Jedes Datenpaket in einem IPX-Netz enthält neben Ziel- und Quelladressen auch Ziel- und Quell-Sockets. Sockets bezeichnen die Prozesse, für die die Daten in dem Paket bestimmt sind. Für die Sockets aus dem lokalen sowie aus den entfernten Netzen gibt es jeweils eine entsprechende Filtertabelle, die die Filter beinhaltet, mit denen einzelne Ziel-Sockets oder ganze Gruppen von der Übertragung ausgeschlossen werden können. Einige Sockets, die bekanntermaßen häufig für unerwünschte Verbindungen sorgen, sind als Voreinstellung schon in der Socket-Filtertabelle eingetragen.
- **RIP- und SAP-Informationen**
Über die RIPs teilt ein Router nach dem Split-Horizon-Prinzip den anderen Routern alle ihm bekannten Routen (Wege in andere Netze) mit. Das sind sowohl die Einträge aus der eigenen Routing-Tabelle und auch alle Routen, die der Router von anderen Routern gelernt hat. Er lernt dabei sowohl von Routern aus lokalen als auch aus entfernten Netzen. Alle verfügbaren Routing-Informationen trägt er in seiner internen RIP-Tabelle ein.
In den SAP-Informationen bieten die Server ihre Dienste an. Die verschiedenen Dienste werden innerhalb der SAP-Infos durch Nummern dargestellt. Jeder Dienst (z.B. File-Server oder Print-Server) hat eine eindeutige Nummer. Der Router nimmt die Informationen über die verfügbaren Dienste in die interne SAP-Tabelle auf und trägt ein, welcher Service in welchem Netz an welcher MAC-Adresse verfügbar ist. Dabei lernt er auch, ob der angebotene Dienst lokal oder in einem entfernten Netz liegt, und kann den Dienst so ohne Verbindungsaufbau propagieren.



Im IPX-Modul (setup/IPX-Modul/RIP-Einstellung bzw. SAP-Einstellung) der Router können Sie die RIP- und SAP-Tabellen mit den aktuellen Werten einsehen.

RIP- und SAP-Informationen sind natürlich sehr wichtig für die Kommunikation der Geräte in einem Netz, daher gibt es verschiedene Möglichkeiten, die Übertragung dieser Pakete einzustellen:

- Mit einer LAN- und einer WAN-Filtertabelle kann der Router angewiesen werden, Informationen über Routen zu bestimmten Netzen bzw. über bestimmte verfügbare Dienste nicht in die interne RIP- oder SAP-Tabelle zu übernehmen. Die betroffenen Routen werden also nicht verwendet und auch nicht weiter bekanntgegeben, die Dienste werden nicht im eigenen Netz angeboten.
- RIP- und SAP-Pakete werden ohne Filter, also immer übertragen. Diese belegen jedoch auf jeden Fall einen Teil der Verbindungsleitung.
- Die RIP- und SAP-Pakete werden nur dann versendet, wenn sich Änderungen in der Information ergeben haben.
- RIPs und SAPs können in regelmäßigen, einstellbaren Zeiten übertragen werden. Normalerweise werden die Informationen im Abstand von einer Minute verschickt. Mit der Zeiteinstellung kann dieser Abstand auf bis zu 60 Minuten ausgedehnt werden.
- Die gebührenschonendste Behandlung der RIP- und SAP-Pakete überträgt die Informationen einmalig nur dann, wenn eine Verbindung aufgebaut ist.
- IPX- und SPX-Watchdogs:
Mit diesen Datenpaketen erkundigen sich die Server z.B. bei den Arbeitsplatzrechnern, ob sie noch aktiv sind oder ob sie ggf. abgemeldet werden können. Damit diese „Hallo, bist du noch wach?“-Pakete für Rechner in einem entfernten Netz nicht ständig zum Verbindungsaufbau führen, können Sie die Beantwortung dieser Anfragen folgendermaßen einstellen:
 - IPX-Watchdogs bleiben völlig unbeantwortet. Nach der beim Server eingestellten Zeit werden die Rechner abgemeldet.
 - IPX- und SPX-Watchdogs können lokal beantwortet werden. Dieses Verfahren nennt man Spoofing. Der Router antwortet dann anstelle der angesprochenen Rechner, die dann natürlich nie abgemeldet werden. Die Einstellung einer Zeit beim Server, nach der die entsprechenden Geräte auf jeden Fall abgemeldet werden, ist also sinnvoll.

- IPX- und SPX-Watchdogs können natürlich auch ganz normal geroutet werden, führen dann aber recht häufig zum Aufbau einer Verbindung.



Weitere Hinweise zu IPX, zum IPX-Router und zu den zugehörigen Parametern finden Sie im Kapitel 'Setup/IPX-Modul' im Referenz-Handbuch.

12.9 IP-Routing

Ein IP-Router arbeitet zwischen Netzen, die TCP/IP als Netzwerk-Protokoll verwenden. Dabei werden nur Daten übertragen, deren Zieladressen in der Routing-Tabelle eingetragen sind. In diesem Kapitel erfahren Sie, wie die IP-Routing-Tabelle in einem Router von Siemens aufgebaut ist und mit welchen weiteren Funktionen das IP-Routing unterstützt wird.

12.9.1 Die IP-Routing-Tabelle

In der IP-Routing-Tabelle sagen Sie dem Router, an welche Gegenstelle (also welchen anderen Router oder Rechner) er die Daten für bestimmte IP-Adressen oder IP-Adreß-Bereiche schicken soll. So ein Eintrag heißt auch „Route“, weil der Weg der Datenpakete damit beschrieben wird. Da Sie diese Einträge selbst vornehmen und sie solange unverändert bleiben, bis Sie selbst sie wieder ändern oder löschen, heißt dieses Verfahren auch „statisches Routing“. Im Gegensatz dazu gibt es natürlich auch ein „dynamisches Routing“. Dabei tauschen die Router selbständig untereinander Informationen über die Routen aus und erneuern diese fortlaufend. Die statische Routing-Tabelle kann bis zu 64 Einträge aufnehmen, die dynamische Tabelle 128. Bei aktiviertem IP-RIP beachtet der IP-Router beide Tabellen.

Die Routingtabelle finden Sie in Siemens AccessPoint Manager in 'TCP/IP' auf der Registerkarte 'Router' bzw. im Menü /Setup/IP-Router/IP-Routing-Tab. So sieht eine IP-Routing-Tabelle also z.B. aus:

Was bedeuten die einzelnen Einträge in der Liste?

- IP-Adresse und IP-Netzmaske
Das ist die Adresse des Zielnetzes, zu dem Datenpakete geschickt werden können, mit der zugehörigen Netzmaske. Mit der Netzmaske und der Ziel-IP-Adresse aus den ankommenden

den Datenpaketen prüft der Router, ob das Paket in das Zielnetz gehört.

Die Route mit der IP-Adresse „255.255.255.255“ mit Netzmaske „0.0.0.0“ ist die Default-Route. Alle Datenpakete, die nicht durch andere Routing-Einträge geroutet werden können, werden über diese Route übertragen.

- **Router-Name**
Der Router-Name gibt an, was mit den zur IP-Adresse und Netzmaske passenden Datenpaketen geschehen soll. Routen mit dem Router-Namen „0.0.0.0“ bezeichnen Ausschluß-Routen. Datenpakete für diese „Null-Routen“ werden verworfen und nicht weitergeleitet. Damit werden z.B. die im Internet verbotenen Routen (Privat Address Spaces, z.B. 10.0.0.0) von der Übertragung ausgeschlossen. Wird als Router-Name eine IP-Adresse eingetragen, handelt es sich dabei um einen lokal erreichbaren Router, der für die Übertragung der entsprechenden Datenpakete zuständig ist.
- **Distanz**
Anzahl der zwischen dem eigenen und dem Ziel liegenden Router.

Beispiele mit Erläuterungen:

IP-Adresse	IP-Netzmaske	Router-Name	Dist.	Und das passiert:
192.168.130.0	255.255.255.0	192.168.140.123	0	Alle Datenpakete mit den Ziel-IP-Adressen 192.168.130.x werden an den lokal erreichbaren Router mit der IP-Adresse 192.168.140.123 übertragen.
192.168.0.0	255.255.0.0	0.0.0.0	0	Schließt die Übertragung aller Datenpakete in 10er-Netze aus.
172.16.0.0	255.255.0.0	0.0.0.0	0	
10.0.0.0	255.0.0.0	0.0.0.0	0	
224.0.0.0	224.0.0.0	0.0.0.0	0	

Tab. 12.3 IP-Routing-Tabelle

12.9.2 Filter für die TCP/IP-Pakete

Mit den Einträgen in der Routing-Tabelle können Sie schon recht genau festlegen, welche Datenpakete übertragen werden sollen. Zusätzlich können Sie mit dem Eintrag '0.0.0.0' im Feld 'Router-Name' ganze Gruppen von IP-Adressen verwerfen.

Manchmal möchten Sie die Übertragung jedoch noch weiter einschränken. Dazu nutzen Sie die Eigenschaft von TCP/IP, neben den Quell- und Ziel-IP-Adressen mit einem Datenpaket auch Portnummern für Ziel und Quelle zu versenden. Der Ziel-Port in einem Datenpaket steht für den Dienst im TCP/IP-Netz, der angesprochen werden soll. Die Ziel-Ports für verschiedene Dienste im TCP/IP-Netz sind fest definiert (siehe auch 'TCP/IP-Ports' Referenz-Handbuch). Die Quell-Ports hingegen werden in bestimmten Bereichen frei gewählt.

Der Router kann sich die Ziel- und Quell-Ports von solchen Datenpaketen ansehen, die TCP oder UDP als Protokoll verwenden. Aus diesen Ports kann dann abgeleitet werden, für welchen Zweck die Daten gedacht sind. So können z.B. FTP-Zugriffe oder Telnet-Sitzungen erkannt werden.

12.9.3 Proxy-ARP

Eine Besonderheit im IP-Router stellt die Möglichkeit des Proxy-ARP dar. „Proxy“ ist ein englischer Begriff und heißt auf deutsch „Stellvertreter“. Dieser Stellvertreter wird dann eingesetzt, wenn die Datenübertragung zu IP-Adressen im gleichen logischen Netz wie der Absender erfolgt, die Zieladresse dennoch über einen Router zu erreichen ist. Das ist z.B. bei der Anbindung von einzelnen Arbeitsplatzrechnern (Teleworkern) über TCP-IP an das Firmen-Netz der Fall. Der Teleworker hat dann eine IP-Adresse, die im gleichen lokalen Netz liegt wie alle anderen Rechner im LAN. Normalerweise würde ein Datenpaket aus dem LAN für den Teleworker also nur lokal einen Abnehmer suchen, leider aber nicht finden.



Um diese Funktion zu nutzen, muß die Option 'Proxy-ARP' eingeschaltet werden (im AccessPoint Manager im Konfigurationsbereich 'TCP/IP' auf der Registerkarte 'Router' oder im Menü /setup/IP-Router-Modul bei anderen Konfigurationsmöglichkeiten).

Mit folgendem Eintrag in der Routing-Tabelle wird der Router zum Stellvertreter des Teleworkers:

IP-Adresse	IP-Netzmaske	Router-Name	Distanz	IP-Masque- rading
192.168.110.123	255.255.255.255	Teleworker01	0	aus

Tab. 12.4 Proxy ARP mit dem IP-Router

Da der Router auf einen ARP-Request für den Proxy-Rechner mit seiner eigenen MAC-Adresse antwortet, werden Proxy-Hosts in einem RIP-Paket nicht propagiert. In der Routing-Tabelle wird die Distanz auf '0' gesetzt, um das zu verdeutlichen.

Der Router beantwortet nun die Frage nach der MAC-Adresse zur IP-Adresse 192.168.110.123 mit seiner eigenen MAC-Adresse. Dadurch werden alle Pakete für den Teleworker im LAN nun automatisch zum Router geschickt, der die Daten zum Rechner auf der anderen Seite der Verbindung weiterleitet.

12.9.4 Lokales Routing

Sie kennen das folgende Verhalten der Arbeitsplatzrechner in einem lokalen Netz: Möchte der Rechner ein Datenpaket an eine IP-Adresse senden, die nicht in seinem eigenen LAN liegt, sucht er nach einem Router, der ihm weiterhelfen kann. Dieser Router wird normalerweise dem Betriebssystem durch den Eintrag als Standard-Router oder Gateway bekanntgegeben. Gibt es in einem Netz mehrere Router, so kann oft nur ein Standard-Router eingetragen werden, der alle dem Arbeitsplatzrechner unbekannt IP-Adressen erreichen können soll. Manchmal kann dieser Standard-Router jedoch nicht selbst das Zielnetz erreichen, er kennt aber einen anderen Router, der zu diesem Ziel findet.

Wie helfen Sie dem Arbeitsplatzrechner nun weiter?

Standardmäßig schickt der Router dem Rechner eine Antwort mit der Adresse des Routers, der die Route ins Ziel-Netz kennt (diese Antwort nennt man ICMP-Redirect). Der Arbeitsplatzrechner übernimmt daraufhin diese Adresse und schickt das Datenpaket sofort an den anderen Router.

Manche Rechner können mit den ICMP-Redirects leider nichts anfangen. Um die Datenpakete trotzdem zustellen zu können, verwenden Sie das lokale Routing (im Siemens AccessPoint Manager im Konfigurationsbereich 'TCP/IP' auf der Registerkarte 'Router'

oder im Menü /Setup/IP-Router-Modul/Lok.-Routing Ein). Dadurch weisen Sie den Router in Ihrem Gerät an, das Datenpaket selbst zum anderen, zuständigen Router zu senden. Außerdem werden dann keinen ICMP-Redirects mehr geschickt.

Ist im Prinzip ja eine tolle Sache, trotzdem sollte das lokale Routing nur im „Notfall“ verwendet werden, denn diese Funktion führt zu einer Verdoppelung aller Datenpakete zum gewünschten Zielnetz. Die Daten werden erst zum Standard-Router und von diesem erneut zum eigentlich zuständigen Router im lokalen Netz geschickt.

12.9.5 Dynamisches Routing mit IP-RIP

Neben der statischen Routing-Tabelle verfügen Router von Siemens auch über eine dynamische Routing-Tabelle mit bis zu 128 Einträgen. Diese Tabelle füllt der Anwender im Gegensatz zu der statischen nicht selbst aus, das erledigt der Router selbst. Dazu nutzt er das Routing Information Protocol (RIP). Über dieses Protokoll tauschen alle Geräte, die RIP beherrschen, Informationen über die erreichbaren Routen aus.

Welche Informationen werden über IP-RIP propagiert?

Ein Router teilt in den IP-RIP-Informationen den anderen Routern im Netz die Routen mit, die es in seiner eigenen statischen Tabelle findet. Nicht berücksichtigt werden dabei die folgenden Einträge:

- Routen, die mit der Router-Einstellung '0.0.0.0' verworfen werden.
- Routen, die auf andere Router im lokalen Netz lauten.

Welche Informationen nimmt der Router aus empfangenen IP-RIP-Paketen?

Wenn der Router IP-RIP-Pakete empfängt, baut er sie in seine dynamische IP-Routing-Tabelle ein, und die sieht etwa so aus:

IP-Adresse	IP-Netzmaske	Zeit	Distanz	Router
192.168.120.0	255.255.255.0	1	2	192.168.110.1
192.168.130.0	255.255.255.0	5	3	192.168.110.2
192.168.140.0	255.255.255.0	1	5	192.168.110.3

Tab. 12.5 Dynamisches Routing mit IP-RIP

Was bedeuten die Einträge?

IP-Adresse und Netzmaske bezeichnen das Ziel-Netz, die Distanz gibt die Anzahl der zwischen Sender und Empfänger liegenden Router an, die letzte Spalte zeigt an, welcher Router diese Route bekanntgemacht hat. Bleibt die 'Zeit'. Damit zeigt die dynamische Tabelle an, wie alt die entsprechende Route ist. Der Wert in dieser Spalte gilt als Multiplikator für das Intervall, in dem die RIP-Pakete eintreffen, eine '1' steht also für etwa 30 Sekunden, eine '5' für etwa 2,5 Minuten usw. Wenn eine Information über eine Route neu eintrifft, gilt diese Route natürlich als direkt erreichbar und erhält die Zeit '1'. Nach Ablauf der entsprechenden Zeit wird der Wert in dieser Spalte automatisch erhöht. Nach 3,5 Minuten wird die Distanz auf '16' gesetzt (Route nicht erreichbar), nach 5,5 Minuten wird die Route gelöscht.

Wenn der Router nun ein IP-RIP-Paket empfängt, muß er entscheiden, ob er die darin enthaltenen Routen in seine dynamische Tabelle aufnehmen soll oder nicht. Dazu geht er wie folgt vor:

- Die Route ist in der Tabelle noch gar nicht vorhanden, dann wird sie aufgenommen (sofern Platz in der Tabelle ist).
- Die Route ist in der Tabelle vorhanden mit der Zeit von '5' oder '6'. Die neue Route wird dann verwendet, wenn sie die gleiche oder eine bessere Distanz aufweist.
- Die Route ist in der Tabelle vorhanden mit der Zeit von '7' bis '10', hat also die Distanz '16'. Die neue Route wird auf jeden Fall verwendet.
- Die Route ist in der Tabelle vorhanden. Die neue Route kommt von dem gleichen Router, der auch diese Route bekanntgegeben hat, hat aber eine schlechtere Distanz als der bisherige Eintrag.

Zusammenspiel: statische und dynamische Tabelle

Aus der statischen und der dynamischen Tabelle stellt der Router die eigentliche IP-Routing-Tabelle zusammen, mit der er den Weg für die Datenpakete bestimmt. Dabei nimmt er zu den Routen aus der eigenen statischen Tabelle die Routen aus der dynamischen Tabelle auf, die er selber nicht kennt oder die eine kürzere Distanz aufweisen als die eigene (statische) Route.

12.9.6 IP-Masquerading (NAT, PAT)

Ein ständig wachsendes Problem des Internets ist die Begrenzung der verfügbaren und allgemein gültigen IP-Adressen. Darüber hinaus ist die Zuweisung von festen IP-Adressen für das Internet durch das Network Information Center (NIC) eine kostspielige Sache. Was liegt also näher, als sich mit mehreren Rechnern eine IP-Adresse zu teilen?

Die Lösung heißt hier IP-Masquerading. Bei diesem Verfahren tritt nur ein Router des LANs mit einer IP-Adresse im Internet in Erscheinung. Diese IP-Adresse wird dem Router z.B. fest vom NIC oder temporär von einem Internet-Provider zugewiesen. Alle anderen Rechner im Netz „verstecken“ sich dann hinter dieser einen IP-Adresse. Neben dem angenehmen Spareffekt bildet das IP-Masquerading auch einen sehr effektiven Schutz gegen Zugriffe aus dem Internet auf das lokale Netz.

Zwei Adressen für den Router

Bei Masquerading treffen zwei gegensätzliche Forderungen an den Router aufeinander: Zum einen soll er eine im lokalen Netz gültige IP-Adresse haben, damit er aus dem LAN erreichbar ist, zum anderen soll er eine im Internet gültige Adresse haben. Da diese beiden Adressen prinzipiell nicht in einem logischen Netz liegen dürfen, hilft hier nur eins: Zwei IP-Adressen müssen her.

Der Router bekommt also nun eine Internet-Adresse und eine Intranet-Adresse, jeweils natürlich mit passender Netzmaske. Mit der Option 'Maskierung' in der Routing-Tabelle informieren Sie den Router darüber, welche der beiden Adressen er bei der Weitergabe der Pakete verwenden soll.

- 'aus': Es wird keine Maskierung durchgeführt.
- 'dyn.': Mit diesem Eintrag fordern Sie von Ihrem Provider die Zuweisung einer beliebigen, im Internet gültigen IP-Adresse an, die Sie im weiteren für die Verbindung und die Maskierung verwenden wollen.
- 'stat.': Mit diesem Eintrag fordern Sie von Ihrem Provider die Zuweisung einer bestimmten, unter /setup/TCP als IP-Adresse eingetragenen Adresse an, die Sie im weiteren für die Verbindung und die Maskierung verwenden wollen.

Wird dabei vom Provider eine bestimmte Adresse angefordert, gibt es zwei Möglichkeiten der tatsächlichen Adreßzuweisung:

- Der Provider weist dem Router die gewünschte Adresse zu. Die Netzmaske entscheidet nun, wie viele Rechner hinter dem Router maskiert werden.
 - IP-Adresse mit voll ausgefüllter Netzmaske '255.255.255.255': Dieses ist Ihre eigene, einzige vom NIC registrierte IP-Adresse. Alle anderen Rechner im Netz haben keine im Internet gültigen Adressen und werden hinter der festen Adresse der Router maskiert.
 - IP-Adresse mit nicht voll ausgefüllter Netzmaske, z.B. '255.255.255.248': Sie haben mehrere registrierte IP-Adressen, von denen Sie eine dem Router geben. Die anderen IP-Adressen vergeben Sie fest an Geräte im Intranet, die dann über unmaskierte Verbindungen auf das Internet zugreifen können. Die anderen Geräte können trotzdem über maskierte Verbindungen ins Internet.
- Der Provider weist dem Router eine andere Adresse zu. Dann werden alle Rechner im lokalen Netz hinter der zugewiesenen Adresse maskiert.

Wie funktioniert IP-Masquerading?

Das Masquerading nutzt die Eigenschaft der Datenübertragung über TCP/IP aus, daß neben der Quell- und Ziel-Adresse auch Portnummer für Quelle und Ziel verwendet werden. Bekommt der Router nun ein Datenpaket zur Übertragung, merkt er sich die IP-Adresse und den Port des Absenders in einer internen Tabelle. Dann gibt er dem Paket seine eigene IP-Adresse und eine beliebige neue Portnummer. Diesen neuen Port trägt er ebenfalls in der Tabelle ein und leitet das Paket mit den neuen Angaben weiter.

Die Antwort auf dieses Paket geht nun an die IP-Adresse des Routers mit der neuen Absender-Portnummer. Mit dem Eintrag in der internen Tabelle kann der Router diese Antwort nun wieder dem ursprünglichen Absender zuordnen.



In den Statistiken des Routers können Sie sich diese Tabellen genau ansehen (siehe auch 'Status' im Referenz-Handbuch).

Einfaches und inverses Masquerading

Diese Maskierung funktioniert in beide Richtungen: Wenn ein Rechner aus dem LAN ein Paket ins Internet schickt, wird das lokale Netz hinter der IP-Adresse des Routers maskiert (einfaches Masquerading).

Schickt umgekehrt ein Rechner aus dem Internet ein Paket z.B. an einen FTP-Server im LAN, so sieht es für diesen Rechner so aus, als wäre der Router der FTP-Server. Der Router liest aus dem Eintrag in der Service-Tabelle die IP-Adresse des FTP-Servers im LAN (im Siemens AccessPoint Manager im Konfigurationsbereich 'TCP/IP' auf der Registerkarte 'Masq.' oder im Menü Setup/IP-Router-Modul/Masquerading/Service-Tabelle). Das Paket wird an diesen Rechner weitergeleitet. Alle Pakete, die vom FTP-Server im LAN kommen (Antworten des Servers), werden hinter der IP-Adresse des Routers versteckt.

Der kleine Unterschied:

- Beim Zugriff aus dem LAN auf das Internet hingegen wird der Eintrag in der Tabelle mit Port- und IP-Adreß-Informationen durch den Router selbst vorgenommen.
Die entsprechende Tabelle kann max. 2048 Einträge aufnehmen, also gleichzeitig 2048 Übertragungen zwischen dem maskierten und dem unmaskierten Netz ermöglichen.
Nach einer einstellbaren Zeit geht der Router jedoch davon aus, daß der Eintrag nicht mehr benötigt wird, und löscht ihn selbständig wieder aus der Tabelle.

Welche Protokolle können mit IP-Masquerading übertragen werden?

Natürlich nur solche, die auch über Ports kommunizieren. Protokolle, die ohne Portnummern arbeiten oder die oberhalb von IP im OSI-Modell Ports verwenden, können nicht ohne spezielle Behandlung maskiert werden.

In der aktuellen Version führt der Router ein Masquerading für folgende Protokolle durch:

- TCP (und alle darauf aufbauenden Protokolle wie FTP, HTTP etc.)
- UDP
- ICMP

12.9.7 DNS-Forwarding

Beim Zugriff auf das Internet werden meistens keine IP-Adressen verwendet, um einen Server zu erreichen, sondern Namen. Wer weiß auch schon, welche Adresse sich hinter 'www.domain.com' verbirgt? Der DNS-Server!

DNS heißt Domain Name Service und bezeichnet die Zuordnung von Domain-Namen (wie domain.com) zu den entsprechenden IP-Adressen. Diese Informationen müssen natürlich ständig gepflegt und immer weltweit verfügbar gehalten werden. Dazu gibt es eben diese DNS-Server, die lange Tabellen mit IP-Adressen und Domain-Namen anbieten.

Wenn nun ein Rechner aus dem Intranet eine Homepage aufrufen möchte, sendet er zunächst einen DNS-Request aus: „Welche IP-Adresse gehört zu www.domain.com?“

- Der Router sucht zunächst in seinen eigenen Einstellungen, ob ein DNS-Server eingetragen ist (in Siemens AccessPoint Manager im Konfigurationsbereich 'TCP/IP' auf der Registerkarte 'Adressen' oder im Menü /Setup/TCP-IP-Modul). Wird er dort fündig, holt er die gewünschte Information von diesem Server. Durch dieses Verfahren benötigen Sie keine Kenntnisse über die Adressen eines DNS-Servers. Außerdem wird damit die Adresse des DNS-Servers automatisch aktualisiert. Sollte z.B. der Provider, der diese Adresse mitteilt, seinen DNS-Server umbenennen, oder Sie sollten zu einem anderen Provider wechseln, erhält Ihr lokales Netz stets die aktuellen Informationen.

12.9.8 Zeitsteuerung für die Default-Route

Ähnlich dem Least-Cost-Routing (LCR) ist die Zeitsteuerung für die Default-Route eine Funktion, mit der automatisch je nach Uhrzeit der Provider mit dem günstigsten Tarif gewählt wird.

Sobald ein IP-Paket zu einer Verbindung über die Default-Route führen möchte, wird zuerst einmal nicht die in der Default-Route eingetragene Gegenstelle angewählt, sondern es wird vorher in der Zeitsteuerungstabelle geprüft, welche Gegenstelle zu benutzen ist.

In dieser Zeitsteuerungstabelle geben Sie an, an welchen Wochentagen und zu welcher Uhrzeit ein bestimmter Provider zu benutzen ist. Sobald nun ein IP-Paket einen Aufbau der Default-Route erfordert, wird zunächst geprüft, ob die Verwendung der Zeitsteuerungstabelle aktiviert ist. Anschließend wird in der Tabelle ein Eintrag gesucht, der den aktuellen Wochentag und die aktuelle Uhrzeit abdeckt. Wird ein solcher Eintrag gefunden, baut der Router eine Verbindung zu der dort eingetragenen Gegenstellen auf. Findet sich in der Zeitsteuerungstabelle kein passender Eintrag, kehrt der Router

zurück in die IP-Routing-Tabelle und verwendet die dort eingetragene Gegenstelle.

Die Einstellungen für die Zeitsteuerung der Default-Route finden Sie unter Siemens AccessPoint Manager im Konfigurationsbereich 'IP-Router' auf der Registerkarte 'Router' und bei der Konfiguration über Telnet unter setup/IP-Router-Modul. Die einzelnen Tage werden dabei in der gleichen Syntax eingetragen wie beim LCR. Die Definition der Feiertage wird ebenfalls vom LCR-Modul übernommen.

12.9.9 Policy Based Routing

Policy Based Routing bezeichnet ein Verfahren, bei dem bestimmte Datenpakete bevorzugt behandelt werden sollen. Dazu wird ein spezielles Feld innerhalb der IP-Datenpakete ausgewertet, das Type-of-Service(TOS)-Feld. Diese bevorzugte Behandlung einiger Datenpakete soll z.B. die Konfiguration der Router über das WAN erleichtern, wenn gleichzeitig viele Daten übertragen werden sollen.



Weitere Informationen zu Policy Based Routing finden Sie in der 'Beschreibung der Menüpunkte' im Referenz-Handbuch.

12.10 Automatische Adreßverwaltung mit DHCP

Für einen reibungslosen Betrieb in einem TCP/IP-Netzwerk benötigen alle Geräte in einem lokalen Netzwerk eindeutige IP-Adressen.

Zusätzlich brauchen sie noch die Adressen von DNS- und NBNS-Servern sowie eines Standard-Gateways, über das Datenpakete von lokal nicht erreichbaren Adressen geroutet werden sollen.

Bei einem kleinen Netzwerk ist es durchaus noch denkbar, allen Rechnern im Netz „von Hand“ diese Adressen einzutragen. Bei einem großen Netz mit vielen Arbeitsplatzrechnern wird das jedoch leicht zu einer unüberschaubaren Aufgabe.

In solchen Fällen bietet sich die Verwendung des DHCP (Dynamic Host Configuration Protocol) an. Über dieses Protokoll kann ein DHCP-Server in einem TCP/IP-basierten LAN den einzelnen Stationen die benötigten Adressen dynamisch zuweisen.

12.10.1 Der DHCP-Server

Der Siemens I-GATE 11M AccessPoint kann als DHCP-Server die IP-Adressen in seinem TCP/IP-Netz verwalten. Dabei teilt er den Arbeitsplatzrechnern die folgenden Parameter mit:

- IP-Adresse
- Netzmaske
- Broadcast-Adresse
- DNS-Server
- NBNS-Server
- Default-Gateway
- Gültigkeitsdauer der zugewiesenen Parameter

Der DHCP-Server entnimmt die IP-Adressen entweder aus einem frei definierten Adreß-Pool oder ermittelt die Adressen selbständig aus der eigenen IP-Adresse (oder Intranet-Adresse).

Ein völlig unkonfiguriertes Gerät kann sogar im DHCP-Automodus die IP-Adressen für sich selbst und für die Rechner im Netz selbständig festlegen.

Im einfachsten Fall müssen Sie daher nur das neue Gerät im Auslieferungszustand in einem Netz ohne andere DHCP-Server anschließen und einschalten. Der DHCP-Server regelt im Zusammenspiel mit Siemens AccessPoint Manager über einen Assistenten dann alle weiteren Adreß-Zuweisungen im lokalen Netz selbst.

12.10.2 DHCP – 'Ein', 'Aus' oder 'Auto'?

Der DHCP-Server kann drei verschiedene Zustände annehmen:

- 'Ein': Der DHCP-Server ist dauerhaft eingeschaltet. Bei der Eingabe dieses Wertes wird die Konfiguration des Servers (Gültigkeit des Adreß-Pools) überprüft.
 - Bei einer korrekten Konfiguration bietet das Gerät sich als DHCP-Server im Netz an.
 - Bei einer fehlerhaften Konfiguration (z.B. ungültige Pool-Grenzen) wird der DHCP-Server wieder abgeschaltet und wechselt in den Zustand 'Aus'.
- 'Aus': Der DHCP-Server ist dauerhaft abgeschaltet.
- 'Auto': Der Server befindet sich im Automodus. In diesem Zustand sucht das Gerät nach dem Einschalten im lokalen Netz nach anderen DHCP-Servern.

- Wird mindestens ein anderer DHCP-Server gefunden, schaltet das Gerät seinen eigenen DHCP-Server aus. Damit wird u.a. verhindert, daß ein unkonfiguriertes Gerät nach dem Einschalten im Netz Adressen vergibt, die nicht im lokalen Netz liegen.
 - Werden keine anderen DHCP-Server gefunden, schaltet das Gerät seinen eigenen DHCP-Server ein.
- Ob der DHCP-Server letztendlich ein- oder ausgeschaltet ist, kann den DHCP-Statistiken entnommen werden.
Die Default-Einstellung für den Zustand ist 'Auto'.

12.10.3 So werden die Adressen zugewiesen

Zuweisung von IP-Adressen

Damit der DHCP-Server den Rechnern im Netz IP-Adressen zuweisen kann, muß er zunächst einmal wissen, welche Adressen er für diese Zuweisung verwenden darf. Für die Auswahl der möglichen Adressen gibt es drei verschiedene Optionen:

- Die IP-Adresse kann aus dem eingestellten Adreß-Pool genommen werden (Start-Adreß-Pool bis End-Adreß-Pool). Hier können beliebige im lokalen Netz gültige Adressen eingegeben werden.
- Es verwendet dann selbst die IP-Adresse '10.0.0.254' und den Adreß-Pool '10.x.x.x' für die Zuweisung der IP-Adressen im Netz. In diesem Zustand weist der DHCP-Server den anderen Rechnern im Netz nur die IP-Adresse und deren Gültigkeit zu, nicht jedoch die anderen Informationen.

Wenn nun ein Rechner im Netz gestartet wird, der mit seinen Netzwerk-Einstellungen über DHCP eine IP-Adresse anfordert, wird ihm ein Gerät mit aktiviertem DHCP-Modul die Zuweisung einer Adresse anbieten. Als IP-Adresse wird dabei eine gültige Adresse aus dem Pool genommen. Wurde dem Rechner in der Vergangenheit bereits schon mal eine IP-Adresse zugewiesen, so fordert er eben diese Adresse wieder an, und der DHCP-Server versucht ihm diese Adresse wieder zuzuweisen, wenn sie nicht bereits einem anderen Rechner zugewiesen wurde.

Der DHCP-Server prüft zusätzlich, ob die ausgesuchte Adresse im lokalen Netz noch frei ist. Sobald die Eindeutigkeit einer Adresse festgestellt wurde, wird dem anfragenden Rechner die gefundene Adresse zugewiesen.

Zuweisung der Netzmaske

Die Zuweisung der Netzmaske erfolgt analog zur Adreßzuweisung. Wenn im DHCP-Modul eine Netzmaske eingetragen ist, wird diese bei der Zuweisung verwendet. Ansonsten wird die Netzmaske aus dem TCP/IP-Modul verwendet.

Zuweisung der Broadcast-Adresse

In der Regel wird im lokalen Netz für Broadcast-Pakete eine Adresse verwendet, die sich aus den gültigen IP-Adressen und der Netzmaske ergibt. Nur in Sonderfällen (z.B. bei Verwendung von Sub-Netzen für einen Teil der Arbeitsplatzrechner) kann es nötig sein, eine andere Broadcast-Adresse zu verwenden. In diesem Fall wird die zu verwendende Broadcast-Adresse im DHCP-Modul eingetragen.



Die Änderung der Voreinstellung für die Broadcast-Adresse wird nur für erfahrene Netzwerk-Spezialisten empfohlen.

Zuweisung von DNS- und NBNS-Server

Hierzu werden die zugehörigen Einträge aus dem 'TCP-Modul' herangezogen.

Ist bei den entsprechenden Feldern kein Server angegeben, so gibt der Router seine eigene IP-Adresse als DNS-Adresse weiter. Diese wird bestimmt, wie unter 'Zuweisung einer IP-Adresse' beschrieben. Der Router verwendet dann DNS-Forwarding (siehe auch 'DNS-Forwarding'), um DNS- oder NBNS-Anfragen des Hosts aufzulösen.

Zuweisung des Default-Gateways

Das Gerät weist dem anfragenden Rechner standardmäßig seine eigene IP-Adresse als Gateway-Adresse zu.

Falls erforderlich, kann diese Zuweisung durch die Einstellungen am Arbeitsplatzrechner überschrieben werden.

Gültigkeitsdauer einer Zuweisung

Die dem Rechner einmal zugewiesenen Adressen haben nur eine begrenzte Gültigkeit. Nach Ablauf dieser Gültigkeitsdauer darf der Rechner sie nicht mehr verwenden. Damit der Rechner die Adressen (vor allem seine IP-Adresse) danach nicht immer wieder verliert, beantragt er rechtzeitig eine Verlängerung, die ihm in der

Regel auch immer gewährt wird. Nur wenn die Gültigkeitsdauer abläuft, während der Rechner abgeschaltet ist, verliert er die Adresse.

Bei jeder Anfrage kann ein Host eine bestimmte Gültigkeitsdauer fordern. Ein DHCP-Server kann dem Host aber auch eine davon abweichende Gültigkeitsdauer zuweisen. Das DHCP-Modul bietet zwei Einstellungen, um die Gültigkeitsdauer zu beeinflussen:

- **Maximale Gültigkeit in Minuten**
Hier kann die maximale Gültigkeitsdauer eingetragen werden, die der DHCP-Server einem Host zuweist.
Fordert ein Host eine Gültigkeit an, die die maximale Dauer überschreitet, so wird ihm nur diese maximale Gültigkeit zugewiesen!
Der Defaultwert von 6000 Minuten entspricht ca. 4 Tagen.
- **Default-Gültigkeit in Minuten**
Hier kann die Gültigkeitsdauer eingetragen werden, die zugewiesen wird, wenn der Host überhaupt keine Gültigkeitsdauer anfordert. Der Defaultwert von 500 Minuten entspricht ca. 8 Stunden.

Vorfahrt für den DHCP-Server – Zuweisung anfordern

Standardmäßig sind fast alle Einstellungen in der Netzwerkumgebung von Windows so eingestellt, daß die benötigten Parameter über DHCP angefragt werden. Überprüfen Sie die Einstellungen mit einem Klick auf **Start -> Einstellungen -> Systemsteuerung -> Netzwerk**. Wählen Sie den Eintrag für 'TCP/IP' an Ihrem Netzwerkadapter, und öffnen Sie die Eigenschaften.

Auf den verschiedenen Registerkarten können Sie nun nachsehen, ob spezielle Einträge z.B. für die IP-Adresse oder das Standard-Gateway vorhanden sind. Wenn Sie alle Werte vom DHCP-Server zuweisen lassen wollen, löschen Sie nur die entsprechenden Einträge.

Vorfahrt für den Rechner – Zuweisung überschreiben

Sollte ein Rechner andere Parameter verwenden als die ihm zugewiesenen (z.B. ein anderes Standard-Gateway), so müssen diese Parameter direkt am Arbeitsplatzrechner eingestellt werden. Der Rechner ignoriert dann die entsprechenden Parameter in der Zuweisung durch den DHCP-Server.

Unter Windows geschieht das z.B. über die Eigenschaften der Netzwerkumgebung.

Klicken Sie auf **Start -> Einstellungen -> Systemsteuerung -> Netzwerk**. Wählen Sie den Eintrag für 'TCP/IP' an Ihrem Netzwerkadapter und öffnen die Eigenschaften.

Auf den verschiedenen Registerkarten können Sie nun die gewünschten Werte eintragen.

Im DHCP-Modul kann über den Punkt 'Setup/DHCP/Tabelle-DCHP' die Zuweisung von IP-Adressen an die jeweiligen Rechner überprüft (bzw. nachgeschaut) werden. Diese Tabelle zeigt die zugewiesene IP-Adresse, die MAC-Adresse, die Gültigkeitsdauer, den Namen des Rechners (falls vorhanden) sowie den Typ der Adreß-Zuweisung.

Im Feld 'Typ' wird angegeben, wie die Adresse zugewiesen wurde. Das Feld kann die folgenden Werte annehmen:

- neu
Der Rechner hat zum ersten Mal angefragt. Der DHCP-Server überprüft die Eindeutigkeit der Adresse, die dem Rechner zugewiesen werden soll.
- unbek.
Bei der Überprüfung der Eindeutigkeit wurde festgestellt, daß die Adresse bereits an einen anderen Rechner vergeben wurde. Der DHCP-Server hat leider keine Möglichkeit, weitere Informationen über diesen Rechner zu erhalten.
- stat.
Ein Rechner hat dem DHCP-Server mitgeteilt, daß er eine feste IP-Adresse besitzt. Diese Adresse darf nicht mehr verwendet werden.
- dyn.
Der DHCP-Server hat dem Rechner eine Adresse zugewiesen.

12.10.4 Konfiguration des DHCP-Servers

Bei der Konfiguration als DHCP-Server gibt es prinzipiell zwei Ausgangssituationen:

- Sie haben bisher noch kein Netzwerk eingerichtet, oder Ihr vorhandenes lokales Netz verwendet kein TCP/IP. Mit dem DHCP-Server in Ihrem neuen Siemens-Gerät können Sie auf einen Streich allen Rechnern im Netz und dem Gerät selbst IP-Adressen zuweisen.
- Sie haben auch bisher schon ein Netz mit TCP/IP, aber ohne DHCP-Server betrieben und stellen nun auf DHCP-Betrieb um.

Konfiguration mit Siemens AccessPoint Manager und den Assistenten

In beiden Situationen hilft Ihnen Siemens AccessPoint Manager mit einem Assistenten, die notwendigen Einstellungen vorzunehmen:

1. Verbinden Sie das unkonfigurierte Gerät über das Netzwerkkabel mit Ihrem lokalen Netz.
2. Schalten Sie das Gerät ein. Es findet dann zunächst keinen anderen DHCP-Server im Netz und aktiviert seine eigenen DHCP-Funktionen.
3. Falls noch nicht geschehen, installieren Sie das Protokoll 'TCP/IP' auf allen Rechnern im lokalen Netz.
 - Bei der Installation des Protokolls werden die Rechner meist standardmäßig so eingestellt, daß Sie die IP-Adresse automatisch von einem DHCP-Server beziehen wollen. Nach einem Neustart, der mit dieser Installation verbunden ist, fordern die Rechner automatisch eine IP-Adresse vom DHCP-Server an.
 - Wenn Sie das Protokoll schon installiert haben, aktivieren Sie nun die DHCP-Funktion auf allen Rechnern im lokalen Netz. Öffnen Sie dazu z.B. unter Windows 95 mit **Start -> Einstellungen -> Systemsteuerung -> Netzwerk** das Fenster zur Konfiguration der Netzwerkeigenschaften. Doppelklicken Sie den Eintrag für das Protokoll 'TCP/IP'. Aktivieren Sie die Option 'IP-Adresse automatisch beziehen'. Wechseln Sie auf die Registerkarte 'DNS-Konfiguration', und löschen Sie alle vorhandenen DNS-Adressen. Löschen Sie dann auf der Registerkarte 'Gateway' alle evtl. vorhandenen Einträge und schließen alle Fenster mit OK. Nach einem Neustart, der mit dieser Einstellung verbunden ist, fordern die Rechner automatisch eine IP-Adresse aus dem Adreß-Pool des DHCP-Servers an.
4. Installieren Sie Siemens AccessPoint Manager auf einem der Rechner im Netz.
5. Starten Sie das Programm aus der Programmgruppe 'Siemens I-Gate'. Beim Start bemerkt Siemens AccessPoint Manager, daß sich ein unkonfigurierter Router im Netz befindet, und startet den Assistenten für die Grundeinstellungen.
 - Wenn Sie bisher noch keine IP-Adressen in Ihrem Netz verwendet haben, wählen Sie in diesem Assistenten die Option 'Alle Einstellungen automatisch vornehmen', und betätigen Sie im nächsten Fenster die Schaltfläche Fertigstellen.

- Der Assistent weist dem Router nun die IP-Adresse '10.0.0.1' mit der Netzmaske '255.255.255.0' zu und schaltet den DHCP-Server ein. Aus der IP-Adresse ermittelt das Gerät dann den gültigen Adreß-Pool für die DHCP-Zuweisung.
- Wenn Sie auch vor der Umstellung auf DHCP-Betrieb IP-Adressen in Ihrem Netz verwendet haben, wählen Sie in diesem Assistenten die Option 'Ich möchte die Einstellungen selber vornehmen'. Geben Sie im nächsten Fenster eine freie IP-Adresse aus dem bisher verwendeten Adreßbereich ein, und schalten Sie den DHCP-Server ein.
- Der Assistent weist dem Gerät nun die eingestellte IP-Adresse mit der zugehörigen Netzmaske zu. Aus der IP-Adresse ermittelt das Gerät dann den gültigen Adreß-Pool für die DHCP-Zuweisung.
- Nach einigen Sekunden werden automatisch alle Rechner im Netz überprüft und erhalten ggf. eine neue IP-Adresse vom DHCP-Server. Zusätzlich werden den Rechnern dann auch die weiteren Parameter wie Broadcast-Adresse, DNS-Server, Default-Gateway etc. mitgeteilt.

Manuelle Konfiguration

Wenn die Konfiguration mit dem Assistenten von Siemens AccessPoint Manager für Sie nicht in Frage kommt, können Sie die Parameter für den DHCP-Server auch von Hand einstellen: in Siemens AccessPoint Manager im Konfigurationsbereich 'TCP/IP' auf der Registerkarte 'DHCP' oder im Menü /Setup/DHCP-Modul.

12.11 DHCP-Relay-Agent

12.11.1 Netzwerkkonfiguration über ISDN übertragen

Bei der Anbindung von einzelnen Arbeitsplatzrechnern über IP an das LAN einer Zentrale wird in der Regel die Proxy-ARP-Funktion genutzt. Dabei wird dem einwählenden Rechner eine vorher festgelegte IP-Adresse aus dem Adreßbereich der Zentrale zugewiesen.

Soll ein ganzes IP-Netzwerk einer Filiale mit mehreren Rechnern mit dem LAN der Zentrale gekoppelt werden, wird eine LAN-LAN-Kopplung realisiert. Dabei liegen die beiden Netzwerke jedoch in verschiedenen IP-Adreßkreisen.

Während innerhalb des LANs der Zentrale alle Adressen und weitere Netzwerkinformationen komfortabel über DHCP zugewiesen werden können, hört dieser Komfort bei der LAN-LAN-Kopplung auf.

12.11.2 DHCP-Informationen aus dem entfernten Netz holen

Die Funktion „DHCP-Relay-Agent“ erlaubt auch die Übertragung von DHCP-Informationen über ISDN-Leitungen. Damit wird es möglich, auch über eine ISDN-Strecke hinweg mehrere Rechner in einem Netzwerk in den IP-Adreßkreis der Zentrale einzubinden.

Dazu wird der DHCP-Server im Netz der Filiale in den Relay-Agent-Modus geschaltet. Die DHCP-Anfragen werden damit an einen anderen Server weitergeleitet, dessen Adresse fest eingetragen wird. Über einen entsprechenden Eintrag in der IP-Routing-Tabelle kommt die Verbindung zum Netz der Zentrale zustande.

Wird nun ein Rechner im Netz der Filiale gestartet, der eine IP-Adresse von einem DHCP-Server anfordert, gibt der DHCP-Relay-Agent diese Anfrage über die ISDN-Strecke an den DHCP-Server im Netz der Zentrale weiter. Dieser Server gibt dem anfragenden Rechner dann anhand der übermittelten MAC-Adresse eine vorher festgelegte IP-Adresse.

Damit sind auch schon alle notwendigen Einstellungen genannt:

1. Der DHCP-Server im Router des Filial-Netzes wird auf das Weiterleiten der DHCP-Anfragen eingestellt. Dazu wird die IP-Adresse des DHCP-Servers im LAN der Zentrale eingetragen.
2. Dieser Router muß außerdem alle Informationen zum Verbindungsaufbau mit dem Netz der Zentrale haben (normale LAN-LAN-Kopplung).
3. Im DHCP-Server in der Zentrale werden neben den üblichen Routing-Informationen alle entfernten Stationen mit MAC-Adresse und der IP-Adresse eingetragen, die ihnen zugewiesen werden sollen. Dazu wird der Name des entsprechenden Rechners eingetragen, der für den DNS-Server verwendet werden soll.

12.11.3 DHCP-Informationen anpassen

Nun werden also alle DHCP-Informationen vom DHCP-Server in der Zentrale bezogen. Das führt allerdings auch dazu, daß sich der Router in der Zentrale als Gateway für die Filiale präsentiert. Will nun ein Rechner aus der Filiale auf das Internet zugreifen, wird die Anfrage an das Gateway in der Zentrale weitergegeben. Die Internet-Verbindung läuft also über das Netz der Zentrale ab. Um diesen Umweg zu vermeiden, kann der DHCP-Relay-Agent eine Funktion nutzen, mit der die Antworten des entfernten DHCP-Servers an die Anforderungen des eigenen LANs angepaßt werden können. Netzmaske, Broadcast-Adresse und Gateway werden dann nicht mehr aus dem Netz der Zentrale bezogen.

12.11.4 Boot-Images aus dem entfernten Netz holen

Für die Anbindung von Filialnetzen, in denen keine vollständigen Arbeitsplatzrechner stehen, sondern nur Terminals ohne bootfähige Festplatten, stellt der DHCP-Server nun auch die Möglichkeit bereit, ein komplettes Boot-Image über die ISDN-Leitung zu beziehen. Damit kann die gesamte Konfiguration der Terminals an einer zentralen Stelle gepflegt und gewartet werden.

Im Netz der Filiale wird dazu der DHCP-Relay-Agent konfiguriert. Im Netz der Zentrale wird neben den Einträgen der IP-Adresse für die jeweilige MAC-Adresse auch festgelegt, welches Boot-Image zu verwenden ist. Das Boot-Image wird dabei über einen symbolischen Namen angegeben. In einer Imagetabelle wird dem symbolischen Namen ein Server zugeordnet und eine Verzeichnis- und Dateiinformaton, mit der das Boot-Image zu finden ist.

Startet nun ein Terminal im Netz der Filiale, baut es über den Router automatisch eine Verbindung zum Netz der Zentrale auf und holt von dort das aktuelle Boot-Image.

Die Einstellungen für den DHCP-Relay-Agent, den zugehörigen Server und die Boot-Images finden Sie unter Siemens AccessPoint Manager im Konfigurationsbereich 'TCP-IP' auf den registerkarten 'DHCP' und 'DHCP/BOOTP' oder bei der Konfiguration über Telnet unter setup/DHCP-Modul.

12.12 DNS

Der Domain-Name-Service (DNS) stellt in TCP/IP-Netzen die Verknüpfung zwischen Rechnernamen bzw. Netzwerknamen (Domains) und IP-Adressen her. Dieser Service ist auf jeden Fall erforderlich für die Kommunikation im Internet, um z.B. einer Anfrage nach 'www.Siemens.ch' die entsprechende IP-Adresse zurückliefern zu können. Aber auch innerhalb eines lokalen Netzes oder bei der LAN-Kopplung ist es sinnvoll, die IP-Adressen im LAN den Namen der Rechner eindeutig zuzuordnen zu können.

12.12.1 Was macht ein DNS-Server?

Die bei einem DNS-Server nachgefragten Namen bestehen aus mehreren Teilen: ein Teil besteht aus dem eigentlichen Namen des Hosts oder Dienstes, der angesprochen werden soll, ein anderer Teil kennzeichnet die Domain. Innerhalb eines lokalen Netzes ist die Angabe der Domain optional. Diese Namen können also z.B. 'www.domain.com' oder 'ftp.domain.com' heißen.

Ohne DNS-Server im lokalen Netz wird jeder lokal unbekannt Name über die DEFAULT-Route gesucht. Durch die Verwendung eines DNS-Servers können alle Namen, die mit ihrer IP-Adresse bekannt sind, direkt bei der richtigen Gegenstelle gesucht werden. Der DNS-Server kann dabei im Prinzip ein separater Rechner im Netz sein. Folgende Gründe sprechen jedoch dafür, den DNS-Server direkt im Siemens I-GATE 11M AccessPoint anzusiedeln:

- Ein Siemens I-GATE 11M AccessPoint kann in der Betriebsart als DHCP-Server die IP-Adressen für die Rechner im lokalen Netz selbständig verteilen. Der DHCP-Server kennt also schon alle Rechner im eigenen Netz, die ihre IP-Adresse per DHCP beziehen, mit Rechnername und IP-Adresse. Ein externer DNS-Server hätte bei der dynamischen Adreßvergabe des DHCP-Servers möglicherweise Schwierigkeiten, die Zuordnung zwischen IP-Adresse und Namen aktuell zu halten.
- Beim Routing von Windows-Netzen über NetBIOS kennt ein Siemens I-GATE 11M AccessPoint außerdem die Rechnernamen und IP-Adressen in den anderen angeschlossenen NetBIOS-Netzen. Außerdem melden sich auch die Rechner mit fest eingestellter IP-Adresse ggf. in der NetBIOS-Tabelle an und sind damit mit Namen und Adressen bekannt.

- Der DNS-Server im Siemens I-GATE 11M AccessPoint kann gleichzeitig als sehr komfortabler Filtermechanismus eingesetzt werden. Anfragen nach bestimmten Domains, die nicht besucht werden dürfen, können durch die einfache Angabe des Domain-Namens für das ganze LAN, nur für Teilnetze (Subnetze) oder sogar für einzelne Rechner gesperrt werden.

Der DNS-Server bezieht bei Anfragen nach bestimmten Namen alle Informationen in die Suche mit ein, die ihm zur Verfügung stehen:

- Zuerst prüft der DNS-Server, ob der Zugriff auf diesen Namen nicht durch die Filterliste verboten ist. Wenn das der Fall ist, wird der anfragende Rechner mit einer Fehlermeldung darüber informiert, daß er auf diesen Namen nicht zugreifen darf.
- Dann sucht er in der eigenen, statischen DNS-Tabelle nach Einträgen für den entsprechenden Namen.
- Steht in der DNS-Tabelle kein Eintrag für diesen Namen, wird die dynamische DHCP-Tabelle durchsucht. Die Verwendung der DHCP-Informationen kann bei Bedarf ausgeschaltet werden.
- Findet der DNS-Server in den vorausgegangenen Tabellen keine Informationen über den Namen, werden die Listen des NetBIOS-Moduls durchsucht. Auch die Verwendung der NetBIOS-Informationen kann bei Bedarf ausgeschaltet werden.

Sollte der gesuchte Name in allen verfügbaren Informationen nicht gefunden werden, leitet der DNS-Server die Anfrage über den normalen DNS-Forwarding-Mechanismus an einen anderen DNS-Server (z.B. beim Internet-Provider) weiter oder schickt dem anfragenden Rechner eine Fehlermeldung.

12.12.2 So stellen Sie den DNS-Server ein

Die Einstellungen für den DNS-Server finden Sie in Siemens AccessPoint Manager im Konfigurationsbereich 'TCP/IP' auf der Registerkarte 'DNS-Server'. Gehen Sie zur Einstellung des DNS-Servers wie folgt vor:

- a) Schalten Sie den DNS-Server ein.
set setup/dns-modul/zustand ein
- b) Geben Sie die Domain ein, in der sich der DNS-Server befindet. Mit Hilfe dieser Domain erkennt der DNS-Server bei Anfrage, ob sich der gesuchte Name im eigenen LAN befindet oder nicht. Die Angabe der Domain ist optional.
set setup/dns-modul/domain ihredomain.de

- c) Geben Sie an, ob die Informationen aus dem DHCP-Server und dem NetBIOS-Modul verwendet werden sollen.

```
set setup/dns-modul/dhcp-verwenden ja
set setup/dns-modul/NetBIOS-verw. ja
```

- d) Der DNS-Server dient hauptsächlich dazu, Anfragen nach Namen im Internet von den Anfragen nach Namen bei anderen Gegenstellen zu trennen. Tragen Sie daher alle Rechner in die DNS-Tabelle ein,

- deren Name und IP-Adresse Sie kennen,
- die nicht im eigenen LAN liegen,
- die nicht im Internet liegen und
- die über den Router erreichbar sind.

Wenn Sie z.B. in einem externen Büro arbeiten und über den Router den Mailserver in der Zentrale (Name: mail.ihredomain.de, IP: 10.0.0.99) erreichen wollen, tragen Sie ein:

```
cd setup/dns-modul/dns-tabelle
set mail.ihredomain.de 10.0.0.99
```

Die Angabe der Domain ist dabei optional, aber zu empfehlen. Wenn Sie nun das Mailprogramm starten, wird es vermutlich automatisch den Server 'mail.ihredomain.de' suchen. Der DNS-Server gibt daraufhin die IP-Adresse '10.0.0.99' zurück. Das Mailprogramm sucht dann nach dieser IP-Adresse. Mit entsprechenden Einträgen in IP-Routing-Tabelle und Namenliste etc. wird dann automatisch die Verbindung zum Netz in der Zentrale hergestellt, wo der Mailserver schließlich gefunden wird.

- e) Mit der Filterliste können Sie schließlich ganz genau bestimmen, wer auf welche Namen oder Domains nicht zugreifen darf.

```
cd setup/dns-modul/filter-liste
set 001 www.gesperrte-domain.de 0.0.0.0 0.0.0.0
```

Mit diesem Eintrag (mit dem Index '001') sperren Sie diese Domain für alle Rechner im lokalen Netz. Der Index '001' ist frei gewählt und dient lediglich der Übersichtlichkeit. Bei der Eingabe der Domain sind auch die Wildcards '?' (steht für genau ein Zeichen) und '*' (für beliebig viele Zeichen) erlaubt. Wenn nur ein bestimmter Rechner (z.B. mit IP 10.0.0.123) nicht auf DE-Domains zugreifen können soll, tragen Sie ein:

```
set 002 *.de 10.0.0.123 255.255.255.255
```



Die Hitliste in der DNS-Statistik zeigt Ihnen die 64 Namen, die am häufigsten nachgefragt werden, und bietet Ihnen damit eine gute Basis für die Einstellung der Filter-Liste.

Durch die geeignete Wahl von IP-Adressen und Netzmasken können bei der Verwendung von Subnetting in Ihrem LAN auch einzelne Abteilungen gefiltert werden. Dabei steht die IP-Adresse '0.0.0.0' jeweils für alle Rechner in einem Netz, die Netzmaske '0.0.0.0' für alle Netze.

12.13 NetBIOS-Proxy

Mit der Funktion als NetBIOS-Proxy kann ein Siemens I-GATE 11M AccessPoint auch NetBIOS-Pakete routen oder als Proxy lokal beantworten. Damit ergibt sich die Möglichkeit, u.a. Windows-Netze über die Routerfunktionen kostengünstig zu verbinden.

Dieser Abschnitt beschreibt die Funktion von NetBIOS-Proxy allgemein und die Konfiguration des Routers und der beteiligten Rechner für die Verbindung von Windows-Netzen.

12.13.1 Kurz und bündig: Was ist NetBIOS?

NetBIOS dient dazu, mehrere Rechner einfach und unkompliziert zu vernetzen. Ein wichtiger Vertreter eines NetBIOS-Netzes ist das Windows-Netz, über das sich mehrere Windows-3.11-, -9x- und -NT-Rechner einfach vernetzen lassen, und in dem die Ressourcen der jeweiligen Rechner (Laufwerke oder Drucker) für alle anderen freigegeben werden können.

In einem Windows-Netz werden die Rechner nur über ihre Namen angesprochen. Mehrere Rechner können zu Gruppen und mehrere Gruppen zu Namenräumen (Scopes) zusammengefaßt werden. Damit ein Rechner auf die Ressourcen der anderen zugreifen kann, müssen die verwendeten Namen im ganzen Netz bekannt sein. Damit nun nicht auf jedem Rechner eine Tabelle der bekannten Namen gepflegt werden muß, geben NetBIOS-Rechner ihre Namen selbständig in regelmäßigen Abständen im Netz bekannt.

Die so bekanntgemachten Namen sollen natürlich auch an einer zentralen Stelle im Windows-Netz gesammelt und bereitgestellt werden. Wenn zwei Windows-Netze über Router gekoppelt werden sollen, muß auf beiden Seiten der Verbindung eine solche Namensammelstelle, ein NetBIOS-Nameserver (NBNS) vorhanden sein.

- Dazu kann z.B. ein eigener WINS-Server (Windows-Internet-Name-Service-Server) im Netz installiert sein.

- Da viele Windows-Netze aber eben ohne eigene Server auskommen wollen oder müssen, bietet sich eine zweite Möglichkeit an: Die Informationen über die verwendeten Namen können auch an einer Art „schwarzem Brett“ gesammelt werden, an dem alle Rechner nur ihren Namen und ihre IP-Adresse hinterlassen. Dabei sind die Rechner selbst für die Konsistenz der Namen im Netz verantwortlich.

Ein Siemens I-GATE 11M AccessPoint verfügt über ein solches schwarzes Brett. Durch diese einfache Realisierung des NBNS ist die Verbindung auch von Windows-Netzen ohne Server möglich. Die Rechner in den verbindungswilligen Netzen geben ihre Namen nun auch im jeweils anderen Netz bekannt und füllen auch dort das schwarze Brett.

12.13.2 **Behandlung von NetBIOS-Paketen**

Das äußerst gesprächige Verhalten der Windows-Rechner kann bei der Verbindung über Wählleitungen hohe Gebühren verursachen, da jedes NetBIOS-Paket mit Namensinformationen automatisch zum Verbindungsaufbau führt (z.B. zum bereits eingerichteten ISP). Durch diese Pakete bleibt die Leitung ständig aufgebaut und es fallen entsprechend hohe Gebühren an, ohne daß wirklich eine Nutzdatenübertragung stattfindet.

Um diesen unnötigen Verbindungsaufbau zu vermeiden, kann ein Siemens I-GATE 11M AccessPoint die NetBIOS-Pakete entweder routen oder als Proxy selbst beantworten:

- Zum Routen der wirklich benötigten Pakete kann im NetBIOS-Modul festgelegt werden, an welche Gegenstellen die Namensinformationen über NetBIOS übertragen werden sollen. Beim Einschalten des NetBIOS-Moduls wird nach einer zufälligen Wartezeit eine Verbindung zu den NetBIOS-Gegenstellen aufgebaut (sofern es sich nicht um einzelne Remote-Access-Rechner handelt). Gelingt der Aufbau nicht, so wird die Spanne der Wartezeit vergrößert. Mit dem anschließenden Austausch der NetBIOS-Informationen wird so erstmalig das schwarze Brett gefüllt.
- In der Funktion als Proxy beantwortet das Gerät Anfragen an die Rechner, die im NetBIOS-Modul (am schwarzen Brett) schon bekannt sind, selbst als Stellvertreter des entsprechenden Rechners. Sowohl bei Nachfragen nach Rechnern im eigenen LAN als auch nach bekannten Rechnern im Netz auf der Ge-

genseite werden also nach dem ersten Informationsaustausch keine neuen Verbindungen aufgebaut.

Damit die Anfragen nach Rechnern, die weder im eigenen LAN noch bei den festgelegten NetBIOS-Gegenstellen zu finden sind, nicht zum Verbindungsaufbau über die DEFAULT-Route ins Internet führen, fängt der voreingestellte IP-Filter für NetBIOS-Ports diese Pakete ab und verhindert den Verbindungsaufbau.

12.13.3 Welche Voraussetzungen müssen erfüllt sein?

Für die einwandfreie Kommunikation von Windows-Netzen über Router müssen einige Komponenten auf den beteiligten Rechnern installiert sein und verschiedene Einstellungen im Betriebssystem vorgenommen werden.

Installierte Komponenten

Die Installation der benötigten Komponenten wird hier am Beispiel von Windows 95 bzw. Windows 98 beschrieben, läuft aber unter Windows 2000 und Windows NT 4.0 ähnlich ab. Installieren Sie die folgenden Komponenten auf allen Rechnern in den zu verbindenden Windows-Netzen:

- Netzwerkprotokoll
- NetBIOS ist völlig unabhängig vom verwendeten Transportprotokoll. So kann ein NetBIOS-Netzwerk über die Protokolle NetBEUI (NetBIOS Extended User Interface), IPX (Internet Packet eXchange, Novell) oder IP (Internet-Protokoll) übertragen werden.



Im Gegensatz zu IPX und IP ist NetBEUI nicht routbar, also nur in einem Windows-Netz verfügbar. Sollen mehrere Windows-Netze über Router verbunden werden, so muß NetBIOS auf einem routbaren Protokoll, z.B. im Siemens I-GATE 11M AccessPoint auf IP aufsetzen!

Das Routing von NetBIOS-Paketen im Siemens I-GATE 11M AccessPoint basiert aufgrund der besseren Filtermechanismen auf TCP/IP. Dieses Protokoll muß also auf allen Rechnern, die gekoppelt werden sollen, installiert sein.

Um das Netzwerkprotokoll zu installieren, klicken Sie **Start -> Einstellungen -> Systemsteuerung -> Netzwerk -> Hinzufügen -> Protokoll**. Wählen Sie 'Microsoft' als Hersteller und 'TCP/IP' als Netzwerkprotokoll aus.

- **Client**
Der Client für Windows-Netzwerke wird benötigt, damit sich die Rechner im Windows-Netz mit Name und Paßwort anmelden können.
Um den Client zu installieren, klicken Sie **Start -> Einstellungen -> Systemsteuerung -> Netzwerk -> Hinzufügen -> Client**. Wählen Sie 'Microsoft' als Hersteller und dann den 'Client für Windows-Netzwerke' aus.
- **Dienst**
Die Datei- und Druckerfreigabe ermöglicht das Freigeben von Laufwerken oder Druckern für andere Benutzer im Windows-Netz.
Um die Datei- und Druckerfreigabe zu installieren, klicken Sie **Start -> Einstellungen -> Systemsteuerung -> Netzwerk -> Hinzufügen -> Dienst**. Wählen Sie 'Microsoft' als Hersteller und dann den 'Datei- und Druckerfreigabe für Windows-Netzwerke' aus.

Einstellungen im Windows-Netzwerk

- **Namen und Gruppenbezeichnung**
Klicken Sie auf **Start -> Einstellungen -> Systemsteuerung -> Netzwerk**, und wechseln Sie auf die Registerkarte Identifikation.
Der Name des Rechners muß eindeutig sein. Das gilt für alle Windows-Netze und alle in diesen Netzen vorhandenen Gruppen, die Sie über NetBIOS verbinden wollen. Auch in verschiedenen Gruppen darf ein Name also nicht mehrfach auftauchen.
- **Datei- und Druckerfreigabe**
Prüfen Sie nach der Installation, ob die Datei- und Druckerfreigabe aktiviert ist. Klicken Sie dazu **Start -> Einstellungen -> Systemsteuerung -> Netzwerk -> Datei- und Druckerfreigabe**. Wählen Sie aus, ob die anderen Benutzer im Windows-Netz den Drucker und/oder die Dateien von diesem Rechner nutzen können.
Alle Benutzer, die auf die freigegebenen Ressourcen zugreifen wollen, müssen sich beim Start von Windows mit Name und Paßwort anmelden.
Klicken Sie dann im Explorer mit der rechten Maustaste die Laufwerke, Ordner oder Drucker, die Sie für die Benutzung durch andere Netzteilnehmer freigeben wollen, und wählen Sie den Punkt Freigabe aus dem Kontextmenü.

Geben Sie dem freigegebenen Ordner einen Namen und tragen Sie ggf. einen Kommentar ein. Mit der Auswahl des Zugriffstyps und der Festlegung der Kennwörter stellen Sie ein, wie der Zugriff auf die freigegebenen Ressourcen erfolgen kann.



Ob die Einstellungen im Windows-Netzwerk korrekt erfolgt sind, können Sie leicht prüfen: Der eigene Rechner muß in der Netzwerkumgebung mit seinem Namen angezeigt werden.

12.13.4 So verbinden Sie zwei Windows-Netze

Nachdem alle Vorbereitungen abgeschlossen sind, können Sie nun zwei Windows-Netze verbinden. Die Einstellungen für Arbeitsgruppennetze und Domänen-Netze (Windows NT) sind dabei ähnlich. Die folgenden Schritte sind für beide Seiten der Verbindung auszuführen.

- a) Stellen Sie die beiden Netze für eine LAN-LAN-Kopplung über TCP/IP ein. Verwenden Sie dazu nach Möglichkeit den komfortablen Assistenten von Siemens AccessPoint Manager.
- b) Prüfen Sie die Einstellung der IP-Filter. Dieser Filter muß alle NetBIOS-Pakete erfassen, die über die DEFAULT-Route geschickt werden sollen, damit NetBIOS-Pakete nicht zum Verbindungsaufbau über die DEFAULT-Route führen. Im Auslieferungszustand der Geräte ist dieser Filter so voreingestellt:
- c) Tragen Sie dann die Gegenstelle für das Routing über NetBIOS ein. Wechseln Sie in Siemens AccessPoint Manager in den Konfigurationsbereich 'NetBIOS', und erstellen Sie einen neuen Eintrag in der Tabelle 'NetBIOS über IP-Routing'.
Bei der Konfiguration über Telnet geben Sie alternativ ein:

```
cd /Setup/NetBIOS-Modul/Gegenstellen-Tab.
set nhamel.mobil router
```

Der Eintrag im Feld 'Typ' gibt an, ob die Gegenstelle nach dem Einschalten des NetBIOS-Moduls direkt angewählt werden soll, um die Namens-Informationen auszutauschen.



Der Parameter 'NT-Domain' kann bei Windows-95- oder Windows-98-Netzen i.d.R. frei gelassen werden. Beim Zugriff auf Windows-NT-Maschinen muß die entsprechende Domain bzw. Arbeitsgruppe manuell eingetragen werden.

- d) Verwendet die NetBIOS-Kopplung eine PPP-Verbindung, müssen Sie in der PPP-Liste die Aktivierung von NetBIOS für den entsprechenden Eintrag prüfen.
- e) Wenn alle Gegenstellen eingetragen sind, aktivieren Sie die NetBIOS-Funktion.
`cd /Setup/NetBIOS-Modul`
`set zustand ein`
 Nach dem Einschalten wird (nach einer zufälligen Wartezeit) eine Verbindung zu allen Gegenstellen aufgebaut, die nicht als Einwahl-Knoten gekennzeichnet sind. Bei dieser ersten Verbindung werden dann die notwendigen Informationen über die Rechner in den Netzen ausgetauscht. Erst danach kann auf die Rechner der Gegenseite zugegriffen werden.

12.13.5 So wählt sich ein Remote-Access-Rechner ein

Der Zugriff von einzelnen, entfernten Rechner über Remote-Access auf ein Windows-Netz ist ebenfalls schnell erledigt.

- a) Siemens I-GATE 11M AccessPoint und Remote-Access-Rechner werden auf den Netz-Zugriff vorbereitet. Auch in diesem Fall sind die IP-Filter im Siemens I-GATE 11M AccessPoint zu prüfen (siehe 'So verbinden Sie zwei Windows-Netze').
- b) Wenn die Zuweisung der IP-Adresse für die remote Gegenstelle aus dem IP-Pool realisiert wird, muß für diese Gegenstelle zusätzlich eine Route in der IP-Routing-Tabelle angelegt werden.
- c) Erstellen Sie auch für die remoten Gegenstellen einen Eintrag in der NetBIOS-IP-Routing-Tabelle.
`cd /Setup/NetBIOS-Modul/Gegenstellen-Tab.`
`set nhamel.ras workstation`



Kennzeichnen Sie diesen Eintrag auf jeden Fall als 'einzelne Station', damit diese Gegenstelle nach dem Einschalten des NetBIOS-Moduls nicht automatisch angerufen wird.

- d) Verwendet die NetBIOS-Kopplung eine PPP-Verbindung, müssen Sie in der PPP-Liste die Aktivierung von NetBIOS für den entsprechenden Eintrag prüfen.

12.13.6 Gesucht – Gefunden: Die Netzwerkumgebung

Wenn alle Beteiligten auf das NetBIOS-Routing vorbereitet sind, kann das Windows-Networking losgehen.

NetBIOS-Routing über LAN-LAN-Kopplung

Nachdem die Netze nach dem Einschalten der NetBIOS-Module gegenseitig die Informationen über die verfügbaren Rechner ausgetauscht haben, ist im Siemens I-GATE 11M AccessPoint nun eine Liste mit diesen Rechnernamen verfügbar. Über Telnet kann mit

```
dir /Setup/NetBIOS-Modul/host-liste
```

die Liste mit den aktuell erreichbaren Rechnern aufgerufen werden, die z.B. so aussieht:

Name	Typ	IP-Adresse	Gegenstelle	Time-out	Flags
DOKUNOTE-BOOK	00	10.10.0.53	NHAMEL.MOBIL	4939	0020
DOKUNOTE-BOOK	20	10.10.0.53	NHAMEL.MOBIL	4939	0020
Siemens	1d	10.10.0.53	NHAMEL.MOBIL	4939	0020
Siemens.DO-KU	1d	10.1.253.246	4935	0000	
Siemens.DO-KU	1d	192.168.100.162	4997	0000	
NHAMEL.MOBIL	00	10.10.0.1	NHAMEL.MOBIL	0	0020

Tab. 12.6 NetBIOS-Routing über LAN-LAN Kopplung

Aus dieser Tabelle können Sie nun ablesen, daß z.B. der Rechner mit dem Namen 'DOKUNOTEBOOK' mit der IP-Adresse '10.10.0.53' über die Gegenstelle 'NHAMEL.MOBIL' zu erreichen ist. Die weiteren Parameter werden in der Menü-Beschreibung erläutert.

Um auf die freigegebenen Ressourcen dieses Rechners zugreifen zu können, lassen Sie einfach den Explorer nach dem entsprechenden Rechner suchen mit **Start -> Suchen -> Computer**:



Die Arbeitsgruppen und Rechner des entfernten Netzes können aus technischen Gründen nicht über die Funktion 'gesamtes Netzwerk durchsuchen' in der Windows-Netzwerkumgebung gefunden werden. Stattdessen kann nach entfernten Computern wie oben beschrieben gesucht werden, bzw. es können Verknüpfungen und Laufwerksverbindungen eingerichtet werden.

NetBIOS-Routing über RAS-Zugang

Etwas anders sieht das Verfahren beim Zugang zum Windows-Netz über RAS (Remote Access) aus. Die beiden grundlegenden Unterschiede zur LAN-LAN-Kopplung:

- Auf der Seite des Einwahl-Knotens ist keine Host-Liste vorhanden, aus der die verfügbaren Rechner im Windows-Netz auf der Gegenseite abgelesen werden könnten. Der RAS-Benutzer muß also die Namen der Rechner kennen, auf die er zugreifen darf und will.
- Die Verbindung wird nicht automatisch aufgebaut. Der RAS-Benutzer muß also erst eine Verbindung über das DFÜ-Netzwerk zum Siemens I-GATE 11M AccessPoint herstellen.

Wenn die Verbindung dann steht, kann er genau wie bei der LAN-LAN-Kopplung (über **Suchen -> Computer**, nicht über die Netzwerkumgebung!) die Computer im anderen Netz suchen und darauf zugreifen.

12.14 Der Least-Cost-Router

Seit der Liberalisierung des Telefonmarktes in der Schweiz und in Europa stehen dem Benutzer von Telekommunikationsdiensten eine Reihe von Providern (Netzbetreiber) mit z.T. verschiedenen Tarifen zur Auswahl. Die Provider unterscheiden sich außerdem danach, ob man fest mit diesem Anbieter verbunden ist und automatisch immer dessen Netz verwendet (Preselection) oder ob man sich bei jedem Anruf frei entscheidet, welchen Provider man nutzen möchte (Call-by-Call). Um eine Verbindung über einen Call-by-Call-Provider aufzubauen, wählt man nach dem Abheben zunächst die passende Vorwahl, um in das entsprechende Leitungsnetz zu kom-

men. Erst nach dieser Netzkennziffer wählt man die normale Telefonnummer, um seine Gegenstelle zu erreichen.

Für Telefonate zu bestimmten Tageszeiten und in verschiedenen Regionen ist der jeweils günstigste Tarif jedoch leider nicht bei immer demselben Provider, sondern oft bei verschiedenen Anbietern zu finden: morgens Provider 1, nachmittags Provider 2 und für Auslandsgespräche evtl. Provider 3. Um immer besonders günstig zu telefonieren, im Internet zu surfen oder Daten zu anderen Netzen zu übertragen, müßten Sie nun eigentlich vor jeder Verbindung überlegen, welcher Tarif nun gerade der günstigste ist. Ein Siemens I-GATE 11M AccessPoint nimmt Ihnen diese Arbeit ab. Least-Cost-Routing (LCR) heißt die Funktion, die hier hilft. Sie definieren dabei einmal, welche Provider für Ihre Bedürfnisse die günstigsten Tarife haben, und das Gerät wählt bei jeder Verbindung (egal ob über Router, CAPI etc.) automatisch den Anbieter mit dem günstigsten Tarif.

12.14.1 So arbeitet der Least-Cost-Router im I-GATE 11M AccessPoint

Der LCR analysiert die Ziffern, die z.B. vom Router oder der CAPI gewählt werden.

Nach jeder Ziffer wird im Gerät überprüft, ob in der LCR-Tabelle eine eindeutige Übereinstimmung mit der bisher gewählten Nummer (Vorwahl) zu finden ist. Wird ein passender Eintrag gefunden, der zudem für die aktuelle Uhrzeit und das aktuelle Datum gültig ist, dann wird die Netzkennzahl für die Umleitung der Verbindung noch vor der Vorwahl eingefügt. Erst wenn die Rufnummer auf diese Weise vervollständigt wurde, wird sie nach außen an die Vermittlungsstelle weitergegeben.

Der LCR benötigt also folgende Eingaben:

- Ein Wählpräfix (Vorwahl), das bestimmt, welche Rufe für eine Umleitung in Frage kommen.
- Eine oder mehrere Netzkennzahlen, die den Provider bestimmen, der für dieses Wählpräfix genutzt werden soll.
- Die Wochentage und Feiertage, für die der Eintrag gültig ist.
- Die Tageszeit, zu der dieser Eintrag gültig ist.

Die ersten Versuche

Mit einigen wenigen Einträgen können Sie schon eine Menge an Gebühren sparen. An einem einfachen Beispiel wollen wir die Programmierung des LCRs erläutern.

Sie wissen z.B., daß man insbesondere bei Fern- oder Auslandsverbindungen mit dem Call-by-Call-Verfahren sparen kann. Sie haben sich außerdem bei einigen Call-by-Call-Anbietern (CbC) erkundigt und haben die jeweils günstigsten Tarife herausgesucht. Die ersten Einträge in der LCR-Tabelle sehen dann z.B. folgendermaßen aus:

Wählpräfix	Netzkennzahl des CbC	Wochentage	Tageszeit
01	10753	Sa + So	0:00h bis 23:59h
01	10781	Mo + Di + Mi + Do + Fr	8:00h bis 18:00h
00	10753	So	0:00h bis 23:59h

Tab. 12.7 Least-Cost-Routing

Diese Einträge bedeuten, daß alle Verbindungen am Wochenende nach Zürich (oder andere Nummern, die mit '01' beginnen) über den Provider mit der Netzkennzahl '10753' geführt werden. Wochentags wird für diese Rufe in der Zeit zwischen 8:00 Uhr und 18:00 Uhr der Provider mit der Netzkennzahl '10781' verwendet. Auslandsgespräche am Sonntag gehen über den Provider mit der Netzkennzahl '10753'.

Für Fortgeschrittene: LCR mit System

Im ersten Beispiel haben Sie gesehen, daß Sie bereits mit wenigen Einträgen Gebühren sparen können. Wenn Sie das Least-Cost-Routing optimal nutzen möchten, müssen Sie sich zunächst genau über die Tarifstruktur der Call-by-Call-Anbieter informieren, die für Sie in Frage kommen. Anschließend überlegen Sie, wie die Tarife und Tarifzonen am besten auf die LCR-Tabelle im Siemens I-GATE 11M AccessPoint abgebildet werden können. Dazu gibt es verschiedene Ansätze:

Im ersten Beispiel haben Sie gesehen, daß Sie bereits mit wenigen Einträgen Gebühren sparen können. Wenn Sie das Least-Cost-Routing optimal nutzen möchten, müssen Sie sich zunächst genau

über die Tarifstruktur der Call-by-Call-Anbieter informieren, die für Sie in Frage kommen. Anschließend überlegen Sie, wie die Tarife und Tarifzonen am besten auf die LCR-Tabelle im Siemens I-GATE 11M AccessPoint abgebildet werden können. Dazu gibt es verschiedene Ansätze:

- Eindeutige Sparmöglichkeiten können Sie direkt eintragen: '00' für Auslandsverbindungen
- Mit einer einzigen '0' werden zunächst alle Verbindungen umgeleitet, die mit der Null beginnen. Da es aber i.d.R. angrenzende Ortsnetze gibt, deren Nummer ebenfalls mit '0' beginnt, die aber trotzdem als Ortsgespräch berechnet werden, sollten Sie diese Vorwahlen separat aufführen und die Umleitung wieder aufheben. Denken Sie bei dieser Strategie auch an Sonderrufnummern wie '0800', '0190' etc.
- Eine andere Strategie zielt auf die möglichst vollständige Regelung der Umleitungen ab. Dabei beginnen Sie mit den Vorwahlen des Ortsbereiches und definieren dann die größeren Zonen. Die nahen und damit günstigeren Tarifzonen werden dabei mit längeren Wahlpräfixen festgelegt, die verbleibenden, weiter entfernten Tarifzonen werden mit wenigen Ziffern erfaßt.

Diese Einstellung können Sie bei Bedarf natürlich weiter verfeinern und ausbauen. Hier einige Anregungen, was Sie dabei beachten können:

- Einige Ortsnetze erreichen Sie zwar über eine Vorwahl, trotzdem aber zum normalen Ortstarif. Falls Sie diese Bereiche mit einem allgemeinen Eintrag umgeleitet haben, können Sie die Vorwahlen mit Ortstarif über die Vorwahl Ihrer Telefongesellschaft umleiten. Ein leerer Eintrag für die Netzkennzahl bedeutet ebenfalls „keine Umleitung“.
- Vielleicht geht der größte Teil Ihrer ISDN-Verbindungen in die gleichen Ortsnetze. Wenn die meisten Ihrer Gegenstellen in München liegen, können Sie diese Gegenstellen über einen bestimmten Anbieter erreichen.
- Untersuchen Sie die verschiedenen Tarifzonen. Welche Vorwahlen in welche Zone gehören, können Sie z.B. unter www.bil-liger-telefonieren.de im Internet nachsehen.

Wenn Sie die Vorwahlen gefunden haben, die Sie umleiten möchten, können Sie an die Zuweisung der Call-by-Call-Provider gehen. Dazu brauchen Sie natürlich die aktuellen Tarife möglichst aller Telefongesellschaften. Auch hier hilft das Internet. Adressen wie z.B.

'www.billiger-telefonieren.de' oder 'www.focus.de' verraten Ihnen tagesaktuell die Preise für alle denkbaren Verbindungen. Mit diesen Informationen können Sie sich nun daran machen, Ihren Least-Cost-Router zu füttern ...

12.14.2 So stellen Sie den Least-Cost-Router ein

Zur Einstellung des Least-Cost-Routers sind im wesentlichen zwei Fragen zu klären:

- Welche Betriebsarten im Siemens I-GATE 11M AccessPoint sollen die Dienste des Least-Cost-Routers nutzen?
- Welche Rufe sollen wann über welchen Provider geführt werden?

Um diese Fragen zu beantworten, gehen Sie so vor:

- a) Wechseln Sie im Siemens AccessPoint Manager im Konfigurationsbereich 'Least-Cost-Router' auf die Registerkarte 'Allgemein'.
- b) Aktivieren Sie die Funktion des Least-Cost-Routers. Der Least-Cost-Router läßt sich nur dann aktivieren, wenn die Zeit des Geräts entweder manuell gesetzt wurde oder wenn schon einmal eine gültige Zeit aus dem ISDN-Netz übermittelt wurde (siehe auch 'Die Uhrzeit für die Auswahl' weiter unten). Schalten Sie den LRC je nach Bedarf für die folgenden Betriebsarten ein:
 - Router
 - CAPI



Wenn Sie das Least-Cost-Routing auch für die Router-Module eingeschaltet haben, werden ggf. auch Verbindungen über Provider aufgebaut, die keine Gebühreninformationen übertragen! Die Gebührenüberwachung geht damit evtl. unbemerkt verloren. Verwenden Sie in diesem Fall alternativ die Zeitbudgets.

- c) Wechseln Sie auf die Registerkarte 'Zeiten und Feiertage'. Öffnen Sie die Least-Cost-Tabelle, fügen Sie einen neuen Eintrag hinzu, und geben Sie die benötigten Daten ein:
 - Welche Vorwahl soll umgeleitet werden?
 - Über welche Provider soll diese Vorwahl umgeleitet werden? Wenn Sie hier mehrere Netzkennzahlen durch Semikola getrennt eintragen, wechselt der LCR automatisch zur nächsten Vorwahl, wenn eine vorherige besetzt ist.

- An welchen Tagen und zu welchen Uhrzeiten soll die Umleitung aktiv sein? Beachten Sie bitte, daß keine tagesübergreifenden Uhrzeiten (18:00 Uhr bis 6:00 Uhr) möglich sind!
 - Soll der Anruf über die normale Telefongesellschaft geführt werden, wenn alle Call-by-Call-Leitungen besetzt sind? Wenn der 'automatische Rückfall' ausgeschaltet ist, beginnt der LCR ggf. nach der letzten Netzkennzahl wieder mit der ersten ...
- d) Wenn Sie in der LCR-Tabelle auch Einträge für Feiertage gemacht haben, öffnen Sie anschließend die Liste der Feiertage. Tragen Sie jeden Feiertag mit dem vollständigen Datum ein (TT.MM.JJJJ).
- e) Kontrollieren Sie die interne Uhr des Geräts (inkl. Datum), damit der LCR auch zur richtigen Zeit die Umleitungen aktiviert (siehe auch weiter unten, 'Die Uhrzeit für die Auswahl').



Bauen Sie Ihre LCR-Tabelle schrittweise auf, und überprüfen Sie jeweils das Ergebnis. Öffnen Sie dazu z.B. den Siemens AccessPoint Monitor und starten Sie über die Siemens CAPI Verbindungen zu Gegenstellen, die der Tabelle nach umgeleitet werden sollten. Anhand der gewählten Rufnummer können Sie leicht ablesen, ob die Einstellung des LCRs Ihren Wünschen entspricht. Für Routerverbindungen können Sie die gewählte Nummer aus dem Logfile ablesen (AccessPoint Monitor: **Gerät -> Eigenschaften -> Protokoll -> Anzeigen**).

Die Uhrzeit für die Auswahl

Damit der Least-Cost-Router mit Hilfe der Tabelleneinträge tatsächlich die richtige Verbindung auswählt, muß die interne Uhr im Siemens I-GATE 11M AccessPoint natürlich immer auf dem aktuellen Stand sein. Aber auch hier hilft sich der Router selbst: Er kann entweder bei jedem Verbindungsaufbau oder bei jedem Einschalten des Geräts die interne Uhrzeit mit der aktuellen Zeit im ISDN-Netz abgleichen.

- a) Wechseln Sie im Siemens AccessPoint Manager im Konfigurationsbereich 'Management' auf die Registerkarte 'Datum/Zeit'.
- b) Aktivieren Sie ggf. die Option für den automatischen Zeitabgleich bei jedem Verbindungsaufbau. Falls Sie die Zeit lieber manuell eintragen möchten, schalten Sie diese Option aus.
- c) Beim Ausschalten verliert das Gerät die aktuelle Zeit. Geben Sie die Rufnummer einer beliebigen Gegenstelle ein, wenn das Gerät direkt nach dem Einschalten eine Verbindung aufbauen

und so die Zeit mit dem ISDN-Netz abgleichen soll. Wählen Sie dabei aus, ob es sich um eine digitale Gegenstelle (z.B. Mailboxen oder Internet-Provider) handelt oder um eine analoge Gegenstelle (Telefonansage oder Sprachdienst).



Bitte prüfen Sie die Zeit nach der ersten Übermittlung. Manche TK-Anlagen übermitteln dem Router z.B. ungünstige Zeiten, die die Funktion des Least-Cost-Routers beeinträchtigen!

12.15 Bürokommunikation und Siemens CAPI

Die CAPI von Siemens ist eine spezielle Form der weit verbreiteten CAPI-Schnittstelle. CAPI steht für Common ISDN Application Programming Interface und stellt die Verbindung von ISDN-Adaptoren zu Kommunikationsprogrammen her. Diese Programme wiederum stellen den Rechnern Funktionen der Bürokommunikation wie z.B. ein Fax oder einen Anrufbeantworter bereit.

Dieses Kapitel stellt Ihnen die CAPI sowie die mitgelieferten Anwendungsprogramme zur Bürokommunikation kurz vor und gibt Ihnen Hinweise, die bei der Installation der einzelnen Komponenten wichtig sind.

12.15.1 Die Siemens CAPI

Welche Vorteile bietet die CAPI ?

Beim Versenden von Faxen wird z.B. am Arbeitsplatz ein Faxgerät simuliert. Mit der CAPI leitet der PC das Fax über das Netzwerk an einen Router weiter, welcher die Verbindung zum Empfänger herstellt.

Installation des CAPI-Clients

Die CAPI besteht aus zwei Komponenten, einem Server (im Siemens I-GATE 11M AccessPoint) und einem Client (auf den PCs). Der CAPI-Client wird auf den Rechnern im lokalen Netz installiert, die die Funktionen der CAPI nutzen möchten.

- a) Legen sie die Siemens I-GATE 11M-CD in Ihr CD-ROM-Laufwerk ein. Wenn das Setup-Programm beim Einlegen der CD nicht automatisch startet, klicken Sie im Explorer von Windows einfach auf die 'autorun.exe' auf der Siemens I-GATE 11M-CD.
- b) Wählen Sie den Eintrag 'I-GATE 11M AccessPoint Tools installieren'.

- c) Markieren Sie die Option 'Siemens CAPI'. Klicken Sie auf Weiter, und folgen Sie den Hinweisen der Installationsroutine.

Nach dem evtl. erforderlichen Neustart des Rechners ist die CAPI bereit, alle Aufgaben der Bürokommunikationssoftware entgegenzunehmen. Die Siemens CAPI ist nach erfolgreicher Installation als Icon in der Symbolleiste zu sehen. Ein Doppelklick auf dieses Symbol öffnet ein Statusfenster, in dem Sie jederzeit aktuelle Informationen zur Siemens CAPI abrufen können.

Einstellen des CAPI-Clients

Bei der Einstellung des Clients für die CAPI legen Sie fest, welche CAPI-Server verwendet werden sollen und wie diese überprüft werden. Wenn Sie nur ein Siemens I-GATE 11M AccessPoint in Ihrem LAN als CAPI-Server betreiben, können Sie im Prinzip alle Parameter in den Voreinstellungen belassen.

- a) Starten Sie den CAPI-Client aus der Programmgruppe 'Siemens I-Gate'. Auf der Registerkarte 'Allgemein' finden Sie Informationen zum Treiber zum bereitgestellten Dienst.
- b) Wechseln Sie auf die Registerkarte 'CAPI-Server'. Hier können Sie zunächst wählen, ob der PC seinen CAPI-Server selbst suchen soll oder ob ein bestimmter Server verwendet werden soll.
- Im ersten Fall legen Sie fest, in welchem zeitlichen Intervall der Client nach einem Server sucht. Dabei sucht er so lange, bis er die im nächsten Feld eingestellte Anzahl an Servern gefunden hat. Hat er die geforderte Zahl an Servern gefunden, hört er mit der Suche auf.
 - Wenn der Client nicht automatisch nach Servern suchen soll, geben Sie in der Liste die IP-Adressen der Server an, die der Client verwenden soll. Diese Festlegung ist z.B. dann sinnvoll, wenn Sie mehrere Siemens I-GATE 11M AccessPoints in Ihrem LAN als CAPI-Server betreiben und eine Gruppe von PCs einen bestimmten Server verwenden sollen.
 - Für beide Optionen können Sie auch einstellen, in welchem Intervall der Client prüft, ob die gefundenen oder per Liste definierten Server noch aktiv sind.

Einstellen des CAPI-Servers

Bei der Einstellung des CAPI-Servers werden im Prinzip zwei Fragen behandelt:

- Auf welche Rufnummer aus dem Telefonnetz soll die CAPI reagieren?
- Welche der Rechner im lokalen Netz sollen über die CAPI Zugang zum Telefonnetz erhalten?

So stellen Sie die entsprechenden Parameter ein:

- a) Starten Sie Siemens AccessPoint Manager aus der Programmgruppe 'Siemens I-Gate'. Öffnen Sie die Konfiguration des Routers durch einen Doppelklick auf den Gerätenamen in der Liste, und wählen Sie den Konfigurationsbereich 'CAPI'.
- b) Schalten Sie den CAPI-Server ein, oder lassen Sie nur abgehende Anrufe zu. In diesem Fall reagiert die CAPI nicht auf ankommende Rufe und kann z.B. nicht zum Empfangen von Faxmitteilungen eingesetzt werden. Lassen Sie z.B. dann nur abgehende Rufe zu, wenn Sie für die Siemens CAPI keine eigene Rufnummer frei haben.
- c) Wenn der CAPI-Server eingeschaltet ist, geben Sie im Feld 'Rufnummern' die Telefonnummern ein, auf die CAPI reagieren soll. Mehrere Rufnummern können Sie durch Semikola getrennt eingeben. Wenn Sie hier keine Rufnummer eingeben, werden alle eingehenden Rufe an die CAPI gemeldet.
- d) Der von der CAPI verwendete Port ist auf '75' (any private telephony service) voreingestellt. Verändern Sie diese Einstellung nur dann, wenn dieser Port in Ihrem lokalen Netz schon für andere Dienste verwendet wird.
- e) Falls nicht alle Rechner aus dem lokalen Netz Zugriff auf die Funktionen der CAPI haben sollen, können Sie in der Zugangsliste die berechtigten Teilnehmer (über die IP-Adressen) genau festlegen.



Wenn Sie mehrere Rufnummern für die CAPI eingeben, können Sie den einzelnen Arbeitsplätzen z.B. ein persönliches Fax oder einen persönlichen Anrufbeantworter bereitstellen. Dazu geben Sie bei der Installation der Kommunikationsprogramme wie z.B. RVS-COM an verschiedenen Arbeitsplätzen jeweils verschiedene Rufnummern an, auf die das Programm reagieren soll.

Wechseln Sie auf die Registerkarte 'Verfügbarkeit'. Hier legen Sie fest, wie sich ein Siemens I-GATE 11M AccessPoint verhält, wenn über die CAPI eine Verbindung aufgebaut werden soll (ankommen-

der oder abgehender Ruf), beide B-Kanäle jedoch besetzt sind (Prioritätensteuerung). Mögliche Optionen sind hier:

- Die Verbindung über die CAPI kann nicht aufgebaut werden. Ein Faxprogramm, das die CAPI nutzt, wird dann wahrscheinlich zu einem späteren Zeitpunkt den Versand erneut versuchen.
- Die Verbindung über die CAPI kann aufgebaut werden, wenn ein Hauptkanal frei ist. Ein Hauptkanal ist der erste B-Kanal, der bei einer Routerverbindung aufgebaut wird. Nebkanäle werden zur Kanalbündelung hinzugenommen.
- Die Verbindung über die CAPI kann auf jeden Fall aufgebaut werden, eine bestehende Routerverbindung wird ggf. für die Dauer des Gespräches abgebaut. So ist z.B. die Faxfunktion immer erreichbar.

So verwenden Sie die CAPI

Zur Verwendung der CAPI gibt es zwei Möglichkeiten:

- Sie setzen eine Software ein, die direkt auf einer CAPI-Schnittstelle (in diesem Fall der CAPI) aufsetzt, wie z.B. RVS-COM. Eine solche Software sucht bei der Installation nach der CAPI und verwendet diese anschließend automatisch.
- Andere Programme wie LapLink können Verbindungen über verschiedene Wege aufbauen, z.B. über das DFÜ-Netzwerk von Windows. Beim Anlegen einer neuen DFÜ-Verbindung können Sie auswählen, welches der installierten Kommunikationsgeräte Sie verwenden möchten. Wählen Sie für die CAPI den Eintrag 'ISDN WAN Line 1'.

12.16 Reservierung von B-Kanälen

Mit der Reservierung von B-Kanälen wird das Ziel verfolgt, jederzeit ankommende oder abgehende Rufe zu erlauben und somit für externe Gegenstellen immer erreichbar zu sein oder jederzeit selbst Rufe aufbauen zu können.

Dazu wird für jedes S₀-Interface festgelegt, wie viele Verbindungen maximal gleichzeitig auf einem Interface bestehen dürfen, getrennt nach ein- und ausgehenden Rufen.



Die Beschränkung der Verbindungsanzahl bezieht sich auf alle Betriebsarten des Geräts, also auf Router, CAPI, evtl. vorhandene a/b-Ports etc.

Die Werte für B-Kanal-Reservierung werden in der Interface-Tabelle als Maximal-Wert für ein- und ausgehende Verbindungen eingetragen:

- Standardmäßig stehen beide Werte auf 2. Damit können sowohl zwei parallele ausgehende Verbindungen aufgebaut werden als auch zwei eingehende Anrufe angenommen werden.
- Wird der Wert für die maximale Zahl eingehender Rufe auf 1 gesetzt, kann das Gerät auf diesem Interface nur einen Anruf annehmen. Kommt ein weiterer Anruf herein, wird dieser abgelehnt, obwohl vielleicht noch ein B-Kanal frei ist. Dieser Kanal wird dann jedoch für eigene abgehende Rufe reserviert. Für die maximale Zahl ausgehender Rufe gilt dieses Prinzip sinngemäß.
- Wird der Wert für die maximale Zahl eingehender Rufe auf 0 gesetzt, können auf diesem Interface keine Rufe angenommen werden. Es kann dann nur die maximale Zahl zugelassener ausgehender Verbindungen aufgebaut werden.



Stehen beide Werte auf 0, kann über dieses Interface überhaupt keine Verbindung mehr aufgebaut werden!

Die Einstellungen für die B-Kanalreservierung finden Sie unter Siemens AccessPoint Manager im Konfigurationsbereich 'Management' auf der Registerkarte 'Interface', bei der Konfiguration über Telnet unter setup/WAN-Modul/Interface-Liste.

12.17 Accounting

Beim Accounting werden die Online-Zeiten und die übertragenen Datenvolumen ermittelt und nach den verursachenden Rechnern aufgeschlüsselt. Die Accounting-Daten werden in einer Liste für die aktuellen Verbindungen und in einer akkumulierten Liste abgelegt.

Dabei werden die folgenden Daten erfaßt:

- User (Name, IP-Adresse, MAC-Adresse)
Die Online-Zeiten und die übertragenen Datenvolumen werden zunächst den MAC-Adressen der Rechner-Netzwerk-Interfaces im LAN zugeordnet. Aus DHCP- oder DNS-Server-Modulen kann der Router ggf. zusätzliche Informationen über die Zuordnung von MAC-Adressen und Rechnernamen verfügen. In diesem Fall kann die Online-Zeit auch direkt den Rechnernamen zugeordnet werden. Ist eine Zuordnung von MAC-Adresse

zu Rechnernamen nicht möglich, wird eine andere verfügbare Information zur Kennzeichnung der Nutzer eingetragen, z.B. die IP-Adresse.

Bei Netzwerk-Teilnehmern, die über eine Dial-In-Verbindung Zugriff auf das LAN haben, ist i.d.R. die MAC-Adresse nicht bekannt. In diesem Fall erzeugt der Router eine Pseudo-Adresse, mit der die Dial-In-Gegenstellen beim Accounting identifiziert werden.

- Gegenstelle, zu der die Verbindung aufgebaut wurde
- Art der Verbindung
- Datenvolumen in Sende- und Empfangsrichtung
- Online-Zeit

Bei Wählverbindungen, die von mehreren Usern gemeinsam verwendet werden, kann die gesamte Dauer einer Verbindung länger sein als ein Teilnehmer sie wirklich benutzt. Daher wird in diesen Fällen die Dauer der Verbindung anhand der ersten und der letzten Aktion eines Users berechnet, zuzüglich der für die Verbindung gültigen Haltezeit.

- Anzahl der Verbindungen
In diesem Feld wird angezeigt, wie oft die Aktion eines Users zu einem Verbindungsaufbau geführt hat.

12.17.1 Konfiguration des Accountings

Die Einstellungen für das Accounting sind unter /Setup/Accounting zu finden. Dort können das Accounting ein- oder ausgeschaltet und die Speicherung im Flash-ROM aktiviert werden. Außerdem kann hier die Sortierung der akkumulierten Tabelle nach Online-Zeit oder Transfervolumen beeinflusst werden.

12.17.2 Ablesen der Accounting-Informationen

Eine Anzeige der aufgezeichneten Daten ist möglich über Siemens AccessPoint Monitor. Dabei können die Daten auch als Datei auf einen Datenträger gesichert werden.

Beim Zugriff über Telnet können die jeweils aufgezeichneten Daten ebenfalls unter /Setup/Accounting abgefragt werden.

Aufgeschlüsselt nach Benutzername und Gegenstelle werden jeweils die folgenden Informationen aufgelistet:

- Username
Name des Users oder seine Layer-3-Adresse (IP-Adresse, IPX-Adresse oder im Bridge-Betrieb nochmal die MAC-Adresse)
- Gegenstelle
Gegenstelle, mit der der Nutzer Daten ausgetauscht hat
- Verbindungs-Typ
Art der Verbindung
- Rx-Bytes, Tx-Bytes
Datenvolumen auf dem Interface
- Gesamtzeit
Gesamt Online-Zeit für genau diesen User zu genau dieser Gegenstelle
- Verbindungen
Anzahl der für den User zu dieser Gegenstelle gezählten Verbindungen



Wenn ein User eine Verbindung zu einer anderen Gegenstelle aufbaut, wird ein neuer Eintrag in der Tabelle erzeugt. Alle Transfervolumen und Online-Zeiten von einem User zu einer Gegenstelle werden in einem Eintrag erfaßt.

Je nach Sortierung der Liste werden 512 Einträge mit dem größten Transfervolumen oder mit der größten Online-Zeit in der Tabelle erfaßt.

13 Fehlersuche

Wenn Sie Schwierigkeiten bei der Inbetriebnahme Ihres I-GATE 11M WLANs haben, ist im Folgenden eine sinnvolle Vorgehensweise zur Fehlereingrenzung angegeben (siehe auch Kapitel "1.4 Falls Sie Hilfe brauchen").

Weitere Informationen finden Sie im Internet unter:

www.siemens.com/i-gate

Die Kommunikation im I-GATE 11M Netzwerk basiert auf dem IP-Netzprotokoll. Mit dem AccessPoint Manager können Sie daher erst arbeiten, wenn auf IP-Level alles in Ordnung ist. Mit der folgenden Checkliste können Sie feststellen, ob diesbezüglich alles stimmt:

- **Ist der MobilePort Treiber erfolgreich geladen?** Kapitel 13.1
- **Stimmt die SSID (= WLAN-Domain) Ihrer MobilePort Rechner?** Kapitel 13.2
- **Ist das TCP/IP-Protokoll geladen und richtig konfiguriert?** Kapitel 13.3
- **Ist eine IP-Kommunikation zwischen zwei WLAN-Rechnern oder zwischen Rechner und AccessPoint möglich?** Kapitel 13.4
- **Ist der AccessPoint nicht erreichbar oder funktioniert er nicht mehr?** Kapitel 13.5

13.1 Ist der MobilePort Treiber erfolgreich geladen?

Einen ersten wichtigen Hinweis gibt die LED auf dem MobilePort. Bei erfolgreich geladenem Treiber muss sie permanent blinken oder leuchten:

Grün blinken = MobilePort sucht AccessPoint (Scanning)

Grün leuchten = MobilePort hat AccessPoint gefunden (Associated)

Weitere Hinweise zu aufgetretenen Fehlern erhalten Sie mit den folgenden Diagnosetools.

Windows 95/98

Schauen Sie im Gerätemanager (**Start -> Einstellungen -> Systemsteuerung -> System -> Register Geräte-Manager**) nach, ob die Netzwerkkarte 'I-GATE 11M PCI' fehlerfrei, so wie in **Bild 13.1** abgebildet, eingetragen ist.

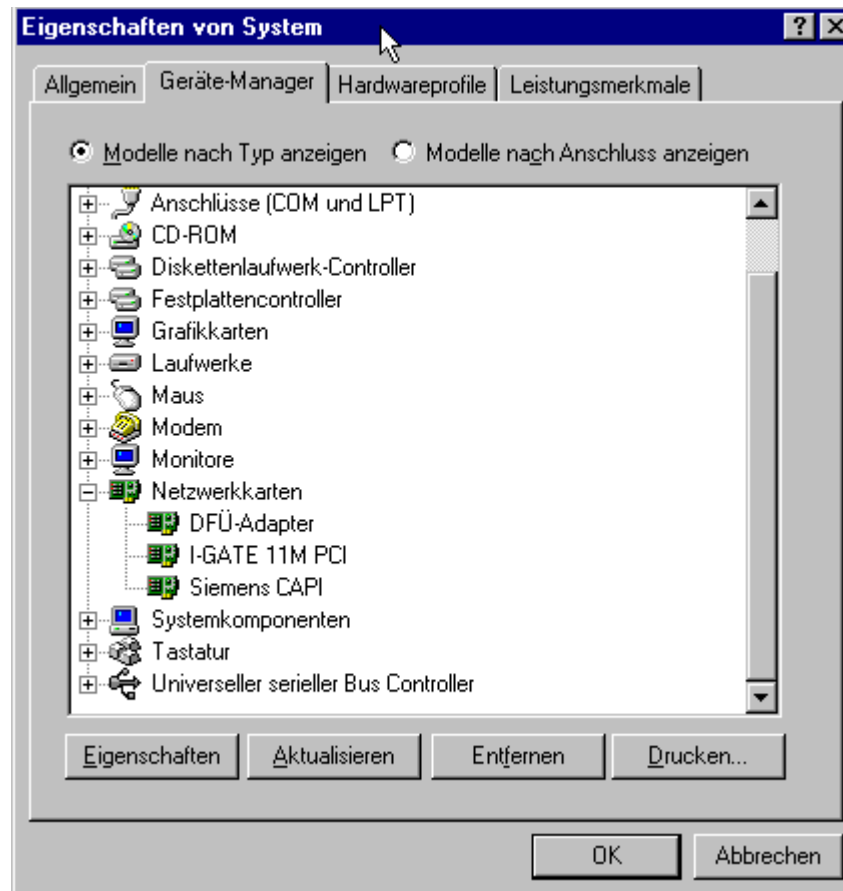


Bild 13.1 Eintrag im Windows 98 Geräte-Manager (Desktop PC)

Windows NT

Schauen Sie im NT-Geräte-Manager (**Start -> Einstellungen -> Systemsteuerung -> Geräte**) nach, ob der 'I-GATE 11M PC Card / PCI Adapter' (Desktop PC) wie in **Bild 13.2** gezeigt, erfolgreich gestartet wurde.

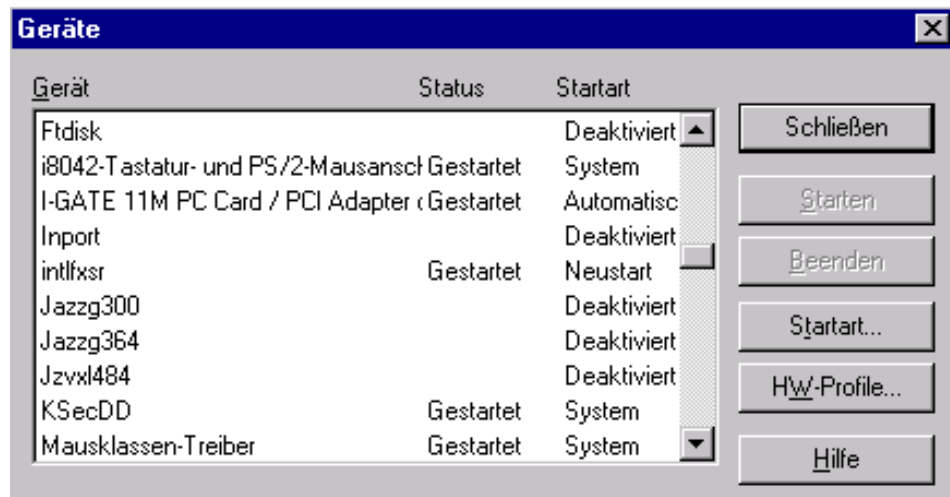


Bild 13.2 Eintrag im NT-Geräte-Manager (Desktop PC)

Windows NT Notebook: Wenn der Eintrag 'I-GATE 11M PC Card / PC Card plus' fehlt, kann es daran liegen, dass Sie keine Software die Spannungsumschaltung auf 3,3 Volt durchführt in Ihrem Notebook installiert haben:

- Prüfen Sie auf der mit Ihrem Notebook gelieferten CD, ob solche Software dort vorhanden ist.
- Wenn Sie dort keine solche Software finden, besuchen Sie z.B. **www.systemsoft.com** und laden Sie SystemSoft's 'Card-Wizard' Software herunter.

Windows 2000

Schauen Sie im Geräte-Manager (**Start -> Einstellungen -> Systemsteuerung -> System -> Hardware -> Geräte-Manager...**) nach, ob der 'I-GATE 11M PCI' Treiber wie in **Bild 13.3** gezeigt, erfolgreich gestartet wurde.

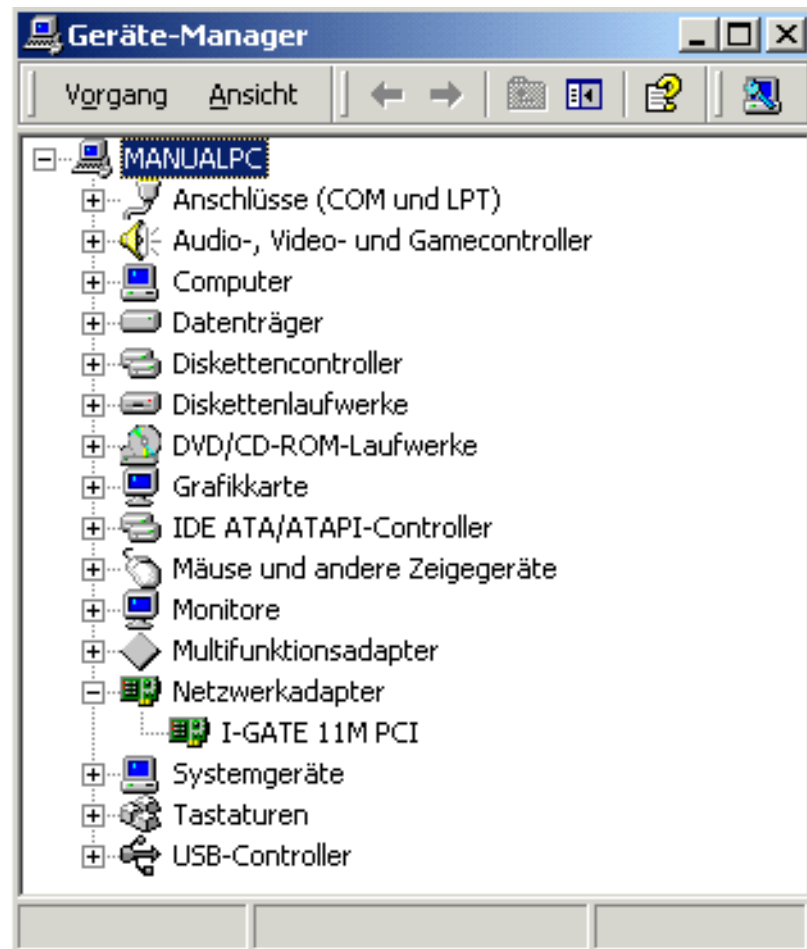


Bild 13.3 Eintrag im Windows 2000 Geräte-Manager (Desktop PC)

13.2 Stimmt die SSID (= WLAN-Domain) Ihrer MobilePort Rechner?



Bei Auslieferung entspricht die WLAN-Domain des AccessPoints der Seriennummer auf der Rückseite des Gehäuses. Falls die WLAN-Domain bereits geändert wurde, muss der aktuelle Wert eingegeben werden.

Die Eigenschaft SSID (= WLAN Domain) muss auf allen MobilePort Rechnern und dem I-GATE 11M ISDN AccessPoint unbedingt identisch sein. (Gross-/Kleinschreibung der Seriennummer beachten!)

Am schnellsten kontrollieren Sie die SSID Ihres MobilePort indem Sie den MobilePort Manager öffnen und prüfen Sie ob Sie den korrekten Wert im Feld SSID eingetragen haben (Bild 13.4).

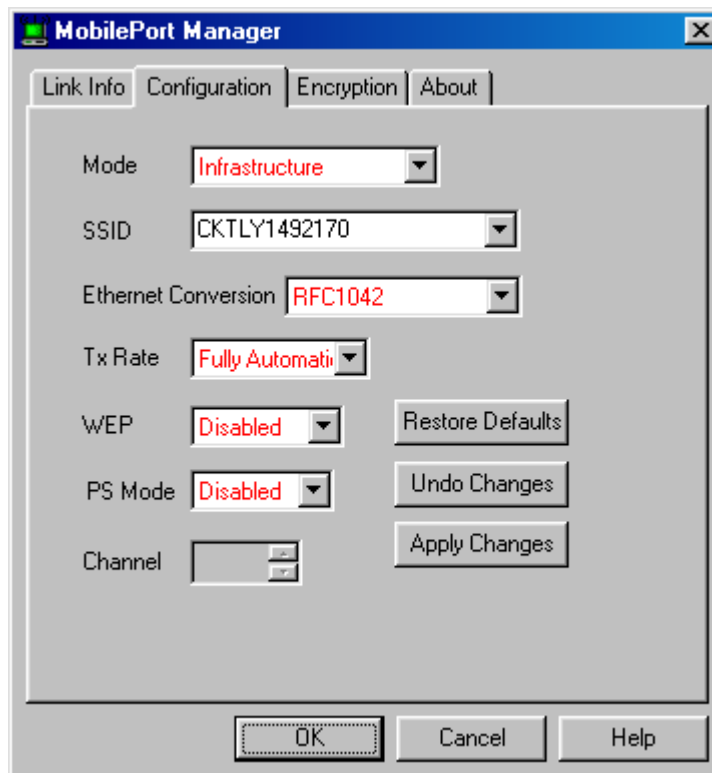


Bild 13.4 MobilePort Manager Configuration

13.3 Ist das TCP/IP-Protokoll geladen und richtig konfiguriert?

Windows 95/98 (DHCP-Betrieb)

Kontrollieren Sie die Einstellungen Ihres TCP/IP-Stacks für den MobilePort. Geben Sie hierzu nach **Start -> Ausführen** den Programm-Namen `wiipcfg` ein. Das Fenster 'IP-Konfiguration' öffnet sich. Klicken Sie auf **Weitere Info >>**. Wählen Sie den Eintrag 'I-GATE 11M PCI'. Überprüfen Sie die Werte in den Feldern 'IP-Adresse', 'Subnet Mask' und 'DHCP-Server'. Die 'Physische Adresse' muss mit '00-90' beginnen. Wenn Sie den AccessPoint mit seiner Defaultadresse betreiben, muss die Konfiguration ungefähr so wie in **Bild 13.5** aussehen. Einen Test des DHCP-Servers können Sie durch drücken von **Alles freigeben** und anschliessend **Aktualisieren** durchführen. Beenden Sie mit **OK**.

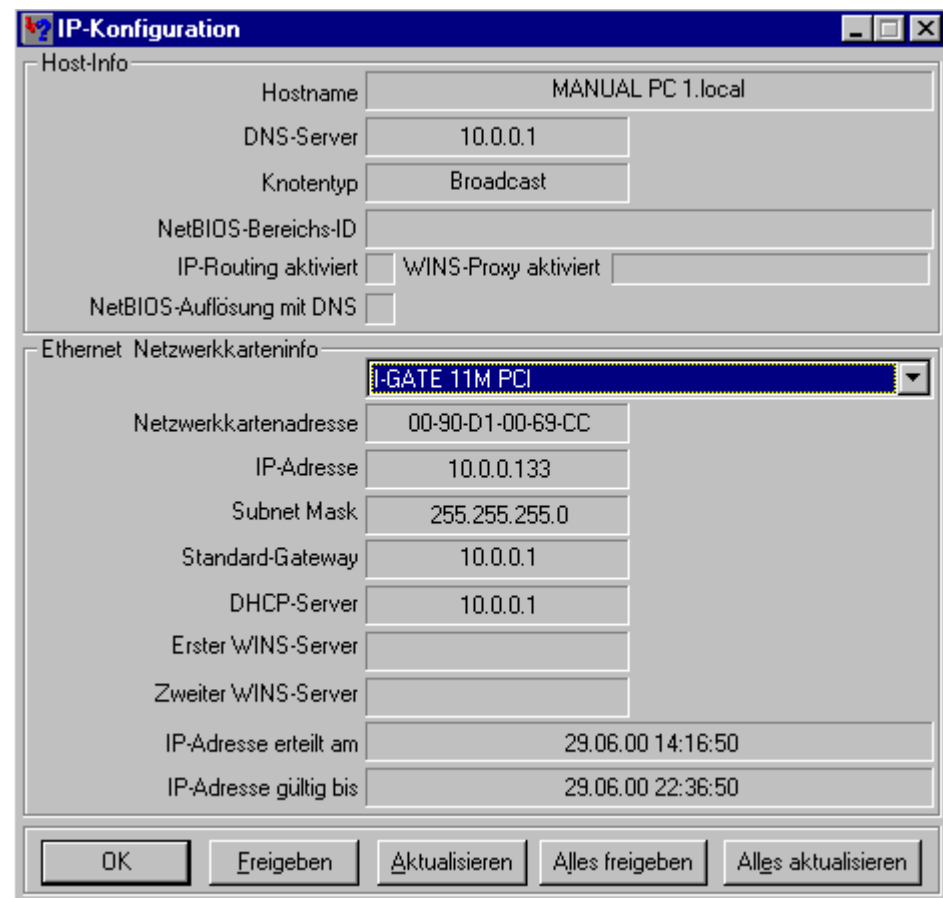


Bild 13.5 IP-Konfiguration Windows 95/98 (DHCP-Betrieb)

Fehlerhafte Einstellungen korrigieren Sie über den Netzwerk-Setup (**Start -> Einstellungen -> Systemsteuerung -> Netzwerk**), indem Sie dort die Eigenschaften von **TCP/IP** bzw. **TCP/IP -> I-GATE 11M PCI** auswählen.

Hinweis:

Die IP-Adressen in den Feldern 'DNS-Server', 'Standard-Gateway' und 'DHCP-Server' sind bei Betrieb des I-GATE 11M Netzwerkes mit DHCP ('IP-Adresse automatisch beziehen') identisch mit der IP-Adresse des AccessPoints. Sofern Sie diese in den I-GATE 11M AccessPoint Grundeinstellungen nicht geändert haben, ist die IP-Adresse des AccessPoints 10.0.0.1 und Ihr MobilePort Rechner bekommt eine weitere freie IP-Adresse der Form 10.0.0.x zugewiesen.

Windows NT (DHCP-Betrieb)

Kontrollieren Sie die Einstellungen Ihres TCP/IP-Stacks für den MobilePort. Geben Sie hierzu in einem DOS-Fenster den Befehl `ipconfig /all` ein. Die 'Physische Adresse' muss mit '00-90' beginnen. Wenn Sie den AccessPoint mit seiner Defaultadresse betreiben, muss die Konfiguration ungefähr so wie in [Bild 13.6](#) aussehen. Einen Test des DHCP-Servers können Sie durch Eingabe von `ipconfig /release` und anschließend `ipconfig /renew` durchführen. Schliessen Sie das DOS-Fenster.

```

C:\>ipconfig/all

Windows NT IP-Konfiguration

    Host-Name . . . . . : testpc.local
    DNS-Server. . . . . : 10.0.0.1
    Knotentyp . . . . . : Broadcast
    NetBIOS-Bereichs-ID . . . . . :
    IP-Routing aktiviert. . . . . : Nein
    WINS-Proxy aktiviert. . . . . : Nein
    NetBIOS-Auswertung mit DNS : Nein

Ethernet-Adapter CW101:

    Beschreibung. . . . . :
    Physische Adresse . . . . . : 00-90-D1-00-69-CC
    DHCP aktiviert. . . . . : Ja
    IP-Adresse . . . . . : 10.0.0.133
    Subnet Mask . . . . . : 255.255.255.0
    Standard-Gateway. . . . . : 10.0.0.1
    DHCP-Server . . . . . : 10.0.0.1
    Lease erhalten. . . . . : Donnerstag, 29. Juni 2000 14:46:58
    Lease läuft ab. . . . . : Donnerstag, 29. Juni 2000 23:06:58

C:\>
  
```

Bild 13.6 IP-Konfiguration Windows NT (DHCP-Betrieb)

Fehlerhafte Einstellungen korrigieren Sie über den Netzwerk-Setup (**Start -> Einstellungen -> Systemsteuerung -> Netzwerk -> Register Protokolle**) über den Button **Eigenschaften** für das TCP/IP-Protokoll.

Hinweis:

Die IP-Adressen in den Feldern 'DNS-Server', 'Standard-Gateway' und 'DHCP-Server' sind bei Betrieb des I-GATE 11M Netzwerkes mit DHCP ('IP-Adresse automatisch beziehen') identisch mit der IP-Adresse des AccessPoints. Sofern Sie diese in den I-GATE 11M AccessPoint Grundeinstellungen nicht geändert haben, ist die IP-Adresse des AccessPoints 10.0.0.1 und Ihr MobilePort Rechner be-

kommt eine weitere freie IP-Adresse der Form 10.0.0.x zugewiesen.

Wenn Sie die IP-Konfigurationsdaten von [Bild 13.5](#) bzw. [Bild 13.6](#) bei einem noch nicht konfigurierten AccessPoint abrufen, ist als 'DHCP-Server' die IP-Adresse 10.0.0.254 eingetragen. Die Felder 'DNS-Server' und 'Standard-Gateway' sind noch leer.

Windows 2000 (DHCP-Betrieb)

Kontrollieren Sie die Einstellungen Ihres TCP/IP-Stacks für den MobilePort Rechner. Geben Sie hierzu in einem DOS-Fenster den Befehl `ipconfig /all` ein. Die 'Physische Adresse' muss mit '00-90' beginnen. Wenn Sie den AccessPoint mit seiner Defaultadresse betreiben, muss die Konfiguration ungefähr so wie in [Bild 13.7](#) aussehen. Einen Test des DHCP-Servers können Sie durch Eingabe von `ipconfig /release` und anschließend `ipconfig /renew` durchführen. Schliessen Sie das DOS-Fenster.

```

Windows 2000-IP-Konfiguration

Hostname . . . . . : manualpc
Primäres DNS-Suffix . . . . . :
Knotentyp . . . . . : Broadcastadapter
IP-Routing aktiviert. . . . . : Nein
WINS-Proxy aktiviert. . . . . : Nein
DNS-Suffixsuchliste . . . . . : local

Ethernetadapter "LAN-Verbindung 2":

    Verbindungsspezifisches DNS-Suffix: local
    Beschreibung. . . . . : I-GATE 11M PCI
    Physische Adresse . . . . . : 00-90-D1-00-69-CC
    DHCP-aktiviert. . . . . : Ja
    Autokonfiguration aktiviert . . . . . : Ja
    IP-Adresse. . . . . : 10.0.0.133
    Subnetzmaske. . . . . : 255.255.255.0
    Standardgateway . . . . . : 10.0.0.1
    DHCP-Server . . . . . : 10.0.0.1
    DNS-Server . . . . . : 10.0.0.1
    Lease erhalten. . . . . : Donnerstag, 29. Juni 2000 17:08:0
    Lease läuft ab. . . . . : Freitag, 30. Juni 2000 01:28:00
  
```

Bild 13.7 IP-Konfiguration Windows 2000 (DHCP-Betrieb)

Fehlerhafte Einstellungen korrigieren Sie über den Netzwerk-Setup (**Start -> Einstellungen -> Systemsteuerung -> Netzwerk- und DFÜ Verbindungen -> LAN-Verbindung 2 -> Eigenschaften -> Internetprotokoll [TCP/IP] -> Eigenschaften**).

Hinweis:

Die IP-Adressen in den Feldern 'DNS-Server', 'Standard-Gateway' und 'DHCP-Server' sind bei Betrieb des I-GATE 11M Netzwerkes mit DHCP ('IP-Adresse automatisch beziehen') identisch mit der IP-Adresse des AccessPoints. Sofern Sie diese in den I-GATE 11M AccessPoint Grundeinstellungen nicht geändert haben, ist die IP-

Adresse des AccessPoints 10.0.0.1 und Ihr Rechner bekommt eine weitere freie IP-Adresse der Form 10.0.0.x zugewiesen.

Wenn Sie die IP-Konfigurationsdaten von [Bild 13.5](#), [Bild 13.6](#) oder [Bild 13.7](#) bei einem noch nicht konfigurierten AccessPoint abrufen, ist als 'DHCP-Server' die IP-Adresse 10.0.0.254 eingetragen. Die Felder 'DNS-Server' und 'Standard-Gateway' sind noch leer.

13.4 Ist eine IP-Kommunikation zwischen zwei WLAN-Rechnern oder zwischen Rechner und AccessPoint möglich?

Testen Sie die Kommunikation zwischen Rechner und AccessPoint mit dem Befehl

```
ping <IP-Adresse>
```

in einem DOS-Fenster. Der AccessPoint muss anschliessend antworten.

Die IP-Adresse des AccessPoint entnehmen Sie im obigen DOS-Beispiel in der letzten Zeile unter 'Standard-Gateway'.

Die Kommunikation zwischen zwei Rechnern können Sie ebenfalls mit einem 'ping' von einem Rechner auf die IP-Adresse des anderen Rechners testen.

13.5 Ist der AccessPoint nicht erreichbar oder funktioniert er nicht mehr?

Wenn Sie

- der Überzeugung sind, dass der MobilePort funktioniert ([13.1](#) - [13.3](#) sind in Ordnung) und der AccessPoint Manager den AccessPoint trotzdem nicht findet oder nicht mehr erreichen kann oder
- z.B. nicht mehr sicher sind, ob Sie auf MobilePort und AccessPoint noch die gleiche WLAN-Domain eingestellt haben, können Sie einen Software-Reset oder als letzte Massnahme einen Konfigurations-Reset des AccessPoints durchführen.

Software-Reset AccessPoint

Einen Software-Reset des AccessPoints erreichen Sie durch ein kurzzeitiges Unterbrechen der Stromversorgung des AccessPoints.

Ziehen und stecken Sie hierzu entweder das Steckernetzteil oder das Stromversorgungskabel direkt am AccessPoint.

Konfigurations-Reset AccessPoint

Links neben den Leuchtdioden befindet sich eine kleine Bohrung im Gehäuse des AccessPoints. Unter dieser Bohrung befindet sich ein Reset-Taster auf der Hauptplatine des AccessPoints. Zu seiner Betätigung benötigen Sie z.B. eine aufgebogene Büroklammer. (Ein spitzer Gegenstand reicht nicht aus, da sich der Taster ca. 2 cm tief unter der Gehäuseoberfläche befindet.)

Wenn Sie den Reset-Taster mindestens 6 Sekunden gedrückt halten, lösen Sie einen Konfigurations-Reset aus. Das Auslösen des Resets wird durch ein kurzes Aufleuchten aller LEDs angezeigt. Das Gerät verhält sich nach diesem Reset wieder so, als hätten Sie es nach dem Kauf gerade ausgepackt und erstmalig in Betrieb genommen, d.h. auch die WLAN-Domain des Funk-LANs wird wieder auf die Seriennummer des AccessPoints zurückgesetzt. Vergewissern Sie sich nun, ob auf dem Rechner mit dem MobilePort im I-GATE 11M Treibersetup auch wieder die Seriennummer des AccessPoints als WLAN-Domain eingestellt ist.

Bei intakter Hardware und einem funktionstüchtigem TCP/IP-Stack auf dem MobilePort muss der I-GATE 11M ISDN AccessPoint jetzt vom AccessPoint Manager in jedem Fall wieder erkannt werden.

14 Technische Daten

14.1 Funkkanäle

I-Gate Funk-Netzwerkkarten sind gemäss dem IEEE Standard 802.11 für den Betrieb im ISM (Industrial, Scientific, Medical) Frequenzband zwischen 2.4 und 2.4835 GHz vorgesehen. Weil jeder der 14 verwendbaren Funkkanäle durch dem DSSS-Verfahren (Digital Sequence Spread Spectrum) eine Breite von 22 MHz beansprucht, stehen maximal 3 von einander unabhängigen Kanäle (z.B. 3, 8 und 13) zur Verfügung. Aus der Tabelle entnehmen Sie die in Ihrem Land zulässigen Kanäle.

Tab. 14.1 Funkkanäle mit Frequenzen in MHz

Kanal-Nr.	EC & CH	Frankreich	Japan	FCC & IC
1	2412			2412
2	2417			2417
3	2422			2422
4	2427			2427
5	2432			2432
6	2437			2437
7	2442			2442
8	2447			2447
9	2452			2452
10	2457	2457		2457
11	2462	2462		2462
12	2467	2467		
13	2472	2472		
14			2484	

14.2 Technische Daten

Die technischen Daten Ihrer I-GATE 11M Produkte finden Sie in den PDF Datenblätter auf der I-GATE 11M CD-ROM unter **CD durchsuchen -> document -> Ihre Sprache -> Daten** oder auf dem Internet unter **www.siemens.com/i-gate**.

14.3 Artikelnummern

Eine Aufstellung über die Artikelnummern der I-GATE 11M Produkte finden Sie als PDF auf der I-GATE 11M CD-ROM unter **CD durchsuchen -> document -> Ihre Sprache -> Daten** oder auf dem Internet unter **www.siemens.com/i-gate**.

15 Allgemeine Garantiebedingungen

15.1 Garantieuumfang

- a) Die Garantie erstreckt sich auf die gelieferten Geräte mit allen Teilen, nicht aber auf die Installation und Konfiguration. Sie wird in der Form geleistet, dass Teile, die nachweislich trotz sachgemässer Behandlung und Beachtung der Gebrauchsanweisung aufgrund von Fabrikations- und/oder Materialfehlern defekt geworden sind, nach unserer Wahl kostenlos ausgetauscht oder repariert werden. Blitzschäden sind ausgeschlossen. Alternativ hierzu behalten wir uns vor, das defekte Gerät gegen ein Nachfolgeprodukt auszutauschen oder dem Käufer den Originalkaufpreis gegen Rückgabe des defekten Geräts zu erstatten. Handbücher und evtl. mitgelieferte Software sind von der Garantie ausgeschlossen.
- b) Die Kosten für Material und Arbeitszeit werden von uns getragen, nicht aber die Kosten für den Versand vom Erwerber zur Service-Werkstätte und/oder zu uns.
- c) Ersetzte Teile gehen in unser Eigentum über.
- d) Wir sind berechtigt, über die Instandsetzung und den Austausch hinaus technische Änderungen (z.B. Firmware-Updates) vorzunehmen, um das Gerät dem aktuellen Stand der Technik anzupassen. Hierfür entstehen dem Erwerber keine zusätzlichen Kosten. Ein Rechtsanspruch hierauf besteht nicht.
- e) Weitergehende Ansprüche sind ausgeschlossen.

15.2 Garantiezeit

Die Garantiezeit beträgt ein Jahr ab Verkaufsdatum (Beleg). Die Garantiezeit beginnt mit dem Tag der Lieferung des Gerätes durch den Fachhändler. Garantieleistungen bewirken weder eine Verlängerung der Garantiefrist, noch setzen sie eine neue Garantiefrist in Gang. Die Garantiefrist für eingebaute Ersatzteile endet mit der Garantiefrist für das ganze Gerät.

16 Service

16.1 Falls Sie Hilfe brauchen

Wenn Sie mit der Installation oder dem Betrieb mit I-GATE 11M Probleme haben, stehen Ihnen folgende Möglichkeiten offen:

- Tipps im Kapitel "**13 Fehlersuche**"
- Internet: **www.siemens.com/i-gate**
- Ihr Fachhändler
- Die unten aufgeführte Servicenummer für Ihr Land

Ihr **Fachhändler** beantwortet gerne Fragen betreffend Gerätebedienung. **Siemens Service** hilft Ihnen gerne weiter bei Geräteproblemen. Kontaktieren Sie Ihre **Telefongesellschaft** mit Fragen betreffend Ihrem ISDN - respektiv DSL - Anschluss. Kontaktieren Sie Ihren **Internet Service Provider** mit Fragen betreffend Ihres Internet Anschlusses.

16.2 Servicenummern

Stand: 25.04.2000.

Besuchen Sie **www.siemens.com/i-gate** für aktuelle Nummern.

Tab. 16.1 Servicenummern

Land	Service	Telefon
Abu Dhabi	Siemens Service Center	02713500
Australia	Siemens	1800622414
Austria	Siemens	0517075004
Bangladesh	Siemens	017527447
Belgium	Siemens	078152221
Brunei	incomm	02151
Bulgaria	Omnitel	02739488
China	Siemens	02150318149
Croatia	Siemens	016105381
Czech Republic	Siemens	0233032727

Tab. 16.1 Servicenummern

Land	Service	Telefon
Denmark	Siemens	35258600
Dubai	Siemens Service Center	04699720
Egypt	Siemens	23313129
Finland	Siemens	0922943700
France	Siemens	0156384200
Germany	Siemens	01805333220
Greece	Siemens	016864389
Hong Kong	Siemens	22583636
Hungary	Siemens	0614712444
Iceland	Smith & Norland	5113000
India	Siemens	116923988
India	Siemens	116925589 (ISDN)
Indonesia	Dian Graha Elektr.	0214615081
Ireland	Siemens	1850777277
Italy	Siemens	0269893691
Jordan	F.A. Kettaneh	079559663
Kuwait	NGEECO	4818749
Latvia	Siemens	7501114
Lebanon	F.A. Kettaneh	01443043
Lithuania	Siemens	822391555
Malaysia	Siemens	037514974
Marocco	SETEL S.A.	2352409
Mauritius	Ireland Blyth	2116213
Netherlands	Siemens	0703333100
Norway	Siemens	22633314
Oman	Siemens Service Center	791012

Tab. 16.1 Servicenummern

Land	Service	Telefon
Pakistan	Siemens	0215673565
Philippines	Siemens	28149888
Poland	Siemens	0800220990
Portugal	Siemens	014178393
Russia	Siemens	80957371801
Saudi Arabia	Siemens	026655058
Singapore	Siemens	8454818
Vietnam	Opticom	090456789
Luxembourg	Siemens	43843399
Slovak Republic	Siemens	0759682266
Slovenia	Siemens	0611746336
South Africa	Siemens	0800114050
Spain	Siemens	902115061
Sweden	Siemens	087509911
Switzerland	Siemens	012120090
Taiwan	Siemens	0225186504
Thailand	Siemens	26791777
Turkey	SIMKO	02122528835
United Kingdom	Siemens	0990334411

17 Stichwörter

Numerics

1TR6 (Nationales ISDN) 193

A

AccessPoint

Konfigurations-Reset 265

Software Reset 264

AccessPoint Manager

AccessPoints erkennen 156

Firmware Update 159

Konfiguration sichern 159

Konfigurationsdialog 157

Provider löschen 162

Provider wechseln 160

Telnet Sitzung 162

AccessPoint Monitor 162

Protokolldatei 164

Verbindung trennen 163

Accounting 251

Artikelnummern 16, 268

B

Betriebsarten 21

LAN-LAN Kopplung 170

LAN-LAN-Kopplung mit

NetBIOS 238

Wireless LAN-LAN

Kopplung 24, 170

WLAN im Ad-hoc-Modus 28

WLAN im Infrastruktur-Modus 22

WLAN mit Internet-Zugang 23

WLAN mit Remote Access (RAS) 24

WLAN Roaming über Funk 25

WLAN Roaming über Kabel 26

WLAN-LAN Internet-Zugang 27

WLAN-LAN Kopplung 25

B-Kanal 193

-Reservierung 250

Boot-Image über ISDN-Leitung

beziehen 230

C

Call-by-Call 241

CAPI 171, 247

-Interface-Einstellungen 194

CE-Konformität 12

CHAP 187, 198, 201

D

Datei- und Druckerfreigabe 122

Daten-Kompression 195

DHCP 221

-Informationen über ISDN-
Leitungen 229

-Relay-Agent 229

DHCP-Server

Konfigurieren 226

Zustände 222

DHCP-Server Zuweisung

IP-Adressen 223

Netzmaske 224

DHCP-Server Zuweisungen

Broadcast-Adresse 224

Default-Gateway 224

DNS- und NBNS-Server 224

Gültigkeit 224

D-Kanal-Protokoll 193

DNS 220

-Forwarding 219

-Request 220

DNS-Server 219

Einstellen 232

Funktion 231

Domain Name Service (DNS) 220, 231

DSL 182

DSL-Firmware 182

DSS1 Punkt-zu-Punkt 193
DSS1(Euro-ISDN) 193
DSSS (Digital Sequence Spread
Spectrum) 267
dynamische Routing-Tabelle 215

E

Elektromagnetische Verträglichkeit 12
E-Mail-Adresse 15, 272
Encapsulation 195
Ethernet
802.3 205
Encapsulation 205
-Header hinzufügen 195
Ethernet conversion
802.1h 112
encapsulated 112
RFC1042 112
Euro-ISDN 193
Exponential-Backoff 205
-Algorithmus 208

F

Fachhändler 272
Fast-Call-Back 188
Fehlersuche 254
Festverbindung Gruppe 0 193
Filter
IPX-Pakete 208
TCP/IP-Pakete 213
Firmware
DSL-Upload 182
LAN-Upload 182
Upload mit FirmSafe 178
Firmware Update 159
FTP 213
Funkkanäle 267
Funkzulassungen 13

G

Garantie 270

Gebührenmanagement 160, 190
Gebührensperre 160
Einstellung 146
Get Nearest Server Request 206
Gültigkeit
DHCP-Server Zuweisungen 224

H

Haupt-MSN 193
HDLC-Verbindungen 195
HotLine 15, 272

I

I/LAN AccessPoint
als LAN-WLAN Bridge 166
ICMP 219
-Redirect 214
Inband-Konfiguration 172
Internet
Browser einrichten 146
Provider löschen 162
Provider wechseln 160
Interoperabilität 29
IP-Adressen 198
ipconfig 261, 263
IPCP (IP Control Protocol) 198
IP-Masquerading 189
(NAT, PAT) 217
IP-Masquerading (NAT, PAT)
Protokolle 219
IP-RIP 215
IP-Routing 211
Default-Route 212
dynamische Routing Tabelle 211
statische Routing-Tabelle 211
IPX 211
-Pakete 205
-Paketfilter 208
-Routing 203
IPX (Internet Packet eXchange,
Novell) 236

IPX- und SPX-Watchdogs 210

ISDN

Applikationen 171

Modem 171

ISDN-Verbindungen 190

ISDN-Namenliste 191

Layername 192

Rückruf 192

Round-Robin-Liste 192

S0-Anschluss-Einstellungen 192

K

Kanalbündelung 195

Kommunikationslayer 194

Konfiguration über Web Browser 174

Konfigurations-Reset des

AccessPoints 265

Kosten 160

Kostenverteilung über Rückruf 188

Künstliche Alterung 206

L

LAN-LAN Kopplung

Setup-Assistent 170

LAN-LAN-Kopplung mit NetBIOS 238

Layer 3

PPP-Liste 195

Script-Liste 195

Layer-3

-Adresse für Accounting 253

Layer-Liste 194

Daten-Kompression und

Kanalbündelung 195

Encapsulation 195

Layer 1 195

Layer 2 195

Layer 3 195

Layername 194

Layername

ISDN-Namenliste 192

LCP (Link Control Protocol) 198, 202

LCR (Least-Cost-Router) 220, 241

Einstellen 245

-Tabelle 243

Uhrzeit 246

LEDs

I/LAN AccessPoint

DSL nach Strom- & DSL-

Anschluss 130

ISDN nach Strom-& ISDN-

Anschluss 128

LAN nach Strom- & LAN-

Anschluss 129

Übersicht ISDN/DSL Mode 133

Übersicht ISDN/LAN Mode 131

ISDN AccessPoint

nach Strom-& ISDN-

Anschluss 125

Übersicht 126

MobilePort in AccessPoint

nach AccessPoint

Stromanschluss 126

MobilePort in Rechner

nach AccessPoint

Stromanschluss 126

MobilePort Manager

nach AccessPoint

Stromanschluss 126

nach Treiber

Installation 63, 94, 106

MobilePorts in Rechner

nach Treiber Installation 42

Lieferumfang 17

Login-Sperre 185

Lokales Routing 214

Loop Propagieren 207

M

MAC

-Adresse für Accounting 251

-Adresse in IPX-Netze 203

-Adressenliste für WLAN Zugriff auf

WAN 150
-Filter für WLAN Zugriff auf WAN 150
MobilePort
Arbeitsgruppennamen 37, 69
Computernamen 37, 69
MS Loopback-Adapter 81
MobilePort Manager PC Icon
nach AccessPoint
Stromanschluss 126
nach MobilePort Treiber
Installation 63, 94, 106
MobilePorts
für Frankreich 13
Modem
ISDN 171
MS Loopback-Adapter 81
MS-CHAP 187, 198, 201
MSN 193

N

Namenliste
ISDN- 191
NetBEUI (NetBIOS Extended User
Interface) 236
NetBIOS 205
Definition 234
-Kopplung mit PPP-Verbindung 239
-Nameserver (NBNS) 234
-Pakete 205, 235
-Ports 236
Propagated Frames 205
-Proxy 234
-Routing über LAN-LAN
Kopplung 240
-Routing über RAS-Zugang 241
über IP-Routing 238
Voraussetzungen 236
zwei Windows-Netze verbinden 238
Network Basic Input/Output System
(NetBIOS) 205
Netzwerkkonfiguration über ISDN

übertragen 229
Normen 12
NT
Service
Pack 14, 64, 95, 107, 138, 147
NT-Domain 238

P

PAP 187, 198, 201
parallel Verbindungen zu unterschiedli-
chen Gegenstellen 193
Passwort setzen 185
PC Card Software für NT Notebook 256
Peer-to-LAN 166
Peer-to-Peer Netzwerke
mit AccessPoint 167
ohne AccessPoint 120
ping 264
Point-to-Point Protocol (PPP)
Definition 198
Policy Based Routing
Type-of-Service(TOS)-Feld 221
Portnummern 213
Power Management 118
PPP
-Liste 200
-Statistik 200
-Trace 200
-Verhandlungsphasen 199
PPP-Liste
für Rufannahme Gegenstellen 187
Layer 3 195
Passwort nach PAP, CHAP oder MS-
CHAP 187
Preselection 241
Produkte
11 Mbit 10
2 Mbit 10
Artikelnummern 16
künftige 11Mbit 12
Lieferumfang 17

Technische Daten 16

Protokoll-Einstellungen

Encapsulation 195

Layername 194

Proxy-ARP 213

Q

Quell-Ports 213

R

redundante Routen

Split Horizon 207

Remote Access

NetBIOS-Routing 241

Setup Assistant 169

Reservierung B-Kanälen 250

RIP- und SAP-Tabellen 206

künstliche Alterung 206

Round-Robin-Liste 192, 195

Router-Interface-Einstellungen 193

Unterdrückung der eigenen

Rufnummer 193

Y-Verbindung 193

Routing Information Protocol

(RIP) 206, 215

Rückruf 188

ISDN-Namenliste 192

Rückruf starten 197

Rufannahme 186, 197

für Routerfunktionen 196

RVS-COM 249

S

S0-Anschluss-Einstellungen 192, 193

Schutzanforderungen 12

Script-Liste 196

Layer 3 195

Service 15, 272

Service Advertising Protocol (SAP) 206

Service Pack 14, 64, 95, 107, 138, 147

Setup Assistant

Remote Access 169

Setup-Assistent

LAN-LAN Kopplung 170

Wireless LAN-LAN Kopplung 170

Sicherheit 184

Fast-Call-Back 188

Gebührensperre 160

IP-Masquerading 189

Kostenverteilung über Rückruf 188

Login-Sperre 185

MAC-Filter für WLAN Zugriff auf

WAN 150

Nummernliste

Rückruf starten 197

Rufannahme 197

Passwort 185

PPP-Liste

PAP, CHAP, MS-CHAP 201

Rückruf 188

Rufannahme 186

Rufannahme für

Routerfunktionen 196

Rufannahme Gegenstellen 187

mit Passwort nach PAP, CHAP

oder MS-CHAP in PPP-Liste 187

TCP/IP Paketfilter 213

TCP/IP Zugangskontrolle 186

WEP 189

AccessPoint Einstellungen 152

MobilePort Einstellungen 113

SNMP 181

Socket-Filtertabelle 209

Sockets 209

Software-Reset des AccessPoints 264

Spannungsumschaltungssoftware 256

Split Horizon 207, 209

SSID (=WLAN-Domain)

kontrollieren im MobilePort 258

SSID (=WLAN-Domain) ändern 147

im AccessPoint 147

im MobilePort 148

Standard Installation 10, 21
 Ablauf 29
 WLAN mit Internet-Zugang 23
 WLAN-LAN Internet Zugang 27
 WLAN-LAN Kopplung 25
Support 15, 272
Systemanforderungen 14

T

TCP 219
TCP/IP Zugangskontrolle 186
TCP/IP-Paketefilter 213
Technische Daten 16, 268
Telnet 162
Type-of-Service(TOS)-Feld 221

U

UDP 213, 219
Unterdrückung der eigenen
 Rufnummer 193
Upload
 DSL-Firmware 182
 LAN-Firmware 182

W

WEBconfig 174
WEP 189
 AccessPoint Einstellungen 152
 MobilePort Einstellungen 113
Windows NT auf Notebook
 PC Card Software 256
winipcfg 259
WINS-Server (Windows-Internet-Name-
 Service-Server) 234
Wireless LAN-LAN Kopplung
 Setup-Assistent 170
WLAN-Domain (=SSID) ändern 147
 im AccessPoint 147
 im MobilePort 148
www.siemens.com/i-gate 15, 272

X

xDSL 182

Y

Y-Verbindung 193

Z

Zeitsteuerung für die Default-Route 220
Zeitsteuerungstabelle 220
Ziel-Ports 213