

SIEMENS



Hicom 150 H / Hicom 150 E Office **Administrationsanleitung für** **HiPath HG 1500**

Gültigkeitsbereich

Dieses Handbuch beschreibt die HiPath HG 1500 Version 2.0.

Die HiPath HG 1500 kann sowohl an der Hicom 150 E Office Point/Com/Pro (ab Release 2.2) als auch an der Hicom 150 H Office Point/Com/Pro (ab Version 1.0) sowie HiPath 3000 V3.0 mit neuen Baugruppen (siehe →Seite 82) betrieben werden.

Die im Handbuch aufgeführten „System-Clients“ bezeichnen den „C55 optiClient“/ „optiClient 130 V1.0 und V2.0,“den Adapter „optiPoint IPadapter“ und das IP-Telefon optiPoint 400.

Wegweiser zum Lesen der Anleitung

Fett markierte Ausdrücke im Fließtext sind Originalbegriffe, die Sie so im Administrationsprogramm Assistant I oder im Betriebssystem als Schaltflächen oder Textstellen wiederfinden.

- Texte mit dieser Markierung sind Aufzählungen
- Numerierte Texte beschreiben Tätigkeitsschritte, die der Reihe nach auszuführen sind.



Dieses Zeichen weist auf besondere Hinweise und zusätzliche Informationen hin!

Benutzerkreis

Dieses Handbuch ist für den Netzwerk-Administrator, der für LANs und deren Kommunikation nach außen zuständig ist. Der Administrator sollte Grundkenntnisse über ISDN besitzen. Alle kundenindividuell notwendigen Funktionen können vom Administrator mit dem Administrationsprogramm Assistant I angepasst werden.

Aufbau des Handbuchs

Das Kapitel **Übersicht über die Leistungsmerkmale** gibt einen kurzen Überblick über die Fähigkeiten der eingesetzten Baugruppe

Das Kapitel **Inbetriebnahme** erläutert die notwendigen Arbeitsschritte zur Inbetriebnahme des Systems sowie zur Einrichtung des Administrationsprogramms der HiPath HG 1500.

Im Kapitel **Administration mit Assistant I** werden die einzelnen Menüpunkte und Icons aufgeführt und beschrieben. Es gibt Ihnen eine Übersicht über alle veränderbaren Parameter.

Im Kapitel **Anwendungen** sind die einzelnen Anwendungen, wie Voice over IP, Routing, Telematikdienste, etc. aufgeführt. Im Einzelnen werden die Einrichtungen der Anwendungen beschrieben.

Das Kapitel **Einrichtungsbeispiele** enthält eine Sammlung von Anwenderhilfen zur Einrichtung der HiPath HG 1500 und der mit ihr verbundenen Anwendungen.

Das Kapitel **Anhang** hilft Ihnen bei der Beseitigung von Fehlern, die bei der Einrichtung oder dem laufenden Betrieb der HiPath HG 1500 auftreten können. Hier finden Sie auch die Beschreibung zu weiteren nützlichen Hilfsprogrammen.

Wichtige Hinweise	7
Sicherheitshinweise	7
CE-Kennzeichen	7
Umweltschutz-Kennzeichen	7
Übersicht über die Leistungsmerkmale	8
Inbetriebnahme	11
Übersicht	11
Integration der HiPath HG 1500 in verschiedene Netzwerktopologien	12
Stern-Topologie mit Hub (10/100 BaseT)	12
Einrichten des Admin-PCs	13
Administrationsprogramm einrichten	13
Erstinbetriebnahme über den ersten LAN-Anschluss	14
Erstinbetriebnahme von Remote (Servicezentrum)	14
Erstinbetriebnahme über serielle Schnittstelle	14
Administration mit Assistant I	25
Start von Assistant I	25
Symbol- und Menüleiste	26
Menüleiste	26
Symbolleiste	27
Erstgenerierung	29
Erklärung der Menüfunktionen	33
Menü „Datei“	33
Menü „Einstellungen“	36
Menü „Optionen“	73
Menü „Service“	74
Anwendungen	76
Voice over IP	76
Allgemeine Parameter für Voice over IP	76
System-Client	77
H.323-Client	79
IP Networking (PBX-Routing)	81
Einleitung	81
KDS um Informationen für IP Networking ergänzen	82
Einstellungen der HiPath HG1500-Baugruppe(n) vornehmen	86
Bandbreitenmanagement	89
Quality of Service (QoS)	90
Telematik mit dem vCAPi-Client	93
Prinzip der virtuellen bzw. verteilten CAPI (vCAPi)	93
Identifizierung der CAPI-Teilnehmer	93

Einrichtung vCAPi-Client	94
vCAPi und Smartset.	96
vCAPi und TAPI	97
vCAPi und Fax	98
vCAPi und Filetransfer.	100
vCAPi und Internet.	101
Routing	102
LAN-LAN und Teleworking	102
Besonderheiten bei Windows-Netzwerken	106
Gebührenzuordnung/Callback	107
Internetzugang.	108
IP-Adressmapping	114
Remote Control	116
Schutzmechanismen („Security“)	117
Firewall	118
Gatekeeper	122
Gatekeeper mit einer HiPath HG 1500	123
Gatekeeper mit mehreren HiPath HG 1500s.	125
Mehrere Gatekeeper mit einer HiPath HG 1500 und mehreren H.323-Zonen.	126
SNMP anwenden	128

Einrichtungsbeispiele 130

Internet Provider	130
Routing HiPath HG 1500 zu HiPath HG 1500	134
Hostrouting	136
Remote Access Service (RAS)	137
DFÜ-Netzwerk	139
ITK Columbus Client Pro	140
AVM Netways (ab Version 3.0 Revision 3)	141
WindowsNT 4.0 Workstation mit Teleworking / RAS	144
Teleworking mit Log-in an NT Domäne	145
HiPath HG 1500, IPX Routing und Teleworking an Novell.	146
Routing und Callback mit Cisco-Routern	148
Telematik	150
Rufnummernvergabe bei Telematik.	150
FRITZ!vox/fon	151
FRITZ!fax und Rufweiterleitung.	151

Anhang 152

LAN-Lösungsvorschläge	152
BNC-Netz an Twisted Pair	152
3COM Dual Speed HUB	153
Lösungsansatz mit Switch.	154
HiPath HG 1500 in Token Ring Netzwerken	155

Dienstprogramme zur Diagnose von TCP/IP	156
ping	156
ipconfig	158
nslookup	159
hostname	161
netstat	161
nbtstat	165
route	166
tracert	168
arp	169
telnet	170
IP-Adressierung: Subnetze	171
Portnummern	178
Ungewollter Verbindungsaufbau ins Internet (DNS-Anfragen)	180
Kunden-Trace	181
Protokollierungsfunktion	181
ETSI-Fehlermeldungen	181
PC- Soundeinstellungen für Voice over IP	184

Abkürzungsverzeichnis..... 186

Stichwortverzeichnis 189

Wichtige Hinweise

Sicherheitshinweise



Betreiben Sie die Hardware-Komponenten Ihrer HiPath HG 1500 nicht in explosionsgefährdeter Umgebung!



Benutzen Sie nur Siemens Original-Zubehör! Das Benutzen von anderem Zubehör ist gefährlich und führt zum Erlöschen der Garantie und der CE-Kennzeichnung.



Öffnen Sie niemals die Hardware-Komponenten Ihrer HiPath HG 1500! Bei Problemen wenden Sie sich an autorisiertes Fachpersonal.

Die Hardware-Komponenten Ihrer HiPath HG 1500 sollen nicht mit färbenden oder aggressiven Flüssigkeiten, wie z. B. Tee, Kaffee, Säften oder Erfrischungsgetränken in Berührung kommen.

CE-Kennzeichen



Die Konformität des Gerätes zu der EU-Richtlinie 1999/5/EG wird durch das CE-Kennzeichen bestätigt.

Umweltschutz-Kennzeichen



Dieses Gerät wurde nach unserem zertifizierten Umweltmanagementsystem (ISO 14001) hergestellt. Dieser Prozess stellt die Minimierung des Primärrohstoff- und des Energieverbrauchs sowie der Abfallmenge sicher.

Übersicht über die Leistungsmerkmale

Die HiPath HG 1500 ist eine Erweiterungsbaugruppe für die Hicom 150 H Office Point/Com/Pro. Damit können Sie die Hicom 150 H an ein lokales LAN anbinden und Verbindungen zu externen LANs über das ISDN-Betriebersnetz herstellen. Die Hicom 150 H wird somit zum zentralen Kommunikationsserver im LAN. Voraussetzung dafür ist TCP/IP oder IPX/SPX als Transportprotokoll und Windows 95/98, Windows NT 4.0 oder Windows 2000 als Betriebssystem.

Funktionen der HiPath HG 1500:

- **Voice over IP**

Mit der Funktion „Voice over IP“ können die HiPath HG 1500-Clients mit dem PC über das LAN telefonieren und die Leistungsmerkmale der Hicom 150 H Office Point/Com/Pro nutzen. Zusätzlich können H.323-Clients eingerichtet werden, z. B. für NetMeeting.

- **Routing**

HiPath HG 1500 unterstützt die klassischen Funktionen eines ISDN-(IP/IPX-) Routers. Damit können Sie die in der HiPath HG 1500 integrierten Routing- und Sicherheitsfunktionen nutzen (wie z. B. „Central Firewall“, gebührenoptimierter „Short Hold Modus“, Kanalbündelung nach Bedarf, bis zu 16 B-Kanäle (konfigurierbar), Filtern von Broadcasts).

- **LAN-LAN-Kopplung / RAS**

Durch die LAN-LAN-Kopplung werden Ethernet-LANs an verschiedenen Standorten über ISDN-Wählleitungen zu einem einzigen Firmennetz verbunden. So haben Außenstellen und Teleworking-PCs (über RAS) Zugriff auf die Netzwerkressourcen (z. B. Zugriff auf Datenbanken, E-Mails, Faxpostfächer, Druckauftrag einleiten, usw.).

- **vCAPI-Schnittstelle für Telematik-Dienste**

Über die virtuelle CAPI-Schnittstelle (vCAPI) ist PC-gestütztes Telefonieren möglich. Telematik-Funktionen, wie z. B. Faxabruf, EuroFileTransfer, Onlinedienste können genutzt werden.

- **TAPI-Schnittstelle für CTI-Dienste**

Über die TAPI-Schnittstelle (CSTA) ist PC-gestütztes Telefonieren möglich. CTI-Funktionen, wie z. B. Wahlhilfe, Anrufjournal oder „Smartset für ISDN“ können genutzt werden.

- **Internet-Zugang**

Der Internet-Zugang bietet folgende Leistungsmerkmale:

- Dynamischer Bezug der IP-Adresse vom Internet Provider
- Zugang zum Internet über eine einzige IP-Adresse eines Internet Providers, d. h. kostengünstige Lösung für alle PCs im Netzverbund
- Dynamische oder statische Kanalbündelung (Zuschaltung von B-Kanälen je nach Auslastung)

– Anbindung zum Provider über DSL. Neben T-DSL, das **PPPoE** verwendet, wird auch das Protokoll **PPTP** unterstützt (für Provider z. B. in den Niederlanden, in Frankreich und Österreich).

– Zweites LAN-Interface zur Entkopplung vom WAN-Anschluss

- **Administration über PC-Programm Assistant I**

Die HiPath HG 1500 kann über den Admin-PC mit dem Administrationsprogramm Assistant I eingerichtet werden.

- **Kanalbündelung (PPP-Multilink)**

Beim Datenaustausch über ISDN kann durch „Kanalbündelung“ die Datenübertragungsrate auf n-mal 64 Kbit/s gesteigert werden (bis zu 16 Kanälen, anlagenabhängig). Das PPP-Multilink-Protokoll ermöglicht es, Datenpakete über mehrere Datenverbindungen hinweg aufzuteilen.

- **Zugangskontrolle**

Eine Zugangskontrolle (Firewall) verhindert das unberechtigte Eindringen in das firmeneigene LAN. Die Firewallmechanismen sind:

– ISDN-Rufnummernüberprüfung

– Anforderung eines automatischen Rückrufs ohne Herstellung einer kostenpflichtigen ISDN-Verbindung (mit entsprechender Zusatzsoftware)

– Überprüfung der IP- oder IPX-Adressierung

– MAC-Firewall (Überprüfung der Kombination MAC-/IP-Adresse)

– Überprüfung der IP-Adresse bezüglich Portnummern

- **Unterstützung für externen Gatekeeper**

Der Gatekeeper registriert die H.323-Clients und verwaltet deren Rechte und Dienste. Er setzt die Rufnummern der Clients in logische Namen oder IP-Adressen um und umgekehrt. Zudem registriert er die Gateways und kann mit benachbarten Gatekeepern vernetzt werden.

- **Quality of Service (QoS)**

Um die benötigte Bandbreite für Voice over IP zu sichern, können IP-Pakete markiert werden und dadurch im LAN/WAN bevorzugt transportiert werden.

- **Vernetzung von mehreren Anlagen über IP**

Es können mehrere Hicom Telefonanlagen untereinander mit Voice over IP (H.323) zur Telefonie vernetzt werden (gültig ab Hicom 150 H).

- **Authentifizierung**

Wird eine externe Verbindung über die HiPath HG 1500 hergestellt, können zur Erhöhung der Sicherheit in Datennetzen die Verfahren PAP (Password Authentication Protocol) und CHAP (Challenge Handshake Authentication Protocol) zur Authentifizierung der Teilnehmer genutzt werden.

- **Zweiter LAN-Anschluss (optional)**

Zur Entkopplung des DSL-WAN-Anschlusses ist einer zweiter LAN-Anschluss eingerichtet. Die Anbindung zum ersten LAN erfolgt über eine Routing-Funktion.

- **DSL-Unterstützung (optional)**

Die Konfigurations-Datenbasis ist um ein zusätzliches Interface erweitert. Die notwendigen Angaben zur Einwahl in das DSL-Netzwerk werden hier angegeben. Über den Assistant I können die erweiterten Konfigurationsparameter gepflegt werden. Die DSL-Funktionalität ist nur bei einem zweiten LAN-Anschluss möglich.

Inbetriebnahme

Übersicht

Die Inbetriebnahme der HiPath HG 1500 erfolgt zusammen mit dem Netzwerkadministrator und Ihrem Siemens-Servicetechniker.

Die Erstkonfiguration der HiPath HG 1500 (siehe → 13) erfolgt in der Regel über den LAN-Anschluss. Die Erstinbetriebnahme ist auch von Remote möglich (z. B. aus einem Servicezentrum). Bei der Erstkonfiguration über SLIP ist ein V.24-Adapter (S30122-X5468-X3) notwendig. Die Anbindung des Admin-PCs erfolgt hierbei über DFÜ. Die Einrichtung von DFÜ auf dem Admin-PC wird im Kapitel „Einrichten des Admin-PCs“ siehe → 13 beschrieben. Auf dem Admin-PC muss das Administrationsprogramm für HiPath HG 1500 eingerichtet sein.

Bei der Erstinbetriebnahme übertragen Sie zunächst einen Kundendaten-speicher (KDS) zum Admin-PC. Bearbeiten Sie diesen KDS und übertragen Sie ihn anschließend zur HiPath HG 1500. Den Softwarestand der HiPath HG 1500 können Sie unter dem Menüpunkt Grundeinstellungen ablesen.



Nehmen Sie die Erstinbetriebnahme von HiPath HG 1500 bitte nur zusammen mit Ihrem Servicetechniker vor!

Bei Fehlkonfigurationen Ihrer HiPath HG 1500 kann es unter Umständen möglich sein, dass Sie den Zugang zu HiPath HG 1500 sperren!

Die HiPath HG 1500 ist in der Lage, bei entsprechender Konfiguration selbständig gebührenpflichtige Verbindungen aufzubauen. Entsprechend kann auch das LAN durch Routing mit anderen Partnern automatisch verbunden werden. Es wird deshalb dringend empfohlen, den ISDN-Verkehr der Baugruppe durch geeignete Massnahmen (z. B. Leitungstasten) zu kontrollieren und im Zweifelsfall den Verkehr durch Traces zu prüfen.

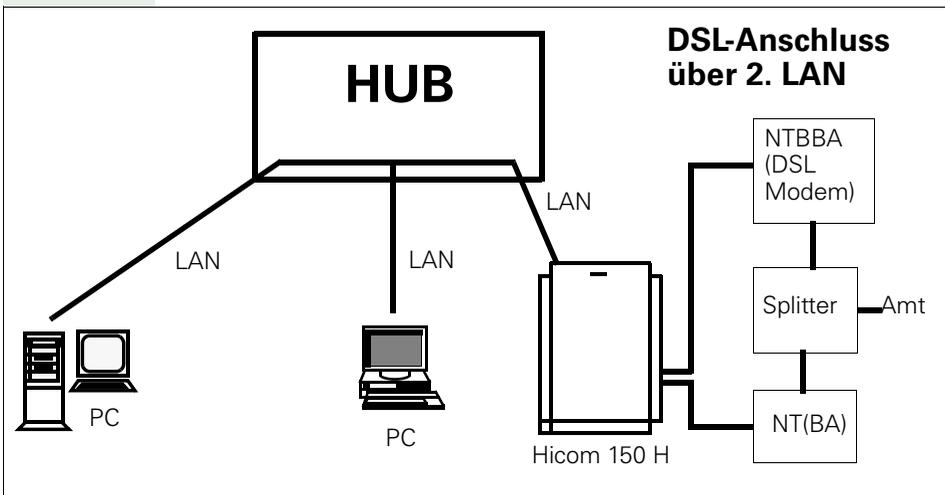
Integration der HiPath HG 1500 in verschiedene Netzwerktopologien

Die HiPath HG 1500 ist mit einem Twisted-Pair Port 10/100 MB autosense ausgerüstet.

In den Abbildungen wird stellvertretend für alle Ethernet-LAN-Typen jedoch der Einfachheit halber immer die Darstellungsform einer Bus-Verkabelung benutzt.

Stern-Topologie mit Hub (10/100 BaseT)

Bei dieser Netztopologie dient ein Hub oder Switch als zentrales Element. Von diesem aus wird jede Datenendeinrichtung über ein eigenes Twisted-Pair Kabel (z. B. 10/100 BaseT-Ethernet) angeschlossen. Ein Standard-Hub bildet dabei intern einen Bus nach. Bei Ausfall eines Kabels ist nur ein Endgerät betroffen. Die integrierte HiPath HG 1500 kann direkt angeschlossen werden.



Hinweise:

- Max. Gesamtlänge vom HUB/Switch zur HiPath HG 1500 = 100 Meter.
- An andere Bus-Topologien (z. B. 10 Base 2) kann die HiPath HG 1500 nur über einen Hub oder Switch angeschlossen werden, der eine entsprechende Umsetzung bietet.

Einrichten des Admin-PCs

Das Betriebssystem Windows 3.11 wird nicht mehr unterstützt.

Voraussetzung:

Die Netzwerkkarte muss mit dem TCP/IP-Protokoll auf dem Admin-PC funktionsfähig installiert sein.

Administrationsprogramm einrichten

Mit dem Administrationsprogramm Assistant I können Sie die HiPath HG 1500 einrichten und verwalten. Bei der Erstinbetriebnahme sollte der Assistant I vom Siemens Servicetechniker auf dem Admin-PC eingerichtet werden.

1. Rufen Sie das Setup-Programm von der Diskette oder der Installations-CD auf. Starten Sie dazu den Windows-Explorer und wechseln Sie auf das Disketten- oder CD-ROM-Laufwerk. Klicken Sie doppelt auf die Datei „setup.exe“
2. Das Setup-Programm des Assistant I wird aufgerufen. Befolgen Sie die Anweisungen des Setup-Programms.
3. Die Programmdateien werden auf Ihre Festplatte kopiert und der Assistant I in der Windows-Startleiste eingerichtet. Die Installation des Assistant I ist abgeschlossen.

Die Einrichtung der HiPath HG 1500 mit Hilfe des Assistant I ist im Kapitel „Administration mit Assistant I“ beschrieben.

Erstinbetriebnahme über den ersten LAN-Anschluss

1. Ist auf der HiPath HG 1500 die Default-IP-Adresse „10.144.233.63“ konfiguriert (Grundeinstellung ab Werk, Default-KDS), so wird ein besonderer Mechanismus aktiviert, um die Erstinbetriebnahme zu erleichtern.

Wenn die Baugruppe mit diesem KDS in Betrieb genommen wird, so schickt sie Anfragen ins LAN, um eine IP-Adresse zu erfragen.

Wird diese Anfrage mit einer IP-Adresse beantwortet, so geht sie mit dieser Adresse in Betrieb und kann für die Administration von dem PC aus, der die Anfrage beantwortet hat, administriert werden.

Mit einem statischen Eintrag in die ARP-Tabelle des Administrations-PC kann der HiPath HG 1500 eine IP-Adresse gegeben werden.

Hierzu wird in einem MSDOS-Kommandofenster der Befehl

```
arp -s ipadresse macadresse  
eingegeben (siehe auch -> arp siehe → 169).
```

Formatbeispiel:

```
arp -s 192.168.100.245 08-00-06-0f-ec-04
```

Die MAC-Adresse der Baugruppe ist durch einen Aufkleber auf der Baugruppe angegeben.

2. Aus dem MSDOS-Kommandofenster einen Ping auf die HiPath HG 1500 mit der neuen IP-Adresse starten. Wenn der Ping von der HiPath HG 1500 erfolgreich beantwortet wurde, kann mit der Administration fortgefahren werden.



Diese Einstellungen sind nur temporär und werden erst durch Eintrag in den KDS dauerhaft auf der Baugruppe gesichert.

Sicherheitshinweis:

Solange noch kein KDS zur Baugruppe übertragen wurde, kann der oben beschriebene Mechanismus von jedem PC im LAN genutzt werden!

Erstinbetriebnahme von Remote (Servicezentrum)

Abhängig von den Administrationsvorgängen durch den Servicetechniker der Hicom-Anlage kann zum Zweck der Erstinbetriebnahme durch das Servicezentrum ein ISDN-Partner und das ISDN2-Interface im Ersthochlauf der HiPath HG 1500 generiert werden. Ebenfalls wird in diesem Fall die IP-Adresse 10.186.237.64 zur Konfiguration freigeschaltet. Dieser Zugang kann nur bei der Erstinbetriebnahme angelegt werden. Entsprechend des gewählten Servicekonzepts muß dieser Eintrag ggf. wieder entfernt werden.

Erstinbetriebnahme über serielle Schnittstelle

Die Erstinbetriebnahme über die serielle Schnittstelle ist nur dann durchzuführen, wenn die Erstinbetriebnahme über LAN-Anschluss nicht möglich ist.

Voraussetzungen:

Die SLIP-Verbindung (DFÜ-Netzwerk) muss – abhängig vom Betriebssystem – installiert sein.

1. Das serielle Schnittstellenkabel (S30122-X5468-X3) anschließen.
2. DFÜ-Netzwerk installieren und konfigurieren, wie nachstehend für die verschiedenen Windows-Versionen beschrieben.
3. IP-Adresse des Admin-PCs (SLIP) „1.0.0.2“ im DFÜ-Netzwerk einstellen.
4. Über DFÜ-Netzwerk Verbindung zur HiPath HG 1500 herstellen.

Vorbereiten des Admin-PC mit WIN 95 Version A oder B



Falls Windows 95 installiert ist, muss WinSock2 durch ein Update aktualisiert werden. Microsoft bietet dieses Windows Socket 2 Update auf seiner Homepage an.

Kontrolle, ob das DFÜ-Netzwerk bereits installiert ist:

Klicken Sie auf **Start/Einstellungen/Systemsteuerung/Software/Windows-Setup/Verbindungen/Details**. Ist das DFÜ-Netzwerk mit einem Häkchen markiert, ist es bereits installiert. Sie können in diesem Fall das DFÜ-Netzwerk einrichten. Ist es nicht markiert, müssen Sie es zuvor installieren.

Installation des DFÜ-Netzwerks:

1. Klicken Sie auf **Start/Einstellungen/Systemsteuerung/Software/Windows-Setup/Verbindungen/Details**.
2. Klicken Sie **DFÜ-Netzwerk** an und bestätigen Sie mit OK.
3. Legen Sie die Windows-CD in das CD-ROM-Laufwerk ein. Das DFÜ-Netzwerk wird installiert.

Einrichten des DFÜ-Netzwerks:

1. Klicken Sie doppelt auf **Arbeitsplatz/DFÜ-Netzwerk**.
2. Es startet der Assistent zum Einrichten des DFÜ-Netzwerks. Klicken Sie auf **Weiter**.
3. Klicken Sie die Option **Modem auswählen (Keine automatische Erkennung)** an, Wählen Sie im nächsten Fenster als Standardmodemtyp **Standard-9600-bps-Modem** aus und geben Sie im folgenden Fenster einen COM-Anschluss an (z. B. COM1). Das Modem wird installiert.
4. Geben Sie Land, Vorwahl und als Wahlverfahren **MFV (Ton)** an. Das Modem ist konfiguriert.
5. Zuletzt müssen Sie der neuen DFÜ-Verbindung noch einen Namen geben (z. B. „SLIP zu HiPath HG 1500“) und im nächsten Fenster im Feld **Rufnummer** eine „1“ eingeben. Wenn Sie mit **Weiter** und **Fertig stellen** abschließen, wird die neue Verbindung erstellt.
6. Damit die SLIP-Eigenschaften definiert werden können, muss die Scriptunterstützung nachinstalliert werden. Die Installation der Scriptunterstützung ist von der verwendeten Windows-Version abhängig:
Windows 95 A oder B Update-Version:
Legen Sie die Windows-CD in das CD-ROM-Laufwerk und wechseln Sie mit dem Windows-Explorer in das CD-Verzeichnis
„...Admin\Apptools\DScript\SLIP.“Aktivieren Sie „Scriptunterstützung für DFÜ-Netzwerk.“Die Scriptunterstützung wird von der CD geladen.
Windows 95 A oder B OEM-Version:

Wechseln Sie mit dem Windows-Explorer in das LAN-Bridge-Verzeichnis „...\\LAN Bridge\\SLIP dfue\\Neu“ auf Ihrer Festplatte. Klicken Sie mit der rechten Maus-Taste auf die Datei „Rnapius.inf“ und wählen Sie den Menüpunkt **Installieren**. Klicken Sie im nachfolgenden Fenster auf **OK** und geben Sie anschließend das gleiche Verzeichnis wie vorher „...\\LAN Bridge\\SLIP dfue\\Neu“ ein für die gesuchte Datei „cis.scp“. Bestätigen Sie mit OK und die Scriptunterstützung ist nachinstalliert.

7. Eigenschaften der DFÜ-Verbindung definieren:
Wählen Sie die neu angelegte DFÜ-Verbindung aus über **Arbeitsplatz/DFÜ-Netzwerk/SLIP zu HiPath HG 1500**. Öffnen Sie mit der rechten Maus-Taste den Menüpunkt **Eigenschaften**. Klicken Sie auf die Schaltfläche **Servertypen** und wählen Sie den Typ **SLIP: Unix Connection** aus. Deaktivieren Sie die Option **Am Netzwerk anmelden**. Klicken Sie auf die Schaltfläche **TCP/IP-Einstellungen** und geben Sie die IP-Adresse „1.0.0.2“ ein. Die Optionen **IP-Header-Komprimierung** und **Standard-Gateway im Remote-Netzwerk verwenden** deaktivieren. Bestätigen Sie anschließend mehrmals mit OK.
8. Öffnen Sie das Fenster „Eigenschaften für DFÜ-Treiber“ über **Start/Einstellungen/Systemsteuerung/Netzwerk/DFÜ-Adapter** mit der Schaltfläche **Eigenschaften**. Im Register **Bindungen** soll nur „TCP/IP -> DFÜ-Treiber“ markiert sein.
9. Öffnen Sie das Fenster „Eigenschaften für TCP/IP“ über **Start/Einstellungen/Systemsteuerung/Netzwerk/TCP/IP** mit der Schaltfläche **Eigenschaften**. Im Register **IP-Adresse** muss die Option **IP-Adresse automatisch beziehen** markiert sein. Ansonsten können die Default-Einstellungen verwendet werden.
10. Starten Sie Windows neu.
Wenn Sie die DFÜ-Verbindung über **Arbeitsplatz/DFÜ-Netzwerk/SLIP zu HiPath HG 1500** per Doppelklick starten, wird nach Bestätigung des Anmelde-Fensters ein Symbol in der Taskleiste abgelegt und die Verbindung bleibt im Hintergrund aktiv.

Vorbereiten des Admin-PC mit WIN 95 Version C



Falls Windows 95 installiert ist, muss WinSock2 durch ein Update aktualisiert werden. Microsoft bietet dieses Windows Socket 2 Update auf seiner Homepage an.

Kontrolle, ob das DFÜ-Netzwerk bereits installiert ist:

Klicken Sie auf **Start/Einstellungen/Systemsteuerung/Software/Windows-Setup/Verbindungen/Details**. Ist das DFÜ-Netzwerk mit einem Häkchen markiert, ist es bereits installiert. Sie können in diesem Fall das DFÜ-Netzwerk einrichten. Ist es nicht markiert, müssen Sie es zuvor installieren.

Installation des DFÜ-Netzwerks:

1. Klicken Sie auf **Start/Einstellungen/Systemsteuerung/Software/Windows-Setup/Verbindungen/Details**.
2. Klicken Sie **DFÜ-Netzwerk** an und bestätigen Sie mit OK.
3. Legen Sie die Windows-CD in das CD-ROM-Laufwerk ein. Das DFÜ-Netzwerk wird installiert.

Einrichten des DFÜ-Netzwerks:

1. Klicken Sie doppelt auf **Arbeitsplatz/DFÜ-Netzwerk/Neue Verbindung erstellen**.
2. Es startet der Assistent zum Einrichten des DFÜ-Netzwerks. Klicken Sie auf **Weiter**.
3. Geben Sie der neuen DFÜ-Verbindung einen Namen (z. B. „SLIP zu HiPath HG 1500“) und wählen Sie als Modem **Standard-9600-bps-Modem** aus. Bestätigen Sie mit **Weiter**.
4. Tragen Sie die Vorwahl ein, geben im Feld **Rufnummer** eine „1“ ein und wählen Sie Ihre Landeskennzahl aus. Wenn Sie mit **Weiter** und **Fertig stellen** abschließen, wird die neue Verbindung erstellt.
5. Eigenschaften der DFÜ-Verbindung definieren:
Wählen Sie die neu angelegte DFÜ-Verbindung aus über **Arbeitsplatz/DFÜ-Netzwerk/SLIP zu HiPath HG 1500**. Öffnen Sie mit der rechten Maus-Taste den Menüpunkt **Eigenschaften**. Klicken Sie auf die Schaltfläche **Servertypen** und wählen Sie den Typ **SLIP: Unix Connection** aus. Deaktivieren Sie die Option **Am Netzwerk anmelden**. Klicken Sie auf die Schaltfläche **TCP/IP-Einstellungen** und geben Sie die IP-Adresse „1.0.0.2“ ein. Die Optionen **IP-Header-Komprimierung** und **Standard-Gateway im Remote-Netzwerk verwenden** deaktivieren. Bestätigen Sie anschließend mehrmals mit OK.

6. Öffnen Sie das Fenster „Eigenschaften für DFÜ-Treiber“ über **Start/Einstellungen/Systemsteuerung/Netzwerk/DFÜ-Adapter** mit der Schaltfläche **Eigenschaften**. Im Register **Bindungen** soll nur „TCP/IP -> DFÜ-Treiber“ markiert sein.
7. Öffnen Sie das Fenster „Eigenschaften für TCP/IP“ über **Start/Einstellungen/Systemsteuerung/Netzwerk/TCP/IP** mit der Schaltfläche **Eigenschaften**. Im Register **IP-Adresse** muss die Option **IP-Adresse automatisch beziehen** markiert sein. Ansonsten können die Default-Einstellungen verwendet werden.
8. Starten Sie Windows neu.
Wenn Sie die DFÜ-Verbindung über **Arbeitsplatz/DFÜ-Netzwerk/SLIP zu HiPath HG 1500** per Doppelklick starten, wird nach Bestätigung des Anmelde-Fensters ein Symbol in der Taskleiste abgelegt und die Verbindung bleibt im Hintergrund aktiv.

Vorbereiten des Admin-PC mit WIN 98

Kontrolle, ob das DFÜ-Netzwerk bereits installiert ist:

Klicken Sie auf **Start/Einstellungen/Systemsteuerung/Software/Windows-Setup/Verbindungen/Details**. Bei Windows 98 ist das DFÜ-Netzwerk in der Regel bereits installiert. Sie können in diesem Fall das DFÜ-Netzwerk einrichten. Ist das DFÜ-Netzwerk nicht mit einem Häkchen markiert, müssen Sie es zuvor installieren.

Installation des DFÜ-Netzwerks:

1. Rufen Sie die Installation des DFÜ-Netzwerks über **Start/Einstellungen/Systemsteuerung/Software/Windows-Setup/Verbindungen/Details** auf.
2. Klicken Sie die Option **DFÜ-Netzwerk** an und bestätigen Sie mit OK.
3. Legen Sie die Windows-CD in das CD-ROM-Laufwerk ein. Das DFÜ-Netzwerk wird installiert.

DFÜ-Netzwerkconfiguration:

1. Klicken Sie doppelt auf **Arbeitsplatz/DFÜ-Netzwerk**.
2. Es startet der Assistent zum Einrichten des DFÜ-Netzwerks. Klicken Sie auf **Weiter**.
3. Klicken Sie die Option **Modem auswählen (Keine automatische Erkennung)** an, Wählen Sie im nächsten Fenster als Standardmodemtyp **Standard-9600-bps-Modem** aus und geben Sie im folgenden Fenster einen COM-Anschluss an (z. B. COM1).
Das Modem wird installiert.
4. Geben Sie Land, Vorwahl und als Wahlverfahren **MFV (Ton)** an. Das Modem ist konfiguriert.

5. Klicken Sie doppelt auf **Neue Verbindung erstellen**. Geben Sie der Verbindung z. B. den Namen: „SLIP zu HiPath HG 1500.“Im nächsten Fenster geben Sie für die Rufnummer „1“ ein. Wenn Sie mit **Weiter** und **Fertig stellen** abschließen, wird die neue Verbindung erstellt.
6. Eigenschaften der DFÜ-Verbindung definieren:
Wählen Sie die neu angelegte DFÜ-Verbindung aus über **Arbeitsplatz/DFÜ-Netzwerk/SLIP zu HiPath HG 1500**. Öffnen Sie mit der rechten Maus-Taste den Menüpunkt „Eigenschaften.“Klicken Sie auf die Schaltfläche „Servertypen“ und wählen Sie den Typ **SLIP: Unix Connection** aus. Deaktivieren Sie die Option **Am Netzwerk anmelden**. Klicken Sie auf die Schaltfläche „TCP/IP-Einstellungen“ und geben Sie die IP-Adresse „1.0.0.2“ an. Die Optionen **IP-Header-Komprimierung** und **Standard-Gateway im Remote-Netzwerk verwenden** deaktivieren. Bestätigen Sie anschließend mehrmals mit OK.
7. Öffnen Sie das Fenster „Eigenschaften für DFÜ-Treiber“ über **Start/Einstellungen/Systemsteuerung/Netzwerk/DFÜ-Adapter** mit der Schaltfläche **Eigenschaften**. Im Register **Bindungen** soll nur „TCP/IP -> DFÜ-Treiber“ markiert sein.
8. Öffnen Sie das Fenster „Eigenschaften für TCP/IP“ über **Start/Einstellungen/Systemsteuerung/Netzwerk/TCP/IP** mit der Schaltfläche **Eigenschaften**. Im Register **IP-Adresse** muss die Option **IP-Adresse automatisch beziehen** markiert sein. Ansonsten können die Default-Einstellungen verwendet werden.
9. Starten Sie Windows neu.
Wenn Sie die DFÜ-Verbindung über **Arbeitsplatz/DFÜ-Netzwerk/SLIP zu HiPath HG 1500** per Doppelklick starten, wird nach Bestätigung des Anmelde-Fensters ein Symbol in der Taskleiste abgelegt und die Verbindung bleibt im Hintergrund aktiv.

Vorbereiten des Admin-PC mit NT4.0

Kontrolle, ob das DFÜ-Netzwerk bereits installiert ist:

Klicken Sie auf das Symbol **Arbeitsplatz** auf Ihrem Desktop und prüfen Sie ob ein Symbol für das DFÜ-Netzwerk vorhanden ist. Bei Windows NT ist das DFÜ-Netzwerk in der Regel bereits installiert. Ist kein DFÜ-Netzwerk vorhanden, müssen Sie es installieren.

Installation des DFÜ-Netzwerks:

1. Klicken Sie auf **Start/Einstellungen/Systemsteuerung/Netzwerk/Dienste**.
2. Fügen Sie den Dienst **RAS-Dienst** hinzu.
3. Legen Sie die Windows-CD in das CD-ROM-Laufwerk ein. Das DFÜ-Netzwerk wird installiert.

Einrichten des DFÜ-Netzwerks:

1. Klicken Sie doppelt auf **Arbeitsplatz/DFÜ-Netzwerk**.
2. Es startet der Assistent zum Einrichten des DFÜ-Netzwerks. Klicken Sie auf **Installieren** und anschließend auf **Ja**.
3. Klicken Sie die Option **Modem auswählen (Keine automatische Erkennung)** an, Wählen Sie im nächsten Fenster als Standardmodemtyp **Standard-9600-bps-Modem** aus und geben Sie im folgenden Fenster einen COM-Anschluss an (z. B. COM1). Klicken Sie auf **Weiter**.
4. Geben Sie Land, Vorwahl und als Wahlverfahren **MFV (Ton)** an. Das Modem ist konfiguriert.
5. Klicken Sie auf Fertigstellen. In den folgenden Fenstern „RAS-Gerät hinzufügen“ und „RAS Setup“ sollten Sie die vorgegebenen Einstellungen beibehalten. Klicken Sie dazu auf **OK** bzw. **Weiter**.
6. Klicken Sie nochmals doppelt auf **Arbeitsplatz/DFÜ-Netzwerk**.
7. Bestätigen Sie die Meldung „Telefonbuch leer“ mit **OK**. Es öffnet sich das Fenster „Assistent für neue Telefonbucheinträge“
8. Geben Sie der neuen DFÜ-Verbindung einen Namen (z. B. „SLIP zu Hi-Path HG 1500“) und aktivieren Sie im nächsten Fenster die dritte Option **Der Nicht-WindowsNT-Server...**. Geben Sie in den folgenden Fenstern im Feld **Rufnummer** eine „1“ ein und aktivieren Sie die Optionen **SLIP (Serial Line Internet Protocol)** und **Terminalfenster verwenden**. Bestätigen Sie jeweils mit **Weiter**.
9. Es erscheint das Fenster „Adressen des Namens-Servers.“ Lassen Sie die beiden IP-Adressen auf „0.0.0.0.“ Wenn Sie mit **Weiter** und **Fertigstellen** abschließen, wird die neue Verbindung erstellt.

10. Eigenschaften der DFÜ-Verbindung definieren:
Wählen Sie die neu angelegte DFÜ-Verbindung aus über **Arbeitsplatz/DFÜ-Netzwerk/SLIP zu HiPath HG 1500**. Klicken Sie auf die Schaltfläche **Weiteres** und wählen Sie den Menüpunkt **Eintrags- und Modemeigenschaften** aus. Wählen Sie als Typ des DFÜ-Servers **SLIP Internet** aus und aktivieren Sie die Option **TCP/IP**. Klicken Sie auf die Schaltfläche **TCP/IP-Einstellungen** und geben Sie im folgenden Fenster die IP-Adresse „1.0.0.2“ an. Die Optionen **IP-Vorspannkomprimierung** und **Standard-Gateway im Remote-Netzwerk verwenden** deaktivieren. Ansonsten können die Default-Einstellungen verwendet werden. Bestätigen Sie mit OK.
11. Öffnen Sie das Fenster „Eigenschaften für DFÜ-Treiber“ über **Start/Einstellungen/Systemsteuerung/Netzwerk/DFÜ-Adapter** mit der Schaltfläche **Eigenschaften**. Im Register **Bindungen** soll nur „TCP/IP -> DFÜ-Treiber“ markiert sein.
12. Öffnen Sie das Fenster „Eigenschaften für TCP/IP“ über **Start/Einstellungen/Systemsteuerung/Netzwerk/TCP/IP** mit der Schaltfläche **Eigenschaften**. Im Register **IP-Adresse** muss die Option **IP-Adresse automatisch beziehen** markiert sein. Ansonsten können die Default-Einstellungen verwendet werden.
13. Starten Sie Windows neu.
Wenn Sie die DFÜ-Verbindung „SLIP zu HiPath HG 1500“ über **Arbeitsplatz/DFÜ-Netzwerk** starten, können Sie nach erfolgreicher Verbindung das Fenster „Verbindung hergestellt“ mit **OK** schließen. Es wird dann ein Symbol in der Taskleiste abgelegt und die Verbindung bleibt im Hintergrund aktiv. Wenn Sie auf das Symbol in der Taskleiste klicken, können Sie sich Informationen zu der bestehenden Verbindung anzeigen lassen.

Vorbereiten des Admin-PC mit Windows 2000

Prüfen, ob das Standard-9600bps-Modem installiert ist:

1. Klicken Sie auf Start/Einstellungen/Systemsteuerung
2. Klicken Sie auf Telefon- und Modemoptionen
3. Wenn dort kein „Standard 9600bps-Modem“ aufgeführt ist, klicken Sie auf „hinzufügen“
4. Aktivieren Sie „Modem auswählen“ und „weiter“
5. Wählen Sie das „Standard 9600bps Modem“ aus der Liste aus und „weiter“
6. Wählen Sie die gewünschte COM-Schnittstelle aus und „weiter“, „Fertig stellen“

Damit ist das Modem eingerichtet.

Einrichten des DFÜ-Netzwerks

1. Klicken Sie auf Start/Einstellungen/Netzwerk- und DFÜ-Verbindungen/ Neue Verbindung erstellen
2. Der Netzwerkverbindungsassistent öffnet sich. Wählen Sie „In ein privates Netzwerk einwählen.“
3. Wählen Sie das Modem Standard 9600bps aus der Liste aus und „weiter“
4. Als Rufnummer geben Sie z. B. eine „1“ ein und „weiter“
5. Wählen Sie „für alle Benutzer verwenden“ und „weiter“
6. Geben Sie einen Namen ein, z. B. „SLIP zu HiPath HG 1500“ und „Fertig stellen“
7. Klicken Sie auf „Eigenschaften“
8. Im Register „Netzwerk“ unter „Typ des anzurufenden Einwählservers“ „SLIP Unix-Verbindung“ auswählen. Aktivieren Sie als Protokoll nur „TCP/IP“ und „Eigenschaften“
9. Wählen Sie „Folgende IP-Adresse verwenden“ und tragen Sie die „1.0.0.2“ ein.
10. Unter „Erweitert -> Allgemein“ deaktivieren Sie die Kontrollkästchen für „Standardgateway für das Remotenetzwerk verwenden“ und „IP-Headerkomprimierung“
11. Bestätigen Sie alle Eingaben.

Nun ist das DFÜ-Netzwerk eingerichtet.

Für die Administration der HiPath HG 1500 können Sie jetzt über „Start/Einstellungen/Netzwerk- und DFÜ-Verbindungen/SLIP zu HiPath HG 1500“ Verbindung über die serielle Schnittstelle mit der Baugruppe aufnehmen.

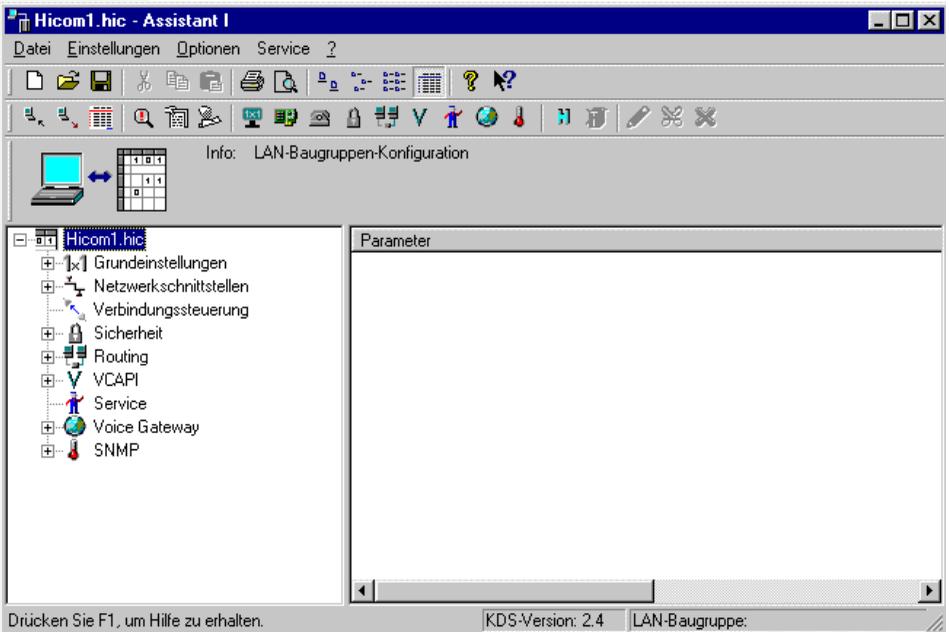
Administration mit Assistant I

Sie können von Ihrem PC die HiPath HG 1500 mit Hilfe des Administrationsprogramms Assistant I einrichten und Änderungen in der Konfiguration vornehmen. Erklärungen zu den einzelnen Schritten erhalten Sie auch über die kontextsensitive Windows-Hilfe, indem Sie an der entsprechenden Stelle die F1-Taste drücken.

Start von Assistant I

Der Start des Assistant I erfolgt über die Startleiste des Windows Betriebssystems.

➡ Zum Starten des Assistant I ist ein Benutzername und ein Kennwort erforderlich. Das Kennwort sollte nur den Administratoren von HiPath HG 1500 bekannt gegeben werden.



Symbol- und Menüleiste

Im folgenden ist der Inhalt der Menüleiste und die Bedeutung der Symbole in der Symbolleiste erklärt.

Menüleiste

Die Menüleiste besteht aus einer Reihe von Hauptmenüpunkten. Wenn Sie mit der linken Maustaste auf einen dieser Hauptmenüpunkte klicken, öffnet sich ein entsprechendes Untermenü (Pulldown-Menü) mit weiteren Menüpunkten.

Menü „Datei“

KDS <u>n</u> eu anlegen	Strg+N	siehe → 33
KDS <u>ö</u> ffnen...	Strg+O	siehe → 33
KDS <u>s</u> peichern...	Strg+S	siehe → 34
KDS <u>s</u> peichern <u>u</u> nter...		siehe → 34
KDS <u>d</u> rucken...	Strg+P	siehe → 34
S <u>e</u> itenansicht		siehe → 34
S <u>e</u> iteneinrichtung...		siehe → 34
Ü <u>b</u> ertragen des KDS zum PC	Strg+T	siehe → 34
Ü <u>b</u> ertragen des KDS zur Hicom Xpress @LAN	Strg+U	siehe → 35
Ü <u>b</u> ertragen des KDS zur Hicom Xpress @LAN mit Xpress Client-Paßwörtern	Strg+J	siehe → 35
Ü <u>b</u> ertragen der Log-Datei zum PC		siehe → 35
<u>B</u> eenden		siehe → 35

Menü „Einstellungen“

<u>G</u> rundeinstellungen	Alt+G	siehe → 36
<u>N</u> etzwerkschnittstellen	Alt+N	siehe → 40
<u>V</u> erbindungssteuerung	Alt+V	siehe → 46
<u>S</u> icherheit	Alt+S	siehe → 48
<u>R</u> outing	Alt+R	siehe → 51
<u>V</u> CAPi-Teilnehmer	Alt+C	siehe → 61
<u>S</u> ervice		siehe → 63
<u>V</u> oice Gateway	Alt+I	siehe → 67
<u>S</u> NMP	Alt+P	siehe → 71

Menü „Optionen“

Programmeinstellungen...	Strg+E	siehe → 73
Zurücksetzen der LAN-Baugruppe	Strift+H	siehe → 73
Administrierbare LAN-Baugruppen	Strg+H	siehe → 73
Benutzername und Kennwort wechseln...		siehe → 73
KDS konvertieren		siehe → 73

Menü „Service“

Empfangen+Speichern des Fehlerspeichers	Strg+L	siehe → 74
Empfangen+Speichern des Kunden-Trace		siehe → 74
Lösche Kunden-Trace		siehe → 74
Rufnummern anfordern		siehe → 74
PBX-Routingtabelle importieren		siehe → 74
APS-Transfer	Shift+A	siehe → 74
APS+KDS-Transfer		siehe → 74
APS-Transfer über TFTP		siehe → 75
Reset der LAN-Baugruppe		siehe → 75
Datum und Uhrzeit auf Baugruppe übertragen		siehe → 75

Menü „?“ (Hilfe)

Hilfe	F1
Info über Hicom Xpress @LAN...	

Symbolleiste

Über die Symbolleiste können Sie wichtige Funktionen, die Ihnen auch über die Menüleiste zur Verfügung stehen, direkt und somit schneller aufrufen. Hier sind die Symbole aufgelistet, die den Assistant I betreffen.



Kundendatenspeicher neu anlegen



Kundendatenspeicher öffnen



(KDS) speichern



(KDS) drucken



Seitenansicht



Übertragen des Kundendatenspeichers zum PC



Übertragen des Kundendatenspeichers zur HiPath HG 1500



Übertragen der Log-Datei zum PC



Empfangen+Speichern des Fehlerspeichers



Empfangen+Speichern des Kundentrace



Lösche Kunden-Trace



Bearbeiten der Grundeinstellungen



Bearbeiten der Netzwerkeinstellungen



Bearbeiten der Verbindungssteuerung



Bearbeiten der Sicherheitsparameter



Bearbeiten der Routing-Einstellungen



Bearbeiten der vAPI-Clients



Bearbeiten der Service-Einstellungen



Bearbeiten der System-Clients



Bearbeiten der SNMP-Einstellungen



HiPath HG 1500 Gegenstellen



Zurücksetzen der temporär genutzten HiPath HG 1500



Neu anlegen



Ändern



Löschen

Erstgenerierung

Voraussetzungen für die Erstgenerierung

Benötigte Daten:

- IP-Adresse und Subnetzmaske für HiPath HG 1500
- IP-Adresse und Subnetzmaske für den Admin-PC
- Rufnummer des Routers der HiPath HG 1500
- Teilnehmername, IP-Adresse und Rufnummer der HiPath HG 1500-Clients (System Clients, H323-Clients und vCAPi-Clients)

Mit Hicom 150 H müssen die auf der HiPath HG 1500 verwendeten Rufnummern in der Hicom zugeordnet worden sein (z. B. durch den Systemadministrator der Hicom), getrennt nach System-Clients und allen übrigen Teilnehmern (S₀-Teilnehmer, z. B. VCAPi, Router, H.323 etc.).

Wird die Vernetzung mehrerer Anlagen über IP aktiviert, so sind dafür in der Hicom Leitungen einzurichten. Die hierfür reservierten B-Kanäle stehen dann auf der HiPath HG 1500 nicht für andere Dienste (Routing, System-Clients, VCAPi etc.) zur Verfügung.

Die Obergrenze der verwendbaren B-Kanäle wird durch die beiden Parameter unter „Service“ siehe → 63 begrenzt.

- Werden mehr als zwei B-Kanäle von der HiPath HG 1500 benutzt, wird eine Lizenznummer zur Freischaltung der weiteren Kanäle notwendig.

Um die Daten aus der HiPath HG 1500 zu laden, müssen zuvor im Assistent I folgende Einstellungen durchgeführt werden:

1. Assistent I starten.
2. Geben Sie in den Felder „Benutzername“ und „Kennwort“ die aktuellen Kennungen der Hicom 150 E Office ein, um sich bei Assistent I anzumelden. Benutzername und Kennwort kann nur in der Hicom geändert werden.
3. Im Menü **Optionen** den Menüpunkt **Administrierbare** HiPath HG 1500 auswählen.
4. In der linken Spalte HiPath HG 1500-**Gegenstellen** auswählen und auf die Symbolschaltfläche „Neu“ in der Symbolleiste klicken.
5. Im folgenden Fenster den HiPath HG 1500 Namen eingeben, z. B. „LAN,“ und mit **OK** bestätigen.
6. In der linken Spalte den eben erstellten Eintrag auswählen, z. B. „LAN,“ und in der rechten Spalte unter „ IP-Adresse:“ die IP-Adresse der HiPath HG 1500 eingeben. Hier ist die IP-Adresse anzugeben, die der Baugruppe vom Administrations-PC aus zugeteilt wurde, siehe → 14.
7. Im Menü **Datei** den Menüpunkt **Übertragen des KDS zum PC** auswählen.

8. Im folgenden Fenster den zuvor festgelegten Namen der HiPath HG 1500, z. B. „LAN,“auswählen und mit **OK** bestätigen. Jetzt werden die Standard-Daten der HiPath HG 1500 in den PC übertragen.



Ab Hicom 150 H V1.0 kann an jeder Stelle, an der eine interne Rufnummer der Hicom eingetragen werden muss, mit Hilfe einer Auswahlbox direkt auf die in der Hicom vorkonfigurierten Rufnummern zurückgegriffen werden. Diese Tabelle wird bei jedem „Übertragen des KDS zum PC“ aus der Hicom ausgelesen. Die Rufnummern, die schon im KDS vergeben wurden, werden hier nicht mehr angezeigt.

Einstellungen bei der Erstgenerierung

Es wurde ein Kundendatenspeicher mit den Standardwerten von der HiPath HG 1500 in den Assistent I übertragen.

1. Im Menü **Einstellungen** den Menüpunkt **Service** auswählen. In der rechten Spalte unter „➡️ Lizenzierte B-Kanäle:“ die Anzahl der mit der HiPath HG 1500 erworbenen B-Kanäle einstellen (es sind nur gerade Werte erlaubt). Bei Veränderungen dieses Wertes ist eine Lizenznummer erforderlich. Diese wird beim Einspielen des KDS auf die HiPath HG 1500 abgefragt.

Die Anzahl der tatsächlich genutzten B-Kanäle kann unter „➡️ Maximal verwendbare B-Kanäle“ im gleichen Menü begrenzt werden. Dieser Wert kann in Einerschritten eingegeben werden.

Im Menü **Einstellungen** den Menüpunkt **Grundeinstellungen** auswählen. In der rechten Spalte unter „➡️ Anzahl vom Router verwendbarer B-Kanäle“ kann die Anzahl der gleichzeitig für Routing verwendbaren B-Kanäle eingestellt werden.
2. In der rechten Spalte unter „➡️ HiPath HG 1500 Anmelderufnummer:“ eine interne Teilnehmerrufnummer eintragen, die nach einem Reset der Anlage bzw. Laden des KDS in die HiPath HG 1500 automatisch angerufen wird. Hierbei ist zu beachten, dass genügend freie Rufnummern vorhanden sein müssen. Die Rufnummer des Routingports steht in der Anruferliste des AnmeldeTeilnehmers. Ist dies nicht der Fall, ist die Rufnummer in der Hicom nicht verfügbar (Freie Rufnummern in der Hicom überprüfen, Rufnummern müssen im Rufnummernhaushalt eingetragen sein, dürfen jedoch nicht hardwaremäßig vorhandenen Baugruppen zugeordnet sein).

Die Anmelderufnummer dient zur Einrichtungsdiagnose und kann nach erfolgreicher Inbetriebnahme wieder ausgetragen werden.
3. In der linken Spalte den Menüpunkt **IP-Adressliste zur Konfiguration** doppelt anklicken und mit der Symbolschaltfläche „Neu“ in der Symbolleiste die IP-Adresse des Admin-PCs (PC mit dem Assistent I) einrichten.

Hier können auch ganze Netze (z. B. das Service-Center für die Remote-Administration) zur Administration freigegeben werden.
4. In der linken Spalte den Menüpunkt **Routerrufnummer** anklicken und in der rechten Spalte unter „➡️ Routerrufnummer:“ die Rufnummer eintragen, unter der die HiPath HG 1500 von außen angewählt werden kann. Alle Anwendungen, die die Routerfunktionalität nutzen sind unter dieser einen Durchwahl von außen erreichbar. Die Verwaltung bzw. Zuordnung der B-Kanäle wird von der HiPath HG 1500 übernommen. Diese Rufnummer steht nach Erstinbetriebnahme in der Anruferliste des Endgeräts mit der Anmelderufnummer.

Externe Routingpartner, die die Protokolle V.34 bzw. V.110 benutzen, müssen jeweils andere Rufnummern benutzen: diese werden als **Durchwahl** bei den **ISDN-Partnern** konfiguriert.

5. Im Menü **Einstellungen** den Menüpunkt **Netzwerkschnittstellen** auswählen. In der linken Spalte den Menüpunkt **Netzwerkinterfaces** doppelt anklicken und die aktiven Netzwerkschnittstellen einstellen (z. B. LAN und ISDN 1/2/3, mindestens aber LAN).

Unter **LAN** die IP-Adresse (IP-Adresse der HiPath HG 1500) und die IP-Netzmaske (Netz-Klasse A, B oder C) eingeben (abhängig vom Kunden-netzwerk).

Unter **ISDN1** die IP-Adresse Ihrer WAN-Seite eingeben. Die IP-Adresse der WAN-Seite muss im selben Netz liegen wie die IP-Adresse der ISDN-Partner (Die ISDN-Einstellungen sind nur nötig bei Routing, Tele-arbeitsplatz, Internetzugang, Remotezugang).
6. Im Menü **Einstellungen** den Menüpunkt Routing auswählen. In der lin-ken Spalte den Menüpunkt **ISDN-Partner** doppelt anklicken und mit der Symbolschaltfläche „Neu“ in der Symbolleiste einen neuen ISDN-Partner einrichten. Unter dem Menüpunkt **Rufnummernliste** mit der Symbolschaltfläche „Neu“ in der Symbolleiste die Rufnummer des ISDN-Teilnehmers eingeben. Rufnummer anklicken und unter „ Rufrichtung:“ die Rufrichtung festlegen. Klicken Sie den ISDN-Partner an und konfigurieren Sie Parameter des Partners, z. B. die IP-Adresse, die B-Kanäle, das Protokoll (V.34 für analoge und V.110 für di-gitale Modems) oder möglicherweise eine Durchwahl.
7. Im Menü **Einstellungen** den Menüpunkt **Sicherheit** auswählen und überprüfen, ob die Parameter „IP-Firewall“, „MAC-Überprüfung“ und „IPX-Firewall“ ausgeschaltet sind.

Sicherheitshinweis: Zur Erleichterung der Inbetriebnahme ist hier der Firewall ausgeschaltet. Mit der erfolgreichen Ersteinwahl sollten aber die verschiedenen Sicherheitseinstellungen konfiguriert und aktiviert werden, um einen sicheren Betrieb zu gewährleisten.
8. Im Menü **Datei** den Menüpunkt **Übertragen des KDS zur** HiPath HG 1500 auswählen. Im folgenden Fenster den zuvor festgelegten Namen der HiPath HG 1500 (z. B. „LAN“) auswählen und mit **OK** bestätigen. Jetzt werden die Daten zur HiPath HG 1500 übertragen. Nach dem er-sten Zurückspielen der Daten führt die HiPath HG 1500 einen Baugrup-pen-Reset durch.
9. Von einem beliebigen Rechner im ersten LAN kann über das IP-Proto-koll mit dem Testprogramm „PING“ und der IP-Adresse der HiPath HG 1500 die Grundfunktion der Baugruppe getestet werden.

Ab jetzt kann die weitere Konfiguration über die erste LAN-Schnittstelle erfolgen, unabhängig vom Zugang für die Ersteinbetriebnahme (z. B. SLIP). Hierzu gegebenenfalls die IP-Adresse des Admin-PCs wieder auf ihren ursprünglichen Wert zurückstellen.

Erklärung der Menüfunktionen

Die im vorherigen Abschnitt dargestellte Menüstruktur ist hier mit zusätzlichen Erklärungen zu einzelnen Menüpunkten versehen. Die dargestellten Informationen entsprechen zum Teil der Online-Hilfe des Assistent I.

Menü „Datei“



KDS neu anlegen

Mit Hilfe dieses Kommandos wird ein neuer Kundendatenspeicher im Hauptspeicher des Admin-PCs angelegt. Da immer nur ein KDS gleichzeitig bearbeitet werden kann, besteht die Möglichkeit, einen vorher geladenen Datensatz zu sichern.

Ein neu erzeugter KDS enthält noch keine Datenstrukturen, die vom Kundenprofil her abhängig sind. Es sind folglich noch keine ISDN-Partner, vCA-PI-Teilnehmer, IP/IPX/MAC-Firewalls etc. definiert.

Beim Einrichten dieser Datensätze können dann u.a. vom Anwender definierbare Default-Werte eingetragen werden (vgl. Menüpunkt „Einstellungen“). Diese werden in der Konfigurationsdatei Hlb_Cfg.def im HOME-Verzeichnis der Anwendung gesichert.

Die Grundeinstellungen (z. B. IP-Adresse erster LAN-Interface) sind bereits vorkonfiguriert und vom Kunden auf die entsprechende Umgebung einzurichten.

Ein KDS enthält nur Konfigurationsdaten einer HiPath HG 1500-Baugruppe. Namen und IP-Adressen, unter denen zu administrierende HiPath HG 1500-Baugruppen erreichbar sind, werden unter „Administrierbare HiPath HG 1500“ eingestellt. Diese werden in einer separaten Konfigurationsdatei im HOME-Verzeichnis der HiPath HG 1500-Anwendung gespeichert.



KDS öffnen

Hier kann ein vorkonfigurierter oder gesicherter KDS von der Festplatte des Admin-PCs (oder von einem anderen Datenträger) in den Hauptspeicher geladen werden. Vorher bearbeitete Datensätze können zuvor gesichert werden. Eine KDS-Datei hat im allgemeinen die Extension „.hic“ (für HICOM).

Beim Einlesen werden die Daten einer Konsistenzprüfung unterzogen.



KDS speichern

Ein editierter Kundendatenspeicher kann mit Hilfe dieses Menüpunktes auf einem Datenträger abgelegt werden.



KDS speichern unter

Dieser Menüpunkt ermöglicht die Sicherung des KDS auf einem Datenträger unter einem wählbaren Namen und Pfad. Vorgegeben (und empfohlen) wird die Extension „*.hic.“



KDS drucken

Dieser Menüpunkt ermöglicht den Ausdruck des KDS. Bei Auswahl dieser Option wird ein POP-UP-Fenster zur Auswahl des Druckers und der Druckoptionen angeboten.



Der Ausdruck des KDS ist vor unbefugtem Zugriff zu schützen.



Seitenansicht

Hier wird die Möglichkeit geboten, den Ausdruck des KDS zuvor noch einmal zu betrachten. Hier können Sie auch den Drucker, seine Eigenschaften und die Papiergröße einrichten.

Seiteneinrichtung

Unter diesem Menüpunkt wird das Kontextmenü zur Druckereinrichtung des Betriebssystems aufgerufen. Hier können der Drucker, seine Eigenschaften und die Papiergröße eingerichtet werden.



Übertragen des KDS zum PC

Hier kann ein KDS von einer HiPath HG 1500 auf den Admin-PC geladen werden. Eine sich bereits im Hauptspeicher des PCs befindliche Konfiguration kann zuvor gesichert werden. Es muss daraufhin eine HiPath HG 1500-Gegenstelle (konfigurierbar unter „Administrierbare HiPath HG 1500“) aus einer Liste ausgewählt werden. Der Name wird nur beim ersten Zugriff auf die Baugruppe abgefragt. Diese Auswahl bleibt solange aktiv, bis sie durch Zurücksetzen der temporär genutzten HiPath HG 1500 zurückgesetzt wird. Der Name der aktuell verwendeten HiPath HG 1500 ist in der Statuszeile des Programmfensters zu sehen. Nach dem Einlesevorgang wird eine Konsistenzprüfung der Baugruppen-Konfigurationsdaten durchgeführt.



Übertragen des KDS zu HiPath HG 1500

Hier kann ein editierter oder neu erstellter KDS zur HiPath HG 1500 übertragen werden. Ist bereits eine Baugruppe selektiert worden (z. B. durch vorheriges Laden eines KDS von der Baugruppe auf den Admin-PC), so wird diese auch als Ziel für die jetzige Übertragung angenommen.

Übertragen des KDS zu HiPath HG 1500 mit System-Client-Passwörtern

Hier kann ein editierter oder neu erstellter KDS zur HiPath HG 1500 übertragen werden. Ist bereits eine Baugruppe selektiert worden (z. B. durch vorheriges Laden eines KDS von der Baugruppe auf den Admin-PC), so wird diese auch als Ziel für die jetzige Übertragung angenommen. Zusätzlich werden alle System-Client-Passwörter zur HiPath HG 1500 übertragen.



Jeder Nutzer der System-Clients kann sein Passwort vom Client aus ändern. Die Passwörter der System-Clients sind Bestandteil des KDS, werden aber auf der HiPath HG 1500 nur überschrieben, wenn diese Option benutzt wird oder wenn einzelne Passwörter gezielt mit dem Assistent I geändert wurden. Mit dieser Option können die Passwörter wieder auf einen definierten Wert gesetzt werden. Die Benutzer der Clients müssen darüber informiert werden.



Übertragen der Log-Datei zum PC

Laden der Log-Datei zum PC, die gespeichert werden kann.

Beenden

Beendet den Assistent I und fordert gegebenenfalls zum Speichern von ungesicherten Daten auf.

Menü „Einstellungen“



Grundeinstellungen

Parameter	Wert
→ LAN-Baugruppen-Anmelderufnummer:	nicht verwendet
→ Codierung:	A-Law
→ Anzahl vom Router verwendbarer B-Kanäle:	2
→ Mapping Netmask:	255.255.255.0
→ IEEE802.1p:	deaktiviert
→ VLAN-ID:	0
→ QoS-Verfahren:	Autodetect
→ PBX-Knoten Überwachung:	aktiviert
→ IP-Adresse des TFTP-Server:	0.0.0.0
→ Pfad und Dateiname des APS-File:	
→ Mac-Adresse der Baugruppe:	000000000000
→ LAN-Baugruppen-Software:	0.0.0.0
→ LAN-Baugruppen-Firmware:	

Konfiguriert die Grundeinstellungen. Diese Daten existieren nur einmal innerhalb des KDS. Folgende Parameter sind direkt der Kategorie „Grundeinstellungen“ zugeordnet:

→ HiPath HG 1500-Anmelderufnummer:

Hier wird eine interne Teilnehmer-Rufnummer eingetragen. Bei Erstinbetriebnahme und nach jedem Reset der HiPath HG 1500 wird dieser Teilnehmer nach dem Hochlauf und nach jedem Neustart eines VCAPI-Clients automatisch angerufen. In der Anruferliste steht die Routerrufnummer, Rufnummern bzw. Teilnehmernamen der erfolgreich angemeldeten VCAPI-Clients. Dieser Dienst zur Einrichtungsdiagnose kann nach erfolgreicher Inbetriebnahme wieder ausgetragen werden.

→ Codierung:

Dieser Schalter beeinflusst die Sprachcodierung zur ISDN-Seite.

→ Anzahl vom Router verwendbarer B-Kanäle:

Die HiPath HG 1500 verfügt über maximal 16 B-Kanäle. Ein Kunde kann eine bestimmte Anzahl B-Kanäle lizenzieren. Von diesem Kontingent kann hier eine bestimmte Anzahl für das Routing zur Verfügung gestellt werden. Der Router verwendet dann maximal diese Anzahl von Kanälen in Abhängigkeit des Datenvolumens bei dynamischer Kanalbündelung. Dies ist vor allem dann sinnvoll, wenn eine Mindestanzahl von B-Kanälen immer für HiPath HG 1500-Clients (VCAPI, H.323, System-Cli-

ents etc.) verfügbar sein soll. Sind 6 Kanäle lizenziert, lassen sich beispielsweise 4 davon dem Router zuordnen. Dadurch ist gewährleistet, dass immer 2 B-Kanäle den HiPath HG 1500-Clients zugänglich sind.

➔ Mapping Netmask

Gibt die Netzmaske an, die den Host-Anteil für das Adressmapping definiert, siehe → 114 IP-Adressmapping.

➔ IEEE802.1p

Mit diesem Parameter kann das Ethernet-Format eingestellt werden. Der Parameter wirkt nur auf Pakete, die von der Baugruppe verschickt werden (Defaultwert ist deaktiviert).

Für alle Pakete, die an die Baugruppe gesendet werden, ist eine automatische Erkennung aktiv, siehe → 90, QoS.

➔ VLAN-ID

Bei der Verwendung von 802.1p wird im Header die VLAN-ID 0 übertragen. Diese ID führt bei bestimmten Switchen (z.B. Cisco) zu Problemen, deshalb kann die VLAN ID administriert werden.

Defaultwert : 0

Wertebereich: 0 ... 4094 (0xFFE)

➔ QoS-Verfahren

Definiert das Quality of Service-Verfahren, nach welcher die HiPath HG 1500 eine Priorisierung von IP-Paketen anhand der Information im IP-Header vornimmt (ToS-Feld, Type of Service).

Als Wert kann DiffServ, IP-Precedence oder Autodetect (Defaultwert) ausgewählt werden. Mit der Einstellung „Autodetect“ werden DiffServ und IP-Precedence akzeptiert und entsprechend für Routing bewertet, siehe → 90 QoS.

➔ PBX-Knoten Überwachung

Für HG1500 V1.x:

Mit diesem Parameter wird die Überwachung zwischen vernetzten PBX/HiPath Knoten aktiviert.

Achtung: Dieser Parameter muss in allen Knoten gleich gesetzt sein.

Ab HG1500 V2.0 wird dieser Parameter knotenspezifisch unter Voice Gateway->PBX-Knoten eingerichtet.

➔ IP-Adresse des TFTP-Server

Gibt die IP Adresse des TFTP-Server an.

➔ Pfad und Dateiname des APS-File

Gibt den Pfad und den Dateinamen des APS-files auf dem TFTP Servers an.

➔ Mac-Adresse der Baugruppe

Hier wird die MAC-Adresse der Baugruppe (LAN-Interface) angezeigt.

➔ LAN-Baugruppen-Software (HiPath HG 1500):

Hier wird die aktuelle Version der auf der HiPath HG 1500 verwendeten Software angezeigt.

➔ LAN-Baugruppen-Firmware:

Angabe der Aktuellen Firmware

IP-Adressliste zur Konfiguration

Unter dieser Kategorie sind bis zu 10 IP-Adressen (auch Netzadressen) definierbar. Diese geben an, von welchem Admin-PC die HiPath HG 1500 konfiguriert werden darf.

Hier können auch ganze Netze (z. B. das Service-Center für die Remote-Administration) zur Administration freigegeben werden.



Diese Liste ist stets aktuell zu halten und sollte nicht mehr Einträge als unbedingt erforderlich enthalten.

Routerrufnummer

➔ Routerrufnummer:

Hier wird die Durchwahl der Hicom angegeben, unter der die HiPath HG 1500 von außen angewählt werden kann. Alle Anwendungen, die die Routerfunktionalität nutzen, sind unter dieser einen Durchwahl von außen erreichbar. Die Verwaltung bzw. die Zuordnung der B-Kanäle wird von der HiPath HG 1500 übernommen.

Diese Rufnummer sollte nach Erstinbetriebnahme in der Anruferliste des Anmeldeteilnehmers stehen.

Scriptbearbeitung

Bei einigen Internet Providern ist für den Zugang die Abarbeitung eines LOGIN-Scriptes gefordert. In der Regel wird PAP oder CHAP gefordert (siehe → 52, Menüpunkt „Einstellungen – Routing – ISDN-Partner“).

Dabei kommen verschiedene Parameter zum Tragen, wie USER, LOGIN, HOST und PASSWORD.

Die Maske ist so aufgebaut, dass in den Parameterfeldern die benötigten Zeichen eingegeben werden müssen.

Die Abarbeitung kann deaktiviert werden, dieses Script ist einmalig im Kundendatenspeicher vorhanden und ist für alle ISDN-Partner gültig, die die Scriptbearbeitung aktiviert haben.

Beispiel:

gefordertes Script:

HOST: ERT005

USER: KJUMBERT

PASSWORD: 34Ik98uF5

Folgende Zeichen müssen nun in der Maske eingegeben werden:

- ➡ Kennung 1: HOST:ERT005
- ➡ Kennung 2: USER:KJUMBERT
- ➡ Passwort: PASSWORD 34Ik98uF5

**QoS-Prioritätsklassen**

Die HiPath HG 1500 benutzt vier Prioritätsklassen, um ihren eigenen IP-Datenverkehr (abgehend) zu priorisieren. Die Werte können hier eingestellt werden. Die Defaultwerte brauchen in der Regel nicht verändert werden, siehe → 90 QoS.

- ➡ Voice Payload:
H.323-Pakete, welche die Sprachinformation enthalten.
- ➡ Call Signaling:
werden für den Verbindungsaufbau (z. B. H.323) benötigt.
- ➡ Data Payload:
z. B. für FAX-Daten für die IP-Vernetzung.
- ➡ Network Control:
z. B. SNMP-Traps.

Die Werte für die einzelnen Klassen werden aus der Liste der „AE/EF Codepoints“ selektiert.

**AE/EF Codepoints**

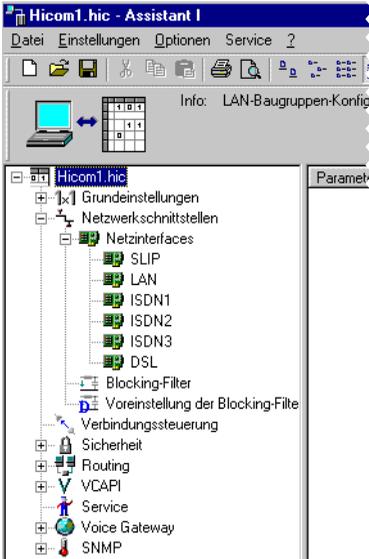
Hier werden die Werte definiert, welche die unterschiedlichen Priorisierungen festlegen. Der einzugebende Hex-Wert entspricht dem ToS-Feld (Type of Service) im IP-Header. Die untersten beiden Bits sind immer Null, deshalb sind hier nicht alle Werte erlaubt (nur die obersten 6 Bits werden bewertet). Die Defaultwerte brauchen in der Regel nicht verändert werden, siehe → 90 QoS.



Der Wert „0“ ist erlaubt, bedeutet aber, dass alle „normalen“ unmarkierten Pakete (ToS-Feld=0) in der entsprechenden Klasse transportiert werden.



Netzwerkschnittstellen



Die HiPath HG 1500 verfügt über 6 Netzwerkschnittstellen. Dazu gehören das erste LAN-Interface (LAN), welches an das Firmennetz angeschlossen ist, das ISDN-Interface ISDN1, das ISDN-Interface ISDN2, das ISDN3-Interface für den Einsatz als Internetzugang mit NAT/SUA (ISDN3) sowie das DSL/LAN2-Interface als vollwertiges additives 10BT-LAN-Interface mit Unterstützung im IP/IPX-Router durch QoS und Firewalls. Das DSL-Interface unterstützt die Protokolle **PPPoE** und **PPTP**. Das SLIP-Interface benötigt Ihr Siemens Servicetechniker für die Erstinbetriebnahme der HiPath HG 1500.

Die Konfiguration einer gültigen Protokolladresse (IP und/oder IPX) aktiviert den Protokollstack für das Interface. Der Hauptkategorie „Netzwerkschnittstellen“ ist direkt nur der folgende Parameter zugeordnet:

➔ Aktive Netzwerkschnittstellen:



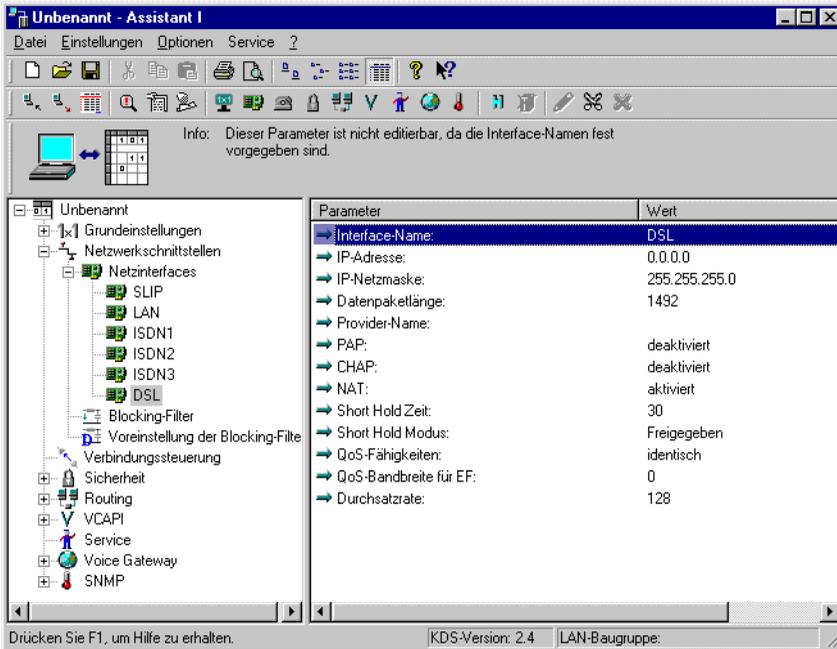
Hier können die 5 Netzwerkschnittstellen

LAN, ISDN1, ISDN2, ISDN3 und DSL(PPPoE)/LAN2/PPTP

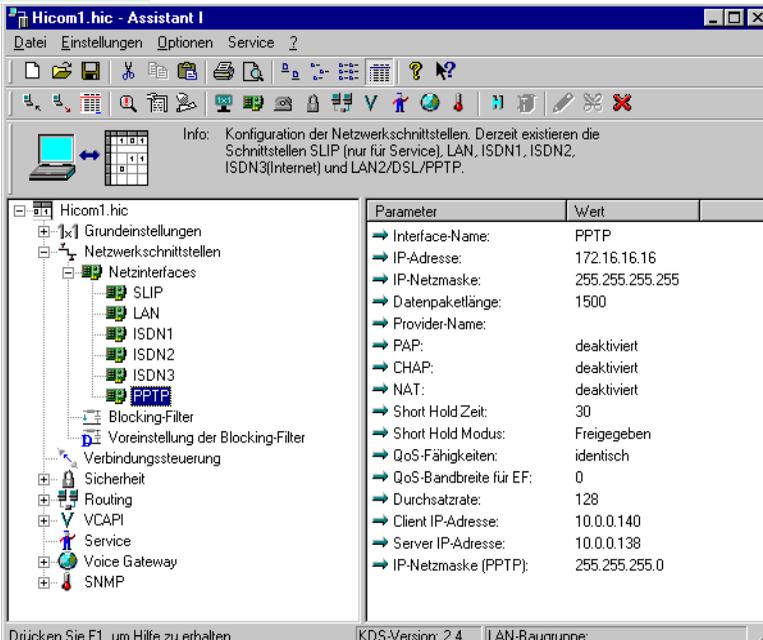
aktiviert oder deaktiviert werden. Dabei sind alle Möglichkeiten des gemeinsamen Ein- und Ausschaltens gegeben.



Bei LAN2 kann über eine Auswahlbox zwischen LAN2, DSL(PPPoE)-Schnittstelle und PPTP gewählt werden.



Beispiel 1 für die Konfiguration eines zweiten LAN-Interface



Beispiel 2 für die Konfiguration eines zweiten LAN-Interface

Netzinterfaces

➔ SLIP:

Das SLIP-Interface benötigt Ihr Servicetechniker unter Umständen für die Erstinbetriebnahme der HiPath HG 1500.

ISDN1, ISDN2, LAN und DSL/LAN2 sind durch folgende Parameter gekennzeichnet:

➔ Interface-Name:

Bei LAN2 besteht die Auswahlmöglichkeit zwischen DSL und LAN2. Als Default ist DSL eingestellt.

➔ IP-Adresse:

Dies ist die IP-Adresse des Interfaces. Erlaubt sind nur Adressen von Class A, B oder C-Netzen. Weiter muss Eindeutigkeit, sowohl innerhalb der drei Interfaces, als auch bezogen auf die IP-Adressen der ISDN-Partner, gegeben sein.

Class A-Netze:

nnnnnn . hhhhhhhh . hhhhhhhh . hhhhhhhh

Standard-Netzmaske: 255.0.0.0

Class B-Netze:

nnnnn . nnnnnnn . hhhhhhhh . hhhhhhhh

Standard-Netzmaske: 255.255.0.0

Class C-Netze:

nnnnn . nnnnnnn . nnnnnnn . hhhhhhhh

Standard-Netzmaske: 255.255.255.0

Dabei gilt: n = Netz, h = Host

➔ IP-Netzmaske:

Die Netzmaske dient zur Erstellung von Subnetzen (siehe → 171). So kann eine Class B-Adresse, bei der normalerweise die Bits 2 bis 15 das Netz und die Bits 16 bis 31 die Arbeitsstation kennzeichnen durch Verwendung der Netzmaske 255.255.240.0 zu mehreren Subnetzen führen, die allerdings nur innerhalb der Firmennetzstruktur bekannt sind. Durch obige Netzmaske wird die Trennlinie zwischen Netz-Bits und Host-Bits in das dritte Oktett verschoben und zwar so, dass nun auch die Bits 16 bis 19 für die Netz-Kennzeichnung verwendet werden, während nur noch Bits 20 bis 31 die Arbeitsstation beschreiben. Dieses Verfahren bietet den Vorteil, ein Firmennetz übersichtlich strukturieren zu können und die Wartung zu vereinfachen. Kleinere Firmen besitzen zum Beispiel oft nur eine Class C-Adresse (von der IEFTE oder autorisierten nationalen Instituten vergeben).

Besteht die Firma jedoch aus mehreren lokal getrennten Büros, müssen diese über WAN-Verbindungen (Wide Area Network) gekoppelt

werden. Ein Router, der eine solche Aufgabe wahrnimmt, geht jedoch davon aus, verschiedene Netze miteinander zu verbinden. Um jeder Zweigstelle ein eigenes IP-Netz zur Verfügung zu stellen (trotz nur einer offiziellen IP-Adresse), kann die Class C-Adresse mit Hilfe einer Subnetzmaske in solche aufgeteilt werden. Diese Neuaufteilung gilt allerdings nur im internen Firmennetz. Zum Internet hin besitzt die Firma nach wie vor nur ein Class C-Netz.

➔ Datenpaketlänge:

Die maximale Paketlänge in Bytes, sowohl für das IP- als auch für das IPX-Protokoll. Sie kann im Wertebereich von 500 bis 1500 liegen. Bei DSL-Betrieb sind nur 1492 Byte erlaubt.

➔ IPX-Netzwerknummer:

Eine IPX-Adresse besteht aus einer (genau) 8-stelligen Hexadezimalzahl für die Netzwerkennung und einer (genau) 12-stelligen Hexadezimalzahl, die die Arbeitsstation referenziert. Die Netzwerknummer darf nicht die Werte 0x00000000 oder 0xFFFFFFFF annehmen. Darüber hinaus müssen sich die Netzwerknummern der drei Netzwerkschnittstellen voneinander unterscheiden.

➔ IPX-Node:

Dieser Teil der IPX-Adresse charakterisiert die Arbeitsstation innerhalb eines IPX-Netzes. Ein Node (Knoten) besteht aus einer (genau) 12-stelligen Hexadezimalzahl. Die Werte 0x000000000000 und 0xFFFFFFFFFFFFFF sind unzulässig.

ISDN3 wird ausschließlich für den Internetzugang benutzt. Auf dieser Schnittstelle wird NAT/SUA angewendet, siehe → 112. Weiterhin ist es nicht für den Einsatz des IPX-Protokolles vorgesehen.

Der Definitionswert eines neu angelegten KDS für die IP-Adresse ist 1.1.1 mit der Netzmaske 255.0.0.0 und kann manuell durch die Eingabe einer anderen Adresse geändert werden. Bei der Nutzung des ISDN3 Interfaces wird die Verwendung der IP-Adresse 0.0.0.0 mit der Netzmaske 255.255.255.248 empfohlen.

Ein Ping auf eine IP-Adresse ist über das ISDN3 Interface nicht möglich.

NAT/SUA = Network Address Translation / Single User Access, d. h. das gesamte Netz mit allen freigegebenen PCs wird zum Internet über eine IP-Adresse, die man vom Provider nach dem Verbindungsaufbau zugeteilt bekommt, abgebildet.

DSL/LAN2

Bei dem Menüpunkt „Netzinterfaces“ gibt es noch folgende zusätzliche Untermenüpunkte für DSL (PPPoE), (DSL) PPTP oder LAN2:

➔ Provider-Name (bei DSL):

Name des Providers

➡ PAP (bei DSL):

siehe → 55

➡ CHAP (bei DSL):

siehe → 56

➡ NAT (bei DSL):

Mit diesem Parameter wird für das Interface „NAT“ aktiviert bzw. deaktiviert. Zur Funktion siehe → 112

➡ Short Hold Zeit (bei DSL):

siehe → 52

➡ Short Hold Modus (bei DSL):

siehe → 53

➡ QoS-Fähigkeiten:

siehe → 55

➡ QoS-Bandbreite für EF:

Mit diesem Parameter kann ein bestimmter Prozentsatz der verfügbaren Bandbreite (unter „Durchsatzrate“ konfiguriert) für den EF-Codepoint reserviert werden, siehe → 90 QoS.

➡ Durchsatzrate (bei DSL):

Der Parameter Durchsatzrate definiert die abgehende Bandbreite in kBit/s auf diesem Interface, um QoS-Regeln anwenden zu können.

Das NAT-Flag (Network Address Translation) kann für das zweite LAN- und für das DSL-Interface durch Einstellung aktiviert werden.

PPTP-Interface

Bei dem Menüpunkt „Netzinterfaces“ gibt es noch folgende zusätzliche Untermenüpunkte für (DSL)PPTP:

➡ Client IP-Adresse:

IP-Adresse des PPTP Interface der LAN-Baugruppe (LAN2).

➡ Server IP-Adresse:

IP-Adresse des fernen PPTP Interface (ADSL-Modem).

➡ IP-Netzmaske (PPTP):

IP-Netzmaske des PPTP Interface

Blocking-Filter

Mit Hilfe der Blocking-Filter können in einem LAN mit IPX-Protokoll für einzelne Novell-Server bestimmte Services pro Netzwerkschnittstelle zugelassen oder nicht zugelassen werden.

Es lassen sich bis zu 30 Einträge anlegen. Ein einzelner Filtereintrag besitzt folgende Parameter:

Servername:

Der Name des Novell-Servers kann bis zu 48 Zeichen lang sein. Handelt es sich um ein Wildcard (genau ein „ * “), so sind alle verfügbaren Server gemeint. Wurde ein Wildcard gewählt, so kann unter „Service“ jedoch nicht der Eintrag „Alle“ gewählt werden. Für einen Server können mehrere Filter angelegt werden, jedoch muss die Kombination aus Servername und Service eindeutig sein.

Service:

Der IPX-Service, der für einen Server freigegeben oder gesperrt werden soll. Wird der Eintrag „Alle“ gewählt, so darf der zugehörige Servername kein Wildcard sein.

Filtermode LAN:

Filtermode ISDN1:

Filtermode ISDN2:

Diese Parameter geben den IPX-Service für den (oder die) angegebenen Novell-Server frei oder sperren sie. Der Default-Eintrag für LAN ist freigegeben, für ISDN1/ISDN2 gesperrt.

Voreinstellung der Blocking-Filter

Filtermode LAN:

Filtermode ISDN1:

Filtermode ISDN2:

Wird ein neuer Blocking-Filter angelegt, so werden die o.g. Einstellungen für die drei Filtermodi als Standardwerte übernommen.



Verbindungssteuerung

Zur Verbindungssteuerung gehören folgende Parameter:

Wahlwiederholungen:

Gibt die maximale Anzahl der Wahlwiederholungen bis zu einem erfolgreichen Verbindungsaufbau an.

Pause:

Gibt die Pause (in Sek.) zwischen den Wahlwiederholungen an.

➔ Obere Schwelle:

Werden für die Verbindung zu einem ISDN-Partner (ohne statisches Channel-Bundling) mehrere B-Kanäle freigegeben, so wird die Kanalbündelung (Channel-Bundling) in Abhängigkeit von der Auslastung vorgenommen. Dazu wird der Datendurchsatz über einen einstellbaren Zeitraum hinweg gemittelt. Über- oder unterschreitet der Durchsatz einen bestimmten Grenzwert (ebenfalls einstellbar), so wird ein B-Kanal entweder zusätzlich aufgebaut oder abgebaut.

Die Obere Schwelle gibt die prozentuale Auslastung eines Kanals an, oberhalb der ein weiterer B-Kanal hinzugeschaltet wird. Der Wert kann zwischen 66% und 100% variieren. Der Wert sollte immer größer als der Wert oberhalb der „unteren Schwelle“ sein.

➔ Überschreitungsdauer:

Dies ist die Zeitspanne in Sekunden, in der im Mittel die Obere Schwelle (s.o.) überschritten sein muss, bis ein weiterer B-Kanal zugeschaltet wird. Der Parameter kann Werte von 3 bis 20 Sekunden annehmen.

➔ Untere Schwelle:

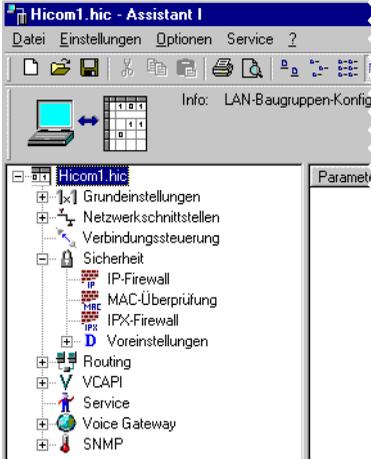
Werden für die Verbindung zu einem ISDN-Partner mehrere B-Kanäle freigegeben, so wird die Kanalbündelung (Channel-Bundling) in Abhängigkeit von der Auslastung vorgenommen. Dazu wird der Datendurchsatz über einen einstellbaren Zeitraum hinweg gemittelt. Über- oder unterschreitet der Durchsatz einen bestimmten Grenzwert (ebenfalls einstellbar), so wird ein B-Kanal entweder zusätzlich aufgebaut oder abgebaut. Die Untere Schwelle gibt die prozentuale Auslastung eines Kanals an, unterhalb der ein B-Kanal abgebaut wird. Der Wert kann sich zwischen 30% und 70% befinden, jedoch immer unterhalb der Oberen Schwelle (s.o.).

➔ Unterschreitungsdauer:

Dies ist die Zeitspanne in Sekunden, in der im Mittel die Untere Schwelle (s.o.) unterschritten sein musste, um den Abbau eines B-Kanals zur Folge zu haben. Der Parameter kann Werte von 3 bis 20 Sekunden annehmen.



Sicherheit



Zum Schutz vor unerwünschten Verbindungen existieren vier verschiedene Sicherheitsmechanismen.

- ➔ Rufnummern-Überprüfung:
- ➔ IP-Firewall:
- ➔ MAC-Überprüfung:
- ➔ IPX-Firewall:

Diese können mit Hilfe dieser Parameter aktiviert oder deaktiviert werden. Die Mechanismen werden im weiteren Verlauf beschrieben.

Für das ISDN3 Interface ist keine Konfiguration von Firewall erforderlich. Diese Einträge werden abgehend dynamisch angelegt (für die Anfragen von außen, siehe ➔ 57, Menüpunkt „Einstellungen – Routing – Internet“).

- ➔ Rufnummern-Überprüfung:

Die Rufnummernüberprüfung bezieht sich nur auf die zentrale Rufnummer des Routers (unter „Grundeinstellungen – Routerrufnummer“). Sie wirkt global, d. h. ist sie aktiviert, werden nur Anrufe entgegengenommen, wenn für die eingehende Rufnummer ein ISDN-Partner (vgl. Routing) definiert ist. Weiterhin werden Anrufe abgelehnt, die keine Rufnummer mit übertragen. Ruft ein Routingpartner die Durchwahlnummer des ISDN-Partners an, so erfolgt seine Identifikation dadurch und es findet keine Rufnummernüberprüfung statt.

IP-Firewall

Diese Kategorie kann bis zu 305 Einträge besitzen. Dieser Firewall wirkt auf das Routingverhalten der HiPath HG 1500. In der Tabelle wird festgelegt, ob zum einen ein LAN-PC über die HiPath HG 1500 in ein anderes Netz IP-Rahmen senden darf oder ob ein externer Rechner oder externes Netz Zugriff auf das lokale LAN hat (Erlaubnisfirewall). Damit wird auch und hauptsächlich das Routing in das ISDN und damit in entfernte Netze erlaubt oder verhindert.

Ein IP-Firewall Eintrag besteht aus den Parametern:

➡ IP-Adresse:

IP-Adresse, auf die der Firewall reagieren soll. Ausgewertet wird bei Quell- und Ziel-IP-Adresse immer der am genauesten zutreffende Eintrag; dies kann eine Netzadresse oder ein einzelner Host sein. Die IP-Routingtabelle wird zur Auswertung der Netzmaske benutzt. Ist für die IP-Adresse ein Routing-Eintrag vorhanden, wird der Adresstyp des Eintrages (Netz oder Host) übernommen.

Beim eingeschalteten IP-Firewall werden standardmäßig alle IP-Adressen gesperrt.

In den IP-Firewall müssen Adressen, die aus dem Internet über ISDN3 erreicht werden sollen, nicht eingetragen sein. Die Auswahl erfolgt über Menüpunkt: Routing->Internet.

IP-Adressen/Netze, die aus dem HiPath HG 1500 -Netz über ISDN3 ins Internet wollen, müssen jedoch eingetragen werden.

Für das ISDN3 Interface werden nur gehende Verbindungen überwacht. Kommende Pakete werden durch einen automatisch aufgebauten Firewall überprüft (siehe → 57, Menüpunkt „Einstellungen – Routing – Internet“).

➡ Ziel-IP-Adresse:

Durch die Ziel-IP-Adresse wird das Netz oder der Host angegeben, zu dem eine Verbindung hergestellt werden darf. Ein Wert von „0.0.0.0“ lässt eine Verbindung zu jeder beliebigen IP-Adresse zu.

➡ IP-Protokoll:

Bei dieser Einstellung kann das IP-Paket, welches die Firewall passieren soll, nach seinem Protokoll genauer spezifiziert werden. Es können für die verschiedenen Protokolle auch einzelne Portnummern konfiguriert werden (Portfirewall, siehe Liste verwendeter Portnummern im Anhang). Folgende Protokolle werden unterschieden:

- TCP (Transmission Control Protocol)
- UDP (User Datagramm Protocol)
- ICMP (Internet Control Message Protocol)



Sicherheitshinweis:

Die Richtung, die durch den Firewall freigeschaltet wurde, kann entsprechend durchlaufen werden. Anschließend ist die Rückrichtung für einige Minuten freigeschaltet, damit die Antwortpakete den Firewall passieren können. Soll der initiale Aufbau aber von der Gegenseite erfolgen, so muss hierfür ebenfalls ein Eintrag erfolgen.

Technische Hinweise:

Beim Einsatz von H.323-Telefonie (Voice over IP) werden dynamisch TCP/UDP-Ports verwendet. Die Konfiguration eines statischen IP Port Firewalls ist daher problematisch. Siehe hierzu auch die Portnummern der HG1500 im Anhang →Seite 178.



MAC-Überprüfung

Es sind bis zu 100 Einträge zulässig. Jeder PC im LAN besitzt als einzigartiges Merkmal eine MAC-Adresse und eine IP-Adresse. Die Kombination beider wird in einer Tabelle festgehalten. Durch den Eintrag dieser Kombination in einer Tabelle, wird dem PC erlaubt, eine IP-Verbindung zur HiPath HG 1500 aufzubauen. Ist diese Kombination nicht vorhanden, so kann keine Verbindung zur HiPath HG 1500 hergestellt werden. Dadurch wird die Täuschung durch manuelles Ändern der IP-Adresse (Kombination IP-Adresse-<->MAC-Adresse stimmt nicht mehr) unterdrückt. Der MAC-Firewall gilt für beide LAN-Interfaces.



IPX-Firewall

Auch hier sind bis zu 100 Einträgen möglich. Dieser Firewall wirkt auf IPX-Pakete in kommender wie auch gehender Richtung. Ein ankommendes IPX-Paket beinhaltet die Nodeadresse und die Netzwerknummer. Anhand der Kombination beider in einer Tabelle wird die Berechtigung des Partners geprüft. Stimmt einer der beiden Parameter nicht in dieser Kombination, so wird dieses Paket verworfen.

D Voreinstellungen für IP-Firewall und IPX-Firewall

Beim Neuanlegen eines entsprechenden Firewall-Eintrages, werden die angegebenen Voreinstellungen übernommen. Für den IP-Firewall sind die Routing-Berechtigungen voreinstellbar, beim IPX-Firewall dagegen die Netzwerknummer.

Routing



IP-Routing

Unter dieser Parameterkategorie können bis zu 100 Einträge vorgenommen werden. Durch sie erfolgt die Festlegung, welches IP-Netz, beziehungsweise welcher einzelne IP-Rechner über welches Gateway zu erreichen ist. Die direkt an die HiPath HG 1500 angeschlossenen Netzwerke (LAN, ISDN1, ISDN2, DSL/LAN2/PPTP) sind dem internen Router bekannt. Daher werden dafür keine Routing-Einträge ausgewertet. Ein Eintrag besitzt folgende Parameter:

➔ IP-Adresse:

Dies ist die IP-Adresse des Zielsystems oder -netzes.

➔ IP-Netzmaske:

siehe → 43 und siehe → 171

Besitzt die Netzmaske den Wert „255.255.255.255“, so wird die zugehörige IP-Adresse als Adresse eines Einzelsystems interpretiert, ansonsten als die eines ganzen Netzes. In diesem Fall kann die IP-Adresse den Wert „0.0.0.0“ annehmen, wodurch das Gateway (s.u.) zum Default-Gateway wird.

➔ Gateway:

Das Gateway ist der nächste Rechner/Router, über den das gewünschte Ziel (beschrieben durch die IP-Adresse) erreichbar ist. Beschreibt die Zieladresse ein Netz (d. h. Netzmaske ungleich „255.255.255.255“), so wird das Gateway mit der IP-Adresse „0.0.0.0“ zum Default-Gateway. Dieses ist notwendig für alle Ziele, die nicht explizit in der Routing-

Tabelle aufgeführt sind. Ansonsten sind die IP-Adressen „0.0.0.0“ oder „255.255.255.255“ für Gateways nicht zulässig.

IP-Mapping

Hier können bis zu 20 IP-Adresspaare eingetragen werden. Durch diese Einträge erfolgt beim Routing mit entsprechend parametrisierten ISDN-Partnern (IP-Mapping aktiviert) ein Austausch der IP-Adresse zwischen dem internen LAN und der (externen) ISDN-Seite.

Dadurch können z. B. mehrere IP-Netze mit gleichen Adressen erreicht werden, wenn der Zugang zu diesen Netzen jeweils über eine HiPath HG 1500 erfolgt, siehe → 55, IP-Adressmapping. Der Eintrag besteht aus zwei Werten:

➔ Interne IP-Adresse:

Dies ist die IP-Adresse auf der LAN-Seite.

➔ Externe IP-Adresse:

Dies ist die IP-Adresse, mit der die interne Adresse von aussen erreicht werden kann.

ISDN-Partner

Es können bis zu 70 Partner konfiguriert werden. Diese Datenstruktur beschreibt eine ISDN-Gegenstelle, die sich über die Hicom in das Firmennetz einwählt oder vom Firmennetz erreicht werden soll. Die direkt zu dieser Kategorie zählenden Parameter sind

➔ Name:

Der Name eines ISDN-Partners darf bis zu 14 beliebige Zeichen besitzen und muss eindeutig sein.

➔ IP-Adresse:

Dies ist die IP-Adresse des ISDN-Partners. Die IP-Adresse „0.0.0.0“ ist nicht zugelassen. Als Sonderfall gilt der Wert „255.255.255.255“. Damit wird das IP-Protokoll für diesen Partner deaktiviert. Weiterhin muss die Adresse eindeutig sein, darf also nicht von anderen Partnern oder den Netzwerkschnittstellen der HiPath HG 1500 verwendet werden.

➔ Node-Adresse:

Dies ist die IPX-Node Adresse des ISDN-Partners. Dieser Teil der gesamten IPX-Adresse charakterisiert die Arbeitsstation innerhalb eines IPX-Netzes. Ein Node (Knoten) besteht aus einer (genau) 12-stelligen Hexadezimalzahl. Der Wert „0x000000000000“ ist unzulässig, während die Node-Adresse „0xFFFFFFFFFFFF“ hier das IPX-Protokoll für diesen Partner deaktiviert.

➔ Short Hold Zeit:

Der Short Hold-Parameter beschreibt die Dauer in Sekunden, nach der eine Verbindung bei Inaktivität abgebaut wird. Fallen neue Datenpakete zur Übertragung an, so wird die Verbindung (für den Anwender transparent) wieder aufgebaut. Dieser Mechanismus wird auch „unterlagerter Verbindungsauf- und abbau“ genannt. Es fallen folglich nur bei tatsächlicher Nutzung der Leitung Kosten an.

➔ Short Hold Modus:

Ein- und Ausschalten des Short Hold Modus.

➔ Short Hold Gebührentaktauswertung

Wird dieser Schalter aktiviert, so wird der Short Hold Modus unter Berücksichtigung des Gebührentaktes optimal gesteuert.

➔ B-Kanäle:

Die HiPath HG 1500 verfügt über maximal 16 B-Kanäle (für die Freigabe von B-Kanälen müssen Lizenzen beantragt werden). Für Routing kann eine bestimmte Anzahl B-Kanäle reserviert werden. Damit wird eine ausreichende Anzahl B-Kanäle für andere Anwendungen (z. B. CTI) freigehalten.

Diese Zuteilung geschieht mit dem Parameter „Grundeinstellungen – Maximale Anzahl der B-Kanäle.“ Dabei kann es wünschenswert sein, die einem bestimmten Partner zur Verfügung stehenden B-Kanäle auch wieder auf ein Maximum zu begrenzen. Dies kann hier geschehen.

➔ Systemstart-Verhalten:

Es besteht die Möglichkeit, beim Systemstart eine automatische Verbindung zu einem bestimmten ISDN-Partner aufzubauen. Dies geschieht, indem der Wert auf „Automatische Verbindung“ gesetzt wird. Solange freie B-Kanäle zur Verfügung stehen, werden Verbindungen zu den betreffenden Partnern aufgebaut. Sind zu viele automatische Verbindungen definiert, so kann es sein, dass ein Teil der Verbindungen nicht aufgebaut wird. Daher ist es sinnvoll, nicht mehr Autostart-Partner zu definieren, als man B-Kanäle zur Verfügung hat.

Dieser automatische Systemstart ist vor allem für IPX Routing sinnvoll, um sich mit fernen Routern auszutauschen.

➔ Rückruf:

Eine anrufende Gegenstelle muss im D-Kanal der ISDN-Verbindung ihre Rufnummer übertragen. Ist der Rückruf eingeschaltet, so wird die Verbindung durch die HiPath HG 1500 abgelehnt und der Partner unmittelbar danach zurückgerufen. Dadurch wird das Einwählen von einer nicht autorisierten Gegenstelle verhindert. Diese Callbackfunktion arbeitet beim initialen Anruf verbindungslos, so dass Kosten nur für die rückrufende Seite entstehen. Der zurückgerufene Partner muss in die-

sem Fall eine Einwahl erlauben.

Der Rückruf sollte nur auf einer der beiden beteiligten Seiten eingerichtet sein, um Schleifen zu verhindern.

➔ Scriptbearbeitung:

An dieser Stelle wird für den ISDN-Partner die unter Grundeinstellungen -> Scriptbearbeitung eingetragenen Parameter aktiviert.

Das Script ist einmalig und Anlagenweit gültig.

➔ Multilink:

Für die Kanalbündelung im PPP-Protokoll kann hier das Multilink-Protokoll ein- oder ausgeschaltet werden. Die Verwendung der Kanäle erfolgt dabei dynamisch oder statisch (siehe unten unter „Statisches Channel Bundling“) je nach Datenaufkommen.

Für die Verwendung des Multilink muss die Gegenstelle dieses Protokoll unterstützen.

➔ Segmentierung:

Um bei der Verwendung von Multilink die Auslastung der verwendeten B-Kanäle möglichst gleichmäßig zu verteilen, kann die Segmentierung eingeschaltet werden. Dabei werden Datenpakete in Untereinheiten geteilt und über die zur Verfügung stehenden Kanäle versendet.

Die Gegenstelle muss diese Eigenschaft unterstützen.

➔ IP-Header Compression:

Hier kann die Komprimierung der TCP-Header aktiviert werden. UDP- und RTP-Header werden (wenn möglich) immer komprimiert. Die Voreinstellung ist **deaktiviert**.

➔ MTU Size Fragmentation:

Damit eine Sprachübertragung nicht durch lange Datenpakete gestört wird, kann mit diesem Parameter die Fragmentierung von Paketen (in 256 Byte Fragmente) erzwungen werden. Die Voreinstellung ist **deaktiviert**.

➔ PPP Default Header:

Für Partner, die den default PPP-Header benötigen, kann das Senden hier aktiviert werden. Die Voreinstellung ist **aktiviert**.

➔ V.34-Gegenstelle:

Aktivierung bei V.34-Gegenstelle (z. B. ein analoges Modem).

➔ V.110-Gegenstelle:

Aktivierung bei V.110-Gegenstelle (GSM oder Digital).

➔ IP-Adresse unterdrücken:

Dieser Parameter wird eingeschaltet, wenn kein Transit-Netz verwendet werden soll. Die Gegenstelle muss dieses Leistungsmerkmal unterstützen.

➔ Statisches Channel Bundling:

Ist dieser Punkt aktiviert, versucht die HiPath HG 1500 beim ersten Verbindungsaufbau alle für den Partner administrierten B-Kanäle aufzubauen.

➔ Durchwahl:

Diese Durchwahl dient zur Identifizierung des Anrufers, wenn dieser keine Rufnummer übermittelt (z. B. analoges Modem). Die Identifizierung erfolgt durch den Anruf dieser Durchwahl anstelle der Routernummer der HiPath HG 1500.

Wenn der Partner keine Rufnummer übermittelt, muss eine Durchwahl konfiguriert werden. Diese muss dann vom Partner angewählt werden.

➔ IP-Adressmapping:

Der Parameter wird auf „ja“ gesetzt, wenn mit diesem Routingpartner nach den unter IP-Mapping hinterlegten Regeln ein Austausch der IP-Adressen erfolgen soll, siehe → 114.

➔ QoS-Fähigkeiten:

Beschreibt die Quality of Service-Fähigkeiten des ISDN-Partners bzw. Interfaces, siehe → 90. Der Defaultwert ist „identisch“, d. h. es wird von den gleichen Fähigkeiten ausgegangen, wie sie auch die HiPath HG 1500 verwendet: Der Partner kann die gleichen Werte im ToS-Feld (Type of Service) des IP-Headers verarbeiten wie die HiPath HG 1500.

- DiffServ: Der Partner arbeitet bevorzugt mit DiffServ, es wird von der HiPath HG 1500 gegebenenfalls eine Umwertung auf DiffServ vorgenommen.
- IP-Precedence: Der Partner arbeitet bevorzugt mit einer Bewertung des IP-Precedence-Felds (3 Bit), deshalb wird ggf. das ToS-Feld von der Baugruppe umgemappt.

➔ QoS-Bandbreite für EF:

Mit diesem Parameter kann ein bestimmter Prozentsatz der verfügbaren Bandbreite für den EF-Codepoint (EF) reserviert werden, siehe → 90 QoS.

➔ PAP:

Für den Gebrauch des Sicherheitsmechanismus PAP innerhalb des PPP-Protokolles muss an dieser Stelle PAP aktiviert werden und folgende Parameter konfiguriert werden:

– HOST:

Dieser Punkt bestimmt, ob die Gegenstelle (CLIENT) oder die Baugruppe (HOST) mit der Authentisierung beginnen soll.

Host aktiviert bedeutet: Die Baugruppe authentisiert sich bei der Gegenstelle.

Host deaktiviert bedeutet: Die Gegenstelle muß sich bei der Baugruppe authentisieren. „Host deaktiviert“ wird in der Regel gegenüber Providern nicht verwendet.

– User-ID:

An dieser Stelle wird die Kennung für PAP oder entsprechende Userkennungen der Diensteanbieter eingegeben.

– Passwort:

Hier wird das entsprechende Passwort für PAP eingegeben.

➔ CHAP:

Eine andere (sicherere) Authentifizierungsmethode gegenüber PAP stellt CHAP dar. Es sollte nur eine Methode verwendet werden, vorzugsweise CHAP.

– HOST:

Ist dieser Schalter deaktiviert, so erwartet die HiPath HG 1500 eine Aufforderung zur Authentifizierung (Challenge). Dies wird beantwortet (Response) und so authentisiert sich die HiPath HG 1500 bei der Gegenstelle.

Diese Einstellung wird häufig bei der Einwahl ins Internet benötigt. Ist der Schalter aktiviert, schickt die HiPath HG 1500 die Aufforderung zur Authentifizierung und erwartet eine Antwort.

– User-ID:

An dieser Stelle wird die Kennung für CHAP oder entsprechende Userkennungen der Diensteanbieter eingegeben.

– Passwort:

Hier wird das entsprechende Passwort für CHAP eingegeben.

Bei dem Menüpunkt „ISDN-Partner“ gibt es noch folgende Untermenüpunkte:

Rufnummernliste

➔ Rufnummer

Die ISDN-Rufnummer, unter der ein Partner erreichbar ist. Sie muss innerhalb der Gesamtkonfiguration eindeutig sein und kann aus bis zu 22 Dezimalziffern (0-9) bestehen. Zusätzlich darf ein Bindestrich zur Abtrennung der notwendigen Amtsholungsziffern eingefügt werden.

➔ Rufrichtung:

Dieser Parameter gibt an, wie eine Verbindung unter der Rufnummer zustande kommen darf. Folgende Werte sind möglich:

- gesperrt:
Die Nummer ist nicht verwendbar.
- kommend:
Der Partner darf anrufen, aber nicht angerufen werden.
- gehend:
Der Partner darf angerufen werden, aber nicht anrufen.
- kommend und gehend:
Der Partner darf sowohl anrufen, als auch angerufen werden.

IPX Reconnect-Filter

Um unnötigen Datenverkehr und damit hohe Verbindungskosten zu vermeiden, können bestimmte IPX-Pakettypen gefiltert werden. Die Filter lassen sich pro ISDN-Partner unter dieser Kategorie aktivieren oder deaktivieren. Das System simuliert bei gesetztem Filter den Austausch der Pakete mit dem Server. Durch Doppelklick auf jeden Filtereintrag wird ein Fenster geöffnet, das die Auswahl „Ein“ oder „Aus“ erlaubt. Ist der Filter eingeschaltet und der Short-Hold Modus aktiv, führen die jeweiligen Pakete nicht zum Wiederaufbau einer Verbindung. Ist die Verbindung ohnehin aufgebaut, so werden diese Pakete übertragen.

Folgende Pakettypen können gefiltert werden:

- ➔ Diagnostic-Pakete
- ➔ Ping-Pakete
- ➔ NDS-Pakete
- ➔ NetBios-Pakete
- ➔ SNMP-Pakete
- ➔ NLSP-Pakete
- ➔ NCP-Exchange-Time
- ➔ Interserver-Pakete
- ➔ RIP/SAP-Änderungen



Internet

Um auch für das Internet Rechner mit WWW-Seiten oder anderen Diensten zur Verfügung stellen zu können und damit nicht die Sicherheitsmechanismen des Firewall zu unterlaufen, können an dieser Stelle bis zu 20 Rechner bezüglich ihrer IP-Adresse und des Dienstes bzw. des verwendeten Protokolls eingetragen werden. Die hier freigeschalteten Dienste sind damit aus dem Internet erreichbar, sobald eine Verbindung zum Internetprovider aufgebaut wurde.

Dabei kennzeichnen folgende Parameter den Eintrag:

- ➔ IP-Adresse: z. B. 135.34.12.178 (z. B. Web-Server im eigenen LAN)
- ➔ PC-Port: z. B. 80 (Protokoll HTTP, Webserver)
- ➔ Port der HiPath HG 1500: z. B. 80
- ➔ Protokoll: TCP

Mit diesem Eintrag kann ein Webserver über die IP-Adresse, die vom Provider für den eigenen Internetzugang vergeben wurde, erreicht werden.

Dieser Menüpunkt wirkt nur auf das ISDN3-Interface und auf das DSL/LAN2/PPTP-Interface bei aktiviertem NAT (siehe ➔ 112).

 Die Ports des PC und der HiPath HG 1500 sind in der Regel identisch.

IP-Accounting

Das Leitungsmerkmal IP Accounting beschreibt die Möglichkeit, Kosten für den Internetzugang nach transferierten Datenmengen und verschiedenen Tarifmodellen, die in der Applikation hinterlegt sind, verursacherorientiert zuzuordnen. Dieses Leistungsmerkmal ist nur auf HG1500-Baugruppen mit 32MB Speicher zu aktivieren.

Dazu ist innerhalb der Administration des Kundendatenspeichers der HG1500 das Leistungsmerkmal zu aktivieren.

Zur Aktivierung sind mittels Assistant I folgende Einstellungen durchzuführen: Unter Routing, IP-Accounting des Administrationsbaums sind alle vier für das IP-Accounting wichtigen Parameter zu finden.

- ➔ Die IP-Adresse Applikations-Client spezifiziert den für das IP-Accounting berechtigten PC. Folgende Einstellungen sind möglich:
- ➔ Die IP-Adresse 255.255.255.255 deaktiviert das IP-Accounting. Dieses entspricht gleichzeitig der Voreinstellung.
- ➔ Die IP-Adresse 0.0.0.0 berechtigt jeden PC zur Abfrage der IP-Accountingdaten, sofern die unten beschriebene Prüfung der Zugangsberechtigung erfolgreich ist. Jede andere IP-Adresse berechtigt nur den PC mit genau dieser eingetragenen IP-Adresse zur Abfrage der IP-Accountingdaten.

Die weitergehende Berechtigungsprüfung erfolgt durch User-Name und Passwort. Nur PCs, die sich mit korrektem Namen und Passwort an der HG1500 anmelden, sind berechtigt, IP-Accountingdaten zu erhalten. Der User-Name hat eine Länge von 0 bis 20 Zeichen. Das Passwort ist minimal 1 bis maximal 16 Zeichen lang. Bei der Eingabe des Passworts wird der Klartext durch * unkenntlich gemacht.

Der Eintrag IP-Accounting für LAN2 aktiviert das IP-Accounting auch für das LAN-LAN Routing. In der Voreinstellung ist diese Option deaktiviert und das IP-Accounting nur für den ISDN- und den xDSL-Zugang zum Internet aktiviert.

➔ IP-Adresse Applikations-Client:

IP-Adresse des Client PCs. Nur von dieser IP-Adresse können die Datensätze abgefragt werden. Wird hier die Pseudo-IP-Adresse 0.0.0.0 eingetragen, so können alle PCs Daten abfragen, die Authorisierung erfolgt dann allein über User-Name und Passwort.

➔ User-Name:

Loginname der Accounting Applikation. Mit diesem Namen muss sich die Accounting Applikation anmelden.

➔ Passwort:

Passwort der Accounting Applikation. Mit diesem Passwort muss sich die Accounting Applikation anmelden.

Voreinstellungen

IP-Routing

Beim Neuanlegen eines IP-Routingeintrages werden Netzmaske und Gateway mit diesen Voreinstellungen belegt.

➔ Netzmaske:

Hier kann ein Default-Wert für die Netzmaske angelegt werden.

➔ Gateway:

Hier kann ein Default-Wert für das Gateway angelegt werden.

ISDN-Partner

Wird ein ISDN-Partner neu angelegt, so werden die Parameter Short Hold Zeit und Rückruf mit diesen Voreinstellungen versehen.

➔ Short Hold Zeit:

Hier kann ein Default-Wert für die Short Hold Zeit angelegt werden.

➔ Rückruf:

Hier kann ein Default-Wert für Rückruf angelegt werden.

Bei dem Menüpunkt „ISDN-Partner“ gibt es noch folgende Untermenüpunkte:

Rufnummer

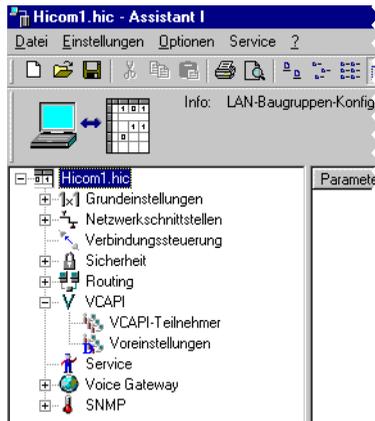
Hier kann ein Default-Wert für die Rufnummer angelegt werden.

IPX Reconnect Filter

Hier können Default-Werte für die IPX Reconnect-Filter angelegt werden.



vCAPI



vCAPI-Teilnehmer

Mit HiPath HG 1500 und der vCAPI Software (virtuelle CAPI) verhält sich der PC wie ein PC mit eigener ISDN-Karte. Die CAPI-Schnittstelle bietet Anwendungen eine standardisierte Möglichkeit, Daten über ISDN auszutauschen. Da innerhalb eines LANs nicht jeder Arbeitsplatz über einen separaten ISDN-Anschluss verfügen kann, ist es notwendig, ein sogenanntes „virtuelles CAPI“ (vCAPI) zu installieren. Dabei wird auf den Arbeitsstationen ein vCAPI-Client benötigt, der den Anwendungen eine CAPI-Schnittstelle zur Verfügung stellt. Dieser kommuniziert mit Hilfe des TCP/IP-Protokolls mit dem vCAPI-Server, der sich auf der HiPath HG 1500 befindet. Der vCAPI Server übernimmt die Datenverteilung an die entsprechenden Clients. Bevor Sie beginnen, vCAPI-Clients im Administrationsprogramm zu konfigurieren, müssen Sie die IP-Adressen der betroffenen Client-PCs feststellen.

Es können bis zu 100 vCAPI-Teilnehmer eingerichtet werden, die folgende Parametern besitzen:

➔ Rufnummer (intern):

Dieser Parameter gibt die Rufnummer an, unter der ein vCAPI-Teilnehmer zu erreichen ist. Ein Teilnehmer kann über mehrere Nummern verfügen (z. B. eine für Fax, eine für Eurofile-Transfer...), die jeweils über bis zu 15 Dezimalziffern (0-9) ohne Sonderzeichen verfügen können. Weiterhin muss sie eindeutig sein.

Die zur Verfügung stehenden Rufnummern können unter Verwendung der Rufnummernliste ermittelt und einfach der vCAPI-Funktionalität zugeordnet werden (siehe → 74).

➔ IP-Adresse:

Die IP-Adresse ist die charakteristische Größe für einen vCAPi-Teilnehmer. Über diese Adresse ist der vCAPi-Client vom vCAPi-Server (Hi-Path HG 1500) erreichbar. Einer IP-Adresse können mehrere Rufnummern zugeordnet sein.

➔ Fax Gruppe3:

Hier kann der Fax-Dienst für eine Rufnummer freigeschaltet oder gesperrt werden.

➔ Voice:

Hier kann Voice für eine Rufnummer freigeschaltet oder gesperrt werden.

➔ Digitale Daten:

Hier kann der Dienst „Digitale Daten“ für eine Rufnummer freigeschaltet oder gesperrt werden.

Für eine Rufnummer ist nur Fax Gruppe3 oder Voice aktivierbar.

Voreinstellungen

vCAPi-Teilnehmer

➔ IP-Adresse:

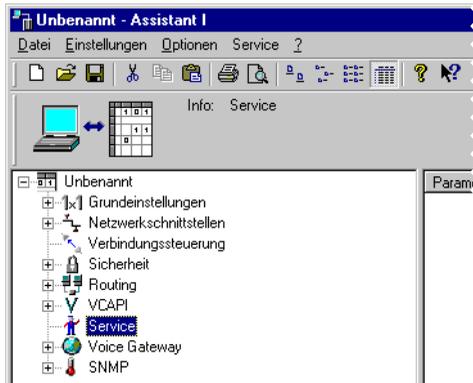
Hier kann ein Default-Wert für die IP-Adresse angelegt werden.

➔ Fax Gruppe3:

Hier kann defaultmäßig Fax Gruppe3 ein- oder ausgeschaltet werden.



Service



➔ Lizenzierte B-Kanäle:

Hier wird hinterlegt, wieviele B-Kanäle lizenziert wurden. Bei Änderung dieses Parameters erfolgt nach einem KDS-Transfer eine Abfrage der Lizenz-Codenummer.

➔ Maximal verwendbare B-Kanäle:

Hier wird eingestellt, wieviel von den lizenzierten B-Kanälen die HiPath HG 1500 benutzen darf.

Trace-Gruppen

Folgende Daten werden in den angegebenen Tracelevel ausgegeben.

➔ TG 112 (Kunden-Trace PPP)

Hier werden Daten zum PPP Aufbau ausgegeben.

- Level 0

Die Gegenseite unterstützt kein CHAP

- Level 1
 - Ablehnung eines Verbindungsaufbaues mit Ausgabe
 - des Grundes und
 - der Calling Number
 - PPP over Ethernet aktiv / Session wird geschlossen
 - PPP, CHAP und PAP timeout
- Level 3
 - Verbindungsaufbau vom Router mit Angabe
 - des ISDN Partners,

- der Calling Number und
- der Called Number
- Verlauf der PPP Aushandlung bis zur PPP connect Meldung
- Level 4
 - IP / IPX Paket, das zum Verbindungsaufbau führt mit Angabe der
 - Quell und Ziel IP
 - Protokoll mit Angabe der benutzten Ports
 - Art der DNS Anfrage
 - Zuschaltung eines weiteren B-Kanals bei Multilink
 - Verspätete CONN_CONF Meldung mit Ausgabe des momentanen States
 - PPP over Ethernet Session open

➡ TG 113 (Kunden-Trace DSS1)

Hier werden ISDN Meldungen des D-Kanals protokolliert.

- Level 2
 - Message Typ mit Causes und Channel ID
- Level 3
 - Rufnummer (Called und Calling Number)
 - Dienst (CIP)

➡ TG 114 (Kunden-Trace CAPI)

Hier werden vCAPI Meldungen ausgegeben.

- Level 1
 - Fehlereintrag: IP Adresse nicht als vCAPI Partner konfiguriert
- Level 3
 - öffnen / schliessen einer IP-Verbindung mit Angabe der IP Adresse des vCAPI Clients
 - Verbindungsaufbau mit Called Number, Calling Number und Channel ID (plci) bei kom-mender Verbindung
 - Called Number und Channel ID bei gehender Verbindung
 - Ablehnung eines Verbindungsaufbaues mit Grund

Verbindungsabbau mit Grund

Der Grund ist nur numerisch und entspricht zum Teil der CAPI 2.0 Spezifikation!

➡ TG 115 (Kunden-Trace H.323 Stack)

Bei diesem Trace werden zur Zeit noch keine Daten ausgegeben.

➔ TG 116 (Kunden-Trace virt. Optiset)

Hier werden Meldungen zum virtual Optiset ausgegeben.

- Level 1
 - Fehler zum Client Login
 - Falsche Rufnummer
 - Zeitdifferenz zwischen PC und Hicom zu groß
 - Falsches Paßwort bei Authentifizierung
 - Doppelte Lizenz vorhanden
- Level 2
 - H.323 Verbindungsaufbau
 - H.323 Verbindung wird einem Kanal zugewiesen
 - H.323 Verbindung konnte keinem Kanal zugewiesen werden
 - H.323 Verbindung wird durchgeschaltet
 - H.323 Verbindung konnte nicht durchgeschaltet werden
 - H.323 Verbindung soll freigegeben werden
 - H.323 Verbindung wurde freigegeben
- Level 3
 - LAN Verbindung zu IP Adresse hergestellt / beendet
 - LAN Verbindung zur IP Adresse hergestellt (vor Login)
 - LAN Verbindung zur IP Adresse beendet
- Level 4
 - Anmeldung des Clients an der Hicom (beim Systemhochlauf)
 - Login Zustand des Clients
 - Client will sich einloggen
 - Client erfolgreich eingeloggt
 - Client will sich ausloggen

➔ TG117 (Kunden-Trace Security)

Hier werden Firewall Meldungen ausgegeben.

- Level 2
 - ISDN Zugangs Firewall Verletzung , Ablehnung des Verbindungsaufbaus
 - Nicht konfigurierte Rufnummer des Anrufers
 - PAP / CHAP falsch
 - MAC Adresse wird doppelt verwendet; Ausgabe der betreffenden MAC Adresse
 - IP Firewall wurde verletzt; Ausgabe der Quell- und Ziel IP
- Level 3
 - MAC Firewall wurde verletzt; Ausgabe der IP- und MAC Adresse
 - NAT Firewall wurde verletzt (nur bei ISDN3 Interface); Ausgabe der Quell IP und des verwendeten Ports

TG118 (Kunden-Trace PBX-Routing)

Hier werden beim PBX-Routing folgende Meldungen ausgegeben:

- Level 1
 - Message Type (kommend)
- Level 2
 - Causes, Channel Ident, Called- und Calling Party Number
- Level 3
 - Rufnummer (Called- und Calling Number)
- Level 4
 - Gehende Meldungen

Die Trace-Gruppen 119 bis 121 werden nicht benutzt.

Tracelevel

- Level 0 deaktiviert die Tracegruppen.
- Level 1-4 pro Level werden die Details der Traceinformationen reduziert (1 = niedrigster Level, 4 = höchster Level mit den meisten Informationen)

Bei einem Überlauf des Tracespeichers setzen Sie den Tracelevel entsprechend von 4 auf eine niedrigere Stufe herab.

 Eingeschaltete Trace-Gruppen gehen zu Lasten der Performance. Deswegen sollten Trace-Gruppen nur zur Problembhebung eingeschaltet werden, im normalen Betrieb sind alle auf 0 zu setzen.



Voice Gateway



Die HiPath HG 1500 bietet Ihnen mit Voice over IP die Möglichkeit, mit dem HiPath HG 1500 Client Leistungsmerkmale der Hicom zu nutzen. Sie haben insbesondere die Möglichkeit, dies auch auf einem Teleworking-PC anzuwenden.

Daneben ist es zusätzlich möglich, H.323 Clients für zum Beispiel NetMeeting zu nutzen.

Für beide Clients gelten Grundeinstellungen, die durch folgende Parameter beschrieben werden:

➔ Echo:

Hiermit können Echos kompensiert werden, die bei Verbindungen über das Voice-Gateway zu herkömmlichen Telefonen entstehen können.

➔ Traffic-Statistik:

Hier legen Sie fest, ob für die Clients eine Traffic-Statistik geführt werden soll, die über SNMP ausgewertet werden kann.

➔ Codierung:

Dieser Schalter beeinflusst die Sprachcodierung zur ISDN-Seite hin.

➔ Max. Anzahl gleichzeitiger Rufe:

Von dem Kontingent lizenzierter B-Kanäle kann hier eine bestimmte Anzahl für Voice over IP zur Verfügung gestellt werden. Dies ist vor allem dann sinnvoll, wenn eine Mindestanzahl von B-Kanälen immer für

Routing verfügbar sein soll. Sind 6 B-Kanäle lizenziert, lassen sich beispielsweise 4 davon dem Voice over IP zuordnen. Dadurch ist gewährleistet, dass immer 2 B-Kanäle dem Routing zugänglich sind.

➔ AudioCodecs für Voice Clients

Mit diesem Eintrag werden die AudioCodecs für Verbindungen zu den Clients und die Reihenfolge ihrer Verwendung festgelegt (G.723 komprimiert die Sprache, G.711 ist unkomprimiert).

PBX-Knoten (ab Hicom 150 H V1.0)

Hier werden zu jedem Knoten (Hicom-Anlage), jeweils identifiziert durch eine Nummer von 1-64, die IP-Adressen Ihrer HiPath HG 1500-Baugruppen konfiguriert. Pro Knoten können bis zu drei HiPath HG 1500 konfiguriert werden, siehe → 81.

➔ AudioCodecs:

Mit diesem Eintrag werden die AudioCodecs für Verbindungen zwischen den PBX-Knoten und die Reihenfolge ihrer Verwendung festgelegt (G.723 komprimiert die Sprache, G.711 ist unkomprimiert).

➔ PBX Knoten Überwachung:

Mit diesem Parameter wird die Überwachung zwischen vernetzten PBX/HiPath Knoten aktiviert.

Achtung: Dieser Parameter muss in allen Knoten gleich gesetzt sein.

Ab HG1500 V2.0 wird dieser Parameter knotenspezifisch unter Voice Gateway->PBX-Knoten eingerichtet.

➔ Paketierung:

Mit diesem Parameter wird die Anzahl der Frames pro RTP-Paket festgelegt. Ein höherer Wert bedeutet ein besseres Verhältnis von Nutzdaten zu Paketoverhead aber auch eine höhere Verzögerung. Es kann hier ein Wert von 1 bis 3 angegeben werden. (voreingestellt ist 1).

PBX-Routing (ab Hicom 150 H V1.0)

Hier können bis zu 2000 Rufnummern (auch Präfixe möglich) mit ihren zugehörigen Diensten eingetragen werden, die über eine IP-Vernetzung in einer anderen Hicom-Anlage erreicht werden können. Zu der Rufnummer wird der gewünschte Dienst konfiguriert: Dieser kann Voice, Modem oder FAX sein.

System-Clients

Zu den System -Clients gehört der „ C55 optiClient“ (neuer Name: optiClient 130 V1.0 oder V2.0), der „optiPoint IPadapter“ (ab Hicom 150 H V1.0) und optiPoint 400

➔ Interne Rufnummer des System -Client:

Die zuvor festgelegte Hicom interne Rufnummer wird hier dem entsprechendem HiPath HG 1500-Client zugeordnet.

➔ Authentifizierung:

Hier legen Sie fest, ob dieser Client sich bei HiPath HG 1500 identifizieren muss, um benutzt werden zu dürfen. Dies ist insbesondere bei Clients von Vorteil, die nicht im eigenen LAN liegen, sondern sich von außen einwählen.

➔ Passwort:

Hier geben Sie ein frei für diesen Client auswählbares Passwort für die Authentifizierung ein. Dieser Parameter ist nur aktiv, wenn Authentifizierung auf „Ja“ gesetzt wurde.

➔ Statusmeldungen übertragen:

Hier kann das Übertragen von Statusmeldungen (z. B. Displaymeldungen und LED-Informationen) ein- oder ausgeschaltet werden. Bei Remote-Clients sollte dieser Parameter auf „aus“ sein, da sonst kein Short Hold für diese Verbindung möglich ist.



H.323-Clients

Ein H.323 Client stellt Ihnen auf dem Netzwerk-PC Voice- und Datendienste zur Verfügung, die auch über Internet nutzbar sind. Hier werden keine Hicom Leistungsmerkmale unterstützt. Bei Nutzung der HiPath HG 1500 als Gateway für H.323 Clients sind nur Voice-Funktionen nutzbar.

Bevor Sie H.323 Clients im Administrationsprogramm konfigurieren, müssen Sie die IP-Adressen der betroffenen Client-PCs feststellen.

➔ Interne Rufnummer des H.323 Clients:

Geben Sie hier die interne Hicom Rufnummer ein, die für diesen Teilnehmer vorgesehen ist.

Die zur Verfügung stehenden Rufnummern können unter Verwendung der Rufnummernliste ermittelt und einfach der H.323-Funktionalität zugeordnet werden (siehe → 74)

➔ IP-Adresse:

Hier wird die IP-Adresse eingetragen, die dem Client-PC auch für das Networking zugewiesen wurde. Soll für einen Client Gatekeeper-Unterstützung benutzt werden, so ist die IP-Adresse 255.255.255.255 einzutragen.



Ab der Softwareversion HiPath 3000 V3.0 mit neuen Baugruppen (siehe →Seite 82) erfolgt die Anmeldung für System- und H.323-Clients nicht mehr unter „Voice Gateway“ im Assistant I sondern in der Hicom Administration im Assistant E. Ab der Softwareversion HiPath 3000 V3.0 wird der optiPoint IPadapter nicht mehr unterstützt.



Gatekeeper

Der Gatekeeper registriert die H.323 Clients und verwaltet deren Rechte und Dienste. Er setzt die Rufnummern der Clients in logische Namen oder IP-Adressen um und umgekehrt. Zudem registriert er die Gateways und kann mit benachbarten Gatekeepern vernetzt werden.

H.323 Clients mit Gatekeeper-Anbindung müssen mit der IP-Adresse „255.255.255.255“ eingerichtet werden.

→ IP-Adresse:

Hier wird die IP-Adresse des PCs mit dem Gatekeeper eingetragen.

→ Gatekeeper benutzen:

Hier können Sie die Gatekeeper-Unterstützung aktivieren.

→ Präfix:

Kennzahl eingeben, mit der der am Gatekeeper registrierte Teilnehmer einen direkt an der Hicom angeschlossenen Teilnehmer erreichen kann.

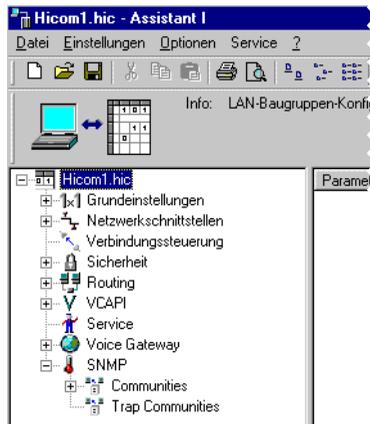


Voreinstellungen

→ IP-Adresse:

Hier kann ein Default-Wert für die IP-Adresse angelegt werden.

SNMP



Das Simple Network Management Protocol ist ein Standard, der es ermöglicht, Informationen zum Zustand der HiPath HG 1500 im Netz zu übertragen. HiPath HG 1500 bietet die Möglichkeit, Daten für die Auswertung durch ein Standard SNMP Programm zur Verfügung zu stellen.

Hierfür können folgende Parameter gesetzt werden:

- ➡ Minimum Severity für General-Traps
- ➡ Minimum Severity für Voice-Traps
- ➡ Minimum Severity für Data-Traps
- ➡ Minimum Severity für Security-Traps
- ➡ Kontaktperson (MIB-2)
- ➡ Name des Managed Node (MIB-2)
- ➡ Standort des Managed Node (MIB-2)

Die Werte für Severity können die Ausprägungen warning, minor, major und critical annehmen.

Traps werden erst generiert, wenn auch eine Trap-Community eingerichtet wird.

Communities

Hier definieren Sie Communities für den SNMP-Agenten. Die Parameter für eine Community sind:

➔ Community-Name:

Frei vergebbarer Name (ASCII-Zeichenfolge).

➔ IP-Adresse:

Die IP-Adresse des Managers, der diese Community benutzt. Wird hier kein Wert angegeben oder 0.0.0.0 eingetragen, kann diese Community von jedem Manager benutzt werden.

➔ Berechtigung:

Beschreibt die Zugriffsart für diese Community, die entweder read only oder read/write sein kann.

Trap-Communities

Definiert eine Community, an die Traps gesendet werden sollen. Die Parameter für eine TrapCommunity sind:

➔ TrapCommunity-Name:

Frei vergebbarer Name (ASCII-Zeichenfolge).

➔ IP-Adresse:

Die IP-Adresse des Empfängers

Menü „Optionen“

Programmeinstellungen

Hier kann der Benutzer die Sprache auswählen.



Zurücksetzen der HiPath HG 1500

Soll eine andere HiPath HG 1500-Baugruppe administriert werden, erfordert dies einen vorausgehenden Reset der alten Verbindung, der mit diesem Kommando ausgelöst werden kann.



Administrierbare HiPath HG 1500

Eine zu administrierende HiPath HG 1500 Baugruppe wird hier mit Namen und IP-Adresse eingetragen. Soll ein Datenaustausch erfolgen, kann die gewünschte HiPath HG 1500 aus einer Liste ausgewählt werden.

Benutzername und Kennwort wechseln

Hier kann die Benutzername/Kennwort-Kombination gewechselt werden, um z. B. eine andere HiPath HG 1500 zu administrieren. Benutzername und Kennwörter werden in der Hicom verwaltet und können auch nur dort administriert werden.

KDS konvertieren

Mit dieser Option kann der aktuell geladene KDS konvertiert werden. Dies kann erforderlich sein bei Leistungshüben in der Software der Baugruppe (APS-Wechsel mit geändertem KDS-Layout). Die aktuelle KDS-Version ist aus der Statusleiste ersichtlich.

Menü „Service“



Empfangen+Speichern des Fehlerspeichers

Empfängt und speichert die Fehlermeldungen der HiPath HG 1500 in eine Datei.



Empfangen+Speichern des Kunden-Trace

Empfängt und speichert die Tracemeldungen der vorher unter Service eingeschalteten Trace-Gruppen in einer Datei.



Lösche Kunden-Trace

Löscht den Speicherbereich für den Kunden-Trace in der Baugruppe.

Rufnummerntabelle anfordern

Rufnummern anfordern (nur bei Hicom 150 E ab Rel. 2.2 notwendig) Für die Administration der HiPath HG 1500 in einer 150 E Anlage (ab Rel. 2.2) können hier die in der Hicom konfigurierten Rufnummern (MSN) abgefragt werden. Es besteht die Möglichkeit, die Rufnummern dieser Liste direkt der vCAPi- bzw. H.323-Funktionalität zuzuordnen.

Bei der Hicom 150 H wird automatisch eine Liste verfügbarer Rufnummern (vCAPi-, H.323- oder System-Clients) beim Einrichten des jeweiligen Clients angeboten.

PBX-Routingtabelle importieren

Hier kann eine Datei eingelesen werden, die das Einrichten der Rufnummern für das PBX-Routing erleichtert, siehe → 88,

APS-Transfer

Ermöglicht das Updaten der Software der HiPath HG 1500.

APS+KDS-Transfer

Ermöglicht das Updaten der Software der HiPath HG 1500.

Zusätzlich wird der KDS übertragen. Das ist sinnvoll, wenn sich durch unterschiedliche Releases der HiPath HG 1500 die KDS-Struktur geändert hat. Somit kann der KDS am Remote-Platz konvertiert, und dann zusammen mit dem APS zur HiPath HG 1500 übertragen werden.

Ein APS-Transfer mit KDS-Hub ist wie folgt vorzunehmen:

1. Auslesen des KDS aus der HiPath HG 1500.
2. Mit „Optionen -> KDS konvertieren“ den KDS auf das neue Format bringen.
3. Über „KDS speichern unter“ den KDS auf die Festplatte speichern.

4. „APS+KDS-Transfer“ aktivieren: in der Dateiauswahlbox das neue APS-File angeben, anschliessend den konvertierten KDS angeben.

Jetzt werden beide Dateien auf die HiPath HG 1500 übertragen und im Flash dauerhaft gespeichert. Danach wird ein Reset ausgelöst und die Baugruppe läuft mit dem neuen APS und dem konvertierten KDS wieder hoch.

APS-Transfer über TFTP

Ermöglicht das Updaten der Software der HiPath HG 1500 über TFTP. Die IP-Adresse des TFTP-Server sowie Verzeichnis und Dateiname der APS-Datei müssen konfiguriert sein.

Reset der HiPath HG 1500-Baugruppe

Es ist ein Reset der HiPath HG 1500 über den Assistent I möglich.

Datum und Uhrzeit auf Baugruppe übertragen

Mit dieser Funktion wird das Datum und die Uhrzeit vom PC auf die Baugruppe übertragen (nur bei HiPath 500 möglich).

Anwendungen

Voice over IP

Voice over IP ist eines der herausragenden Leistungsmerkmale von HiPath HG 1500. Die Baugruppe bietet in Verbindung mit am LAN angeschlossenen Clients die Möglichkeit, nicht nur Voice over IP, sondern auch Telefonie-Leistungsmerkmale der Anlage zu nutzen. Sie haben insbesondere die Möglichkeit, dies auch bei Teleworking anzuwenden, das heißt, die Voice over IP Leistungsmerkmale stehen am Teleworking PC voll zur Verfügung. Daneben ist es zusätzlich möglich, H.323 Clients (z. B. NetMeeting) zu nutzen.

Ab der Softwareversion HiPath 3000 V3.0 mit neuen Baugruppen (siehe →Seite 82) erfolgt die Anmeldung nicht mehr unter „Voice Gateway“ im Assistant I sondern in der Hicom Administration im Assistant E.

Allgemeine Parameter für Voice over IP

Bevor Sie beginnen, System-Clients und H.323 Clients einzurichten, sollten Sie die für beide Varianten gültigen Parameter konfigurieren:

➔ Echo:

Hiermit können Echos kompensiert werden, die bei Verbindungen über das Voice-Gateway zu herkömmlichen Telefonen entstehen können.

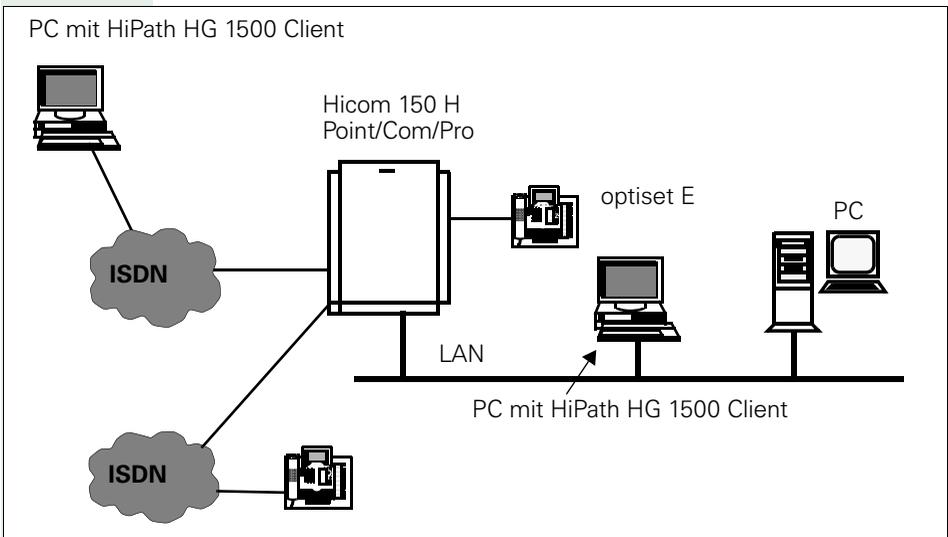
➔ Traffic-Statistic:

Hier legen Sie fest, ob eine Traffic-Statistik angelegt werden soll, die über SNMP abgefragt werden kann.

➔ Codierung:

Mit diesem Parameter wählen Sie die zu nutzende Sprachkodierung aus.

System-Client



Einrichtung eines System-Client

Um einen System-Client im Administrationsprogramm Assistant I einzurichten, klicken Sie mit der linken Maustaste doppelt auf den Punkt „Voice Gateway“ und anschliessend auf den Punkt „System-Clients.“ Dann können Sie mit der Symbolschaltfläche „Neu“ die Rufnummer eines neuen Clients eingeben. Diesen Schritt wiederholen Sie, bis Sie alle vorgesehenen Clients definiert haben.

Unter dem Menüpunkt „Service/Rufnummern anfordern“ kann eine Liste der möglichen Rufnummern angefordert werden.

Nachdem der Client angelegt wurde, müssen folgende Parameter angepasst werden:

Interne Rufnummer des System-Clients:

Hierbei handelt es sich um eine für die HiPath HG 1500 konfigurierte MSN.

Authentifizierung:

Hier legen Sie fest, ob dieser Client sich bei der HiPath HG 1500 beim Software Start mit einem Passwort identifizieren muss. Dies ist insbesondere bei Clients von Vorteil, die nicht im eigenen LAN liegen, sondern sich von außen einwählen.

➔ Passwort:

Hier geben Sie ein frei für diesen Client auswählbares Passwort für die Authentifizierung ein. Dieser Parameter ist nur aktiv, wenn Authentifizierung auf Ja gesetzt wurde.

➔ Statusmeldungen übertragen:

Mit dieser Auswahl legen Sie fest, ob Client-Statusmeldungen(z. B. Stati der Tasten-LED) übertragen werden sollen.

Die Übertragung von Statusmeldungen führt bei Teleworking Arbeitsplätzen u.U. zur Umgehung eines evtl. eingestellten Short Hold!

Weitere Informationen zum System-Client entnehmen Sie bitte seiner Bedienungsanleitung.



Um einen PC-Client nutzen zu können, muss der Client-PC mit einer voll duplexfähigen Soundkarte ausgestattet sein!



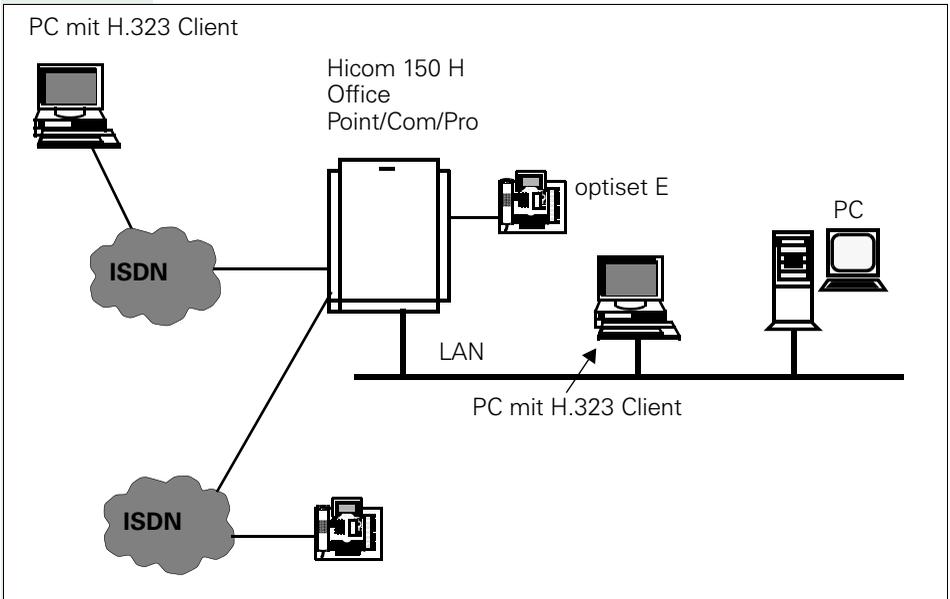
Ab der Softwareversion HiPath 3000 V3.0 mit neuen Baugruppen (siehe →Seite 82) können bis zu 48 Clients pro HXGS und 96 Clients pro HXGM eingerichtet werden. Es werden maximal 16 Konten unterstützt.

Einrichtung eines System-Clients mit Payload-Switching

Ab der Softwareversion HiPath 3000 mit neuen Baugruppen (siehe →Seite 82) können Sie Clients wie optiPoint 400 oder optiClient 130 V2.0 mit Payload-Switching-Fähigkeit einrichten. Während die Anrufsignalisierung über die Hicom erfolgt, wird die Sprachübertragung zwischen zwei Payload-Switching-Clients direkt über das LAN abgewickelt. Mit diesem Verfahren werden DSP-Ressourcen eingespart. Die Übertragung kann sowohl HG 1500- als auch knotenübergreifend erfolgen, sofern die genannten Softwarevoraussetzungen bei allen beteiligten Stationen erfüllt sind.

H.323-Client

Ein H.323 Client stellt Ihnen auf dem Netzwerk-PC Voicedienste zur Verfügung, die auch über das Internet nutzbar sind (Voraussetzung: feste IP-Adressen für alle Teilnehmer und die HiPath HG 1500). Es werden keine Leistungsmerkmale der Hicom unterstützt.



Einrichtung H.323-Client

Um einen H.323 Clients im Administrationsprogramm Assistant I einzurichten, sollte unter Menü „Voice Gateway -> Voreinstellungen“ die IP-Netzadresse abgelegt werden. Die MSNs der H.323-Clients müssen zuvor in der Hicom als S0-Teilnehmer eingerichtet worden sein. Danach können unter "Voice-Gateway-> H.323-Clients" die jeweiligen Clients mit ihrer Hostadresse konfiguriert werden.

Nachdem der Client angelegt wurde, müssen folgende Parameter angepasst werden:

➔ Interne Rufnummer des H.323 Clients:

Hierbei handelt es sich um eine für die HiPath HG 1500 konfigurierte MSN.

➔ IP-Adresse:

Im Anschluss daran öffnet sich automatisch das Fenster für die Eingabe der IP-Adresse, die dieser Rufnummer zugeordnet werden soll. Dies ist die IP-Adresse, die dem Client-PC auch für das Networking zugewiesen wurde.

Voreinstellungen siehe „Voice Gateway – H.323-Client“ (siehe → 70).

Nun können Sie auf den Netzwerk-PCs die H.323 Clients ihrer Wahl einrichten.

Die Gateway IP-Adresse muss in jedem Client eingetragen werden, sie entspricht der IP-Adresse des LAN-Interfaces.

Informationen zur Installation und Konfiguration der Clients entnehmen Sie bitte der Bedienungsanleitung oder Online-Hilfe der jeweiligen Software.

Wenn die Gatekeeper-Unterstützung verwendet werden soll, als IP-Adresse 255.255.255.255 eintragen. Weitere Hinweise siehe → 122.

IP Networking (PBX-Routing)

Einleitung

Neben den bisherigen Möglichkeiten der Vernetzung von Hicom 150 H-Systemen über CorNet-N und QSig kann ab V1.0 auch eine IP-Vernetzung (OfficePro, OfficeCom, OfficePoint) genutzt werden. Ermöglicht wird das Leistungsmerkmal IP Networking durch HiPath HG1500.

Steht ein entsprechendes IP-Netz zur Verfügung, können auf diese Weise erhebliche Gebühreneinsparungen erzielt werden. Dem Anwender stehen darüber hinaus Telefonie-Leistungsmerkmale wie z. B. Namensübermittlung und Rückruf in der gewohnten Art und Weise zur Verfügung.

HW-Voraussetzung für IP Networking ist, dass die jeweils beteiligten Systeme über mindestens eine der folgenden HiPath HG1500-Baugruppen verfügen:

- HXGM: Max. drei Baugruppen können in einer OfficePro eingesetzt werden. Pro HXGM sind 16 IP-Kanäle für Sprachverbindungen (Voice over IP) nutzbar.
- HXGS (Wandgehäuse) oder HXGSR (19"-Gehäuse): Eingesetzt werden können max. zwei Baugruppen in der OfficeCom und max. eine in der OfficePoint. Beide Baugruppen verfügen über jeweils 8 IP-Kanäle für Sprachverbindungen.

Die Administration der IP-vernetzten Systeme und der HiPath HG1500-Baugruppen wird über zwei verschiedene Tools vorgenommen:

- Hicom Assistant E Office: Vorhandenen KDS der Hicom 150 H um Informationen für IP Networking ergänzen (ab →Seite 82)
- Assistant I/HG1500: Einstellungen der HiPath HG1500-Baugruppe(n) vornehmen (ab →Seite 86)



Informationen, die über die vorliegende Dokumentation hinausgehen, können dem Servicehandbuch Hicom 150 H entnommen werden.



Die IP-Adresse, die für PBX-Routing verwendet wird, ist immer die des ersten LAN-Interfaces. Geht das PBX-Routing über ein anderes Interface, z. B. LAN2, so ist durch IP-Routingeinträge sicherzustellen, dass das LAN1-Interface erreicht werden kann.

KDS um Informationen für IP Networking ergänzen

Der vorhandene KDS der Hicom 150 H wird über den Hicom Assistant E Office um Informationen für IP Networking ergänzt.

Die folgenden Angaben beziehen sich auf Hicom 150 H-Systeme mit den zentralen Steuerungen CBMOD (OfficePro) und CBPC (OfficeCom, OfficePoint).

Für Systeme mit den Steuerbaugruppen CBCPR (OfficePro), CBCC (OfficeCom), CBRC (OfficeCom Rack), CBPC (OfficePoint) und CBRP (OfficePoint Rack) ergibt sich ein anderer Aufbau des Dialogs „Netzwerk“ Menü „Einstellungen“).

Schritt	Tätigkeit
1.	Vorhandenen KDS der Hicom 150 H mittels Hicom Assistant E Office herunterladen und sichern.
2.	Falls erforderlich, KDS auf Stand Version 1.0 oder 1.2 konvertieren.
3.	Dialog „Systemweit ...“ im Menü „Systemstatus“ aufrufen.
4.	Registerkarte „Baugruppen“ öffnen. <ul style="list-style-type: none"> • Umschalten zu „SW-Ausbau“: HiPath HG1500-Baugruppe(n) einfügen. • Umschalten zu „BG-Konfig.“ und Registerkarte „HXGM-Konfiguration“ aufrufen: <ul style="list-style-type: none"> – Auswahl: Ist eine OfficePro mit mehreren HXGM-Baugruppen bestückt, kann hier die jeweils zu konfigurierende HXGM ausgewählt werden. – Leitungen: Über „Neue Anzahl“ wird definiert, wieviele der max. möglichen Leitungen (IP-Kanäle) einer HiPath HG1500-Baugruppe eingerichtet werden sollen. Nach Betätigung des Buttons „Einrichten“ erscheinen die Leitungen im entsprechenden Anzeigefeld.
5.	Dialog „Leitungen/Vernetzung ...“ im Menü „Einstellungen“ aufrufen.
6.	Registerkarte „Leitungen“ öffnen. <ul style="list-style-type: none"> • Spalte Richtung: Für IP Networking verwendete Leitungen sind immer der Richtung 16 zuzuordnen. • Spalte Parameter: Durch Doppelklick im Feld Parameter der gewünschten Leitung wird der Dialog „Parameter“ mit dem aktuell eingestellten Protokoll (HXGM/HXGS: Trunk CorNet-N Plus (HiPath AllServe H150)) angezeigt.

Schritt	Tätigkeit
7.	Registerkarte „Richtungen“ öffnen. <ul style="list-style-type: none"> • Richtungsname: Hier kann einer Richtung ein Name zugewiesen werden. Der Richtungsname wird dann anstelle der standardmäßig eingetragenen Richtungsnummer im Listenfeld „Richtungen“ angezeigt. • Anlagenrufnummer: Anhand dieser Nummer wird das System im IP-Netz identifiziert. Die Anlagenrufnummer darf nicht im Rufnummernplan enthalten sein und muss innerhalb des IP-Netzes eindeutig sein. Für die Ländervorwahl und die Ortsnetzkennzahl sind keine Angaben zu machen.
8.	Registerkarte „Richtungsparameter“ öffnen. Die folgenden Einstellungen sind zwingend vorgeschrieben: <ul style="list-style-type: none"> • Rerouting aktiv: Nein • Richtungsflags: Üb.-Dienst 3,1 kHz Audio • Pause vor Wahl: Keine Pause • Amtsrufpause: Nach 6 s • Belegungsart: Linear • Richtungsart: PABX • Nr-Typ, gehend: Intern • Rufnummer Typ: Intern / DUWA
9.	Dialog „Netzwerk“ im Menü „Einstellungen“ aufrufen.
10.	Registerkarte „IP-Parameter“ öffnen. <ul style="list-style-type: none"> • IP-Access: HIP Forwarding auswählen. Die HiPath HG1500-Baugruppe arbeitet im Bridging-Modus, d. h. die HiPath HG1500-BG und die Steuerung der Hicom 150 H haben separate IP-Adressen, die sich ein physikalisches LAN-Interface teilen. • Hicom 150 H <ul style="list-style-type: none"> – IP-Adresse: Hier wird die IP-Adresse hinterlegt, über die die HiPath HG1500-BG die Hicom 150 H anspricht. – Subnet Mask: Subnetz-Maske an der Schnittstelle zwischen Hicom 150 H und HiPath HG1500-BG. – MTU: Maximale Ethernet-Framelänge auf der Strecke zwischen Hicom 150 H und HiPath HG1500-BG. Der voreingestellte Wert sollte nicht verändert werden! • Routing Tabelle: Alle hier eingestellten Werte sollten nicht geändert werden.

Schritt	Tätigkeit
11.	<p>Registerkarte „AllServe Parameter“ öffnen.</p> <ul style="list-style-type: none"> • Server IP-Adresse: nicht relevant • Knoten Knoten-ID: Im IP-Netz muss für jedes System eine eindeutige Knoten-ID vergeben werden. Die verwendete Zahl sollte im Bereich 1 - 64 liegen, da auf der HiPath HG1500-BG ebenfalls eine Knoten-ID benötigt wird und beide ID's identisch sein müssen (Zuordnung Knoten-ID zur IP-Adresse). • AllServe Zugangsberechtigung Spalte Baugruppen: Angezeigt wird, welche HiPath Baugruppe(n) in welchem Slot des Systems gesteckt ist (sind). Das Flag „AllServe Zugang“ ist für die Baugruppe(n) zu setzen, die für die IP Networking vorgesehen sind.
12.	<p>Dialog „Automatische Wegesuche“ im Menü „Einstellungen“ aufrufen. Hinweis: Die eindeutige Nummerierung aller IP-vernetzten Systeme muss vor der Systemgenerierung festgelegt werden, um die Eindeutigkeit aller Rufnummern und Kennzahlen (Leitungen, interne Zugänge, Gruppen usw.) im Netz sicherzustellen. Eine Möglichkeit ist, jedem System ein definiertes Rufnummernband zuzuweisen. Zum Beispiel Eintausender Rufnummern (1001 - 1999) für System 1 (Knoten 1), Zweitausender Rufnummern (2000 - 2999) für System 2 (Knoten 2) usw..</p>
13.	<p>Registerkarte „Codes und Flags“ öffnen.</p> <ul style="list-style-type: none"> • LCR Flags: Flag „LCR freigeben“ setzen, um die automatische Wegesuche zu aktivieren. • Wahlaussendung: Blockweise Wahlaussendung markieren. Gewählte Ziffern werden vom System zwischengespeichert. Die Wahl erfolgt erst nach Ablauf eines Timers nach der letzten gewählten Ziffer oder nach Eingabe des Wahlendekennzeichens „#“.
14.	<p>Registerkarte „Wahlplan“ öffnen.</p> <ul style="list-style-type: none"> • Spalte Gewählte Ziffern: Hier wird definiert, über welche Wahlziffern welches IP-vernetzte System zu erreichen ist. • Spalte Wegetabelle: Die hier eingetragene Wegetabelle bestimmt den Verbindungsaufbau. <p>Beispiel: Gewählte Ziffern = -2XXX, zugeordnete Wegetabelle = 1. Der Verbindungsaufbau aller gewählten Rufnummern von 2000 - 2999 erfolgt anhand Wegetabelle 1.</p>
15.	<p>Registerkarte „Wahlregeltabelle“ öffnen.</p> <ul style="list-style-type: none"> • Spalte Regelname: Hier kann ein bis zu 16 ASCII-Zeichen langer Name frei vergeben werden. • Spalte Regelformat: Die hier eingetragene Regel bestimmt, wie die vom Teilnehmer gewählten Ziffern umgesetzt und vom System gewählt werden sollen. <p>Beispiel: Regelformat = DxxxE1A, wobei xxx die Anlagenrufnummer des zu erreichenden Systems ist (siehe 7).</p>

Schritt	Tätigkeit
16.	Registerkarte "Vegetabelle" öffnen. <ul style="list-style-type: none"><li data-bbox="395 188 1031 236">• Feld Auswahl: Hier ist die in 14 definierte Vegetabelle auszuwählen.<li data-bbox="395 236 1031 268">• Spalte Richtung: Die in 6 gewählte Richtung eintragen.<li data-bbox="395 268 1031 292">• Spalte Wahlregel: Die in 15 definierte Regel eintragen.
17.	KDS sichern und zur Hicom 150 H übertragen.

Einstellungen der HiPath HG1500-Baugruppe(n) vornehmen

- Erstinbetriebnahme der HiPath HG1500-Baugruppe(n) mit Assistant I

Voraussetzung für eine IP Networking ist, dass sich alle PBX-Knoten (Hicom 150 H-Systeme) im gleichen IP-Netz befinden und nicht über IP-Routing (z. B. eine Verbindung über S0-Standleitung) vernetzt sind.

- Einstellungen für IP Networking vornehmen

Schritt	Tätigkeit
1.	Vorhandenen KDS der HiPath HG1500-Baugruppe mittels Assistant I/HG1500 herunterladen und sichern.
2.	Menüpunkt "Grundeinstellungen" im Menü "Einstellungen" aufrufen.
3.	<p>„Grundeinstellungen“ vornehmen:</p> <ul style="list-style-type: none"> • Codierung: Dieser Parameter wird von der Hicom 150 H an die HiPath HG1500-Baugruppe(n) übergeben und ist nicht zu ändern. • Anzahl vom Router verwendbarer B-Kanäle: Max. 16 B-Kanäle sind möglich, wobei eine Mindestanzahl von B-Kanälen immer für HiPath HG1500-Clients verfügbar sein sollte. Sind z. B. sechs Kanäle lizenziert, könnten vier davon dem Router zugeordnet werden. Dadurch wäre gewährleistet, dass zwei B-Kanäle immer den HiPath HG1500-Clients vorbehalten sind. • IEEE802.1p: Parameter für die Einstellung des Ethernet-Formats, wobei zwischen „deaktiviert“ (Defaultwert) und „aktiviert“ gewählt werden kann. Der Parameter wirkt nur auf Datenpakete, die von der HiPath HG1500-BG verschickt werden. Alle Komponenten im LAN, über die oder mit denen die HG1500 Ethernet-Datenpakete austauscht, müssen dieses Format unterstützen. • QoS-Verfahren: Parameter für die Definition des Quality of Service-Verfahrens auf der HiPath HG1500-BG, über das eingehende IP-Datenpakete priorisiert werden. Defaultwert ist „Autodetect.“ • PBX-Knoten Überwachung (Ab SMR15 des Assistant I/ HG1500 ist diese Einstellung unter „PBX-Routing“ im Menüpunkt „Voice Gateway“ zu finden.): Hier kann die Überwachung zwischen den IP-vernetzten Hicom 150 H-Systemen (Knoten) aktiviert werden. Bei Auswahl „aktiviert“ werden im 4 s-Abstand Überwachungsmeldungen zwischen allen Knoten verschickt. Empfängt ein Knoten keine Überwachungsmeldungen mehr, wird IP Networking als ausgefallen gekennzeichnet. Bestehende Gespräche werden getrennt. Der Parameter muss in allen Systemen (Knoten) gleich eingestellt sein.

Schritt	Tätigkeit
4.	<p>„QoS-Prioritätsklassen“ einstellen. HiPath HG1500 benutzt vier Klassen, um den eigenen gehenden IP-Datenverkehr zu priorisieren:</p> <ul style="list-style-type: none"> • Voice Payload: H.323-Pakete, welche die Sprachinformation enthalten. • Call Signaling: Werden für den Verbindungsaufbau (z. B. H.323) benötigt. • Data Payload: Z. B. für FAX-Daten für IP Networking. • Network Control: Z. B. SNMP-Traps. <p>Die Priorität der einzelnen Klassen wird über die „AE/EF Codepoints“ eingestellt. Im allgemeinen können die Defaultwerte beibehalten werden.</p>
5.	<p>„AE/EF Codepoints“ einstellen. Hier werden die Werte definiert, welche die unterschiedlichen Priorisierungen (4) festlegen. Die Defaultwerte sind beizubehalten.</p>
6.	<p>Menüpunkt „Voice Clients“ im Menü „Einstellungen“ aufrufen. (Ab SMR15 des Assistant I/HG1500 heißt dieser Menüpunkt „Voice Gateway.“)</p>
7.	<p>Einstellungen für Voice over IP vornehmen:</p> <ul style="list-style-type: none"> • Echo: Bei Auswahl „ein“ können Echos kompensiert werden, die bei Verbindungen über das Voice-Gateway zu analogen Telefonen entstehen können. • Traffic-Statistik: Bei Auswahl „ein“ wird eine Statistik geführt, die über SNMP ausgewertet werden kann. • Codierung: Dieser Parameter wird von der Hicom 150 H an die HiPath HG1500-Baugruppe(n) übergeben und ist nicht zu ändern. • Max. Anzahl gleichzeitiger Rufe: Von den lizenzierten B-Kanälen (max. 16 bei HXGM, max. 8 bei HXGS, HXGSR) kann hier eine bestimmte Anzahl für Voice over IP zur Verfügung gestellt werden. Diese ist auch abhängig von der Anzahl der installierten HiPath HG1500-Clients (Voice Clients). • Fähigkeiten des H.323 Clients (Ab SMR15 des Assistant I/HG1500 sind diese Einstellungen unter „Audio Codecs für Voice Clients“ zu finden.): Hier werden die Audio-Standards der H.323-Clients bei IP Networking (Voice over IP) definiert. Folgende Einstellungen sind zu wählen: <ul style="list-style-type: none"> – Anzahl der Einträge = 3 – AudioCodec (high priority) = G.723 – AudioCodec (medium priority) = G.711 U-Law – AudioCodec (low priority) = G.711 A-Law <p>Hinweis: G.723 bewirkt eine Komprimierung auf ca. 18 - 20 kBit/s. G.711 erlaubt eine Vollduplex-Verbindung mit 180 kBit/s, allerdings auf Kosten der IP-Datenlast. Hinweis zur Verwendung von IP-Telefonen des Typs optiClient/C55: Bei einer Einrichtung als Heimarbeitsplatz (über ISDN) ist „AudioCodec = G.723“ und bei Einrichtung als Standardarbeitsplatz (über LAN) ist „AudioCodec = G.711 U-Law“ zu wählen.</p>
8.	<p>Menüpunkt „Routing“ im Menü „Einstellungen“ aufrufen.</p>

Schritt	Tätigkeit
9.	Einstellungen unter „PBX-Knoten“ vornehmen (Ab SMR15 des Assistant I/HG1500 ist diese Einstellung im Menüpunkt „Voice Gateway“ zu finden.): Hier wird die Verbindung zwischen der Knoten-Nr. (Knoten-ID, siehe 11 auf →Seite 84) des Hicom 150 H-Systems und den IP-Adressen der HiPath HG1500-Baugruppen hergestellt. <ul style="list-style-type: none"> • PBX-Knoten: Nr. von 1-64, die das Hicom 150 H-System identifiziert (Knoten-ID, siehe 11 auf →Seite 84). • IP-Adresse: Pro Knoten (Hicom 150 H-System) können bis zu drei HiPath HG1500-Baugruppen anhand ihrer IP-Adressen konfiguriert werden.
10.	Einstellungen unter „PBX-Routing“ (IP Networking) vornehmen (Ab SMR15 des Assistant I/HG1500 ist diese Einstellung im Menüpunkt „Voice Gateway“ zu finden.): Hier können bis zu 2000 Rufnummern (Durchwahlnummern oder Präfixe) mit ihren zugehörigen Diensten eingetragen werden, die über IP Networking in einem anderen Hicom 150 H-System erreicht werden können. <ul style="list-style-type: none"> • Rufnummer • Dienst: Ausgewählt werden kann zwischen Voice, Modem und Fax. • PBX-Knoten: Hier ist die Knoten-Nr. (Knoten-ID, siehe 11 auf →Seite 84) des Hicom 150 H-Systems einzutragen, in dem diese Rufnummer erreicht werden soll.
11.	KDS sichern und zur HiPath HG1500-Baugruppe übertragen.

• Routingtabelle

Eine Administrationserleichterung ist der Import einer Tabelle über das Menü „Service“ unter „PBX-Routingtabelle importieren.“ Mit der Auswahl dieses Menüpunkts erscheint eine Dateiauswahlbox. Eine solche Importdatei (einfache Textdatei) hat folgendes Format:

[Routing-Entries]
 <Rufnummer> <NodeNumber> <Dienst>...

[PBX-Nodes]
 <NodeNumber> <IP-Adresse> <IP-Adresse>

Folgendes Beispiel soll dies verdeutlichen:

[Routing-Entries]
 560 1 FAX
 561 1 Voice
 562 1 Modem
 563 1 Voice
 588 2 Voice
 6 14 Voice
 [PBX-Nodes]
 1 192.168.100.254 192.168.100.253
 2 192.168.120.200
 14 192.168.121.253

Es sind vier Rufnummern für Knoten 1 konfiguriert, Knoten 1 hat zwei Hi-Path HG 1500. Eine Rufnummer ist in Knoten 2 konfiguriert. Alle Rufnummern, die mit „6“ beginnen (und von der Hicom auf die HiPath HG 1500 geroutet werden), werden zum Knoten 14 weitervermittelt.

Die HiPath HG 1500 müssen untereinander die nötigen IP-Routeingeeinträge haben, um über IP in beiden Richtungen erreichbar zu sein.

Jede für IP-Vernetzung in der Hicom reservierte Leitung kann auf der Baugruppe nicht für andere Applikationen (Routing, VCAPi, H.323 etc.) verwendet werden. Dies ist auch bei der Lizenzierung der B-Kanäle (im KDS unter „Service“) zu beachten.

Bandbreitenmanagement

Bandbreitenmanagement dient zur Verwaltung der Bandbreite bei Voice over IP zwischen zwei Knoten mit HG 1500, die über ISDN geroutet sind (bei LAN-Verbindungen in der Regel nicht notwendig).

Ist der AudioCodec auf den Wert „G723“ (→Seite 68) eingestellt, so sind über einen ISDN-B-Kanal 5 Gespräche gleichzeitig möglich. Ab dem 6. Gespräch wird automatisch ein weiterer B-Kanal aufgebaut (Voraussetzung: beim ISDN-Partner sind 2 Kanäle oder mehr eingetragen →Seite 53). Die RTP-Kompression wird automatisch ausgehandelt und ist nicht konfigurierbar.

Erfolgt bei Voice over IP gleichzeitig auch Datentransfer über einen gerouteten ISDN-Kanal, so ist die MTU-Size Fragmentation des entsprechenden ISDN-Partners zu aktivieren (siehe →Seite 54).

Um weitere Bytes einzusparen kann die IP-Header Compression aktiviert (→Seite 54) und der PPP Default Header deaktiviert werden (→Seite 54).

Bei gleichzeitigem Voice over IP und Datentransfer sollte der Wert für die Paketierung auf 3 eingestellt sein (siehe →Seite 68).

Quality of Service (QoS)

Quality of Service umfaßt verschiedene Methoden, in paketorientierten Netzen (IP) gewisse Eigenschaften der Übertragung sicherzustellen.

So ist es z. B. für Voice over IP wichtig, eine Mindest-Bandbreite für die Dauer der Übertragung sicherzustellen. Wenn mehrere Applikationen gleichberechtigt über IP arbeiten, so wird die vorhandene Bandbreite einer Übertragungsstrecke (z. B. ein ISDN-B-Kanal, 64kBit/s) aufgeteilt, so daß u.U. eine Voice-Verbindung von Paketverlusten betroffen ist, woraus eine schlechte Sprachqualität resultieren kann.

Die HiPath HG 1500 verwendet verschiedene Verfahren zur Realisierung von Quality of Service.

Auf der Ebene von Schicht 2 (nach OSI, Ethernet) kann eine Erweiterung (IEEE802.1p) gegenüber dem Standard-Ethernet-Format (DIX V2) aktiviert werden, die den Ethernet-Header um einige Informationen erweitert, unter anderem um ein 3 Bit breites Datenfeld. Mit diesem Feld wird dem Datenpaket eine Priorisierungsinformation mitgegeben. Für alle Pakete, die die Baugruppe aus dem LAN erreichen, werden beide Ethernet-Formate (IEEE802.1p und DIX V2) verstanden, für alle Pakete, die von der Baugruppe ins LAN verschickt werden, kann das Format über „Grundeinstellungen->IEEE802.1p“ ausgewählt werden. Bevor dieser Parameter aktiviert wird, sollte geprüft werden, ob alle Komponenten im Netzwerk dieses Format unterstützen. Andernfalls ist unter Umständen vom LAN aus kein Zugang auf die HiPath HG 1500 mehr möglich.

Beim Übergang auf ein anderes Transportmedium (z. B. ISDN) wird der Ethernet-Header nicht weitertransportiert. Ein IP-Router (wie der der HiPath HG 1500) kann daher die Informationen zur Priorisierung nutzen, die im IP-Header enthalten sind. Die Priorisierung auf IP-Ebene können aber auch reine IP-Router nutzen, die z. B. zwei Netzsegmente miteinander verbinden. Im Type of Service-Feld werden entweder 3 Bit (IP-Precedence nach RFC 791, älterer Standard) oder 6 Bit (Differentiated Services oder DiffServ, nach RFC 2474) zur Bildung von unterschiedlichen Klassen ausgewertet. Der IP-Router der HiPath HG 1500 stellt diesen Klassen unterschiedliche Bandbreiten zur Verfügung, so daß z. B. Voice-Pakete vorrangig behandelt werden können. Nach welchem Verfahren die HiPath HG 1500 arbeitet, kann unter „Grundeinstellungen->QoS-Verfahren“ eingestellt werden (Default ist Autodetect).

Für das DiffServ-Verfahren werden verschiedene sogenannte Codepoints („Grundeinstellungen->AF/EF Codepoints“) definiert und anhand dieser Codepoints zwei verschiedene Verfahren für die Behandlung der Payload verschieden markierter Datenströme genutzt:

Das Expedited Forwarded (EF) Verfahren (nach RFC 2598) garantiert eine konstante Bandbreite für die Daten dieser Klasse. Wird der definierte Wert erreicht, werden alle Pakete, die diese Bandbreite überschreiten würden, verworfen. Auf der HiPath HG 1500 ist für EF eine eigene Klasse definiert. Für diese Klasse kann die Bandbreite für jeden ISDN-Partner in Prozent definiert werden (QoS-Bandbreite für EF).

Das Assured Forwarding (AF) Verfahren (nach RFC 2597) garantiert eine minimale Bandbreite für die Daten einer (von mehreren) Klassen. Die Klassen niedrigerer Priorität teilen sich jeweils die von EF bzw. den höher priorisierten Klassen nicht genutzte Bandbreite. Innerhalb jeder Klasse kann über den Dropping Level zusätzlich definiert werden, wie schnell Pakete verworfen werden sollen, wenn sie nicht schnell genug weitertransportiert werden können. So ist es bei Sprachpaketen nicht sinnvoll, sie lange zwischenspeichern (dadurch erhöht sich nur das Delay, die Verzögerung). Bei einer gesicherten Datenübertragung (z. B. einem Filetransfer) ist es hingegen vorteilhaft, einen größeren Zwischenspeicher zu haben, da es andernfalls ohnehin zu Paketwiederholungen zwischen den beiden Endstellen kommen würde.

Auf der HiPath HG 1500 sind vier Klassen für AF reserviert: AF1x (hohe Priorität), AF2x, AF3x und AF4x (niedrige Priorität), wobei „x“ für einen von drei Dropping-Leveln steht: low (1), medium (2) und high (3). Bei „low“ werden Pakete lange zwischengespeichert, bei „high“ werden Pakete früh verworfen, wenn sie nicht weitertransportiert werden können. Unmarkierte IP-Pakete (ToS-Feld=00) werden mit niedrigster Priorität behandelt.

Wenn ein Routing-Partner nur mit einem der beiden Standards (DiffServ oder IP-Precedence) arbeiten kann (z. B. ein älterer Router, der nur mit IP-Precedence arbeitet), so kann die HiPath HG 1500 das ToS-Feld entsprechend übersetzen. Dies kann bei jedem ISDN-Partner bzw. DSL/LAN2/PPTP-Interface über „QoS-Fähigkeiten“ eingestellt werden. Im Default „identisch“ wird nichts übersetzt, mit den beiden Werten „DiffServ“ bzw. „IP-Precedence“ findet jeweils eine Übersetzung gemäß der untenstehenden Tabelle statt, wenn das Feld nicht nach dem eingestellten Standard versorgt ist.

Bei IP-Datenverkehr werden die IP-Pakete, die die HiPath HG 1500 selbst generiert, in fünf Gruppen aufgeteilt (z. B. der VCAPi-Server, H.323-Gateway). Für vier dieser Gruppen kann eingestellt werden, mit welchem Codepoint die Pakete markiert werden sollen. Konfiguriert wird dies unter „Grundeinstellungen->QoS-Prioritätsklassen“:

Voice-Payload für die H.323 Telefonie (Voice over IP)

Call Signaling für den Verbindungsaufbau bei H.323

Data Payload z. B. für IP-Vernetzung mit FAX oder Modem

Network Control z. B. SNMP-Traps

Der übrige Datenverkehr wird mit „deaktiviert,“ also 00 markiert.

Der Zusammenhang zwischen den verschiedenen Codepoints von Diff-Serv, IP-Precedence und dem „User Priority“-Feld im Ethernet-Header ist in der folgenden Tabelle dargestellt.

IP-Header								Ethernet-Header	
DiffServ						vs.	IP-Precedence		IEEE802.1p
Codepoint	Vorbelegung (änderbar)		Drop-Level				Belegung (fest)		
	binär (Bitfeld)	ToS-Feld (hex)	high	med	low		binär (Bitfeld)	ToS-Feld (hex)	User Priority (Binär, Bitfeld)
CS7	111000	E0		x		<->	111	E0	111
AF 11	001010	28			x	->	110	C0	110
AF 12	001100	30		x		<->	110	C0	110
AF 13	001110	38	x			->	110	C0	110
AF 21	010010	48			x	->	101	A0	101
AF 22	010100	50		x		<->	101	A0	101
AF 23	010110	58	x			->	101	A0	101
AF 31	011010	68			x	->	100	80	100
AF 32	011100	70		x		<->	100	80	100
AF 33	011110	78	x			->	100	80	100
AF 41	100010	88			x	<->	011	60	011
AF 42	100100	90		x		<->	011	60	011
AF 43	100110	98	x			<->	011	60	011
EF	101110	B8				<->	110	C0	110
DE (default)	000000	00					000 001, 010	00 20, 40	000

Die Spalte „vs.“ verdeutlicht die Zusammenhänge zwischen den beiden Standards DiffServ und IP-Precedence. Da DiffServ mehr Varianten bietet, wird bei der Übersetzung von IP-Precedence in DiffServ jeweils der Codepoint fest ausgewählt: z. B. wird aus „100“ IP-Precedence der Codepoint „AF31.“ Bei Paketen, die die HiPath HG 1500 in Richtung LAN verlassen, wird bei aktiviertem IEEE802.1p die in der letzten Spalte angegebene User Priority eingestellt.

QoS kann nicht nur für ISDN-Partner, sondern auch für die zweite LAN- bzw. DSL-Schnittstelle aktiviert werden.

Für die DSL-Schnittstelle wird das Interface um eine zusätzliche Begrenzung der Datenrate erweitert. Die Funktionsweise der Qualitätsbewertung entspricht dem Verfahren der ISDN-Partner. Die durchschnittliche Datenrate wird in den Konfigurationsdaten eingestellt.

Telematik mit dem vCAPi-Client

Prinzip der virtuellen bzw. verteilten CAPI (vCAPi)

Genutzt wird das Prinzip, eine in einem Netzwerk-PC bzw. Server eingebaute ISDN-Karte allen Benutzern im Netz verfügbar zu machen, indem auf den PCs eine „virtuelle CAPI-Schnittstelle“ (vCAPi) installiert wird, die das Vorhandensein einer lokalen ISDN-Karte emuliert.

Diese vCAPi-Schnittstelle verhält sich gegenüber einer Applikation weitestgehend wie eine mit einer ISDN-Karte gelieferte CAPI-Schnittstelle. Der Unterschied besteht darin, dass die vCAPi die von der Applikation aktivierten Funktionen nicht direkt an die Karte weiterleitet, sondern in Datenpakete umwandelt und auf das LAN ausgibt (Client-Server-Prinzip).

Um eine oder mehrere ISDN-Karten einsparen zu können, wird durch die Hicom 150 E Office Point/Com/Pro eine ausgelagerte, „virtuelle ISDN-Karte“ zur Verfügung gestellt. Auf allen Netzwerk-PCs ist eine vCAPi-Schnittstelle mit der zuvor beschriebenen Funktionalität installiert (CAPI-Client). Die von den PCs über die vCAPi geschickten Meldungen werden auf der HiPath HG 1500 (CAPI-Server) ausgewertet und anschließend werden mit Hilfe dieser Informationen ein oder mehrere B-Kanal-Verbindungen für den gewünschten Dienst aufgebaut und das gewählte Protokoll abgewickelt. Für kommende Rufe muss der HiPath HG 1500 eine Anzahl von Durchwahlnummern (max. 100) zur Verfügung gestellt werden. Jede dieser Rufnummern muss auf eine Netzwerkadresse abgebildet werden, um einen kommenden Ruf an genau eine der virtuellen CAPI-Schnittstellen vermitteln zu können. Die vCAPi wandelt die Ethernet-Pakete wiederum in die entsprechenden CAPI-Meldungen um.

Identifizierung der CAPI-Teilnehmer

Auf jedem PC, der Telematik-Funktionen nutzen möchte, wird eine vCAPi-Schnittstelle in Form einer DLL installiert (CAPI20.DLL 16 Bit, CAPI2032.DLL 32 Bit). Jeder PC wird über seine IP-Adresse und seine Rufnummern im Netz eindeutig identifiziert.

Die Rufnummer des Zielteilnehmers wird in jedem gehenden Verbindungsaufbau angegeben und ggf. durch die Wahlkontrolle der Hicom 150 E OfficePoint/Com/Pro überprüft. Eine Überprüfung durch die HiPath HG 1500 erfolgt hier nicht.

Anders als bei der Routerfunktionalität sind die dort beschriebenen Sicherheitsmechanismen (Firewalls) für die Telematik-Funktionalität nicht anwendbar. Beispielsweise muss ein PC mit vCAPi auch dann über seine Durchwahlnummer erreichbar sein, wenn der Anruf keine ISDN-Rufnummer hat. (z. B. analoges FAX-Gerät).

Mit HiPath HG 1500 und der vCAPi Software (virtuelle CAPI) verhält sich der PC ähnlich wie ein PC mit eigener ISDN-Karte. Voraussetzungen dafür sind:

- TCP/IP als Transportprotokoll
- WIN 95/98, WIN-NT 4.0 oder Windows 2000 als Client-Betriebssystem

Die Rufnummernvergabe erfolgt in der HiPath HG 1500 durch die Zuordnung einer TCP/IP Adresse zu einer Rufnummer. Für vCAPi Funktionen können maximal 100 Rufnummern verwendet werden.

Hierbei kann es auch notwendig sein einer TCP/IP Adresse für die Nutzung verschiedener Dienste mehrere Rufnummern zuzuordnen. Dies trifft insbesondere dann zu, wenn Sie CTI- und Faxdienste gleichzeitig auf einem PC nutzen wollen.



Es wird nur der CAPI-Standard Version 2.0 unterstützt.
(16 und 32 bit Version / capi20.dll und capi2032.dll)

Unter Windows NT 4.0 und Windows 2000 wird auch eine CAPI als Dienst installiert, z. B. für cFos.

Einrichtung vCAPi-Client

Um die Funktion der virtuellen CAPI im Netzwerk nutzen zu können müssen immer zwei Voraussetzungen geschaffen werden:

- Einrichtung des vCAPi-Teilnehmers im Administrationsprogramm
- Einrichtung des vCAPi-Client auf dem jeweiligen Netzwerk-PC.



Bevor Sie beginnen, vCAPi im Administrationsprogramm zu konfigurieren, müssen Sie die IP-Adressen der betroffenen Client-PCs feststellen und die zu benutzenden internen Hicom Rufnummern festlegen.

Um einen vCAPi-Client im Administrationsprogramm Assistant I einzurichten, sollte unter Menü „vCAPi-> Voreinstellungen“ die IP-Netzadresse abgelegt werden. Die MSNs der vCAPi-Clients müssen zuvor in der Hicom als S₀-Teilnehmer eingerichtet worden sein. Danach können unter „vCAPi → vCAPi-Teilnehmer“ die jeweiligen Clients mit ihrer Hostadresse konfiguriert werden.

Diesen Schritt wiederholen Sie, bis Sie alle vorgesehenen Clients definiert haben.

Nachdem der Client angelegt wurde, müssen folgende Parameter angepasst werden:

➔ Rufnummer (intern):

Hierbei handelt es sich um eine für die HiPath HG 1500 konfigurierte MSN.

➔ IP-Adresse:

Im Anschluss daran öffnet sich automatisch das Fenster für die Eingabe der IP-Adresse, die dieser Rufnummer zugeordnet werden soll. Dies ist die IP-Adresse, die dem Client-PC auch für das Networking zugewiesen wurde.

➔ Fax Gruppe 3:

Hier legen Sie fest, ob ein vCAPi-Teilnehmer auch den Dienst Fax Gruppe 3 nutzen darf. Beachten Sie, dass bei Freigabe dieses Flags und gleichzeitiger Nutzung von CTI eine zweite Rufnummer zu dieser IP-Adresse zugeordnet werden muss, da es ansonsten zu Problemen bei der Rufannahme kommen kann.

➔ Voice:

Hier kann Voice für eine Rufnummer freigeschaltet oder gesperrt werden.

➔ Digitale Daten:

Hier kann der Dienst „Digitale Daten“ für eine Rufnummer freigeschaltet oder gesperrt werden.

Voreinstellungen siehe „vCAPi-Teilnehmer“ (siehe → 62).

Diese Schritte wiederholen Sie, bis Sie alle vorgesehenen Teilnehmer definiert haben.

Anschließend installieren Sie die mit der HiPath HG 1500 ausgelieferte vCAPi Software auf jedem PC, der vCAPi nutzen soll.

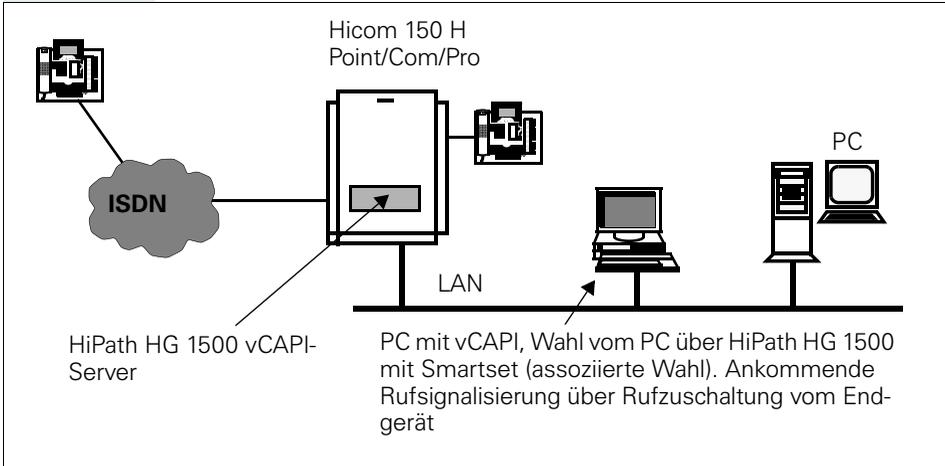
Während der Installation muss die IP-Adresse des LAN-Netzwerkinterfaces eingetragen werden.

Gebühreuzuordnung

Bei Telematik über vCAPi werden die Gebühren der verursachenden Rufnummer/MSN des PCs zugeordnet.

vCAPI und Smartset

Smartset ist ein optionaler CTI-Client, der Ihnen Leistungsmerkmale wie assoziierte Wahl aus einem Telefonbuch, Anruferidentifizierung anhand des Telefonbuchs, Rufzuschaltung und Anruferliste auf Ihrem PC zur Verfügung stellt. Außerdem können bei kommenden ISDN-Anrufen automatisch Dokumente geöffnet werden. Smartset tauscht über DDE- Funktionen Daten mit Ihren Windows-Applikationen aus.

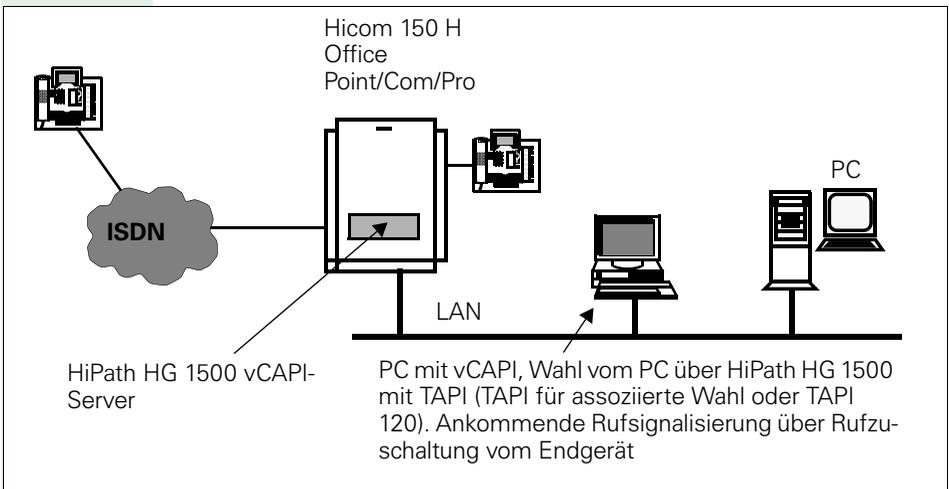


Einrichtung CTI/Smartset

Falls noch nicht geschehen, müssen Sie als erstes einen vCAPI-Teilnehmer einrichten (siehe → 94, Einrichtung vCAPI-Client).

- Hicom: Um die Funktionalität von Smartset nutzen zu können, muss die assoziierte Wahl in der Hicom freigegeben werden.
- Smartset: Tragen Sie die eigene Rufnummer, die Rufnummer des Teilnehmers für den die assoziierte Wahl ausgeführt werden soll und die Kennziffer für Amtsholung ein. (Weitere Hinweise zu Smartset entnehmen Sie bitte der Bedienungsanleitung.)
- Rufzuschaltung: Am Teilnehmertelefon ist das Leistungsmerkmal Rufzuschaltung für den vCAPI-Teilnehmer einzurichten. Erst dann werden kommende Anrufe auch im Smartset angezeigt.

vCAPI und TAPI



TAPI-Clients

Mit der auf vCAPI aufsetzenden TAPI und einer TAPI unterstützenden Applikation kann ebenfalls eine automatische Wahl erfolgen. Ein Beispiel hierzu wäre die Anwahl einer in den „Kontakten“ von MS Outlook gespeicherten Rufnummer.

Hierbei ist zu beachten, dass in MS Outlook Rufnummern im internationalen Format eingegeben werden müssen, z. B. +49(2302)999420.

TAPI für assoziierte Wahl

Um die Funktionalität von TAPI nutzen zu können, muss in der Hicom die assoziierte Wahl freigegeben sein.

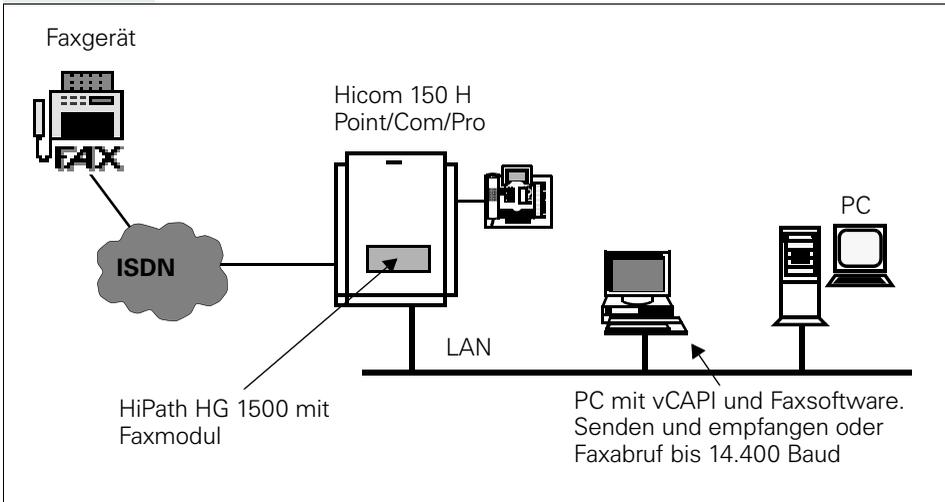
Am Teilnehmertelefon ist das Leistungsmerkmal Rufzuschaltung für den TAPI-Teilnehmer einzurichten.

TAPI 120

Mit der TAPI 120 können bis zu 3 Benutzer direkt über CSTA die Hicom Telephony-Dienste nutzen. Die TAPI 120 verfügt gegenüber der TAPI für assoziierte Wahl über mehr Leistungsmerkmale, so ist hier z. B. auch das „Auflegen“ eines TAPI-Teilnehmers möglich.

vCAPI und Fax

Über die vCAPI der HiPath HG 1500 können Sie Faxe versenden und empfangen. Hierfür benötigen Sie eine optionale Faxsoftware, die auf CAPI aufsetzt.



Faxdienste mit HiPath HG 1500

- Je PC eine eigene Faxdurchwahlnummer
- Fax Gruppe 3 senden und empfangen mit bis zu 14.400 Baud
- Faxabruf in Empfangsrichtung
- Faxweiterleitung im Frei- und Besetztfall auf analoges Fax möglich. (z. B. bei ausgeschaltetem PC)
- Keine B-Kanal Reservierung (für die Zeit in der kein Fax gesendet oder empfangen wird, kann der Kanal durch andere Applikation genutzt werden).
- Je nach Anlagentyp und Anzahl der Baugruppen sind bis zu 9 Faxe gleichzeitig möglich.

Einrichtung Fax

Falls noch nicht geschehen, müssen Sie als erstes einen vCAPi-Teilnehmer einrichten (siehe → 94, Einrichtung vCAPi-Client)

- Faxapplikation installieren und zugeteilte Rufnummer eintragen
- Faxapplikation starten

Die Rufnummer steht nun in der Anruferliste des Anmeldeteilnehmers.

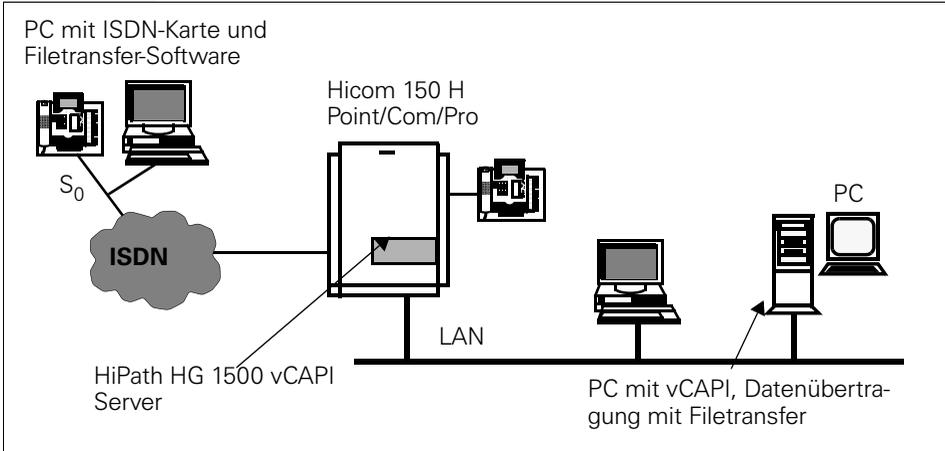
Weitere Hinweise zur Installation der Applikation entnehmen Sie bitte der Softwareinstallationsanweisung.



Wenn Sie auf einem Client-PC CTI und Fax gleichzeitig nutzen wollen, sollten Sie für beide Dienste je eine Rufnummer zuweisen, da es ansonsten zwischen beiden Diensten zu Konflikten bei der Rufannahme kommen kann.

vCAPI und Filetransfer

Mit Filetransfer haben Sie die Möglichkeit, Daten direkt mit Ihrem ISDN-Partner austauschen zu können. Dies kann entweder mit standardisiertem EuroFileTransfer beliebiger Hersteller erfolgen, oder Sie benötigen bei proprietärer Software auf beiden Seiten dieselben Softwareprodukte.



Einrichtung Filetransfer

Falls noch nicht geschehen, müssen Sie als erstes einen vCAPI-Teilnehmer einrichten (siehe → 94, Einrichtung vCAPI-Client)

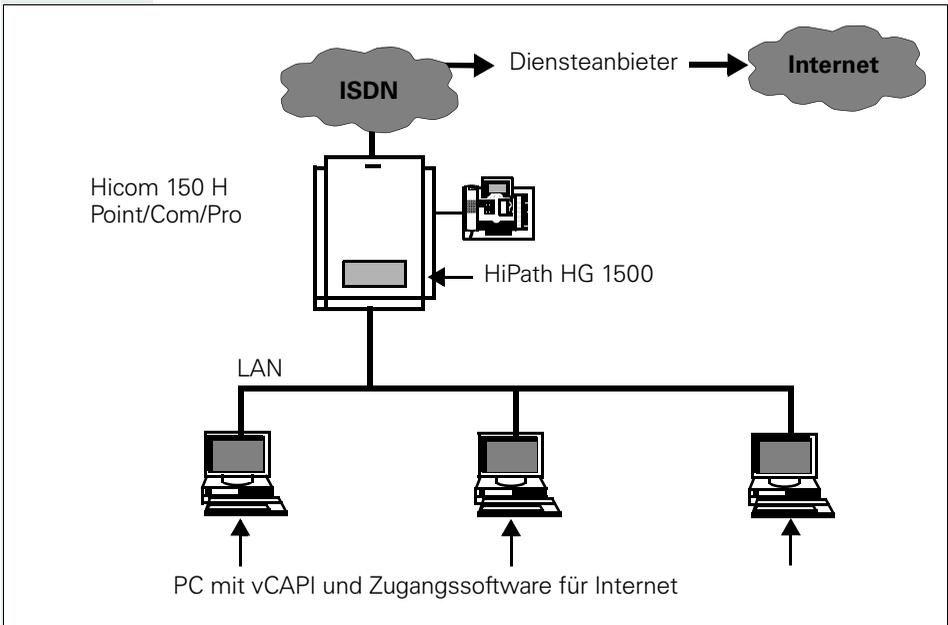
- Filetransferapplikation installieren und Rufnummer eintragen
- Filetransferapplikation starten

Die Rufnummer steht nun in der Anruferliste des Anmeldeteilnehmers.

Weitere Hinweise zur Installation der Applikation entnehmen Sie bitte der Installationsanweisung der von Ihnen eingesetzten Software.

vCAPI und Internet

Den Zugang zum Internet über vCAPI benötigen Sie nur, wenn die Zugangssoftware Ihres Diensteanbieters die CAPI-Schnittstelle benötigt.



Der Zugang zum Internet ist auch über Routing möglich (siehe → 108, Routing – Internet).

Einrichtung Internetzugang über vCAPI

Falls noch nicht geschehen, müssen Sie als erstes einen vCAPI Teilnehmer einrichten (siehe → 94, Einrichtung vCAPI-Client).

- Zugangssoftware für Internet installieren

Weitere Hinweise zur Installation und Konfiguration (IP-Adressen, Gateways, etc.) der Applikation entnehmen Sie bitte der Installationsanweisung der von Ihnen eingesetzten Software.

Routing

LAN-LAN und Teleworking

LAN-LAN-Kopplungen, d. h. WAN Verbindungen können mittels HiPath HG 1500 zu anderen HiPath HG 1500, Hicom LAN-Bridge 1.x und anderen Routern hergestellt werden. Über Routing ist auch der Zugang zu Internetprovidern möglich.

Das Leitungsmerkmal IP Accounting beschreibt die Möglichkeit, Kosten für den Internetzugang nach transferierten Datenmengen und verschiedenen Tarifmodellen, die in der Applikation hinterlegt sind, verursacherorientiert zuzuordnen siehe → 58.

HiPath HG 1500 bietet maximale Kanalbündelung bis zu 16 B-Kanälen (Hicom Office Point bietet amtsseitig maximal 8 B-Kanäle). Es werden die Transportprotokolle IP oder IPX unterstützt.

Mit der HiPath HG1500 mit zwei LAN-Interfaces ist auch Routing zwischen den beiden LAN-Interfaces möglich, siehe → 105.

Leistungsmerkmale

- PPP-Verbindungen (LAN-LAN Kopplung und Teleworking)
- PPP-Multilink Verbindungen (Kanalbündelung)

Firewallmechanismen

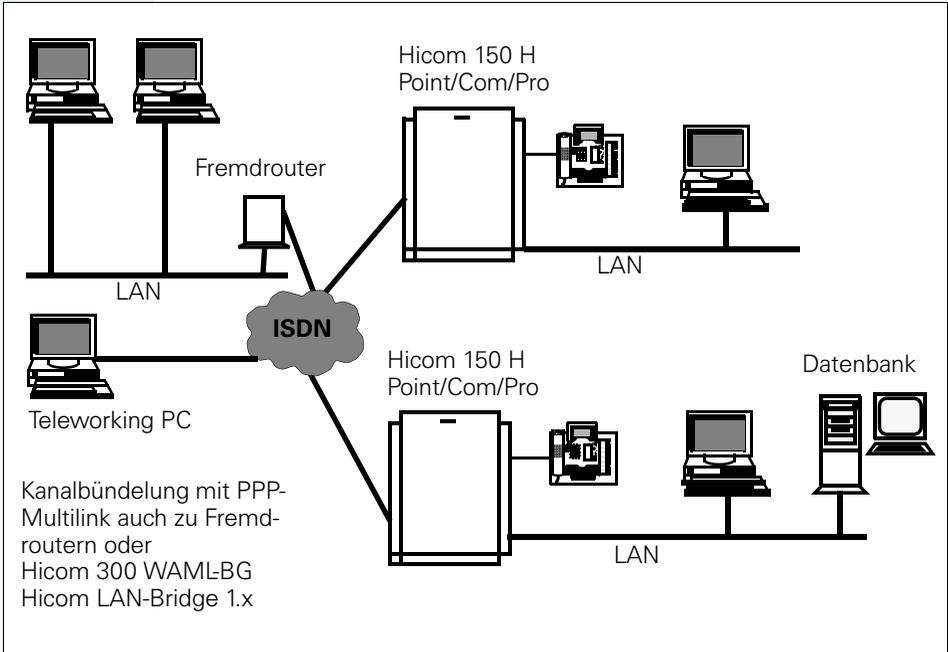
- Überprüfung von MAC-, IP- oder IPX-Adressen
- TCP, UDP und ICMP Portfirewall
- Zugangskontrolle anhand der ISDN-Rufnummern
- Automatischer Rückruf
- PAP (Password Authentication Protocol)
- CHAP (Challenge Handshake Authentication Protocol).

Ein Teleworking Teilnehmer benötigt eine ISDN Karte mit Remote Access Software (z. B. DFÜ-Netzwerk). Über die ISDN-Karte wird eine Netzwerkverbindung zur HiPath HG 1500 aufgebaut.

Über folgende Verbindungen kann ein Zugang zu den lokalen Netzen hergestellt werden:

- Analog V.34 (maximal 33.600 bit/s)
- ISDN DSS1
- GSM V110

Routing mit HiPath HG 1500



Einrichtung LAN-LAN Routing via ISDN

Damit Sie HiPath HG 1500 als ISDN-Router nutzen können, müssen Sie im Administrationsprogramm die folgenden Schritte ausführen:

- IP-Adresse des Remote-LAN feststellen
- IP-Adresse des gemeinsamen WAN (ISDN) festlegen
- bei allen PC's als Gateway die IP-Adresse der HiPath HG 1500 unter Menü „Netzwerkschnittstelle -> Netzinterfaces -> LAN“ eintragen



Netzwerkschnittstellen

Netzwerkkinterfaces

➔ ISDN 1 oder 2

Tragen Sie hier die vorher festgelegte IP-Adresse für das WAN ein.

Geben Sie ggfs. das zu konfigurierende Interface unter dem Menüpunkt „Netzwerkschnittstellen“ frei.



Routing

IP-Routing

Wählen Sie mit der linken Maustaste den Menüpunkt „IP-Routing“ aus und drücken Sie die Symbolschaltfläche „Neu.“ Tragen Sie nun in das Dialogfenster die IP-Adresse des zu erreichenden LANs ein und bestätigen Sie Ihre Eingabe. Um Schreibarbeit zu verringern, können Sie im Menü „Voreinstellungen“ die Werte für „Netzmaske“ und „Gateway“ eingeben.

Markieren Sie mit der Maus den neu erstellten Eintrag.

➔ Netzmaske:

Geben Sie die zum Zielnetzwerk gehörige Netzmaske ein.

➔ Gateway:

Tragen Sie unter Gateway die IP-Adresse des ISDN-Interface der Gegenseite ein.

ISDN-Partner

Wählen Sie mit der linken Maustaste den Menüpunkt „ISDN-Partner“ aus und drücken Sie die Symbolschaltfläche „Neu.“ Tragen Sie in das Dialogfenster den Namen des ISDN-Partners ein und bestätigen Sie Ihre Eingabe.

Markieren Sie mit der Maus den neu erstellten Eintrag.

➡ IP-Adresse:

Tragen Sie die IP-Adresse des ISDN-Netzwerkinterface der Gegenseite ein. Hier wird dieselbe Adresse eingegeben wie unter „Routing – IP-Routing – Gateway“ (IP-Adresse des ISDN-Interface der Gegenseite).

➡ B-Kanäle:

Geben Sie nun die Anzahl der B-Kanäle an, die für diese Verbindung maximal benutzt werden sollen.

Klicken Sie doppelt auf den entsprechenden ISDN-Partner.

Rufnummernliste

Erstellen Sie mit der Symbolschaltfläche „Neu“ einen neuen Eintrag und geben die Rufnummer der Gegenseite ein.

➡ Rufrichtung:

Legen Sie die zulässigen Rufrichtungen für diesen Partner fest.

Anschließend stimmen Sie die restlichen Protokolleinstellungen mit der Gegenseite ab und stellen diese an Ihrer HiPath HG 1500 ein.

Zum Abschluß setzen Sie als Test für die eingegebene Route ein „Ping“ zur Gegenseite ab.

 Wird das Ping nicht ordnungsgemäß beantwortet, kann dies auch daran liegen, dass die Gegenseite falsch konfiguriert ist!

Informationen zu weiteren Parametern erhalten Sie auf siehe → 52.

Einrichtung LAN-LAN Routing zwischen den LAN-Interfaces

Beide LAN-Interfaces können zwei unterschiedliche Netze verbinden. Die Konfiguration des LAN2-Interfaces wird ähnlich wie das erste LAN-Interface eingerichtet.

Für die beiden direkt angeschlossenen Netze müssen keine Routing-Einträge gemacht werden.

Darüber hinaus kann mit dem Parameter „NAT“ eine Address-Translation gegenüber den anderen Interfaces eingerichtet werden siehe → 112.

Besonderheiten bei Windows-Netzwerken

Routing und Namensauflösung

Bei Routing, z. B.: HiPath HG 1500 zu HiPath HG 1500 und Peer to Peer Verbindung (Windows für Workgroup Netzwerk bei IP Routing), muss eine LMHOSTS/HOSTS Datei auf den Client PCs angelegt werden. Bei Windows 95 im Windows Verzeichnis. Bei Windows NT/2000 im folgenden Verzeichnis WINNT\SYSTEM32\DRIVERS\ETC. Dort gibt es eine Datei LMHOSTS.SAM, diese Datei kann erweitert werden, darf aber keine Endung haben (LMHOSTS).

Beispieleintrag:

192.168.10.10 HG1500

192.168.10.20 PC1

hinter dem letzten Eintrag unbedingt Return drücken.

Nach Erstellen der LMHOSTS/HOSTS Datei sollte man zur Funktionsüberprüfung dem Partner einen Ping-Befehl mit dem Namen absetzen (z. B. Ping HG1500). Da bei Routern kein Browsing übertragen wird (Broadcastmeldungen), kann der andere Computer nur mit der rechten Maustaste auf dem Icon „Netzwerkumgebung“ und „Computer suchen“ gefunden werden. Wenn der Computer gefunden wurde, kann jetzt auf die Netzwerkressourcen zugegriffen werden. Über das Öffnen der Netzwerkumgebung ist der Zugriff auf den anderen PC nicht möglich.



Bei der Namensvergabe 8 Zeichen berücksichtigen, da einige Betriebssysteme mit mehr als 8 Zeichen Probleme haben könnten. Änderungen in LMHOSTS/HOSTS werden erst nach Neustart des Computers aktualisiert. Alternativ können Sie unter Windows 95 und 98 auch den Befehl NBTSTAT -R verwenden!

Gebührenzuordnung/Callback

Wird von HiPath HG 1500 eine ISDN Amtsverbindung aufgebaut, so werden der benutzten Rufnummer die auflaufenden Gebühren zugeordnet. Solange diese physikalische Verbindung besteht, können Daten in beiden Richtungen transferiert werden. Besteht eine Verbindung von HiPath HG 1500 A zu HiPath HG 1500 B über Amt, so können alle am LAN von HiPath HG 1500 A und B angeschlossenen Geräte die bestehende Verbindung nutzen. Die Gebühren werden hierbei der Rufnummer des Ports der HiPath HG 1500 A Baugruppe zugeordnet, die eine Verbindung aufgebaut hat.

Wie heute bei Routern üblich, ist keine gezielte Zuordnung der Gebühren zu den Geräten oder Applikationen am LAN möglich, sondern nur zu der Rufnummer des Routers.

Wird über „Short Hold“ die physikalische Verbindung abgebaut, so wird sie beim Eintreffen neuer Meldungen wiederaufgebaut. Wenn dies Daten von HiPath HG 1500 B nach A sind, d. h. HiPath HG 1500 B veranlasst den Verbindungsaufbau, so wechselt auch die Gebührenzuordnung zu B.

Bei aktivierter „call back-Funktion“ werden die Gebühren der gerufenen HiPath HG 1500 zugeordnet, da diese den kommenden Ruf, abweist und selbst aktiv wieder aufbaut (Verbindungsloser Callback). Das heißt, es wird kein B-Kanal aufgebaut. Die Identifizierung erfolgt über die im Setup eingetragene Rufnummer bzw. bei analogen Teilnehmern über die Durchwahlnummer, die unter „ISDN-Partner“ eingetragen ist.

Informationen zu weiteren Parametern erhalten Sie auf siehe → 52.



Wählleitungen können in bestimmten Fällen (z. B. Short-Hold deaktiviert) nur noch von Hand ausgelöst werden.

Internetzugang

Ein oder mehrere Client PC können direkt mit einem Internet-Browser auf das Internet zugreifen. Die Anbindung aus dem LAN erfolgt über ISDN oder DSL. Normalerweise ist ein Zugriff von allen PCs möglich. Manche Provider sperren allerdings diese Möglichkeit, sie muss separat beantragt werden.

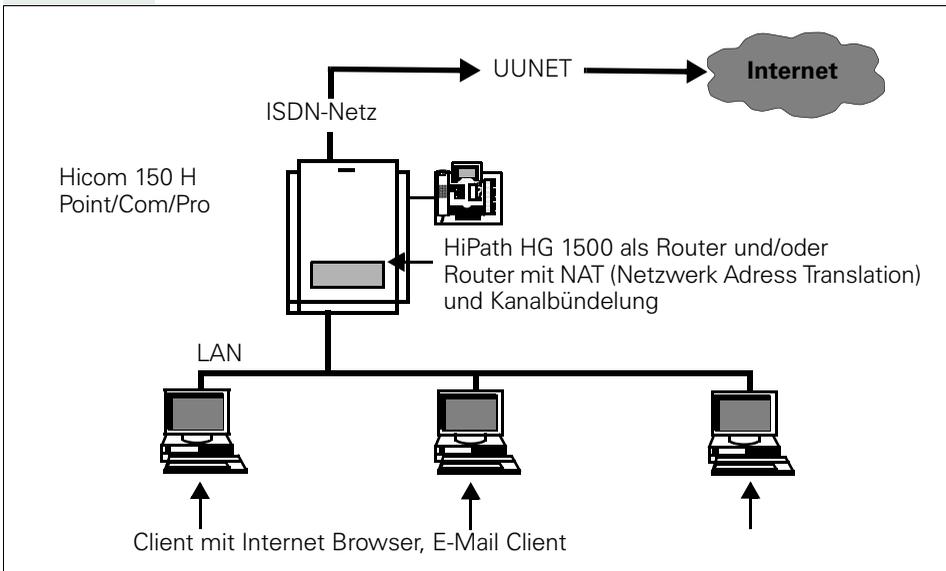
Der Zugriff erfolgt mit dem Transportprotokoll IP über die HiPath HG 1500 zum Internet Provider.

Alle Clients benutzen den gleichen Provider.

Leistungsmerkmale

- Statische oder dynamische IP-Adressen
- Routingfunktion mit NAT/SUA (Netzwerk Address Translation/Single User Access)
- PPP-Multilink (Kanalbündelung)
- PPPoE (bei DSL)
- PPTP (bei DSL)
- PAP (Password Authentication Protocol)
- CHAP (Challenge Handshake Authentication Protocol)

HiPath HG 1500 und Zugang zum Internet über einen Netzanbieter



Internetzugang über T-DSL (T-ISDN DSL)

Seit Ende 1999 bietet die Deutsche Telekom AG mit T-ISDN DSL (auch T-DSL genannt) einen neuen High-Speed-Zugang fürs Internet verbunden mit dem Telefonkomfort von T-ISDN an. (Andere Provider, z. B. in den Niederlanden (siehe Beispiel auf →Seite 133), verwenden DSL mit dem PPTP-Protokoll siehe →Seite 45).

Mit 768.000 Bit/s empfangen TDSL-Nutzer Daten aus dem Internet zwölfmal so schnell wie mit einem normalen ISDN-Anschluss. Beim Senden von Dateien werden 128.000 Bit/s erreicht, also soviel wie beim normalen ISDN-Anschluss durch Bündelung von zwei Kanälen (Leitungen).

T-ISDN DSL ist zunächst ein normaler TNet- oder ISDN-Anschluss als Mehrgeräte- oder Anlagenanschluss.

Über die Funktionen des normalen TNet- bzw. ISDN-Anschlusses hinaus wird dem T-DSL-Anschluss eine Datenschnittstelle für Internet-Verbindungen mit einer Geschwindigkeit von 768 kBit/s Downstream und 128 KBit/s Upstream zur Verfügung gestellt. Die Nutzung dieser Datenschnittstelle belegt keinen Kanal des TNet- oder ISDN-Anschlusses.

Funktionsweise

Am Hauptanschluss wird nicht wie im T-ISDN direkt der NTBA, sondern erst ein sogenannter „ISDN-Splitter“ (BBAE) installiert. Dieses Gerät kann man sich als Verteiler zwischen ISDN-Anschluß und Datenübertragung in DSL-Geschwindigkeit vorstellen.

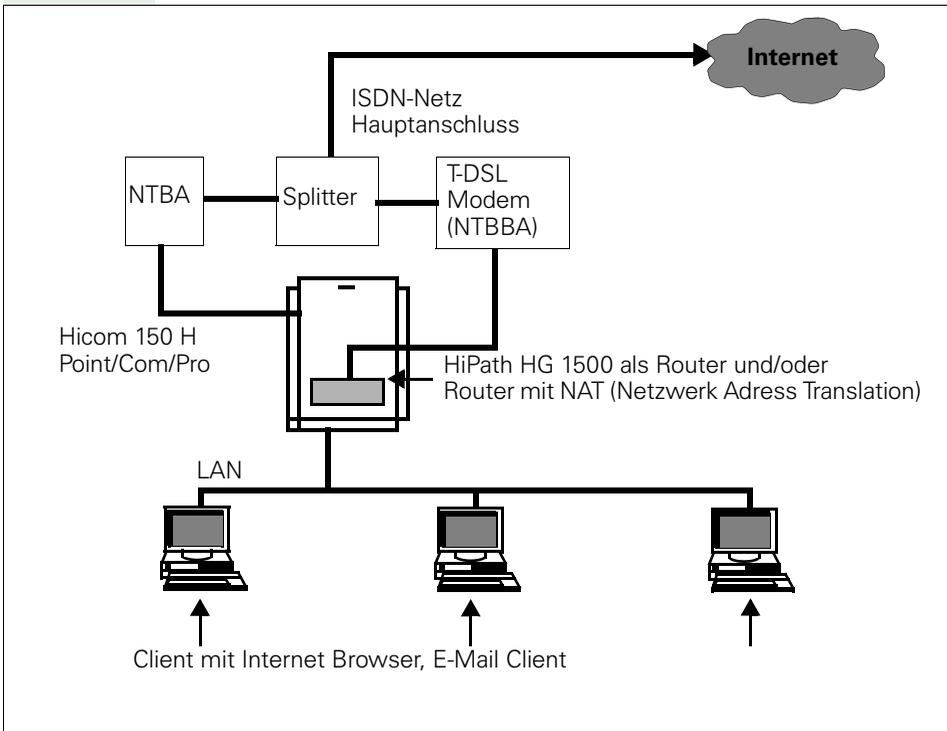
Am Splitter steht eine TAE-Anschlussbuchse zur Verfügung an der der NTBA angeschlossen wird. Die Verbindung zur Hicom 150H erfolgt wie gewohnt.

Zusätzlich verfügt der Splitter über einen Anschluss für das „T-DSL Modem“ (NTBBA), das die Schnittstelle für Datenübertragungen in T-DSL-Geschwindigkeit zur Verfügung stellt.

Der „ISDN-Splitter“, der „NTBA“ und das „T-DSL Modem“ werden von der Deutschen Telekom AG bei T-ISDN DSL Anschlüssen unentgeltlich zur Verfügung gestellt.

Der Anschluss des T-DSL-Modem an der HLB-Baugruppe erfolgt über ein Interface 10BT. Für die Anbindung wird das Protokoll PPPoE (Point to Point Protocol over Ethernet) verwendet.

Einrichtungsbeispiel für T-DSL siehe → 131.



Einrichtung Internetzugang über PPP und NAT/SUA

Bitte beachten Sie, dass keine öffentlichen IP-Adressen verwendet werden. Vergeben Sie eine IP-Adresse aus dem Private Network Bereich.



Netzwerkschnittstellen

Bei der Nutzung des ISDN3 Interfaces wird die Verwendung der IP-Adresse 0.0.0.0 mit der Netzmaske 255.255.255.248 empfohlen.



Routing

IP-Routing

➔ IP-Adresse:

Als zu erreichendes Netzwerk wird als IP-Adresse 0.0.0.0 (IP-Adresse des ISDN3) eingetragen.

➔ Netzmaske:

Tragen Sie nun die zugehörige Netzwerkmaske ein.

➔ Gateway:

Als Gateway tragen Sie eine IP-Adresse aus dem Netz des ISDN3 ein. (z. B. 0.0.0.1)

ISDN-Partner

Wählen Sie mit der linken Maustaste den Menüpunkt „ISDN-Partner“ aus und drücken Sie die Symbolschaltfläche „Neu.“ Tragen Sie nun in das Dialogfenster den Namen des Providers ein und bestätigen Sie Ihre Eingabe.

Markieren Sie mit der Maus den neu erstellten Eintrag.

➔ IP-Adresse:

IP-Adresse eintragen. Dies ist dieselbe Adresse, die unter „Routing – IP-Routing“ eingetragen ist, also z. B. „0.0.0.1“

➔ B-Kanäle:

Geben Sie nun die Anzahl der B-Kanäle an, die für diese Verbindung maximal benutzt werden sollen. (Bei mehr als einem B-Kanal kann es seitens der Diensteanbieter zu Problemen bei der Passwortaushandlung kommen).

➔ PAP oder CHAP:

Für die Authentifizierung beim Provider das festgelegte Passwort unter PAP oder CHAP eintragen.

Weitere Parameter, die für einen erfolgreichen Verbindungsaufbau notwendig sind, erfragen Sie bitte bei Ihrem Provider. Erläuterungen zu diesen Parametern finden Sie im Kapitel „Administration mit Assistant I siehe →Seite 25.



Nach der Einrichtung dieses Internetzugangs sollte geprüft werden, dass die Verbindung auch wieder in den Short-Hold-Modus fällt, wenn kein Datenverkehr mehr gewollt ist. Bleibt die Verbindung offen oder wird sie in regelmäßigen Abständen wieder aufgebaut, so hilft der Kundentrace weiter, siehe → 181 ff.

Funktion von NAT/SUA (Network Address Translation)

Es werden nicht öffentliche IP-Adressen maskiert.

Nicht öffentliche IP-Adressbereiche	Subnet-Mask	(Class)
10.0.0.0	255.0.0.0	A
172.16.0.0 - 172.31.255.255	255.240.0.0	B
192.168.0.0	255.255.255.0	C

Da diese Adressen nicht im Internet weitergeleitet („geroutet“) werden, müssen diese Hosts über die WAN (ISDN) – Adresse der HiPath HG 1500, die vorher über PPP mit dem ISP ausgehandelt wurde, Daten austauschen. Dadurch werden Hosts gegenüber dem Internet unsichtbar, da der Datenaustausch komplett über die NAT/SUA erfolgt.

Das interne Firmen-LAN tritt gegenüber dem Internet mit nur einer einzigen IP-Adresse auf, nämlich der vom Provider für den Zeitraum der Einwahl zugewiesenen. Alle Zugriffe aus dem LAN heraus ins Internet werden über diese Adresse und unterschiedliche Portnummern abgewickelt. Damit werden gleichzeitig alle IP-Verbindungsversuche (auch Angriffe) aus dem Internet auf das Firmen-LAN unterbunden, es sei denn, diese wurden ausdrücklich konfiguriert unter dem Punkt „Routing->Internet“ (siehe → 57).

Konfiguration der PCs für Internetzugang

Bei Verwendung des Internetzugangs direkt über die Baugruppe müssen auf den PCs zwei Konfigurationen getätigt werden:

1. Die Baugruppe muß aus Sicht der PCs zum Default-Gateway werden: In den Netzwerkeinstellungen->TCP/IP der PCs wird unter „Standard-Gateway“ die IP-Adresse der Baugruppe konfiguriert.
2. Für die Namensauflösung muß auf den PCs ein DNS-Server konfiguriert werden:
Netzwerkeinstellungen->TCP/IP DNS-Server eintragen, z. B. einen DNS-Server von T-Online: 194.25.2.129.
Es ist empfehlenswert, den Proxyserver des Internet-Providers im Browser zu konfigurieren. Dadurch verbessert sich die Erreichbarkeit verschiedener Server im Internet, z.B. bei T-Online:
 - - Proxy-Server: www-proxy.btx.dtag.de
 - - Portnummer: 80"



Beim Verbindungsaufbau zum Internetprovider über DSL können durch Wartezeiten bei der Aushandlung Fehlermeldungen (Time-out) am Browser auftreten. In diesem Fall die Anfrage wiederholen.

IP-Adressmapping

Durch die Verbreitung des Internet hat sich vielfach durchgesetzt, nur im Internet die knappen, aber weltweit eindeutigen IP-Adressen zu verwenden und für die IP-Netze in den Firmen auf die sogenannten privaten (nicht öffentlichen, siehe → 112) IP-Adressen zurückzugreifen.

Dadurch kann es vorkommen, daß in vielen Firmen Adressen aus dem gleichen IP-Netz verwendet werden.

Um diese trotzdem jeweils durch einen eindeutigen Routingeintrag erreichen zu können, wurde das Leistungsmerkmal „IP-Adressmapping“ realisiert.

Die HiPath HG 1500 tauscht beim Routing mit bestimmten, durch Konfiguration bestimmten Partnern die privaten, im eigenen LAN verwendeten IP-Adressen gegen andere IP-Adressen aus und ist im Gegenzug von außen über diese erreichbar.

Ein Szenario soll dies verdeutlichen:

Ein Dienstleister möchte die Server bei zwei verschiedenen Kunden (A+B) betreuen. Beide Kunden haben sich die IP-Netzadresse 192.168.1.0 gewählt und verfügen jeweils über eine HiPath HG 1500. Damit der Dienstleister beide Kundennetze erreichen kann, wird bei mindestens einem, in diesem Beispiel bei beiden Kunden das IP-Adressmapping aktiviert.

Um das Beispiel abzurunden, soll beim Kunden B vom Dienstleister nur auf zwei IP-Adressen im LAN zugegriffen werden können.

Der Dienstleister (eigenes Netz: 192.168.100.0) richtet folgendes Routing ein:

Kunde A: IP-Netzadresse: 10.1.1.0, Netzmaske 255.255.255.0

Kunde B: IP-Netzadresse: 10.1.2.0, Netzmaske 255.255.255.0

Beim Kunden A wird eingerichtet:

Grundeinstellungen->Mapping Netmask: 255.255.255.0

ISDN-Partner „Dienstleister“->IP-Adresse 192.168.100.254, IP-Adressmapping: ja

Routing->IP-Routing->IP-Adresse: 192.168.100.0, Netzmaske 255.255.255.0, Gateway: 192.168.100.254

IP-Mapping->externe IP-Adresse: 10.1.1.0, interne IP-Adresse: 192.168.1.0

Der Dienstleister kann jetzt z. B. über die IP-Adresse 10.1.1.1 auf die IP-Adresse 192.168.1.1 beim Kunden A zugreifen.

Beim Kunden B wird eingerichtet:

Grundeinstellungen->Mapping Netmask: 255.255.255.0

ISDN-Partner „Dienstleister“->IP-Adresse 192.168.100.254, IP-Adressmapping: ja

Routing->IP-Routing->IP-Adresse: 192.168.100.0, Netzmaske 255.255.255.0, Gateway: 192.168.100.254

IP-Mapping->externe IP-Adresse: 10.1.2.1, interne IP-Adresse: 192.168.1.200

IP-Mapping->externe IP-Adresse: 10.1.2.2, interne IP-Adresse: 192.168.1.201

Der Dienstleister kann jetzt genau auf zwei Adressen beim Kunden zugreifen:

über die IP-Adresse 10.1.2.1 auf die IP-Adresse 192.168.1.200 beim Kunden B zugreifen,

über die IP-Adresse 10.1.2.2 auf die IP-Adresse 192.168.1.201 beim Kunden B zugreifen.

Alle anderen Adressen im LAN des Kunden B sind für den Dienstleister nicht zugänglich.



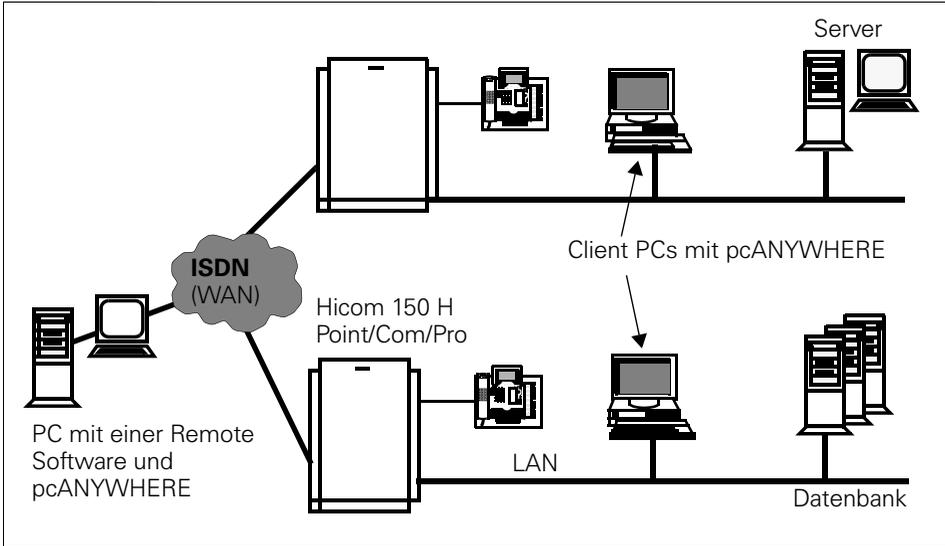
Sowohl bei NAT/SUA über ISDN3 als auch beim IP-Adressmapping gilt folgendes:

Der Austausch der IP-Adressen erfolgt nur im IP-Header. Dieser Mechanismus wirkt nicht, wenn die IP-Adressen auf höheren Protokollschichten, z. B. zwischen den Applikationen ausgetauscht werden. Dies ist zu berücksichtigen, wenn es zu Fehlfunktionen kommt, die es ohne diesen Mechanismus (z. B. beim Direktzugang über eine ISDN-Karte) nicht gibt.

Remote Control

Lösungsansatz pcANYWHERE

Teleworking mit HiPath HG 1500 und pcANYWHERE



Mit der Software "pcANYWHERE" von Symantec kann ein PC im Netz von einem externen PC fernbedient werden.

Voraussetzung:

- Eines der Betriebssysteme Windows 95, Windows 98, Windows NT 4.0 oder Windows 2000
- Verbindungsaufbau über das Transportprotokoll IP oder IPX
- PC ist betriebsbereit (ggf. Bildschirm dunkel)

Schutzmechanismen („Security“)

Allgemeines

Eine Zugangsberechtigung für die Routingfunktionalität ist notwendig, um den Zugang über die HiPath HG 1500 vom internen LAN in Richtung ISDN und umgekehrt zu steuern.

Für Telematik-Funktionen ist ein „Firewall“ nicht sinnvoll. Für diese Funktionen und ihre Rufnummern können Regeln (z. B. Amtsberechtigung) in der Hicom hinterlegt werden.

Die nachfolgenden Betrachtungen sind immer aus der Sicht des Routers (HiPath HG 1500) zu sehen.

Rufnummern-Überprüfung (nur kommand)

Überprüfung der Rufnummer des rufenden Teilnehmers (Teilnehmer-Authentisierung, konfigurierbar) und der IP- bzw. IPX-Adresse, um unzulässige Verbindungen von extern über ISDN zu verhindern.

Überprüfung der IP- bzw. IPX-Adresse (konfigurierbar) von internen LAN-Teilnehmern.

IP-Firewall (Erlaubnis-Firewall)

Ein IP-Firewall besteht aus den folgenden zwei Stufen:

- IP Routing Berechtigung
Hiermit werden Pakete bezüglich Quell-IP- und Ziel-IP-Adresse und den verwendeten Ports geprüft und gegebenenfalls verworfen. Die IP-Adressen können Netzadressen oder einzelne Hosts sein.
- MAC-Überprüfung
Bei der MAC-Überprüfung wird geprüft, ob IP-Pakete, die von der LAN-Schnittstelle kommen in der Kombination IP-Adresse / MAC-Adresse gültig sind.

IPX-Firewall

IPX-Pakete gelten nur als gültig wenn die angegebene Kombination aus Netzwerknummer und Node-Adresse mit der des Absenders übereinstimmt.

Firewall

Eine Firewall dient als Schutz vor unerlaubten Zugriffen. Hierbei soll z. B. das interne LAN (LAN1) vor Zugriffen von außen (z. B. Zugriffe aus dem Internet via DSL) geschützt werden.

Ziel einer Firewall-Konfiguration ist es, einzelnen, ausgesuchten Rechnern einen Zugriff auf ein unsicheres Netz (z. B. Internet) zu ermöglichen. Dabei soll der umgekehrte Zugriff (vom Internet auf diese Rechner) unterbunden werden. Die Baugruppe verfügt über zwei unterschiedliche Schutzmechanismen um diese Sicherheit zu realisieren.

Bei der vorliegenden Firewall handelt es sich um eine sogenannte Erlaubnis-Firewall. D. h. sobald die Firewall eingeschaltet ist, haben nur konfigurierte Komponenten Zugriff auf Dienste der Baugruppe. Allen nicht eingetragenen LAN-Komponenten wird automatisch jeder Baugruppen-Dienst verweigert.



WARNUNG: Das Ein-/Ausschalten von Firewall-Parametern kann die Funktionalität der Baugruppe extrem einschränken (z. B. ist die Administration über LAN ggf. nicht mehr möglich) oder aber der Zugriff auf sensible Daten wird ermöglicht.

MAC – Firewall einrichten

Parameter	Wert
→ IP-Adresse:	10.144.233.10
→ MAC-Adresse:	080006123456

Eine MAC-Firewall hat die Aufgabe Zugriffe auf Dienste der Baugruppe nur für bestimmte MAC/IP-Adresskombinationen zuzulassen. Hierbei besteht der Schutz in der „Nicht-Konfigurierbarkeit“ einer MAC-Adresse. Eine Einschränkung der nutzbaren Internet-Dienste wird hierdurch noch **nicht** erreicht

Um die MAC-Überprüfung einrichten zu können, benötigen Sie eine Liste der MAC und IP-Adresskombinationen ihrer eingesetzten LAN-Karten, die einen Zugriff auf Dienste der Baugruppe erhalten sollen. Die MAC-Adressen finden Sie in der Dokumentation ihres Ethernet-Karten-Herstellers.

Zur Konfiguration gehen Sie bitte folgendermaßen vor:

Klappen Sie das Firewall-Menü im Menübaum (Klick auf das Pluszeichen vor Sicherheit) auf und bestätigen Sie den Warnhinweis mit OK. Anschließend klicken Sie auf den Menüeintrag MAC-Überprüfung und betätigen die „Einf“-Taste. Daraufhin werden Sie gebeten eine IP-Adresse anzugeben, die in die Überprüfung mit aufgenommen werden soll. Nach Bestätigung mit OK müssen Sie die zugehörige MAC-Adresse eingeben und ebenfalls bestätigen.

Wiederholen Sie diesen Vorgang für jede einzelne MAC/IP-Adresskombination.

Zur Korrektur von MAC/IP-Adresskombinationen können Sie den zu korrigierenden Eintrag auswählen indem Sie die Liste der konfigurierten Kombinationen (Klick auf das Pluszeichen vor MAC-Überprüfung) aufklappen und anschließend die gewünschte IP-Adresse auswählen. Im rechten Fenster können Sie nun ein Editierfenster mit Doppelklick auf den gewünschten Eintrag öffnen und anschließend die Änderungen vornehmen.

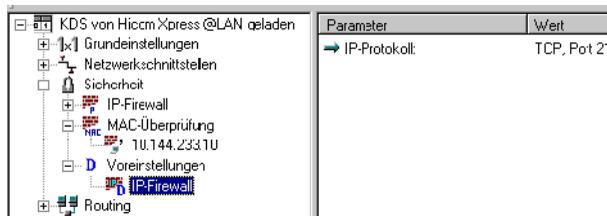
Soll ein Eintrag gelöscht werden (d. h. diesem PC sollen die entsprechenden Rechte entzogen werden) wird einfach die IP-Adresse im aufgeklappten Menübaum selektiert und mit „Entf“ entfernt.

IP-Firewall einrichten

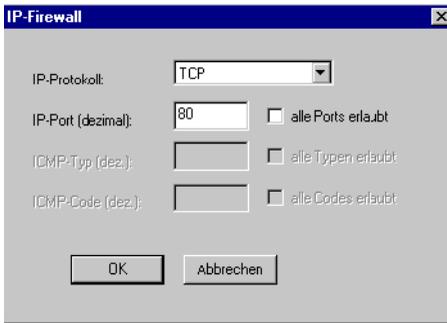
Eine IP-Firewall ist in der Lage, einzelnen oder Gruppen von IP-Adressen (zur Vereinfachung wird im folgenden immer nur von einer IP-Adresse ausgegangen, aber es ist auch möglich hier ganze Netze freizuschalten), Zugriffe auf bestimmte Ziele zu gewähren. Auch hierbei handelt es sich wieder um eine Erlaubnis-Liste, d. h. nur IP-Adressen die hier aufgeführt sind erhalten Zugriff auf den oder die festgelegten Dienste. Die IP-Firewall kann IP-Protokolle und die zugehörigen Dienste (Portnummern) überprüfen.

Um eine genaue Auswahl der gewünschten Funktion festlegen zu können, müssen Sie neben der Ziel-IP-Adresse ggf. auch das zuzulassende Protokoll und die Portnummer kennen.

Voreinstellungen

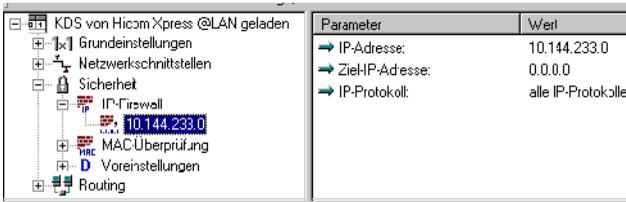


„Voreinstellungen“ zu nutzen ist immer dann sinnvoll wenn viele IP-Adressen mit den gleichen Einschränkungen konfiguriert werden sollen. Hierzu klappen Sie unter dem Punkt Sicherheit die Voreinstellungen auf und wählen IP-Firewall aus. Wählen Sie nun im Editier-Fenster „IP-Protokoll“ aus und nehmen die gewünschten Einstellungen vor:



Um z. B. nur das Surfen im Internet (HTTP-Protokoll) zuzulassen, tragen Sie hier das Protokoll TCP ein und geben den „IP-Port“ 80 vor. Sie können aber auch mit den vorbereiteten Voreinstellungen arbeiten, dann werden alle Protokolle ohne Portfilterfunktionen zugelassen. Diese konfigurierten Voreinstellungen werden nun für die einzugebenden IP-Adressen verwendet.

IP-Adressen einrichten



Unter dem Menübaum-Punkt „Sicherheit, IP-Firewall“ finden nun die gewünschten Freischaltungen statt. Analog zu den vorher beschriebenen Punkten, wählen Sie bitte den Punkt IP-Firewall aus und drücken die „Eingf“-Taste. Geben Sie die IP-Adresse ein, die bestimmte Zugriffsrechte erhalten soll. Nachdem Sie die Eingabe mit OK bestätigt haben, können Sie die IP-Adresse auswählen (siehe Abb.), um weitere Einschränkungen vorzunehmen oder um die IP-Adresse zu korrigieren. Wollen Sie die Rechte dieser IP-Adresse komplett entziehen, so selektieren Sie die Einträge und löschen Sie sie mit der „Entf“-Taste.

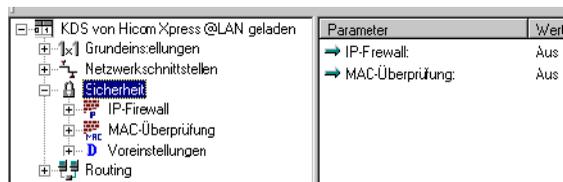
In der Voreinstellung hat die eingetragene IP-Adresse volle Berechtigung und kann somit alle IP-Adressen erreichen und alle Dienste nutzen. Um weitere Einschränkungen vorzunehmen müssen Sie die folgende Schritte ausführen:

Für die aktuellen Einstellungen und Einschränkungen für eine IP-Adresse wählen Sie die IP-Adresse (unter Sicherheit, IP-Firewall) im Menübaum aus. Im Editier-Fenster wird Ihnen neben der gewählten IP-Adresse, die „Ziel-IP-Adresse“ zu der diese IP-Adresse Kontakt aufnehmen darf und das zugelassene Protokoll angezeigt. Der Eintrag 0.0.0.0 unter Ziel-IP-Adresse steht dabei für alle Ziele. Soll die ausgewählte IP-Adresse nur mit einem bestimmten Netz und Host kommunizieren dürfen, so doppelklicken Sie bitte auf „Ziel-IP-Adresse“. In der folgenden Eingabemaske können Sie nun das gewünschte Ziel-Netz oder den entsprechenden Host eintragen.

Sollen Einschränkungen am Protokoll und/oder Port vorgenommen werden so doppelklicken Sie bitte auf den Eintrag „IP-Protokoll.“ In dem folgenden Dialog können Sie das gewünschte Protokoll („alle IP-Protokolle“, „TCP“, „UDP“ oder „ICMP“) auswählen. In Abhängigkeit vom ausgewählten Protokoll können Sie nun ggf. auch eine Einschränkung bezüglich des „IP-Port“ in Form einer Dezimalzahl eingeben oder „alle Ports erlaubt“ auswählen. Auch für das ICMP-Protokoll können Sie Einschränkungen in Form von „ICMP-Type“ und „ICMP-Code“ vornehmen.

Bitte beachten Sie, dass für einige Internet-Protokolle mehrere Portnummern freigegeben werden müssen um einen entsprechenden Internet-Dienst nutzen zu können (z. B. FTP Port 20 und 21).

Firewall aktivieren



ACHTUNG: In der Voreinstellung ist die komplette Firewall deaktiviert. Deshalb muss die gewünschte Firewall-Funktionalität explizit eingeschaltet werden. Alle zuvor vorgenommen Einstellungen werden erst durch diese Aktivierung wirksam.

Zur Aktivierung ist zunächst der Punkt Sicherheit im Menübaum auszuwählen und anschließend die gewünschte Sicherheitsfunktion (IP-Firewall oder MAC-Überprüfung) auszuwählen. Durch einen Doppelklick auf die Sicherheitsfunktion kann zwischen „Ein“ und „Aus“ umgeschaltet werden.

Nachdem alle Einstellungen vorgenommen wurden wird der KDS zur Baugruppe übertragen.

Gatekeeper

Ein Gatekeeper übernimmt in einem H.323-Netzwerk folgende Funktionen:

- Registriert H.323-Endgeräte,
- Verwaltet Rechte und Dienste,
- Setzt Rufnummern in logische Namen oder IP-Adressen um, bzw. umgekehrt,
- Verwaltet die Bandbreite netzseitig,
- Registriert Gateways,
- Registriert Multikonferenz-Einheiten,
- Kann mit benachbarten Gatekeepern (Zonen) vernetzt werden.

IP-Telefonie kann in H.323-Netzwerken auch ohne Gatekeeper durchgeführt werden, wenn keine Gateways oder Multikonferenz-Einheiten betrieben werden. In diesem Fall ist jedoch der Verbindungsaufbau ausschließlich über die IP-Adresse möglich. Nicht möglich sind Berechtigungen und Bandbreitenkontrolle.

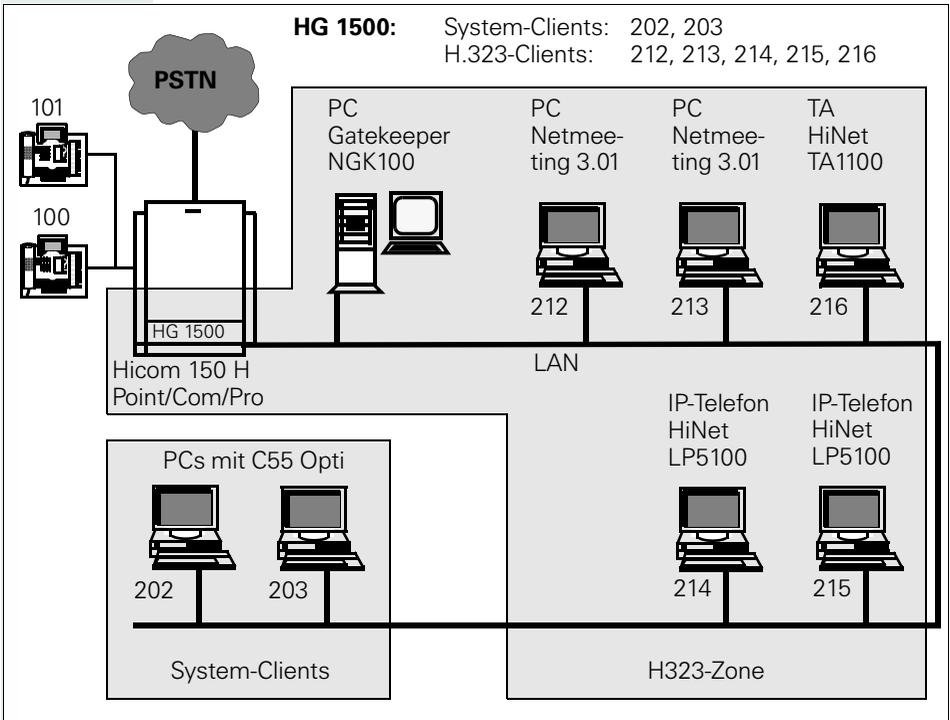
Generell gilt: Ohne Gatekeeper sind Leistungsmerkmale nicht oder nur stark eingeschränkt nutzbar.

Folgende Teilnehmer sind zu unterscheiden:

- Gruppe 1: direkt an der Hicom angeschaltete Teilnehmer (Optisets, NoFe, CMI, ...) sowie die an HiPath HG 1500 registrierten Teilnehmer (System-Clients bzw. optiClient 130, optiPoint Ipadapter und VCAPI-Clients) und alle Leitungszugänge
- Gruppe 2: am Gatekeeper registrierte Teilnehmer (H.323 Clients wie z. B. Netmeeting 3.01, HiNet LP 5100 bzw. optiPoint 300 advance, HiNet TA1100 bzw. HiPath AP1100)

Um einen Port (Teilnehmer/Leitung) der Gruppe 1 zu erreichen, müssen alle Teilnehmer der Gruppe 2 eine Kennzahl benutzen. Diese Kennzahl wird in Richtung zur Hicom von HiPath HG 1500 entfernt und in der Gegenrichtung ergänzt, d. h. Teilnehmer der Gruppe 1 wählen die Kennzahl nicht. Die Kennzahl muss im RADvision-Gatekeeper NGK100 als Service eingerichtet werden (siehe Servicehandbuch) und in der HiPath HG 1500 mit dem Assistant I als Gateway-Präfix (siehe → 70).

Gatekeeper mit einer HiPath HG 1500



An einer HiPath HG 1500 können verschiedene Typen von H.323-Applikationen betrieben werden.

Die C55-Opti-Teilnehmer werden nicht am Gatekeeper angemeldet und sind über den Assistant I als "System-Clients" eingerichtet. Da die HiPath HG 1500 für Gatekeeper-Betrieb eingerichtet ist, findet trotzdem bei jeder C55-Opti-Verbindung Meldungsverkehr zwischen der HiPath HG 1500 und dem Gatekeeper statt, am Gatekeeper ersichtlich in den Zählern und Statistiken zur Bandbreitennutzung und zum Call Logging. Die C55-Opti-Teilnehmer erreichen die anderen Teilnehmer durch Wahl der internen Rufnummer ohne Benutzung eines Präfixes.

Ruft z. B. Tln. 202 den Tln. 101 an, wird ein DSP-Kanal belegt.

Ruft Tln. 202 den Tln. 212 an, werden zwei DSP-Kanäle belegt.

Die H.323-Clients werden für Gatekeeper-Betrieb konfiguriert. Zusammen mit dem Gatekeeper und der HiPath HG 1500 als Gateway bilden sie eine H.323-Zone. In der HiPath HG 1500 müssen diese Teilnehmer als „H323-Clients“ eingerichtet werden. Die zur Rufnummer zugehörige IP-Adresse muss als „255.255.255.255“ eingerichtet sein, da der Gatekeeper die Zuordnung von Rufnummer und IP-Adresse vornimmt. Durch die Registrierung beim Gatekeeper sind die Teilnehmer mobil (Benutzung unterschiedlicher PC's als Arbeitsplatz, Teleworking). Der Gatekeeper darf in den Betriebsarten „Direct Routed“ und „Gatekeeper Routed“ betrieben werden.

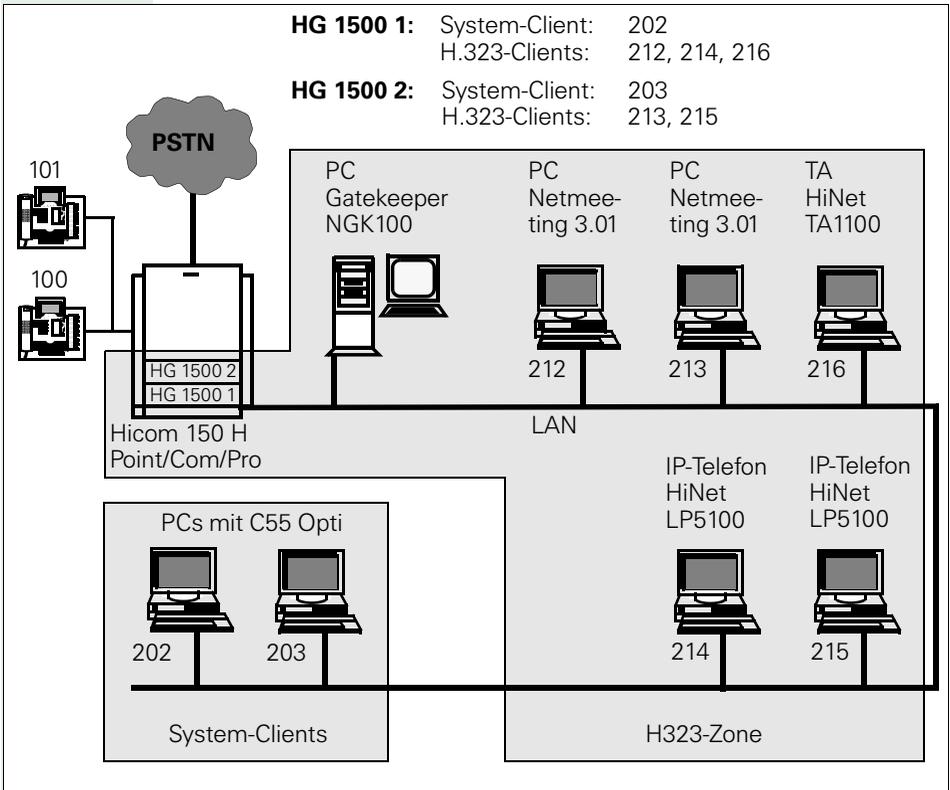
Die H.323-Clients können das HiPath HG 1500-Gateway nur über einen „Service“ ansprechen, der im Gatekeeper eingerichtet werden muss und den Teilnehmern zugeordnet wird. Die Service-Kennzahl muss mit dem Gateway-Präfix übereinstimmen, das über den Assistant I eingerichtet wird und die HiPath HG 1500 im Hochlauf beim Gatekeeper anmeldet.

In dem Beispiel sind Gateway-Präfix in der HiPath HG 1500 und Service-Kennzahl im Gatekeeper als „0“ eingerichtet. Mehrstellige Kennzahlen sind möglich, die Kennzahl darf sich aber nur aus Ziffern zusammensetzen. Die HiPath HG 1500 kann nur über einen Präfix erreicht werden. Die Rufnummern, die an die Clients übermittelt werden, sind um den Präfix ergänzt, so dass die zu wählende Rufnummer angezeigt wird und die Wahl aus Anruferlisten möglich ist.

TIn. 212 kann TIn. 214 über zwei Wege erreichen. Wählt er „214“, findet das Gespräch direkt auf dem LAN statt, wählt er „0214“, findet das Gespräch über die H150E unter Benutzung von zwei DSP-Kanälen in der HiPath HG 1500 statt. Die Optiset-Teilnehmer und C55-Opti-Teilnehmer werden mit „0101“ bzw. „0203“ erreicht.

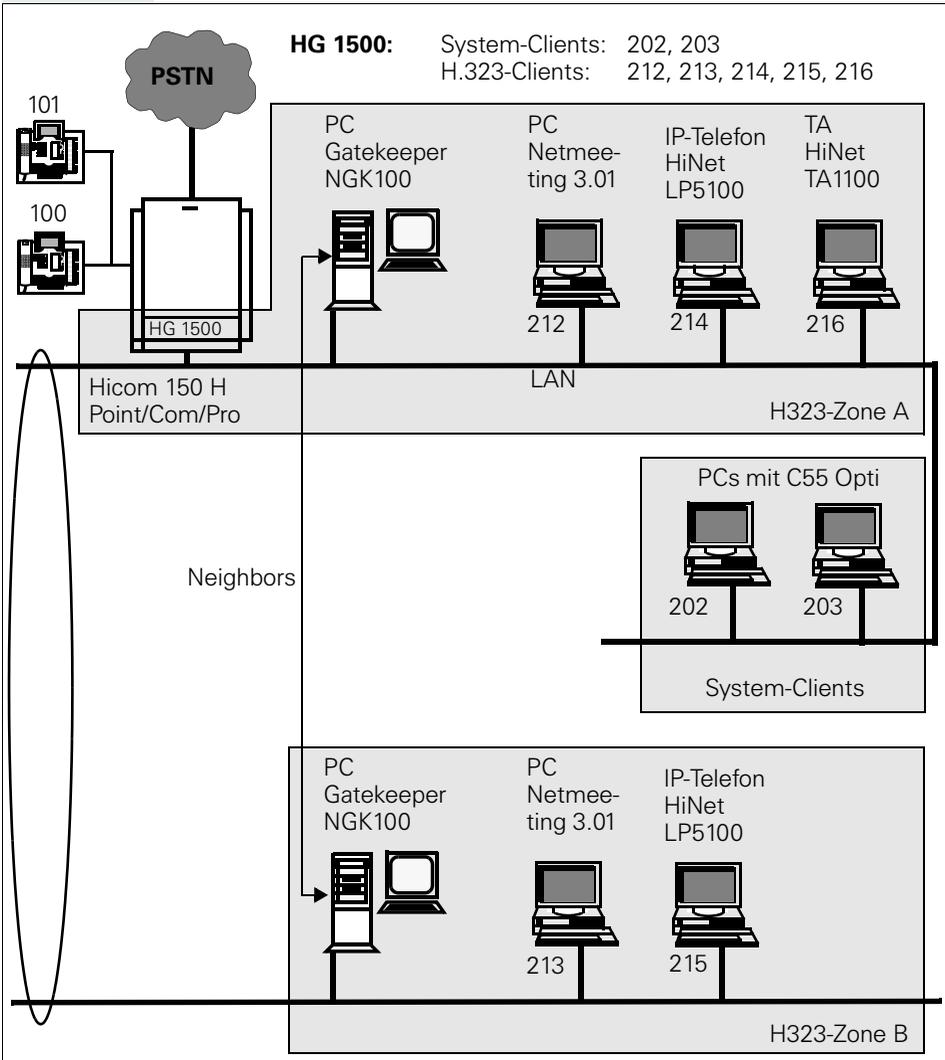
Es ist möglich, in der HiPath HG 1500 auch H.323-Clients einzurichten, die keinen Gatekeeper unterstützen. Dazu muss die zur Rufnummer zugehörige IP-Adresse unter „H.323-Clients“ administriert werden. Der Teilnehmer hat keine Mobility. Der Mischbetrieb von H.323-Clients mit und ohne Gatekeeper-Anbindung an einer HiPath HG 1500 ist möglich, wenn der Gatekeeper in der Betriebsart „Direct Routed“ betrieben wird. Clients, die Gatekeeper-Unterstützung beherrschen, müssen auch in dieser Betriebsart betrieben werden, wenn ein Gatekeeper eingesetzt wird.

Gatekeeper mit mehreren HiPath HG 1500s



Es ist möglich, mehrere HiPath HG 1500s an einem Gatekeeper anzumelden, z. B. um große Teilnehmerzahlen zu verwalten. Die Teilnehmer müssen wie oben dargestellt auf die HiPath HG 1500 verteilt werden. Die Teilnehmer führen die Gespräche immer über die HiPath HG 1500, an der sie angemeldet sind. Es findet kein Load Balancing statt, d. h. wenn auf der Heimat-HiPath HG 1500 keine DSP-Ressource mehr frei ist, wird das Gespräch nicht über eine andere HiPath HG 1500 mit freien DSP-Kanälen aufgebaut. Die HiPath HG 1500s müssen nicht wie im Beispiel mit dem gleichen Gateway-Präfix/Service konfiguriert sein.

Mehrere Gatekeeper mit einer HiPath HG 1500 und mehreren H.323-Zonen



Mit mehreren Gatekeepern können mehrere H.323-Zonen aufgebaut werden. Die HiPath HG 1500 ist in H.323 Zone A als Gateway angemeldet. Die Gatekeeper müssen gegenseitig als Neighbors eingerichtet werden, damit die Teilnehmer untereinander erreichbar sind. Die Betriebsarten "Direct Routed" und "Gatekeeper Routed" sind mischbar. Die Teilnehmer der H.323-Zonen A und B können durch Wahl des Präfixes "0" die Teilnehmer der H150E ansprechen.

Es ist auch möglich, pro H.323-Zone eine eigene HiPath HG 1500 vorzusehen. Die Teilnehmer müssen wie oben dargestellt auf die HiPath HG 1500 verteilt werden. Die Präfixe der HiPath HG 1500s dürfen gleich sein oder sich unterscheiden. Load Balancing ist auch in dieser Konfiguration nicht möglich.



Auch wenn Clients ohne Gatekeeper-Unterstützung an der HiPath HG 1500 betrieben werden, müssen diese bei Gatekeeper-Betrieb vom Gatekeeper über IP erreichbar sein, d. h. das IP-Routing von diesen Clients von und zum Gatekeeper muß möglich sein (Überprüfung mit Ping auf Gatekeeper).

SNMP anwenden

Die Applikation zur Nutzung der SNMP-Funktionalität ist ein MIB-Browser, z. B. Bestandteil des „Network Node Managers“ von Hewlett-Packard (MIB: management information base).

Die SNMP-Funktionen umfassen:

- mit MIB-Browser und Standard-MIB (nach RFC1213):
 - Abfragen und Verändern von Standard-Parametern der MIB 2
- mit MIB-Browser und Private-MIB:
 - Abfragen und Verändern von Parametern der Private-MIB der HiPath HG 1500
- mit Assistant I:
 - Festlegen von Communities zu Standard-Parametern (Berechtigungsklassen)
 - Festlegen von Trap-Communities und Stationen, an die Traps gesendet werden
 - Festlegen der Traplevel für verschiedene Trapgruppen (Empfindlichkeit auf Fehler)
- mit Trap-Empfänger:
 - Empfangen von Traps

Die MIBs beinhalten für jeden Parameter auch einen Kommentar, der kurz die Bedeutung beschreibt.

Einige Parameter sind hier beispielhaft aufgeführt:

- mgmt->mib-2->system->sysUpTime: Zeit seit dem letzten Hochlauf der HiPath HG 1500
- HLB2MIB->siemensUnits->pn->h1b2mib->controlGrouph1b20->sys-SoftwareVersion: SW-Release der BG
- mgmt->mib-2->ip->ipRouteTable: Routing-Tabelle der HiPath HG 1500

Die HiPath HG 1500 sendet SNMP-Traps (Diagnose und Fehlermeldungen) an die unter „SNMP->Trap-Communities“ eingerichteten Stationen. Diese Meldungen werden in Abhängigkeit von den unter „SNMP“ eingestellten Severity-Levels verschickt.

Beispiele für von der HiPath HG 1500 generierte Traps:

- A) generische Traps – nicht abschaltbar:
 - warm start
 - cold start
 - authentication failure
- B) enterprise Traps – konfigurierbar
 - data init (WARNING – erzwungene Neuinitialisierung von Daten)
 - memory low (WARNING – Speicherressourcen unterschreiten Schwellwert)
 - duplicate mac (MINOR – doppelt vorhandene MAC-Adresse)
 - ip firewall (WARNING – IP Firewall Verletzung)
 - mac firewall (WARNING – MAC Firewall Verletzung)
 - isdn access (WARNING – ISDN Zugangskontrolle)

Einrichtungsbeispiele

Dieses Kapitel stellt Ihnen eine Reihe von Standardkonfigurationen zur Verfügung mit denen die Administrierung der HiPath HG 1500 leichter fällt und manche Probleme umgangen werden können.

Internet Provider

Im folgenden wird beschrieben, wie man eine Internetverbindung herstellt.

Beispiel: UUNET

Einstellung beim Client

Protokoll IP
IP Adresse 192.168.30.3
Subnet-Mask 255.255.255.0
Standard-Gateway 192.168.30.254
DNS 192.76.144.66

Einstellungen Microsoft Internet Explorer 4

Unter Verbindung

1. Verbindung über einen Proxy Server herstellen ankreuzen.
2. Adresse des Proxy Servers: Anschluss
3. HTTP: www-proxy.de.uu.net: 3128

Unter Navigation

1. Seite: Startseite
2. Adresse: <http://www.uu.net>

Einstellung HiPath HG 1500

Aktive Netzwerkschnittstellen LAN und ISDN1/2/3 Internet

Netzwerkinterface ISDN3:

- IP- Adresse 0.0.0.0
- Netzmaske 255.255.255.248

IP Routing:

- IP- Adresse 0.0.0.0
- Netzmaske 255.255.255.248
- Gateway 0.0.0.1

ISDN Partner:

- IP Adresse 0.0.0.1
- B- Kanal auf 1 setzen
- CHAP ankreuzen: User- ID XXX, Passwort XXX
- Rufnummer 00211917822 gehend



Normalerweise ist ein Zugriff von allen PCs möglich. Manche Provider sperren allerdings diese Möglichkeit, sie muss separat beantragt werden.

Einrichtungsbeispiele

Beispiel: T-Online/ISDN

Bei der Einrichtung von T-Online als Provider ist folgende Besonderheit zu beachten:

Für den ISDN-Partner ist als Authentisierungsprotokoll PAP einzustellen, der Host-Button muss aktiviert werden.

Die User-ID setzt sich zusammen aus:

<Anschlusskennung><T-Online-Nr>#<Mitbenutzerkennung>

Beispiel:

- Anschlusskennung: 000123456789
- T-Online-Nummer: 02302666555
- Mitbenutzerkennung: 1

Dann ist die User-ID: 00012345678902302666555#0001

Das Passwort ist das persönliche Kennwort.

Beispiel: T-Online/T-DSL

Diese Daten erhalten Sie von T-Online

- Anschlusskennung: 000123456789
- T-Online-Nummer: 02302666555
- Mitbenutzerkennung: 1

Die Konfiguration ist wie folgt vorzunehmen:

Als Authentisierungsprotokoll wird PAP eingestellt. Der Host-Button muss aktiviert werden.

Die User-ID setzt sich zusammen aus:

<Anschlusskennung><T-Online-Nr>#<Mitbenutzerkennung>

Dann ist die User-ID: 00012345678902302666555#0001

Das Passwort ist das persönliche Kennwort.

Dementsprechend ergeben sich folgende Menüeinträge:

Netzwerkschnittstellen->Aktive Netzwerkschnittstellen: LAN2/DSL aktiv

IP-Adresse: 172.16.16.16 (Platzhalter bei DSLZugang)

IP-Netzmaske: 255.255.255.255

Datenpaketlänge: 1492

Provider-Name: t-online.de

PAP:

HOST_Button aktiviert

User-ID:

zusammengesetzt aus:

<Anschlusskennung><T-Online-Nr><#<Mitbenutzer/Suffix>
@t-online.de

Beispiel: 00012345678902302666555#0001@t-online.de

Passwort:

Das Passwort ist das persönliche Kennwort.

CHAP: deaktiviert

NAT: aktiviert

Short Hold Zeit: nach Wunsch

bei Flatrate kann auch

Short Hold Modus: gesperrt

konfiguriert werden

Diese Parameter können entsprechend der eigenen Vorlieben und des Tarifmodells konfiguriert werden.

Durchsatzrate: 128

Dies entspricht der Datenrate in kBit/s, die auf dem DSL-Anschluß ins Internet geschickt werden kann.

Routing->IP-Routing

IP-Adresse:0.0.0.0

Netzmaske: 255.255.255.0

Gateway: 172.16.16.16 (hier gleiche Adresse wie unter Netzwerkschnittstellen->Netzinterfaces->DSL->IP-Adresse) siehe → 113

Einrichtungsbeispiel für die Niederlande

Beispiel: KPN MXSTREAM

Diese Daten erhalten Sie von KPN telecom

- Anschlusskennung: siegoud
- Extension: @mxstreamvalley.extra
- IP-Adresse des ADSL-Modems: 10.0.0.138

Die Konfiguration ist wie folgt vorzunehmen:

Als Authentisierungsprotokoll wird PAP eingestellt. Der Host-Button muss aktiviert werden.

Die User-ID setzt sich zusammen aus:

<Anschlusskennung><Extension>

Dann ist die User-ID:siegoud@mxstreamvalley.extra

Das Passwort ist das persönliche Kennwort.

Dementsprechend ergeben sich folgende Menüeinträge:

Netzwerkschnittstellen->Aktive Netzwerkschnittstellen: LAN2/DSL aktiv

Netzwerkschnittstellen->Netzinterfaces->PPTP: Interface-Name :PPTP

IP-Adresse: 172.16.16.16 (Platzhalter bei DSL-Zugang)

IP-Netzmaske: 255.255.255.255

Datenpaketlänge: 1460

Provider-Name: KPN MXSTREAM

PAP:

HOST_Button aktiviert

User-ID:

zusammengesetzt aus:<Anschlusskennung><Extension>

Beispiel: siegoud@mxstreamvalley.extra

Passwort:

Das Passwort ist das persönliche Kennwort.

CHAP: deaktiviert

NAT: aktiviert

Short Hold Zeit: nach Wunsch

bei Flatrate kann auch

Short Hold Modus: gesperrt

konfiguriert werden

Diese Parameter können entsprechend der eigenen Vorlieben und des Tarifmodells konfiguriert werden.

Durchsatzrate: 128

Dies entspricht der Datenrate in kBit/s, die auf dem DSL-Anschluß ins Internet geschickt werden kann.

Client IP-Adresse: <IP Adresse des 2.LAN Anschlusses>

Beispiel: 10.0.0.140

Server IP-Adresse: <IP Adresse des ADSL-Modems>

Beispiel: 10.0.0.138

IP-Netzmaske(PPTP):

Beispiel: 255.255.255.248

Routing->IP-Routing

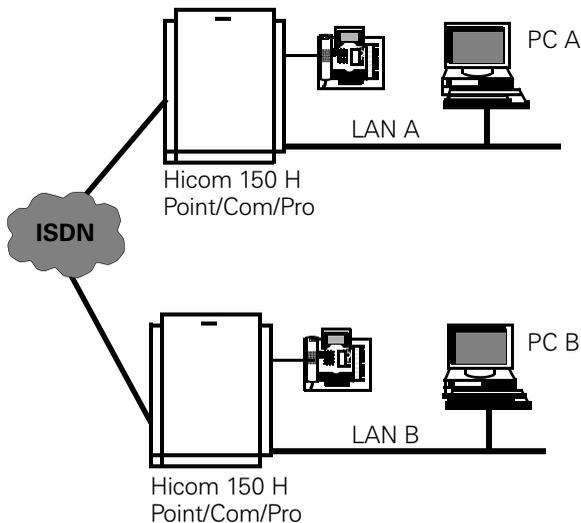
IP-Adresse:0.0.0.0

Netzmaske: 255.255.255.0

Gateway: 172.16.16.16 (hier gleiche Adresse wie unter Netzwerkschnittstellen->Netzinterfaces->DSL->IP-Adresse) siehe → 113

Routing HiPath HG 1500 zu HiPath HG 1500

LAN-LAN Kopplungen, d. h. WAN Verbindungen können mittels HiPath HG 1500 über ISDN-Wählleitungen hergestellt werden. Dabei kann der Partner auch ein Fremdrouter sein. In diesem Fall ist die Konfiguration der B-Seite entsprechend den Konfigurationshinweisen des Fremdherstellers abzuändern.



Einrichtung HiPath HG 1500 A

- PC A : IP: 218.20.56.181
Subnet: 255.255.255.0
Gateway: 218.20.56.254
- HiPath HG 1500 A
LAN IP: 218.20.56.254
Subnet: 255.255.255.0
- HiPath HG 1500 A
ISDN1 IP: 218.20.60.1
Subnet: 255.255.255.0
- Routing A IP: 218.20.55.0
Subnet: 255.255.255.0
Gateway: 218.20.60.2
- ISDN Partner A
Name: LB2
IP: 218.20.60.2
- B Kanal: 1 Rufnummernliste
A 0831396809 Kommend
00831396809 Gehend

Einrichtung HiPath HG 1500 B

- PC B : IP: 218.20.55.181
Subnet: 255.255.255.0
Gateway: 218.20.55.254
- HiPath HG 1500 B
LAN IP: 218.20.55.254
Subnet: 255.255.255.0
- HiPath HG 1500 B
ISDN1 IP: 218.20.60.2
Subnet: 255.255.255.0
- Routing B IP: 218.20.56.0
Subnet: 255.255.255.0
Gateway: 218.20.60.1
- ISDN Partner B
Name: LB2
IP: 218.20.60.1
- B Kanal: 1
- Rufnummernliste
A 0831396820 Kommend
00831396820 Gehend

Beispiel: Nachdem das oben genannte Beispiel eingerichtet ist, sollte folgender Test gemacht werden:

- PC A Ping nach LAN A 218.20.56.254
- PC A Ping nach ISDN1 A 218.20.60.1
- PC A Ping nach ISDN1 B 218.20.60.2
- PC A Ping nach LAN B 218.20.55.254
- PC A Ping nach PC B 218.20.55.181

Hostrouting

Hostrouting / Routing ohne Transfernetz

Bei der LAN-LAN-Kopplung über IP sind üblicherweise drei IP-Netze beteiligt: LAN A, LAN B und ein IP-Transfer-Netz, was zwischen den beiden Routern im WAN (Wide Area Network) konfiguriert wird (auf der HiPath HG 1500 durch die ISDN-Interface).

Zusätzlich gibt es die Möglichkeit, auf die Konfiguration des Transfernetzes zu verzichten. Die Gegenstelle sollte dies unterstützen.

Folgendes Beispiel zeigt die Konfiguration:

- Es gibt ein LAN A mit der Netzadresse 192.168.1.0.
- Es gibt ein LAN B mit der Netzadresse 192.168.2.0.

In jedem der beiden LAN existiert eine HiPath HG 1500.

LAN	NW-IP-Adresse	Netzmaske	IP-Adresse	HiPathHG1500
A	192.168.1.0	255.255.255.0	192.168.1.254	
B	192.168.2.0	255.255.255.0	192.168.2.254	

Die ISDN1-3 Interface beider Baugruppen können beliebig konfiguriert sein. Sie werden für dieses Szenario nicht verwendet.

Parameter	HiPath HG 1500	LAN A	LAN B
Routing->IP-Routing			
IP-Adresse		192.168.2.0	192.168.1.0
Netzmaske		255.255.255.0	255.255.255.0
Gateway		192.168.2.254	192.168.1.254
Routing->ISDN-Partner			
Name		Partner LAN B	Partner LAN A
IP-Adresse		192.168.2.254	192.168.1.254
IP-Adresse unterdrücken		ja	ja

Soll zusätzlich aus LAN A heraus eine RAS-Workstation erreicht werden (Remote-Arbeitsplatz), die die IP-Adresse 192.168.50.1 besitzt, so wird folgender Eintrag benötigt:

```

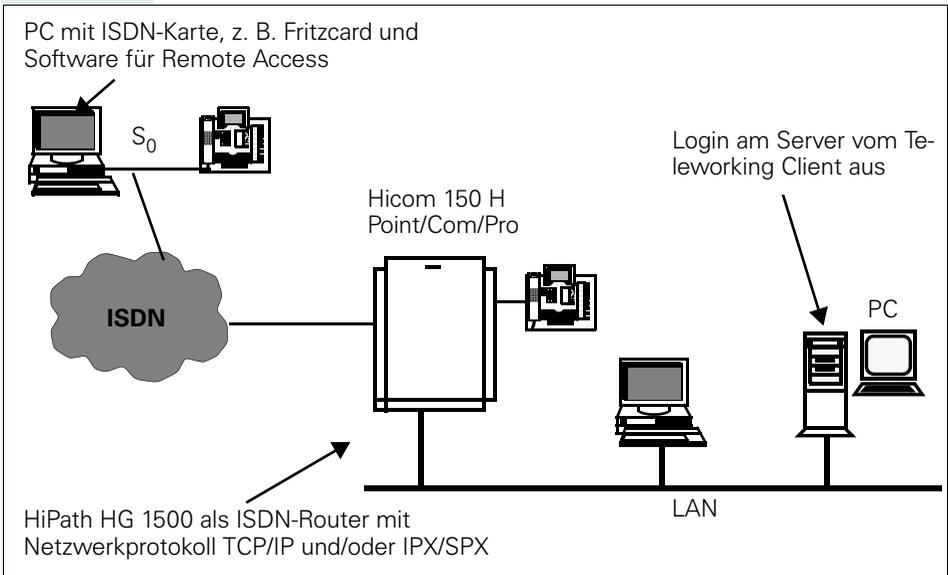
Parameter HiPath HG 1500           LAN A
Routing->ISDN-Partner
Name                               Partner RAS
IP-Adresse                         192.168.50.1
IP-Adresse unterdrücken           ja
    
```

Wie man an diesen Beispielen sieht, wird jeweils kein ISDN-Interface konfiguriert. Die erforderlichen Einträge im Router werden dynamisch angelegt und nicht im KDS angezeigt. Die Aushandlung einer IP-Adresse im IP-Transfernetz wird mit dem Schalter „IP-Adresse unterdrücken“ ausgeschaltet.

 Bis zu acht Einträge können nach dem oben angegebenen Verfahren benutzt werden.

Remote Access Service (RAS)

Teleworking mit HiPath HG 1500



Einstellungen mit HiPath HG 1500

Damit Sie einen PC über ISDN mit HiPath HG 1500 als Teleworking nutzen können, müssen Sie im Administrationsprogramm die folgenden Schritte ausführen:

Zuerst legen Sie die IP-Adresse des RAS/Teleworking-PC fest (muss im WAN (ISDN) liegen).



Routing

ISDN-Partner

Wählen Sie mit der linken Maustaste den Menüpunkt „ISDN-Partner“ aus und drücken Sie die Symbolschaltfläche „Neu.“ Tragen Sie in das Dialogfenster den Namen des ISDN-Partners ein und bestätigen Sie Ihre Eingabe.

Markieren Sie mit der Maus den neu erstellten Eintrag.

➡ IP-Adresse:

Tragen Sie die IP-Adresse des ISDN-RAS/Teleworking ein.

➡ B-Kanäle:

Geben Sie nun die Anzahl der B-Kanäle an, die für diese Verbindung maximal benutzt werden sollen.

Es kann die nachfolgende Software auf dem Teleworking-PC eingesetzt werden.

DFÜ-Netzwerk

Unter Windows 95/98, NT 4.0 und Windows 2000 kann das DFÜ Netzwerk benutzt werden. Voraussetzung ist eine ISDN-Karte z. B.: AVM Fritzcard mit Capiport Treiber.

Nachteil des DFÜ-Netzwerkes (abhängig von der Windows-Variante)

- Im Standard DFÜ-Netzwerk ist nur 1 Kanal-Verbindung möglich.
- Bei Zugriff auf die Netzwerkressourcen muss der Verbindungsaufbau manuell hergestellt werden.
- Nach Verbindungsabbau durch Short Hold muss die Verbindung manuell wieder aktiviert werden.
- IPX Verbindung zu Novell-Servern ist nicht möglich.
- DFÜ-Netzwerk unterstützt keinen verbindungslosen Callback.
- 2 Kanal-Verbindung ist bei Windows 95 nur mit DFÜ-Netzwerk Version 1.3 oder mit der Erweiterung „Demsisdn.exe möglich (auf Microsoft Home Page im Internet).

Einrichten des DFÜ-Netzwerkes

Auf dem Client-PC muss der NDIS-WAN-Treiber unter Netzwerkeigenschaften installiert werden. Als Protokoll wird TCP/IP hinzugefügt. Es ist nicht notwendig IP-Adressen in den Netzwerkeigenschaften einzutragen. Danach können über das Symbol Arbeitsplatz und dann DFÜ-Netzwerk die Komponenten installiert werden, die für das DFÜ-Netzwerk notwendig sind.

Die IP-Adressen werden nach der Installation des DFÜ-Netzwerkes in der Verbindungssteuerung eingegeben, d. h. es kann für jede Verbindung eine andere IP-Adresse genutzt werden. Als Gateway wird die IP-Adresse der ISDN-Seite von der HiPath HG 1500 angegeben.

Die Verbindung kann über das Symbol „Arbeitsplatz“ und „DFÜ-Netzwerk“ hergestellt werden.

Wird der PC dann in den Netzwerkeigenschaften als Mitglied einer Domäne eingerichtet, kann beim Hochfahren in dem Anmeldefenster die Option „Anmeldung über DFÜ“ genutzt werden.

Ein Nachteil des DFÜ-Netzwerkes ist, dass nach jedem Auslösen der Verbindung (Short-Hold) die Verbindung wieder manuell aufgebaut werden muss bzw. ein Anmeldebildschirm erscheint.

ITK Columbus Client Pro

Unter Windows 95/98 und NT 4.0 kann ITK Columbus Client Pro (ITK ix1 connect ws) eingesetzt werden. Verbindungen sind mit 1 oder 2 Kanälen möglich. Vorteil gegenüber dem DFÜ Netzwerk: Rückruf und selbsttätiger Verbindungsaufbau bei Zugriff auf die Netzwerkressourcen möglich. Außerdem sind der Zugriff auf Novell Netzwerke und Verbindungen mit 1 oder 2 Kanälen möglich.

Vorteil gegenüber dem DFÜ-Netzwerk

- Rückruf und selbsttätiger Verbindungsaufbau bei Zugriff auf die Netzwerkressourcen sind möglich.
- Login und Zugriff auf Novell-Netzwerke mittels IPX möglich.

Einrichten des ITK-Clients

Voraussetzung ist eine installierte ISDN-Karte mit der dazugehörenden Capi-Schnittstelle.

Der ITK-Client wird über die mit der ISDN-Karte mitgelieferten Disketten installiert.

Bei der Installation wird ein neuer Adapter in den Netzwerkeigenschaften hinzugefügt. Es kann „keine Unterstützung für Netware“ angekreuzt werden, wenn diese nicht notwendig ist. Als Protokoll wird dann nur TCP/IP ausgewählt.

Die IP-Adresse und der Gateway (IP-Adresse der ISDN-Seite der HiPath HG 1500) wird während der Installation für den ITK-Adapter in den Netzwerkeigenschaften eingegeben.

Über die Verbindungssteuerung des Programms wird dann die entsprechende Verbindung zu HiPath HG 1500 eingerichtet. Hier kann dann unter PPP-Optionen Multilink (2-Kanalverbindung) und Callback eingerichtet werden.

Soll sich der Rechner beim Hochfahren in einer Domäne anmelden, kann dieses in den generellen Einstellungen angegeben werden. Dann wird beim Hochfahren des PCs automatisch eine Verbindung aufgebaut und der Benutzer kann sich dann in der Domäne anmelden als wäre er lokal mit dem Netzwerk verbunden.

Während der Arbeit mit dem PC wird im Hintergrund die Verbindung abgebaut (Short Hold) und sobald auf irgendwelche Netzwerkressourcen zugegriffen wird, baut der ITK-Client automatisch wieder die Verbindung auf.

AVM Netways (ab Version 3.0 Revision 3)

(Die hier dargestellten Einrichtungsbeispiele gelten für die Version 3.0.)
Unter Windows 95 und NT kann AVM Netways eingesetzt werden. Verbindungen sind nur mit einem Kanal möglich. Netways funktioniert nur mit AVM-Karten.

Vorteil gegenüber dem DFÜ-Netzwerk

- Rückruf und selbsttätiger Verbindungsaufbau bei Zugriff auf die Netzwerkressourcen sind möglich.
- Login und Zugriff auf Novell-Netzwerke mittels IPX möglich.

Einrichten des AVM-Clients

Voraussetzung ist eine installierte AVM-ISDN-Karte mit der dazugehörigen Capi-Schnittstelle.

Die Installation erfolgt über ein Setup. Unter anderem wird abgefragt, ob der System-Service aktiviert werden soll. Dieser wird in der Regel nur dann benötigt, wenn der Client sich an einer Domäne anmelden will. (Die Aktivierung hat zur Folge, dass Netways immer gestartet ist und nicht beendet werden kann).

Während der Installation wird ein neuer Adapter in den Netzwerkeigenschaften hinzugefügt. Hier wird die IP-Adresse des Client und des Gateway (ISDN Seite des HiPath HG 1500) eingestellt.

Nach Beenden der Eingabe in den Netzwerkeigenschaften darf der Rechner noch nicht neu gestartet werden, sondern erst nachdem Netways das erste Mal aufgerufen wird und selber zum Neustart des Rechners auffordert.

In Netways wird in der Konfiguration unter „Addresses“ die IP-Adresse noch einmal eingetragen.

Für die Verbindung zu unserer HiPath HG 1500 wird unter Targets eine neue Verbindung eingerichtet. Das Protokoll wird auf PPP eingestellt. Wichtig ist, dass unter den erweiterten Einstellungen bei IP die Auswahl bei „Netbios über IP-Filter“ deaktiviert wird. IPX wird in diesem Fall (nur RAS-Client für NT-Netzwerk) auch deaktiviert.

Multilink (Mehrkanal-Verbindung) ist erst ab Version 4 möglich.

Soll Rückruf genutzt werden, wird dies unter den erweiterten Einstellungen bei COSO und hier auf „Remote“ eingestellt.

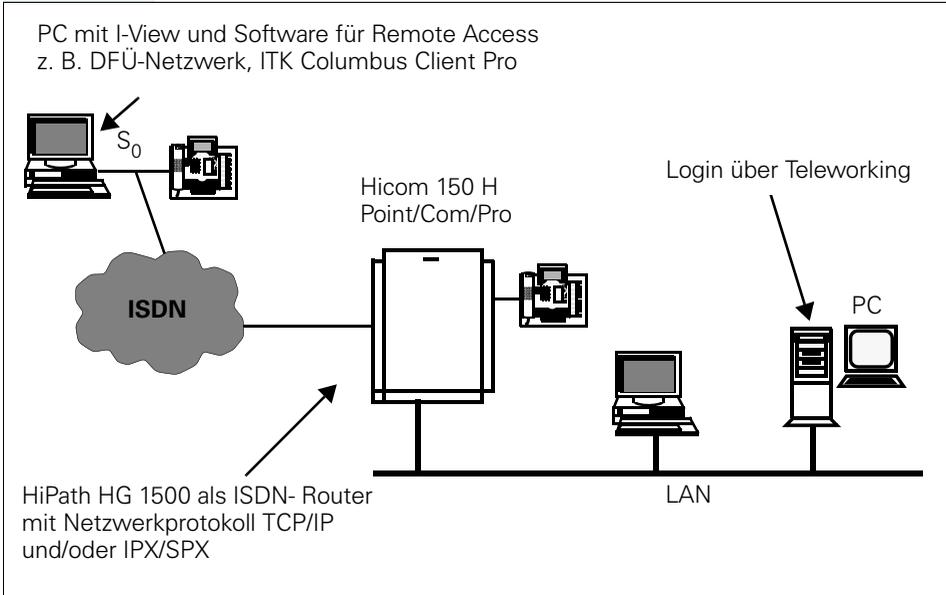
Um sich von der NT-Workstation beim Hochfahren in der Domäne anzumelden, kann Netways in der Konfiguration unter Operation Mode bei Autoconnect auf Dial umgestellt werden und die Verbindung zur HiPath HG 1500 ausgesucht werden. Unter Netways ISDN Service Setup muss der System Service auf Enable gestellt werden.

Jetzt wird beim Hochfahren des PCs automatisch eine Verbindung zu HiPath HG 1500 aufgebaut und es ist möglich, sich in der Domäne anzumelden, als wäre man lokal mit dem Rechner am Netzwerk verbunden.

Während der Arbeit mit dem PC wird im Hintergrund die Verbindung abgebaut (Short Hold) und sobald auf irgendwelche Netzwerkressourcen zugegriffen wird, baut der AVM-Client automatisch wieder die Verbindung auf.

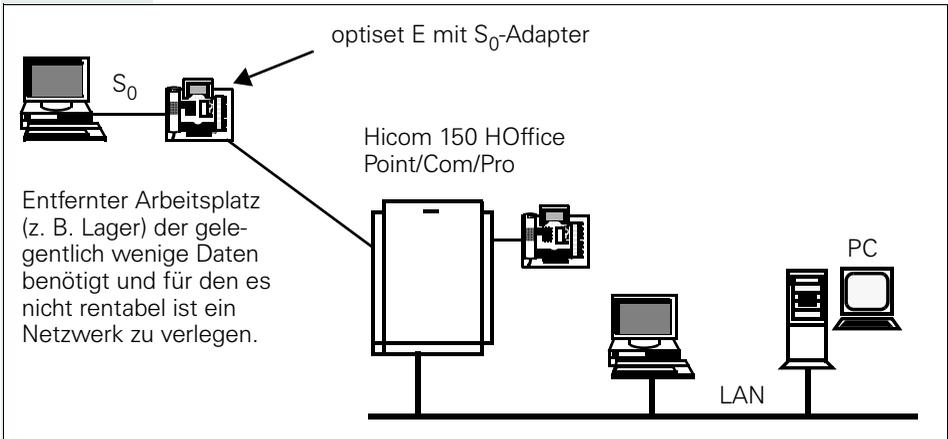
Lösungsansatz I-View unter Windows 95

Teleworking mit HiPath HG 1500 und I-View



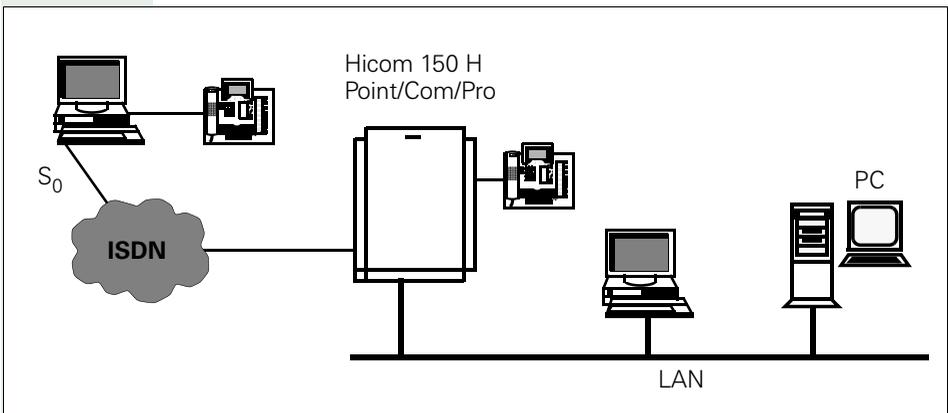
Lösungsansatz über S₀-Adapter am optiset E

Teleworking mit HiPath HG 1500 und optiset E



Lösungsansatz mit Hicom Integrated

Teleworking mit HiPath HG 1500 und S₀-Telefon



Kommunikationszentrale mit optiset E
Integrierte SW für CTI, Gebührenerfassung.

Zur Administration des Systems PC mit ISDN Karte und Remote Access Software, z. B. I-View mit DFÜ-Netzwerk/ITK Columbus Client Pro.

WindowsNT 4.0 Workstation mit Teleworking / RAS

Die HiPath HG 1500 kann in einem Windows-NT Netzwerk unter anderem auch als ISDN RAS Router eingesetzt werden. Dies bedeutet, das Benutzer auch aus der Ferne über ISDN auf das Netzwerk zugreifen können und sich gegebenenfalls auch an einer Domäne mit einer Windows NT-Workstation anmelden können.

HiPath HG 1500 selber muss hierfür nur als Router im Netzwerk eingerichtet sein und zusätzlich müssen die entsprechenden Remote Partner eingetragen werden.

Die Remote Partner (in diesem Fall Windows NT-Workstation) benötigen eine ISDN-Karte und entsprechende Software.

Als Software kann das DFÜ-Netzwerk von Windows genutzt werden. Hierfür muss aber ein passender Treiber (z. B. bei AVM der „AVM NDIS WAN CAPI-Treiber“) vorhanden sein.

Weiterhin gibt es spezielle Software die einen RAS Zugang ermöglichen. In diesem Beispiel wird die Software ITK Columbus Client Pro (ITK ix1-connect/WS for Windows NT 4.0) oder Netways für Windows NT von AVM beschrieben.

Vorteil gegenüber dem DFÜ-Netzwerk

- Multilink (2 ISDN Kanäle, nur ITK),
- Short Hold (automatischer Verbindungsab- und Aufbau beim Zugriff auf das Netzwerk) und
- Rückruf (Callback) nutzbar.

Teleworking mit Log-in an NT Domäne

Grundsätzlich muss eine „LMHOSTS“ Datei angelegt werden in der die Namen und IP-Adressen der Domäne und des Servers enthalten sind. Der Benutzername mit dem sich an der Workstation angemeldet wird, muss ein Konto in der Domäne besitzen.

Beispiel für LMHOST-Eintrag

```
192.168.150.1 NTSRV1 #DOM:NTDOM1
```

Die Einrichtung des Netzwerks erfolgt zuerst nur als Mitglied einer Arbeitsgruppe, wobei der Name der Arbeitsgruppe gleich ist wie der Name der Domäne.

Erst wenn eine Verbindung (über ISDN) mit dem Netzwerk bzw. der Domäne aufgebaut wurde, ist es möglich in den Netzwerkeigenschaften sich als Mitglied einer Domäne einzutragen.

Danach ist es möglich sich mit dem DFÜ-Client oder dem ITK-Client oder AVM Client automatisch beim Start der Workstation über die ISDN-Verbindung in der Domäne anzumelden.

Durch die Anmeldung in der Domäne kann auf die Netzwerkumgebung (Computer bzw. Server) zugegriffen werden. Es ist nicht nötig über die Funktion „Computer suchen...“ Netzwerkverbindungen zu anderen Computern herzustellen.

HiPath HG 1500, IPX Routing und Teleworking an Novell

IPX Routing (Novell Netware) und Teleworking an Novell-Server

Voraussetzung:

Als Voraussetzung für das IPX Routing und den Teleworking an Novell-Server über die HiPath HG 1500 muss zwingend auf den Novell-Server der Frametyp Ethernet_II gebunden werden. Es ist möglich den Frametyp zusätzlich zu den vorhandenen Frametyps zu binden, hierbei ist zu beachten, dass die Netzwerkadresse des gebundenen Frametyp Ethernet_II von der HiPath HG 1500 verwendet wird. (Diese Einstellungen erfolgen in der Regel durch den Systemadministrator.)

HiPath HG 1500 Einstellungen:

In der HiPath HG 1500 muss unter Netzwerkschnittstellen im Netzinterface „LAN“ die IPX-Netzwerknummer des LANs (siehe oben) eingetragen werden um IPX zu aktivieren. Die IPX-Node (MAC-Adresse) ist fest in der HiPath HG 1500 einprogrammiert und kann nicht geändert werden.

Im Netzinterface „ISDN1“ muss die IPX-Netzwerknummer und die IPX-Node für die ISDN-Seite eingetragen werden, um auch für dieses Interface IPX zu aktivieren (siehe oben).

ISDN/IPX-Netzwerknummer = die Netzwerknummer für das virtuelle „ISDN-Netzsegment,“ diese muss für jeden Routing Partner (HiPath HG 1500 / Router), die zusammen arbeiten wollen, gleich sein.

ISDN/IPX-Node = dies ist die Adresse anhand jeder Partner/User identifiziert wird und muss daher für jeden Partner eindeutig sein (Im LAN ist diese durch die Netzwerkkarten fest vorgegeben und wird dort in der Regel nicht frei vergeben). Bei der Vergabe der Nummer sollte von links die ersten Stellen 02 sein, daran lässt sich erkennen, dass sie frei vergeben worden ist.

(Nach diesen Einstellungen, kann mit Hilfe des Befehls „display networks“ auf der Serverconsole festgestellt werden, ob das IPX -Protokoll richtig eingerichtet worden ist. Es muss jetzt auch die IPX-Adresse des ISDN-Netzwerk erscheinen.)

Unter Routing müssen bei „ISDN-Partner“ die Gegenstellen für IPX-Routing und die Teleworking-PCs eingetragen werden.

IPX-Routing Partner:

Für IPX muss in dem Partnereintrag die „Node-Adresse“ eingegeben werden. Dies ist die Adresse die der Partner in seinem „ISDN1-Interface“ als „IPX-Node“ eingetragen hat. (Bei Fremd-Routern gibt es vergleichbare Einstellungen)

Sollte kein zusätzliches IP-Routing aktiviert sein, muss man den Eintrag „Systemstart-Verhalten“ auf „automatische Verbindung“ einstellen, damit nach dem Laden des KDS eine Verbindung zum Partner hergestellt wird und die IPX Routinginformationen zwischen den beiden Netzen ausgetauscht werden können.

Ist zusätzlich IP-Routing aktiviert, kann man die Verbindung durch einen Ping zum Partner aufbauen.

Der „Short Hold“ sollte auf 60 (Sekunden) hochgestellt werden, damit alle IPX-Routinginformationen ausgetauscht werden können.

Die weiteren Einstellungen (Multilink, B-Kanäle, Rückruf...) entsprechen dem des IP Routing.

Partner für Teleworking:

Auch hier muss eine „Node-Adresse“ eingegeben werden. Diese muss die Node-Adresse (MAC-Adresse) sein, die in der Software des Teleworking eingegeben wird oder ist.

Die weiteren Eingaben entsprechen wieder denen eines Teleworking mit IP, wobei auch hier beides zusammen möglich ist.

Hinweis bei Verwendung von IP und IPX:

Bei der Verwendung von IP und IPX zusammen ist generell folgendes zu beachten:

Wird in der HiPath HG 1500 A für den Partner B IPX und IP freigegeben, muss HiPath HG 1500 B für Partner A auch beides Freigeben, wird in der HiPath HG 1500 A für den Partner B nur IPX (oder IP) freigegeben, darf HiPath HG 1500 B für Partner A auch nur IPX (oder IP) freigegeben. Gleiches gilt auch für Teleworking-PCs (Einstellungen am Teleworking beachten).

Hinweis für Teleworking

Für den Teleworking unter Novell wird für den Client PC eine spezielle Software benötigt, da ein Zugang mit dem DFÜ Netzwerk von Microsoft nicht möglich ist (es kann keine Node-Adresse eingegeben werden).

Die Software Netways von AVM ermöglicht ein Login auf einem Novell-Server und wurde auch zertifiziert. Da diese nur mit einer AVM-Karte betrieben werden kann, wurde auch die Software von ITK, WS-Connect bzw. Columbus-Client, erfolgreich mit Novell und der HiPath HG 1500 getestet.

Für die Verwendung der Software mit Novell muss in den Netzwerkeigenschaften das IPX-Protokoll mit dem entsprechenden NDIS-WAN (ISDN) Adapter gebunden werden und hier unter erweiterten Einstellungen als Rahmen-Typ der Frametyp Ethernet_II wieder eingestellt werden. Die Node (Mac) Adresse wird in den Einstellungen der jeweiligen Software eingetragen.

Das einloggen in den Novell Server erfolgt in der Regel, nachdem eine Verbindung mit der Software hergestellt wurde über die Netzwerkumgebung. Hier erscheint jetzt der Novell-Server und man kann sich mit einem einfachen Doppelklick mit seinem Usernamen anmelden.

Routing und Callback mit Cisco-Routern

Mit dem Cisco-Router und dem SW-Release 12.0 ist ein Callback über die Caller ID (rufende Nummer) im D-Kanal möglich. Generell wird als Callback-Nummer die rufende Nummer verwendet. Bei Problemen mit der Rufnummernübertragung ist es auch möglich mit „jokern“ (in Form von x`en) zu arbeiten.

Netzwerkschnittstellen:

LAN = 192.168.40.254

ISDN1 = 192.168.100.31

Verbindungssteuerung:

Wahlwiederholung = 0

Routing:

IP-Adresse = 192.168.70.0

Netzmaske = 255.255.255.0

Gateway = 192.168.100.15

ISDN-Partner (Cisco):

IP-Adresse = 192.168.100.15

B-Kanäle = 2

Rückruf = Nein

Cisco Router:

```
isdn switch-type basic-net3
!
!!
interface Ethernet0
    ip address 192.168.70.128 255.255.255.0
    no ip directed-broadcast
    no mop enabled
!
interface BRI0
    ip address 192.168.100.15 255.255.255.0
    no ip directed-broadcast
    encapsulation ppp
    dialer map ip 192.168.100.31 002112345678
    dialer-group 1
    isdn switch-type basic-net3
    isdn caller xx2112345678 callback!!!!
    isdn calling-number 168
    hold-queue 75 in
```

```
!  
ip classless  
ip route 192.168.30.0 255.255.255.0 192.168.100.31  
ip route 192.168.40.0 255.255.255.0 192.168.100.31  
!  
dialer-list 1 protocol ip permit  
!
```

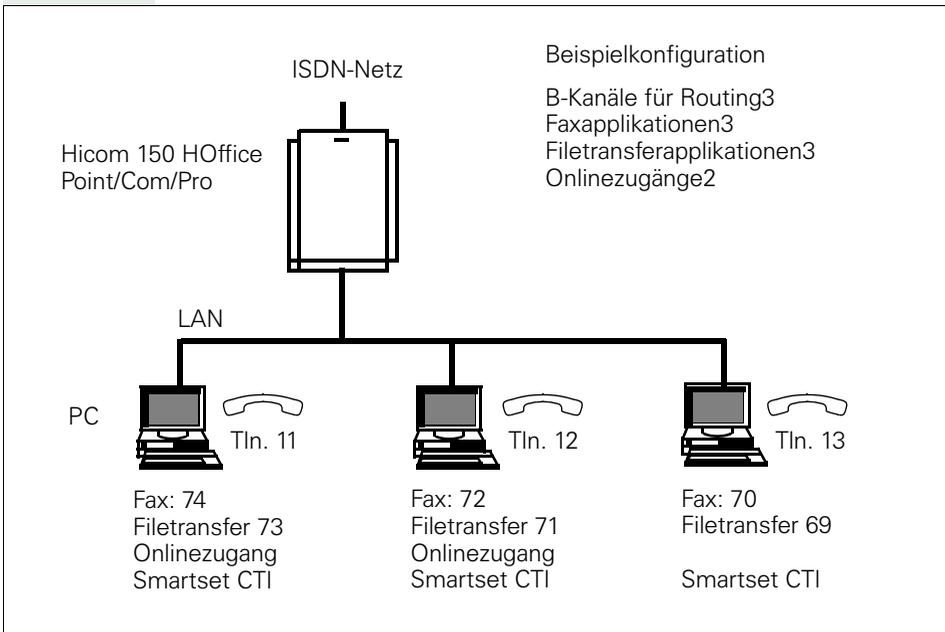
Telematik

Rufnummernvergabe bei Telematik

Alle Telematikfunktionen, die kommend erreicht werden müssen, erfordern eine eigene Durchwahlnummer. Für die HiPath HG 1500 sind also pro FAX-Endstelle und Filetransferapplikation entsprechende Rufnummern zu konfigurieren. Diese Rufnummern dürfen mit dem Rufnummernhaushalt des Systems nicht kollidieren. Die Einrichtung der Rufnummern der Telematikteilnehmer wird von der Administrationskomponente des Anwendungsprogrammes vorgenommen.

Über den Assistant E kann für eine FAX-Applikation eine Rufweeterschaltung zu einem bzw. mehreren Fax-Applikationen administriert werden.

Beispiel für Rufnummernvergabe



Für die CTI-Anwendungen (Smartset) 73, 71, 69 muss die assoziierte Wahl freigeschaltet werden. Soll eine Rufauswertung auf dem PC erfolgen, ist es notwendig, eine Rufzuschaltung von den Endgeräten 11, 12, 13 zu den jeweiligen PCs 73, 71, 69 einzurichten.

Einschränkungen bei Telematikfunktion

In der Hicom 150 E Office Com und Point sind nur zwei FAXe zur gleichen Zeit pro Baugruppe möglich, in der Hicom 150 E Office Pro drei.

vCAPi für die Clients im Netzwerk

Mit HiPath HG 1500 und der vCAPi Software (virtuelle CAPi) verhält sich der PC ähnlich wie ein PC mit eigener ISDN-Karte. Voraussetzung ist:

- TCP/IP als Transportprotokoll
- WIN 95, WIN 98, WIN NT 4.0 oder Windows 2000 als Client-Betriebssystem

Die Rufnummernvergabe erfolgt in der HiPath HG 1500 durch die Zuordnung IP-Adresse → Rufnummer (max 100 Rufnummern).

Hierbei kann es auch notwendig sein einer IP-Adresse mehrere Rufnummern zuzuordnen.

FRITZ!voxfon

Die Module werden unterstützt mit Ausnahme folgender Funktionen:

- Supplementary Services, z. B. Makeln, Rückfrage

FRITZ!fax und Rufweiterleitung

Wenn der PC ausgeschaltet wird bzw. die Faxapplikation nicht im Hintergrund gestartet ist, erhält der ankommende Faxanrufer Freizeichen. Hierzu kann in der Hicom eine Weiterschaltung auf das Kundenfaxgerät eingerichtet werden. Der Nachteil/Vorteil ist, während ein Client mit Fritzfax empfängt oder sendet werden ankommende Faxanrufe die für andere Clients auch weitergeleitet. Die Weiterschaltung lässt sich nur mit dem Assistent der Hicom einrichten, bzw. ändern.

Anhang

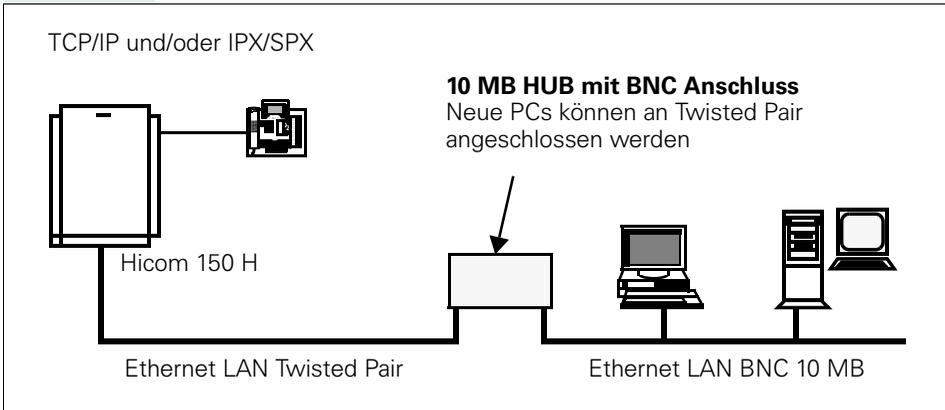
Die Administrierung gekoppelter Netze im WAN/LAN-Bereich ist eine durchaus technisch anspruchsvolle Aufgabe. Im Rahmen dieser Tätigkeit wird ein Netzwerkadministrator früher oder später immer wieder Konfigurationsprobleme entdecken, die es schnell und effizient zu beseitigen gilt. Dieser Anhang soll Ihnen dabei helfen.

LAN-Lösungsvorschläge

BNC-Netz an Twisted Pair

Verlängerung des BNC Netzwerksegment (max. 185 m) um weitere 100 m mit Twisted Pair.

10 MB Ethernet HUB mit BNC-Anschluss



Anbindung des BNC-Netz an Twisted Pair zur HiPath HG 1500

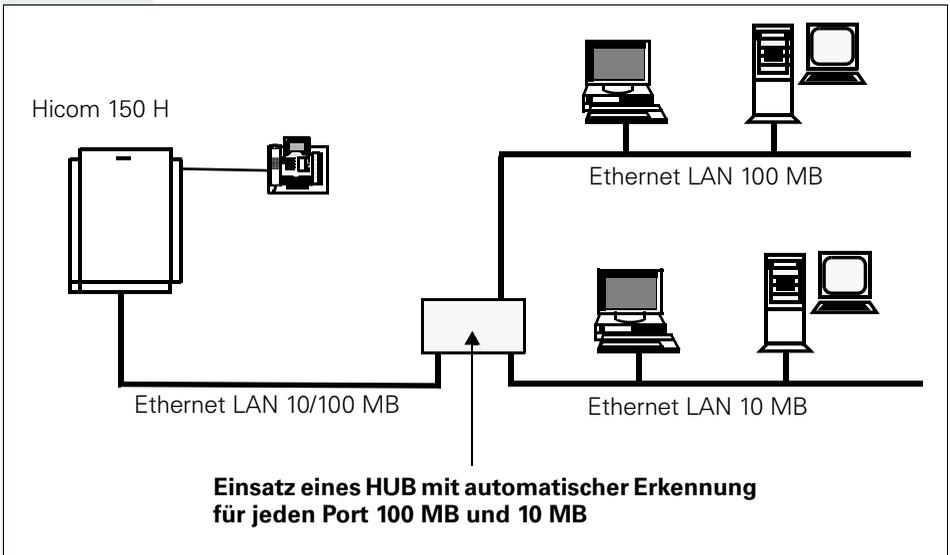
Vorteil:

- Einfache Verlängerung des BNC Netzwerk, z. B. 3COM OfficeConnect
- HUB TP 4 Combo (4xRJ-45, 1xAUI, 1xBNC, unmanaged hub)
- HUB 8/TPC (8xRJ-45, 1xBNC, unmanaged HUB)
- HUB TP16C (16xRJ-45, 1xBNC, unmanaged HUB)

3COM Dual Speed HUB

HiPath HG 1500 in 100 MB Netzwerken

Lösung 3COM Dual Speed HUB



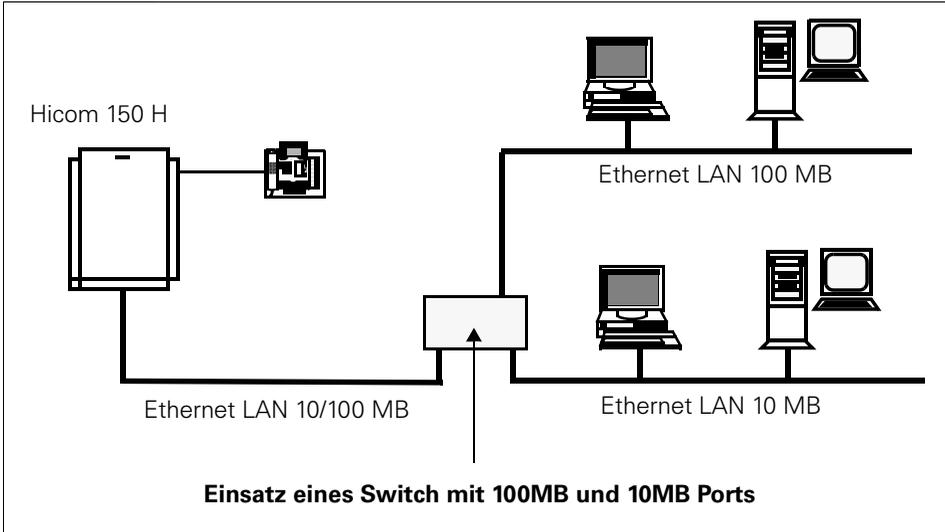
Beispiel: 3COM SuperStack II Dual Speed

- HUB 500 TP 12-Port (12 RJ-45, stackable, manageable)
- HUB 500 TP 24-Port (12 RJ-45, stackable, manageable)

Lösungsansatz mit Switch

HiPath HG 1500 in 100MB Netzwerken

Lösung mit Switch



Beispiel: Siemens HiNet

- WS 4100 (12 Port 10MB, 2 Port 100MB)
- WS 4400 (24 Port 10MB, 2 Port 100MB, managed)
- WS 4700 (24 Port Autosense 10/100MB)

oder 3COM OfficeConnect

- Switch 140M (4x10/100 BaseT, 1x100BASE-TX) DCF:3C16730-ME
- Switch 280 (8x10/100 BaseT, 2x100BASE-TX) DCF:3C16732-ME



Bei Verwendung von Voice over IP empfiehlt es sich generell, Switches einzusetzen, um die Störungen der Sprechverbindungen durch andere Datenlasten im LAN so gering wie möglich zu halten. Es wird empfohlen, Switches einzusetzen, die Quality of Service unterstützen: dadurch kann die nötige Priorisierung von Voicepaketen gegenüber den Daten gesichert werden, dies führt zu einer besseren Qualität der Sprechverbindungen, siehe → 90 QoS.

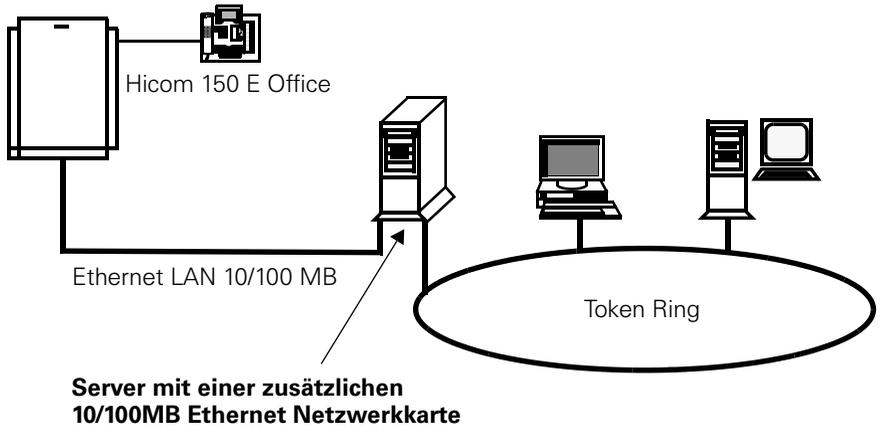
HiPath HG 1500 in Token Ring Netzwerken

Routing durch Netzwerksver (Token Ring > Ethernet 10/100 MB)

Einsatz einer zusätzlichen 10/100MB Ethernet Netzwerkkarte im Server.
(NT Server 3.51/ 4.0, Netware Server 3.12 / 4.X).

Lösung Token Ring Netzwerkkarte

TCP/IP und/oder IPX/SPX



Dienstprogramme zur Diagnose von TCP/IP

Um Fehler in einer TCP/IP Umgebung zu finden, die sich nicht auf eine einfache Ursache zurückführen lassen, stellt jedes Betriebssystem geeignete Werkzeuge zur Verfügung. Da jedes Betriebssystem seine eigenen Tools mit entsprechenden Parametern für die Befehle besitzt, sollen hier nur die wichtigsten Funktionen der Microsoft Betriebssysteme erläutert werden. Weitere Tools für auf UNIX basierende Betriebssysteme werden in der RFC 1147 ausführlich beschrieben. Spezielle Parameter können der Hilfe des jeweiligen Betriebssystems entnommen werden und in der Regel durch Eingabe von <Befehl> -? abgerufen werden.

ping

Das wohl am meisten benötigte Tool ist der PING-Befehl. Mit diesem Befehl kann überprüft werden, ob ein Rechner im Netzwerk erreichbar ist und somit mit ihm kommuniziert werden kann. Dabei wird dem Ziel-Rechner eine ICMP-ECHO-Meldung gesendet, die an den Absender zurückgeschickt wird. Gelangt die Antwort zum sendenden Rechner zurück, so ist eine Kommunikation mit dem angegebenen Rechner möglich. Die meisten Varianten des PING-Befehls geben Statistiken über die Verbindung aus.

Syntax für Windows 95/98/NT:

ping <Host> [<Parameter>]

- | | |
|--------------|--|
| <Host> | Enthält die Zieladresse oder den Host-Namen des Zielrechners |
| <Parameter> | |
| -t | Sendet ununterbrochen Testpakete zum Rechner. Normalerweise werden nur 4 Testpakete gesendet. |
| -a | IP-Adressen werden zu Host-Namen aufgelöst. |
| -n <Anzahl> | Sendet <Anzahl> Testpakete zum Rechner. |
| -l <Größe> | Sendet Testpakete mit <Größe> Bytes |
| -i <TTL> | Anzahl Router-HOPs die für ein Paket erlaubt sind. Der Zähler wird beim Sender auf einen Startwert gesetzt und von jedem Router der das Paket weiterreicht dekrementiert. |
| -w <Timeout> | Zeit in Millisekunden, in der auf eine Antwort gewartet wird. Läuft diese Zeit ab, so erscheint eine Timeout-Meldung. Standardmäßig steht dieser Wert auf 1000 (1s). Bei langsamen Verbindungen z. B. über Modem oder GSM ist es ratsam, diesen Wert auf 5000 (5s) bzw. 10000 (10s) zu setzen. Beträgt die Antwortzeit mehr als 1s erhält man Timeout-Meldungen, obwohl eine Verbindung möglich ist. |

Beispiel:

Verbindung zum lokalen Rechner überprüfen. Der eigene Rechner ist normalerweise unter der Loopback-Adresse „127.0.0.1“ und dem Namen „localhost“ zu erreichen.

```
C:\>ping localhost
PING wird ausgeführt für localhost [127.0.0.1] mit 32
Bytes Daten:
Antwort von 127.0.0.1: Bytes=32 Zeit<10ms TTL=128
```

Meldungen:

Sollte der entfernte Rechner nicht antworten, so kann man anhand der Meldungen auf den Fehler schließen.

- Ungültige IP-Adresse (unknown host):
Der Host-Name konnte nicht in eine gültige IP-Adresse umgewandelt werden. Diese Meldung entsteht, wenn der DNS-Server nicht erreicht werden kann oder ausgefallen ist. Diese Fehlermeldung tritt nur auf, wenn der Host mit einem Namen angesprochen wird.
- Ziel-Host nicht erreichbar (network unreachable):
Es existiert keine gültige Route zum Zielsystem. Die Ziel-Adresse konnte nicht erreicht werden, da ein Gateway ausgefallen ist oder auf dem lokalen Rechner nicht richtig angegeben ist.
- Zeitüberschreitung der Anforderung (Timeout):
Der Rechner verfügt über eine Route zum Zielrechner, aber bekommt keine Antwort. Die Meldung gelangt zwar zum Ziel-Host, kann aber nicht zurückgeschickt werden. Dieser Fehler ist auf ein fehlerhaftes Routing des Zielrechners zurückzuführen.

ipconfig

Einen schnellen Weg, die TCP/IP-Netzwerkconfiguration abzufragen, bietet das Programm „ipconfig.“ Damit lassen sich die IP-Adressen, Subnet-Masks, Gateways und Statistiken der Netzwerkkarten anzeigen. Weiterhin lassen sich über DHCP zugewiesene IP-Adressen freigeben bzw. erneuern.

Syntax für Windows 98/NT:

```
ipconfig [<Parameter>]
```

<Parameter>

- | | |
|--------------------|---|
| /all | Zeigt ausführliche Informationen der Netzwerkconfiguration an. Diese enthalten Host-Name, verwendete DNS-Server, MAC-Adressen der jeweiligen Netzwerkkarten und DHCP Informationen. |
| /release [Adapter] | Gibt die über DHCP zugewiesene IP-Adresse am Adapter frei. |
| /renew [Adapter] | Weist dem Adapter über DHCP eine neue IP-Adresse zu. |

Wird der Adapter bei den Parametern „release“ und „renew“ nicht angegeben, so werden alle IP-Adressen an allen über DHCP zugewiesenen Adaptern freigegeben oder neu zugewiesen.

Beispiel:

Abfrage der aktuellen Konfiguration in ausführlicher Form

```
C:\>ipconfig /all
```

```
Windows NT IP-Konfiguration
```

```
Host-Name .....: myhost.siemens.de
DNS-Server.....: 192.168.50.23
                  192.168.50.160
Knotentyp .....: Broadcast
NetBIOS-Bereichs-ID .....:
IP-Routing aktiviert.....: Nein
WINS-Proxy aktiviert.....: Nein
NetBIOS-Auswertung mit DNS: Ja
```

Ethernet-Adapter El90x2:

```

Beschreibung.....: 3Com 3C90x Ethernet
Adapter
Physische Adresse.....: 00-10-5A-DD-56-55
DHCP aktiviert.....: Nein
IP-Adresse.....: 192.168.129.1
Subnet Mask.....: 255.255.255.0
Standard-Gateway.....:

```

Ethernet-Adapter El90x1:

```

Beschreibung.....: 3Com 3C90x Ethernet
Adapter
Physische Adresse.....: 00-10-5A-37-26-B1
DHCP aktiviert.....: Ja
IP-Adresse.....: 192.168.14.6
Subnet Mask.....: 255.255.255.0
Standard-Gateway.....: 192.168.14.1
DHCP-Server.....: 192.168.11.103
Lease erhalten.....: Di., 17.08.1999
08:43:30
Lease läuft ab.....: Di., 19.01.2038
04:14:07

```

nslookup

Eine IP-Adresse kann durch einen Host-Namen zugeordnet werden. Diese Zuweisung von Namen und IP-Adresse wird im DNS-Server (DNS = Domain Name Server) hinterlegt. Mit dem Befehl „nslookup“ lassen sich die Daten abfragen, die für einen bestimmten Host im DNS-Server gespeichert sind. Durch Eingabe des Befehls „nslookup“ in der MSDOS-Eingabeaufforderung versucht sich das Programm mit dem im Netzwerk hinterlegten DNS-Server zu verbinden. Wird ein Name erfragt, so liefert dieser die zugehörige IP-Adresse zurück. Wird hingegen eine IP-Adresse erfragt, so wird der Host-Name zurückgeliefert. Ist die IP-Adresse oder der Host-Name nicht im DNS-Server hinterlegt, so gibt dieser eine dementsprechende Fehlermeldung aus.

Die Meldung „Ungültige IP-Adresse“ des Ping-Befehls sagt aus, dass der angegebene Host-Name nicht in eine IP-Adresse umgewandelt werden konnte. Dies geschieht, wenn der DNS-Server ausgefallen ist oder der Eintrag nicht existiert. Voraussetzung dabei ist, dass die DNS-Server in der Netzwerkkonfiguration eingetragen und über das Netzwerk ansprechbar sind.

Mit „nslookup“ können verschiedene Einträge (Records) des DNS-Servers abgefragt werden. Nachdem man das Programm gestartet hat, lassen sich durch folgende Einträge die dementsprechenden Daten abfragen.

```
set type=<Typ>
```

```
<Typ>
```

a	Adressen Einträge
any	Alle Einträge
mx	Mail Exchanger Einträge
ns	Name Server Einträge
soa	Start of Authority Einträge
hinfo	Host Info Einträge
axfr	Alle Einträge einer Zone
txt	Text Einträge

Syntax für Windows 98/NT:

```
nslookup <Host>
```

<Host>	Enthält die Zieladresse oder den Host-Namen des Zielrechners
--------	--

Beispiel:

```
C:\>nslookup localhost
Server: ns.domain.com
Address: 192.168.0.1
```

```
Name: localhost
Address : 127.0.0.1
```

Der Host „localhost“ besitzt die IP-Adresse „127.0.0.1“

hostname

Der Befehl „hostname“ gibt den Namen des lokalen Rechners zurück. Im Gegensatz zu anderen Betriebssystemen lässt sich bei Microsoft Betriebssystemen über diesen Befehl der Host-Name nicht verändern.

Beispiel:

```
C:\>hostname  
localhost
```

netstat

Der Befehl „netstat“ dient zum Überprüfen bestehender Verbindungen, eingerichteter Routen und liefert detaillierte Statistiken und Informationen der einzelnen Netzwerkschnittstellen zurück. Die neben der Routingtabelle am meisten benötigte Funktion von „netstat“ ist die Abfrage, welche Verbindungen auf dem lokalen Rechner existieren und in welchem Zustand sie sich befinden.

Syntax für Windows 95/98/NT:

```
netstat [<Parameter>] [<Intervall>]
```

<Parameter>

- a Zeigt alle Verbindungen an, d. h. Anwendungen, die auf eine Verbindung warten, werden ebenfalls angezeigt, z. B. ein Telnet Server.
- e Zeigt die Ethernet-Statistik an
- n Zeigt IP-Adressen anstatt Host-Namen an
- p <Proto> Zeigt Verbindungen an, die über das Protokoll <Proto> laufen
- r Zeigt die Routingtabelle an, die aber auch durch „route print“ angezeigt wird.
- s Zeigt Statistik nach Protokoll an

<Intervall> Wiederholt die Anzeige nach <Intervall> Sekunden

Beispiel:

Abfrage aller Verbindungen im IP-Adressen Format (verkürzt)

```
C:\>netstat -a -n
```

Aktive Verbindungen

Proto	Lokale Adresse	Remote-Adresse	Zustand
....			
....			
TCP	0.0.0.0:25	0.0.0.0:0	LISTENING
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING
....			
....			
TCP	192.168.129.3:110	192.168.129.1:1037	ESTABLISHED
TCP	192.168.129.3:23	192.168.129.2:1038	ESTABLISHED
TCP	192.168.129.3:1031	192.168.129.1:80	ESTABLISHED
....			
....			
UDP	0.0.0.0:25	*:*	
UDP	0.0.0.0:80	*:*	
....			

Mit Hilfe dieser Tabelle ist es möglich, IP-Verbindungen und deren Zustand anzuzeigen. Bevor auf dieses Beispiel näher eingegangen wird, sollen zunächst die Variablen kurz erläutert werden.

- <Proto> Gibt an, über welches Protokoll die Kommunikation abgewickelt wird. Dabei unterscheidet Windows nur zwischen den Protokollen TCP und UDP. Leider werden einige Server, die nur über ein einziges Protokoll laufen, sowohl als TCP- als auch als UDP-Server dargestellt. Aus diesem Grund lässt sich nicht eindeutig darauf schließen, welches Protokoll verwendet wird.
- <lokale Adresse> Gibt die eigene Adresse an, die eine Verbindung aufgebaut hat oder auf eine Verbindung wartet. Die lokale Adresse und die Remote Adresse werden im Format <IP-Adresse>:<Port-Nummer> dargestellt.
- <Remote Adresse> Gibt die entfernte Adresse an, die eine Verbindung aufgebaut hat oder mit der man sich verbunden hat.

<Zustand>

Zeigt den momentanen Zustand der Verbindungen an:

ESTABLISHED	Der lokale Rechner hat eine Verbindung mit einem Server aufgebaut. In diesem Fall ist der lokale Rechner ein Client.
LISTENING	Der lokale Rechner ist bereit eine Verbindung anzunehmen. In diesem Fall ist der lokale Rechner ein Server.
SYN_SENT	Der lokale Rechner signalisiert einem Server, dass er eine Verbindung aufbauen möchte.
SYN_RECEIVED	Der lokale Rechner, auf dem ein Server läuft, hat ein „SYN_SENT“ Signal erhalten, d. h. ein Client möchte mit ihm eine Verbindung aufbauen.
FIN_WAIT_1	Der lokale Rechner möchte die Verbindung mit einem Server beenden.
TIME_WAIT	Der lokale Rechner wartet auf die Bestätigung des Servers, die Verbindung zu beenden.
CLOSE_WAIT	Der lokale Rechner, auf dem ein Server läuft, hat ein „FIN_WAIT_1“ von einem Client erhalten, d. h. der Client möchte die Verbindung beenden.
FIN_WAIT_2	Der lokale Rechner hat die Bestätigung vom Server erhalten die Verbindung zu beenden.
LAST_ACK	Der Server hat die Bestätigung gesendet, dass die Verbindung beendet wird.
CLOSED	Der Server hat die Bestätigung des Clients erhalten, dass die Verbindung beendet wurde.

Ein Rechner kann gleichzeitig sowohl Server als auch Client sein. Dies ist z. B. der Fall, wenn sich der lokale Rechner mit seinem eigenen Server verbindet. Dies ist durch das Loopbackinterface „127.0.0.1“ möglich. Läuft z. B. ein Telnet Server auf dem lokalen Rechner, so kann durch den Befehl „telnet localhost“ eine Telnet Sitzung auf dem eigenen Rechner geöffnet werden.

Um festzustellen, welche Daten aus dem obigen Beispiel gewonnen werden können, soll dies nun schrittweise erklärt werden.

Proto	Lokale Adresse	Remote-Adresse	Zustand
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING
TCP	0.0.0.0:25	0.0.0.0:0	LISTENING

Die ersten beiden Einträge befinden sich im Zustand „LISTENING“, d. h. auf dem lokalen Rechner sind zwei Programme (Server) gestartet, die darauf warten, dass sich ein Client mit ihnen verbindet. Beide sind an die IP-Adresse „0.0.0.0“ gebunden. Diese IP-Adresse sagt aus, dass der Server an alle verfügbaren Netzwerkschnittstellen gebunden ist. Ist eine einzige Netzwerkkarte installiert, hat dieser schon zwei Schnittstellen, nämlich die lokale Netzwerkkarte (192.168.129.3) und die Loopbackschnittstelle „127.0.0.1“, die von Windows standardmäßig installiert wird. In diesem Beispiel laufen auf dem lokalen Rechner jeweils ein HTTP-Server (Port 80) und ein SMTP-Server (Port 25). Um festzustellen, ob die Netzwerkkarte richtig funktioniert, sollte man diese durch „anpingen“ vom lokalen Rechner aus testen, z. B. „ping 192.168.129.3“. Jede Fehlermeldung bei diesem Test stellt eine falsch konfigurierte Netzwerkschnittstelle dar. Möchte man z. B. die Verbindung zum lokalen HTTP-Server testen, so kann man dies einfach mit einem Web-Browser durch Eingabe der URL „http://127.0.0.1“ oder „http://192.168.129.3“ testen. Durch Eingabe von „telnet localhost 25“ oder „telnet 192.168.129.3 25“ ist es möglich, eine Verbindung zum lokalen SMTP-Server herzustellen. Dabei wird durch „25“ der Port, d. h. die Anwendung angegeben.

Die nächsten drei Einträge sind aktive Verbindungen. Diese können entweder vom lokalen Rechner zu einem Remote Rechner, oder von einem Remote Rechner zum lokalen Rechner aufgebaut worden sein.

Proto	Lokale Adresse	Remote-Adresse	Zustand
TCP	192.168.129.3:1037	192.168.129.1:110	ESTABLISHED
TCP	192.168.129.3:1038	192.168.129.2:23	ESTABLISHED
TCP	192.168.129.3:80	192.168.129.1:1039	ESTABLISHED

Damit man eine Unterscheidung zwischen ein- und ausgehenden Verbindungen treffen kann, benötigt man die Einträge, die sich im „LISTENING“-Zustand (Server) befinden. Dazu schaut man, ob der Port, der unter dem lokalen Rechner angegeben ist, selbst auf dem lokalen Rechner läuft. Die erste Zeile gibt den Port „1037“ aus. Dieser Port läuft nicht als Server (LISTENING) auf dem lokalen Rechner (192.168.129.3). Somit muss diese Verbindung vom lokalen Rechner an einen Remote Rechner (192.168.129.1) mit dem Port „110“ (POP3) angebunden sein. Mit anderen Worten holt sich der lokale Rechner gerade seine E-Mails bei einem POP3-Server ab.

Der zweite Eintrag muss auch eine ausgehende Verbindung sein, da sich dieser Port ebenfalls nicht im „LISTENING“-Zustand auf dem lokalen Rechner finden lässt. Der lokale Rechner hat also eine Verbindung mit dem Rechner „192.168.129.2“ und dem Port „23“ (Telnet) aufgebaut. Dies besagt, dass der lokale Rechner eine Telnet Sitzung auf dem Remote PC geöffnet hat.

Im dritten Eintrag passt der lokale Port „80“ (HTTP) mit dem eines Servers zusammen. Der Remote Rechner „192.168.129.1“ öffnet also gerade Webseiten auf dem lokalen Rechner.

nbtstat

Mit Hilfe dieses Dienstprogrammes ist es möglich, die Verbindungen, die das „NetBIOS over TCP/IP-Protokoll“ (WINS-Client(TCP/IP)) benutzen, zu überprüfen. Bei dem „NetBIOS over TCP/IP Protokoll“ wird ein NetBIOS-Paket in ein TCP/IP-Paket verpackt und auf der Gegenseite wieder ausgepackt. Dies wird benötigt, da NetBIOS nicht geroutet werden kann, so wie dies mit TCP/IP möglich ist. Da z. B. die Windows Laufwerksfreigaben nur über NetBIOS laufen, müssen diese in TCP/IP verpackt werden, um in andere physikalische Netze transportiert zu werden. Dazu legt sich Windows einen NetBIOS-Name-Cache an, der auch manuell angelegt werden kann. Dabei werden die IP-Adressen zum Rechnernamen in einer Tabelle aufgelöst. Diese Datei nennt sich „lmhosts“ und steht je nach Betriebssystem im System- oder in einem darunterliegenden Verzeichnis.

Win95/98: %systemroot%

WinNT: %systemroot%\system32\drivers\etc

Windows stellt in diesen Verzeichnissen diverse Beispieldateien bereit, die als Vorlage dienen und in denen der Aufbau der jeweiligen Beispieldatei erklärt ist. Diese Dateien haben die Endung „.sam.“ In diesem Fall heißt die Datei „lmhosts.sam.“ Sollte die Datei „lmhosts“ noch nicht existieren, so kann sie einfach nach „lmhosts“ kopiert und editiert werden.

Syntax für Windows 95/98/NT:

nbtstat [<Parameter>]

<Parameter>

- a <Host-Name> Liefert die Namenstabelle des unter <Host-Name> angegebenen Rechners zurück
- A<IP-Adresse> Liefert die Namenstabelle des unter <IP-Adresse> angegebenen Rechners zurück
- c Der NetBIOS-Name-Cache wird mit NetBIOS-Namen und zugehörigen IP-Adressen aufgelistet
- n Alle verwendeten lokalen NetBIOS-Namen werden aufgelistet
- R Löscht den NetBIOS-Name-Cache und lädt die Datei „LMHOST“ neu
- r Listet die Namensauswertung der Windows Netzwerke auf
- S Zeigt die Verbindungen von Client- und Server-Verbindungen in Form von IP-Adressen an.
- s Zeigt die Verbindungen von Client- und Server-Verbindungen an und löst die IP-Adressen in Namen auf.

route

Möchte man mehrere TCP/IP-Netzwerke miteinander verbinden, so muss man das Routing konfigurieren. Ohne das Routing-Verfahren käme man nicht über das lokale Netz hinaus. Beim Routing ist zu beachten, dass das Gateway, das das lokale Netzwerk mit anderen Netzwerken verbindet, nur im gleichen TCP/IP-Netzwerk liegen kann, in dem man sich selbst befindet.

Syntax für Windows 95/98/NT:

route <Befehl> <Ziel> <mask Subnet> <Gateway> [metric <Hops>] [<Parameter>]

<Befehl>

print	Zeigt die aktuelle Routing-Tabelle an
add	Fügt eine neue Route hinzu
delete	Löscht eine bestehende Route
change	Ändert eine bestehende Route

<Ziel> Gibt den Ziel-Host oder das Ziel-Netzwerk an, welches über das <Gateway> erreichbar ist.

<Subnet> Gibt die Subnet-Mask an.

<Gateway> Gibt die IP-Adresse des Gateways an, über das die unter <Ziel> angegebene IP-Adresse erreicht werden kann.

<Hops> Gibt die Anzahl von Gateways an, die zwischen Absender und Ziel der Daten liegen. Dieser Parameter ist nur relevant, wenn mehrere Routen zu einem Ziel existieren. Durch diesen Parameter können bestimmte Routen bevorzugt werden. Da in den meisten Fällen aber nur ein Gateway existiert, kann man hier den Wert „1“ setzen.

<Parameter>

-f	Löscht alle Routing-Einträge in der Routing-Tabelle
-p	Erstellt einen permanenten Eintrag. Dieser Parameter kann nur mit dem Befehl „add“ angegeben werden. Normalerweise werden die Routen über den „route“ Befehl nur statisch gesetzt, d. h. nach einem Neustart sind die gesetzten Routen nicht mehr vorhanden. Der Parameter „-p“ macht den Eintrag permanent und ist somit auch nach einem Neustart des Betriebssystems noch vorhanden.

Beispiel 1 :

Permanentes Einfügen einer Default Route

```
C:\cmd>route add 0.0.0.0 mask 0.0.0.0 192.168.0.199 -p
```

Beispiel 2:

Abfrage der Routingtabelle

```
C:\>route print
```

Aktive Routen:

Netzwerkadresse	Subnet-Mask	Gateway-Adresse	Schnittstelle	Anzahl
0.0.0.0	0.0.0.0	192.168.128.1	192.168.128.14	1
10.2.0.0	255.255.0.0	192.168.128.1	192.168.128.14	1
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.128.14	255.255.255.255	127.0.0.1	127.0.0.1	1
192.168.128.255	255.255.255.255	192.168.128.14	192.168.128.14	1
224.0.0.0	224.0.0.0	192.168.128.14	192.168.128.14	1
255.255.255.255	255.255.255.255	192.168.128.14	192.168.128.14	1

Bei den letzten beiden Einträgen handelt es sich um Multicast- bzw. Broadcast-Einträge, die hier aber nicht näher erläutert werden sollen.

tracert

Tracert (trace route) wird dazu benutzt, den Weg vom lokalen Rechner zum Ziel-Host zu verfolgen. Dabei gibt es alle Gateways aus, die auf dem Weg zum Ziel-Host passiert wurden.

Syntax für Windows 98/NT:

```
racert <Host> [<Parameter>]
```

<Host> Enthält die Zieladresse oder den Host-Namen des Zielrechners

<Parameter>

-d IP-Adressen werden nicht nach Namen aufgelöst

-h <Anzahl> Gibt die höchstmögliche Anzahl der Gateways bis zum Ziel-Host an

-j <Liste> Schlägt eine Route von zu passierenden Gateways vor

-w <Timeout> Wartet <Timeout> Millisekunden auf einen Antwort

Beispiel:

```
C:\cmd>tracert localhost
```

Verfolgung der Route zu localhost [127.0.0.1] über maximal 30 Abschnitte:

```
1 <10 ms <10 ms <10 ms localhost [127.0.0.1]
```

Route-Verfolgung beendet.

arp

Bevor ein Paket von einem Host zu einem anderen Host geschickt werden kann, muss erst die Hardware-Adresse (MAC-Adresse) der Netzwerkkarte des Ziel-Hosts bekannt sein. Zu diesem Zweck hält sich jeder Rechner, der über das TCP/IP-Protokoll kommuniziert, eine sog. ARP-Tabelle. „ARP“ (Address Resolution Protocol) dient zum Auflösen der IP-Adresse zur Hardware-Adresse (MAC-Adresse). Vor jedem Verbindungsaufbau wird die ARP-Tabelle durchsucht, ob sich der Ziel-Host darin befindet. Ist der Rechner nicht in der Tabelle zu finden, so wird ein ARP-Request mit der IP-Adresse des Ziel-Hosts über das Netzwerk geschickt. Empfängt der Ziel-Host diese Anforderung, schickt dieser seine Hardware-Adresse an den anfordernden Rechner zurück, der diese Hardware-Adresse wiederum in seine ARP-Tabelle einträgt. Bei der nächsten Verbindung ist die Hardware-Adresse des Ziel-Hosts bekannt und kann direkt übernommen werden. Wird eine Hardware-Adresse benötigt, die außerhalb des log. TCP/IP-Netztes liegt, so wird nur die Hardware-Adresse des Routers benötigt, über den der Ziel-Host erreicht werden kann.

Syntax für Windows 95/96/NT:

```
arp <Parameter>
```

```
<Parameter>
```

- a Zeigt die ARP-Tabelle an
- d Löscht einen Eintrag in der ARP-Tabelle
- s Fügt einen Host-Eintrag der ARP-Tabelle hinzu

Beispiel 1:

Eintrag einer neuen MAC-Adresse in die ARP-Tabelle

```
C:\>arp -s 192.168.0.199 02-60-8c-f1-3e-6b
```

Beispiel 2:

Abfrage der ARP-Tabelle

```
C:\>arp -a
```

```
Schnittstelle: 192.168.0.1 on Interface 1
```

Internet-Adresse	Physische Adresse	Typ
192.168.0.1	00-00-5a-42-66-60	dynamisch
192.168.0.10	00-60-70-cd-59-22	dynamisch
192.168.0.199	02-60-8c-f1-3e-6b	statisch

telnet

Telnet ermöglicht dem Benutzer, sich auf einem fremden Rechner einzuloggen. Dabei benutzt das Programm standardmäßig den Port „23.“Möchte man sich zu einem Rechner mit einem anderen Port einloggen, so muss man zusätzlich die Portnummer angeben.

Syntax für Windows 95/96/NT:

```
telnet [<Host> [<Port>]
```

<Host>	Enthält die Zieladresse oder den Host-Namen des Zielrechners
<Port>	Portnummer, die die Anwendung auf dem Zielrechner identifiziert

Beispiel:

```
C:\>telnet localhost 110
```

IP-Adressierung: Subnetze

Um der Verknappung von offiziellen IP-Adressen entgegenzuwirken und um ein IP-Netzwerk in voneinander getrennte Teilnetze zu splitten, bietet sich das Verfahren des „Subnetting“ an.

Bezogen auf die Zuteilung von offiziellen IP-Adressen bietet das Subnetting beispielsweise die Möglichkeit, mit einer vorhandenen Class A, B, C-Netzwerkadresse weitere eigenständige IP-Netzwerke zu generieren.

Bei den Netzwerken hat man sich auf verschiedene Klassen und Standardnetzwerkmasken geeinigt:

Class	Subnet Mask
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Das Aufsplitten in eigenständige Subnetze bietet zudem den entscheidenden Vorteil, dass der lokale Verkehr eines Netzes in den jeweiligen Subnetzen verbleibt. Der Zugriff auf fremde Netze muss über einen Router erfolgen.

Die grundlegende Funktionsweise des Subnetting ist denkbar einfach und basiert auf der sogenannten „Subnet-Mask.“Über diese Maske werden die Bits definiert, die innerhalb einer IP-Adresse den Netzwerk- bzw. Hostteil repräsentieren. Gesetzte Bits (1) geben den Netzwerkanteil an, während gelöschte Bits (0) den Hostanteil angeben.

Um eine Subnet-Mask besser analysieren zu können, betrachtet man diese besser im Binärformat. Als Beispiel soll die Class C Standardnetzwerkmaske „255.255.255.0“ dienen.

	Netzwerk			Host
Bytes	1. Byte	2. Byte	3. Byte	4. Byte
Subnet-Mask	255	255	255	0
Binärformat	1111 1111	1111 1111	1111 1111	0000 0000

Bei der Subnetmask „255.255.255.0“ geben die ersten 3 Bytes den Netzwerkanteil (alle Bits 1) und das letzte Byte den Hostanteil (alle Bits 0) an.

Anhand dieser Subnet-Mask entscheidet ein Host (Router, Workstation o.ä.), ob eine angesprochene IP-Adresse im eigenen Netz liegt oder nicht. Liegt der Ziel-Host nicht im gleichen Netzwerk, so werden Pakete an diese Adresse über entsprechend hinterlegte Routing-Mechanismen weitergeleitet.

Um Subnetze zu erstellen, die auf die jeweiligen Bedürfnisse zugeschnitten sind, muss vorher abgeklärt werden, wie viele Subnetze in einem klassenbasierten Netzwerk (Class A, B, C) gebildet werden sollen. Wird ein Netz aufgeteilt, entstehen immer 2^n Subnetze. Dieses soll anhand eines Beispiels näher erläutert werden.

Das Class C Netzwerk „192.168.1.0“ soll in 4 Subnetze geteilt werden. Standardmäßig hat ein Class C Netzwerk die Subnet-Mask „255.255.255.0.“ Um im binären System 4 verschiedene Kombinationen zu erhalten, benötigt man 2 Bits. Nachfolgende Tabelle zeigt die Abhängigkeit der Bitanzahl zur Anzahl der Netze.

Bits	Kombinationen	Bits	Kombinationen
1	$2^1 = 2$	17	$2^{17} = 131072$
2	$2^2 = 4$	18	$2^{18} = 262144$
3	$2^3 = 8$	19	$2^{19} = 524288$
4	$2^4 = 16$	20	$2^{20} = 1048576$
5	$2^5 = 32$	21	$2^{21} = 2097152$
6	$2^6 = 64$	22	$2^{22} = 4194304$
7	$2^7 = 128$	23	$2^{23} = 8388608$
8	$2^8 = 256$	24	$2^{24} = 16777216$
9	$2^9 = 512$	25	$2^{25} = 33554432$
10	$2^{10} = 1024$	26	$2^{26} = 67108864$
11	$2^{11} = 2048$	27	$2^{27} = 134217728$
12	$2^{12} = 4096$	28	$2^{28} = 268435456$
13	$2^{13} = 8192$	29	$2^{29} = 536870912$
14	$2^{14} = 16384$	30	$2^{30} = 1073741824$
15	$2^{15} = 32768$	31	$2^{31} = 2147483648$
16	$2^{16} = 65536$	32	$2^{32} = 4294967296$

Damit keine Lücken in den Adressbereichen entstehen, fügt man den bereits existierenden Einsen der Subnet-Mask von links nach rechts weitere Einsen hinzu.

Class C	Netzwerk			Host	
Bytes	1. Byte	2. Byte	3. Byte	4. Byte	
Subnet-Mask	255	255	255	0	
Binärformat	1111 1111	1111 1111	1111 1111	0000 0000	
Neu	Netzwerk			Host	
Bytes	1. Byte	2. Byte	3. Byte	4. Byte	
Binärformat	1111 1111	1111 1111	1111 1111	11	00 0000
Subnet-Mask	255	255	255	192	

Rechnet man das neu entstandene Subnetz vom Binärsystem in das Dezimalsystem um, so erhält man die Subnet-Mask „255.255.255.192.“ Für den Netzwerkanteil stehen jetzt 26 Bits und für den Hostanteil 6 Bits zur Verfügung. Rechner, deren Netzwerkanteil gleiche Bitmuster aufweisen, können in einem physikalischen Netzwerk direkt miteinander kommunizieren. Jedes andere Netzwerk kann nur über ein Gateway erreicht werden. Betrachtet man das veränderte 4. Byte mit den beiden neuen Netzwerkbits 25 und 26, so kann man jetzt die neu entstandenen Subnetze berechnen.

4. Byte	Dezimal	Neue Netzwerke	Broadcast Adresse	Hostadressen
<u>00</u> 00 0000	0	192.168.1.0	192.168.1.63	1 - 62
<u>01</u> 00 0000	64	192.168.1.64	192.168.1.127	65 - 126
<u>10</u> 00 0000	128	192.168.1.128	192.168.1.191	129 - 190
<u>11</u> 00 0000	192	192.168.1.192	192.168.1.255	193 - 254

Das eigentliche Subnetting besteht also darin, dass eine Erweiterung des Netzwerkteils einer IP-Adresse erfolgt, indem der Hostanteil entsprechend verkürzt wird. Die Anzahl der zur Verfügung stehenden Subnetze und Hosts ergeben sich durch folgende Bedingungen:

Die Anzahl der verfügbaren Host-Adressen ist weitgehend von der Länge des Hostteils der IP-Adresse abhängig. Ein 6 Bit-Hostanteil stellt – rein rechnerisch – 64 Adressen zur Verfügung. Da aber zu jedem IP-Netzwerk, also auch für ein einzelnes Subnetz, zwei reservierte Adressen gehören, verringert sich die max. Anzahl um 2 Adressen. Es handelt sich dabei um die Host-Adressen, die nur Nullen oder nur Einsen enthalten. Erstere wird für die Adressierung eines Netzwerkes verwendet, während letztere für Broadcasts im jeweiligen Netz genutzt wird.

Wie oben erwähnt werden die neuen Bits des Netzwerkanteils von links nach rechts an die bereits vorhandenen Bits angefügt. Nachfolgend soll gezeigt werden, warum dies so ist. Benutzt man z. B. die Subnet-Mask „255.255.255.3“ für das Netzwerk „192.168.1.0,“ so liegt der Hostanteil inmitten des Netzwerkanteils.

Bytes	Netzwerk			Host	Netzwerk
	1. Byte	2. Byte	3. Byte	4. Byte	
Subnet-Mask	255	255	255	3	
Binärformat	1111 1111	1111 1111	1111 1111	0000 00	<u>11</u>

Mit diesem Subnet erhält man keine zusammenhängenden IP-Adressbereiche, da sich nur die Hosts in einem Netzwerk befinden, die die letzten beiden Bits gesetzt haben. Die sich daraus ergebenden Adressen sind in der nachfolgenden Tabelle aufgeführt.

4. Byte	Dezimal	Neue Netzwerke	Broadcast Adresse	Hostadressen
0000 00 <u>00</u>	0	192.168.1.0	192.168.1.252	4,8,12,16,20,...,248
0000 00 <u>01</u>	1	192.168.1.1	192.168.1.253	5,9,13,17,21,...,249
0000 00 <u>10</u>	2	192.168.1.2	192.168.1.254	6,10,14,18,22,...,250
0000 00 <u>11</u>	3	192.168.1.3	192.168.1.255	7,11,12,19,23,...,251

Aus den Hostadressen kann man ersehen, dass die einzelnen Hosts nicht in zusammenhängenden Bereichen liegen. Diese Art von Subnetting macht die Administration sehr unübersichtlich! Aus diesem Grund sollte diese Art von Subnetting nicht verwendet werden.

Bisher wurde gezeigt, wie man Subnetze bildet. Nachfolgend wird erläutert, wie man die IP-Adressen von Rechnern den jeweiligen Subnetzen zuordnet.

Die folgende Tabelle zeigt 4 IP-Adressen eines Netzwerkes (Class C) und ihre Verbindung zur verwendeten Subnet-Mask „255.255.255.224.“

	Netzwerk	Host
255.255.255.224	11111111.11111111.11111111.111	00000
193.98.44.33	11000001.01100010.00101100.001	00001
193.98.44.101	11000001.01100010.00101100.011	00101
193.98.44.129	11000001.01100010.00101100.100	00001
193.98.44.61	11000001.01100010.00101100.001	11101

Die binäre Darstellung der Maske und Adressen zeigt recht deutlich, welchem Subnetz die jeweiligen IP-Adressen angehören: Adresse 1 und 4 sind im Subnetz „.32“ (00100000), Adresse 2 gehört dem Subnetz „.96“ (01100000) an und Adresse 3 befindet sich in Subnetz „.128“ (10000000).

Legt man für das Beispiel die übliche Standard-Maske „255.255.255.0“ eines Class C-Netzwerkes zugrunde, so würde die Länge des Netzwerkteils 24 Bit betragen, der Hostteil hätte eine Länge von 8 Bit. Durch die Subnet-Maske „255.255.255.224“ ist der Netzwerkteil einer IP-Adresse im Netz genau 27 Bit lang, der Hostteil umfasst dementsprechend nur noch 5 Bit.

Als Referenz sind in der nachfolgenden Übersicht die meistgenutzten Masken der Class C mit den zugehörigen Netz- und Hostverteilungen aufgeführt.

Subnet Mask	Anzahl der Netze	Hosts pro Subnet	Subnet	Broadcast Adresse	Hosts
255.255.255.0	1	253	0	255	1 – 254
255.255.255.128	2	126	0	127	1 – 126
			128	255	129 – 254
255.255.255.192	4	62	0	63	1 – 62
			64	127	65 – 126
			128	191	129 – 190
			192	255	193 – 254
255.255.255.224	8	30	0	31	1 – 30
			32	63	33 – 62
			64	95	65 – 94
			96	127	97 – 126
			128	159	129 – 158
			160	191	161 – 190
			192	223	193 – 222
			224	255	225 – 254
255.255.255.240	16	16	0	15	1 – 14
			16	31	17 – 30
			32	47	33 – 46
			48	63	47 – 62
			64	79	65 – 78
			80	95	81 – 94
			96	111	97 – 110
			112	127	113 – 126
			128	143	129 – 142
			144	159	145 – 158
			160	175	161 – 174
			176	191	177 – 190
			192	207	193 – 206
			208	223	209 – 222
			224	239	225 – 238
			240	255	241 – 254

Beispiel:

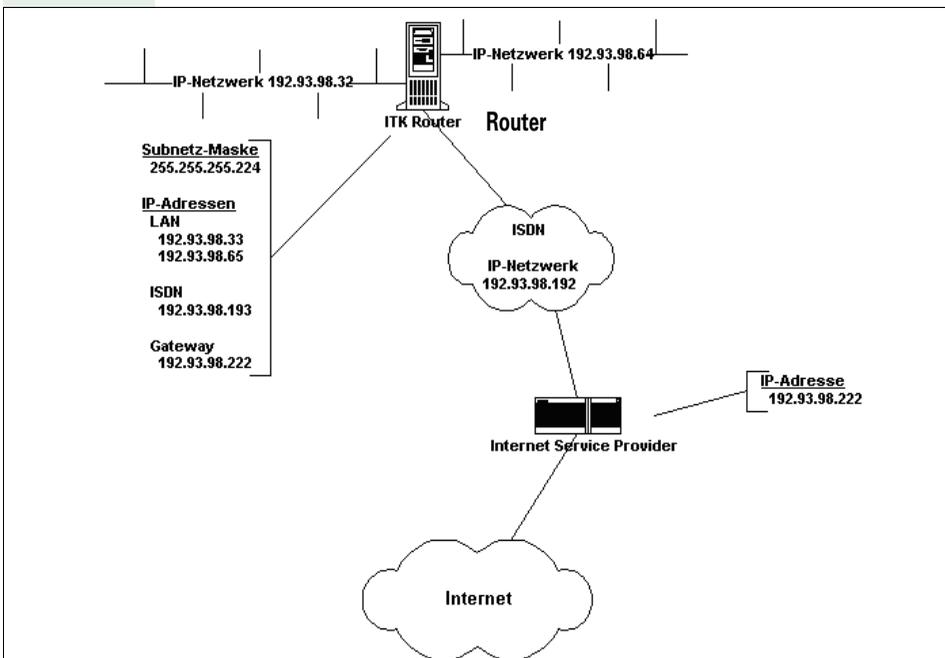
Ein LAN mit zwei Ethernet-Netzwerken soll über einen ISDN-Zugang an das Internet angeschlossen werden. Alle Stationen im lokalen Ethernet sollen Zugriff auf das Internet haben und auch aus dem Internet heraus direkt erreichbar sein. Legt man entsprechende Strukturen einer Class C-Adresse zugrunde, so müsste normalerweise für beide Ethernet-Netzwerke und für das ISDN-Netzwerk je ein komplettes Class C-Netzwerk zur Verfügung gestellt werden. Da in einem Thin Ethernet-Segment die maximale Anzahl der Stationen allerdings auf 30 begrenzt ist, wären schon dort allein 223 Host-Adressen pro Netzwerk verloren.

Genau hier setzt das Subnetting an: Durch die Verwendung einer entsprechenden Subnet-Maske kann mit nur einem Class C-Netzwerk eine vollständige Anbindung des LANs erreicht werden, und zwar ohne die erwähnte Verschwendung von Host-Adressen.

Zu diesem Zweck stellt ein Internet Service Provider ein Class C-Netzwerk mit folgenden Grunddaten zur Verfügung:

IP-Adresse Provider:	192.93.98.222
IP-Adresse Gateway:	192.93.98.222
IP-Adresse Netzwerke:	192.93.98.0
Subnetz-Maske:	255.255.255.0

Die nachfolgende Zeichnung gibt eine entsprechende Konfiguration wieder:



Als Subnetz-Maske bietet sich „255.255.255.224“ an, da diese Maske 8 Subnetze mit je 30 Hosts bereitstellt. Die Anzahl der Hosts in jedem Subnetz deckt sich also mit der maximalen Anzahl von Stationen in einem Ethernet-Segment.

Aus der Darstellung ist ersichtlich, dass zwei Subnetze, hier „192.93.98.32“ und „192.93.98.64,“ den beiden LAN-Baugruppen des ITK Router zugewiesen wurden. Eine der beiden LAN-Baugruppen erhält die IP-Adresse „192.93.98.33“ und die andere „192.93.98.65.“Somit können über jede Baugruppe jeweils 29 weitere Stationen mit IP-Adressen versorgt werden.

Dem ISDN (WANODI oder Virtual Ethernet) wurde die IP-Adresse „192.93.98.193“ aus dem Subnetz „192.93.98.192“ zugeordnet. Als Default-Gateway wird in diesem Fall die IP-Adresse des Provider-Zugangs verwendet. Dies stellt sicher, dass alle Pakete, die an Netze gehen, welche sich nicht in den lokalen Subnetzen des LANs befinden, an den Provider weitergeleitet werden.

Portnummern

Portnummern auf der HG 1500

client/server	Protocol	Server	Client	Anwendung
H.323 (H.225/ Q931)	TCP	1720	kurzlebig (ephemeral)	Voice over IP für Systemclients, H.323 Clients, AllServe- und IP-Networking
RTP/RTCP	UDP	29100...29131	kurzlebig (ephemeral) ^a	
H.245	TCP	kurzlebig (ephemeral) ^b 12100...12115 ^c	kurzlebig (ephemeral) ^d	
Gatekeeper-Registration	UDP		1719	Bei Einsatz eines Gatekeeper
VOPTSET	TCP	4060		System Client
NetworkUnit	TCP	12050	12050	AllServe-, IP-Networking
DataGateway	TCP	8765	8765	AllServe-, IP-Networking
ADMIN	TCP	12000		Administration
VCAPI	TCP	12001		VCAPI
Accounting Server	TCP	13042		IP-Accounting
SNMP (Get/Set)	UDP	161		SNMP-Browser, HiPath FM
SNMP (Traps)	UDP		162	
DSL-Diagnose Server	UDP	12200		DSL-Statusanzeige
Registration	TCP		12061	AllServe - Vernetzung
CallAddressResolution	TCP	12062	12062	
TFTP	UDP	69	69	APS-Transfer mit TFTP

a. wird durch den Partner festgelegt (1024 ... 5000)

b. Bis HG1500 V2.0: ephemeral (1024 ... 5000)

c. Ab HG1500 V2.0: höchste Portnummer wird durch die Anzahl der lizenzierten B-Kanäle bestimmt

d. wird durch den Partner festgelegt (1024 ... 5000)

Portnummern auf dem Allserve Server

client/server	Protocol	Server	Client	Anwendung
ADM	TCP		7000	AllServe - Vernetzung

SYNC	TCP		7024	
FCT	TCP		7100	
CAR_Server	TCP	12062		
REG_Server	TCP	12061		
SNMP (Get/Set)	UDP	161		SNMP-Browser, HiPath FM
SNMP (Traps)	UDP		162	

Portnummern in Hicom

client/server	Protocol	Server	Client	Anwendung
TFTP	UDP	69	69	APS-Transfer mit TFTP, Allserve - Vernetzung
ADM	TCP	7000		Allserve - Vernet- zung
SYNC	TCP	7024		
FCT	TCP	7100		
SNMP (Get/Set)	UDP	161		SNMP-Browser, HiPath FM
SNMP (Traps)	UDP		162	

Ungewollter Verbindungsaufbau ins Internet (DNS-Anfragen)

Sollten von der LAN-Baugruppe ohne ersichtlichen Grund Internetverbindungen aufgebaut werden, oder bereits bestehende Verbindungen nicht automatisch in den Short Hold-Zustand gehen, so liegt das meist an den sog. DNS-Anfragen, die vom PC im LAN ins Internet gesendet werden. Für diesen PC muss dann, um die DNS-Anfragen zu unterbinden, in der auf dem PC befindlichen Host/Lmhost-Datei der entsprechende Eintrag zur Namensauflösung vorgenommen werden, so dass alle weiteren DNS-Anfragen lokal auf dem Rechner beantwortet werden können. Somit wird keine Verbindung ins Internet aufgebaut, ohne dass der Benutzer es initiiert (z. B. durch Start des Browsers). Dieses Problem ist ebenfalls mit anderen handelsüblichen Routern (z. B. 3COM) zu beobachten. Es handelt sich um ein Protokoll-konformes Verhalten, das durch entsprechende Analyse und Konfiguration des Netzwerks/PC aufgehoben werden kann.

Um zu ermitteln, welcher PC für ständige Einwahl ins Internet verantwortlich ist, kann der Kundentrace benutzt werden. Hierzu wird die Tracegruppe 112 (Kundentrace PPP) aktiviert (Wert 4) und der Kundentrace gelöscht. Nach einem beobachteten Einwahlversuch ins Internet stehen im Kundentrace dann Informationen zu der IP-Adresse, die zum Routing geführt hat, sowie TCP/UDP-Portnummern bzw. DNS-Anfragen im Klartext. Daraus kann jetzt der PC bestimmt werden, der für die ständige Einwahl verantwortlich ist und der Dienst (dPort), der angefordert wird.

Sollte die Anfrage tatsächlich eine DNS-Anfrage gewesen sein, so empfiehlt sich folgendes Vorgehen:

Durch die Ermittlung der Absender-IP-Adresse steht der PC fest, der diese Anfragen aus dem LAN sendet. Für diesen PC muss dann der Eintrag in die eigenen Hosts/Lmhosts vorgenommen werden. Der Eintrag in die Hosts/Lmhosts muss den in der Namensanfrage enthaltenen Namen (ebenfalls im Trace) und die damit verbundene IP-Adresse (durch den LAN-Administrator zu ermitteln) beinhalten.

Beispiel:

Eine im LAN installierte Software benutzt einen an den Server angeschlossenen Dongle. Wird die Client-SW auf einem PC gestartet, so wird die Lizenz der SW anhand des Dongles ermittelt. Dafür sendet die Client-SW eine Namensanfrage ins Netz, da Ihr nur der Name des Dongles bekannt ist. Da der Client-PC einen DNS-Eintrag zur Namensauflösung u.a. für den Internetzugang besitzt, sendet er natürlich auch diese Namensanfrage direkt ins Internet. Somit stellt sich hier ebenfalls das o.g. Problem dar. Zur Behebung des Problems wurde hierbei in die Hosts/Lmhosts des Client-PCs die IP-Adresse des Servers (auf dem der Dongle steckte) und der Donglename eingetragen. Damit wurden weiterhin keine automatischen Internetzugänge verursacht. Nach TCP/IP- und Namensauflösungsregeln wird immer zuerst der Name in der Hosts/Lmhosts gesucht. Sollte der Eintrag dort nicht zu finden sein, so wird eine DNS-Anfrage an den konfigurierten DNS weitergeleitet. Als Vorsichtsmaßnahme soll auf jeden Fall die IP-Firewall in der LAN-Baugruppe eingeschaltet werden und die IP-Adresse des PCs, der ins Internet darf, soll nur für die benötigten ISDN Interfaces

freigeschaltet werden. Jetzt kann zum Beispiel der NT Server des Kunden, der nicht in der Firewall eingetragen ist, DNS-Anfragen stellen. Diese werden aber nicht ins Internet geleitet, da die Berechtigung fehlt.

Kunden-Trace

Der Kunden-Trace dient zur weiterführenden Diagnostik der HiPath HG 1500 und liefert detaillierte Informationen, die zur Behebung evtl. aufgetretener Fehler ausgewertet werden können.

Der Kunden-Trace kann also Konfigurationsfehler während der Inbetriebnahme der HiPath HG 1500 aufzeigen und ist nur zur Fehleranalyse zu aktivieren (ansonsten Performance-Verlust).

Protokollierungsfunktion

Aus Datenschutzgründen ist es erforderlich, alle Änderungen, die an einer Kundenanlage lokal oder Remote vorgenommen worden sind, zu protokollieren. Damit wird dem Kunden auf Anforderung die Möglichkeit gegeben, die Änderungen in seiner Anlage nachzuweisen.

Beim Zurückspielen eines KDS auf die HiPath HG 1500 wird zusätzlich ein Datensatz über die geänderten Daten auf die Baugruppe geladen und dort resetfest und nicht löschtbar gespeichert. Dieser Speicher umfasst mindestens 64kB. Dieser Speicher kann über den Menüpunkt „Datei->Übertragen der Log-Datei zum PC“ ausgelesen und in eine Datei gespeichert werden.

ETSI-Fehlermeldungen

Die folgende Tabelle dient Ihnen zur Auswertung der Fehlercodes aus dem Trace. Sie benötigen dazu die vom Tracer ausgegebene Fehlermeldungsnummer und suchen diese in der Tabelle auf. In der rechten Spalte finden Sie dann den Klartext zu dem ausgegebenen Fehlercode.

Da der ausgegebene Wert je nach Trace (Applikationen, Hicom, HiPath HG 1500) in Dezimal oder in Hexadezimal formatiert ist, erscheinen in der Tabelle drei Werte. Die Werte mit dem Offset werden von der Gegenseite geschickt.

dez	Wert		ETSI CAUSE (Network delivered)
	hex	hex mit Off-set 80h	
1	1	81	UNASSIGNED (UNALLOCATED) NUMBER
2	2	82	NO ROUTE TO SPECIFIED TRANSIT NETWORK
3	3	83	NO ROUTE TO SPECIFIED TRANSIT DESTINATION
6	6	86	CHANNEL UNACCEPTABLE
7	7	87	CALL AWARDED IN ESTABLISHED CHANNEL
16	10	90	NORMAL CALL CLEARING
17	11	91	USER BUSY
18	12	92	NO USER RESPONDING
19	13	93	ALERTING – NO ANSWER FROM USER
21	15	95	CALL REJECTED
22	16	96	NUMBER CHANGED
26	1A	9A	NON SELECTED USER CLEARING
27	1B	9B	DESTINATION OUT OF ORDER
28	1C	9C	INVALID NUMBER FORMAT (INCOMPLETE NUMBER)
29	1D	9D	FACILITY REJECTED
30	1E	9E	RESPONSE TO STATUS ENQUIRY
31	1F	9F	NORMAL; UNSPECIFIED
34	22	A2	NO CHANNEL AVAILABLE
38	26	A6	NETWORK OUT OF ORDER
41	29	A9	TEMPORARY FAILURE
42	2A	AA	SWITCHING EQUIPMENT CONGESTION
43	2B	AB	ACCESS INFO DISCARDED
44	2C	AC	REQUESTED CHANNEL NOT AVAILABLE
47	2F	AF	RESOURCES UNAVAILABLE
49	31	B1	QUAL OF SERVICE UNAVAILABLE
50	32	B2	REQUESTED FACILITY NOT SUBSCRIBED
57	39	B9	BEARER CAPABILITY NOT AUTHORIZED
58	3A	BA	BEARER CAPABILITY NOT AVAILABLE

dez	Wert		ETSI CAUSE (Network delivered)
	hex	hex mit Off- set 80h	
63	3F	BF	SERVICE NOT AVAILABLE
65	41	C1	BEARER CAPABILITY NOT IMPLEMENTED
66	42	C2	CHANNEL TYPE NOT IMPLEMENTED
69	45	C5	REQUESTED FACILITY NOT IMPLEMENTED
70	46	C6	ONLY RESTRICTED DIGITAL INFO
79	4F	CF	SERVICE NOT IMPLEMENTED
81	51	D1	INVALID CALL REFERENCE VALUE
82	52	D2	IDENT CHANNEL NOT EXIST
83	53	D3	CALL IDENT NOT EXIST
84	54	D4	CALL IDENT IN USE
85	55	D5	NO CALL SUSPENDED
86	56	D6	CALL ID IS CLEARED
88	58	D8	INCOMPATIBLE DESTINATION
91	5B	DB	INVALID TRANSIT NETWORK
95	5F	DF	INVALID MESSAGE; UNSPECIFIED
96	60	E0	MANDATORY INFORMATION ELEMENT IS MISSING
97	61	E1	INVALID MESSAGE
98	62	E2	MESSAGE NOT EXISTENT
99	63	E3	BAD INFOELEMENT
100	64	E4	BAD INFOELEMENT CONTENTS
101	65	E5	MESSAGE NOT COMPATIBLE CALL ST
102	66	E6	RECOVERY ON TIMER EXPIRY
111	6F	EF	ETSI PROTOCOL ERROR
127	7F	FF	INTERWORKING NOT SPECIFIED

PC- Soundeinstellungen für Voice over IP

Mit der Möglichkeit, mit Voice over IP über Netzwerke und PC zu telefonieren, sind eine Vielzahl von Konfigurationen speziell bei den Soundkarten der PC's zu beachten. Fehler, wie schlechte Sprachqualität und einseitige oder fehlende Gesprächsverbindungen, sind oft mit Veränderung von Einstellungen zu beheben. In dem folgenden Kapitel sind einige Lösungsvorschläge beschrieben, die bei der Einrichtung eines Voice-Clients helfen sollen. Diese Hilfe ist allgemein gehalten, da diese Einstellungen von der Hard- und Software und von der Umgebung, in der sich der PC befindet, abhängig sind. Eine detaillierte Beschreibung ist zu umfangreich, und deshalb unübersichtlich.

Desweiteren sind verminderte Sprachqualität nicht immer ein Zeichen von Konfigurationsfehlern oder Hard- und Softwarefehlern. z. B. Knackgeräusche, d. h. kurze Unterbrechungen (verloren gegangene Sprachpakete), können auch ein Zeichen zu hoher LAN-Last sein. Durch Umstrukturierung des LAN, Umstellung auf 100BaseT oder der Einsatz von Switches kann die Qualität der Voice over IP- Verbindung verbessert werden. Wird der Audiostandard G.711 (64 kbit/s) anstelle von G.723 (5 kbit/s) verwendet, erzeugt das eine weitaus höhere LAN- Last. Bei wenigen aktiven Voice-Applikationen wird G.711 keine spürbaren LAN-Lasten verursachen. Wird aber Voice over IP intensiv genutzt, bei Hicom Office PRO bis zu 48 gleichzeitig möglichen Sprachverbindungen, kann das bei schon ausgelasteten LAN's zur Verschlechterung der Sprachqualität führen.

Konfigurationsmöglichkeiten

1. Gleichzeitiges Sprechen und Hören nicht möglich
 - Soundkartentreiber ist nicht vollduplexfähig, es muss ein Update installiert werden, damit die Karte vollduplexfähig wird
 - Falsche Konfiguration der Voice- Applikation, vollduplex in der Software aktivieren
2. Vollduplexfähigkeit des Soundkartentreibers kann mit Netmeeting getestet werden. Unter Optionen / Audio besteht die Möglichkeit, vollduplex zu aktivieren/deaktivieren. Ist dieser Punkt nicht veränderbar, muss ein vollduplex-fähiger Treiber für die Soundkarte installiert werden.
3. Einseitige Sprechverbindungen
 - vollduplex aktiviert
 - Mikrofon angeschlossen
 - Mikrofon bei der Voiceapplikation aktiviert
 - Einstellung der Lautstärkereglung im PC überprüfen, unter Aufnahme „Mikrofon“ aktivieren
 - Voicegateway in der HiPath HG 1500 falsch oder fehlt

4. Man hört sich selbst direkt oder verzögert
 - Einstellung der Lautstärkereglung im PC überprüfen, unter Wiedergabe „Microfon“ deaktivieren und unter Aufnahme „Wave“ deaktivieren
5. Gesprächspartner hört mich nur sehr leise
 - Einstellung der Lautstärkereglung im PC oder der Voice-applikation überprüfen, Lautstärke erhöhen
 - wenn vorhanden, Microfon-Booster in der Lautstärkereglung / Wiedergabe / erweiterte Einstellungen für Microfon aktivieren
6. Gesprächspartner hört laute Nebengeräusche (übersteuern)
 - wenn vorhanden, Microfon-Booster in der Lautstärkereglung / Wiedergabe / erweiterte Einstellungen für Mikrofon deaktivieren
 - Empfindlichkeit des Mikrofons in der Voice-Applikation verändern, z. B. bei Netmeeting unter Optionen / Audio Microfon „Manuell einstellen“ aktivieren und Empfindlichkeit verändern
 - Aufnahmelautstärke verändern, z. B. bei Netmeeting unter Optionen / Audio den Audioassistenten starten
 - Audio- Standard verändern, z. B. bei Netmeeting unter Optionen / Audio / Erweitert von G.723 Audio- Codec auf G.711 Audio-Codec stellen (auf Kosten der LAN- Last)
7. Aufbau einer sekundenlangen Verzögerung während des Gespräches
 - Netmeeting 2.1 zeigt im Zusammenspiel mit dem Voicegateway der HiPath HG 1500 Probleme, Netmeeting auf Version 2.11 updaten

Abkürzungsverzeichnis

Diese Liste enthält die in dieser Anleitung verwendeten Abkürzungen.

Abkürzung	Definition
AF	Assured Forwarding (siehe auch RFC 2597)
APS	Anlagen Programm System
CAPI	Common ISDN Application Programming Interface
CHAP	Challenge Handshake Authentication Protocol
CSTA	Computer Supported Telecommunications Applications
CTI	Computer Telephony Integration
DDE	Direct Data Exchange
DFÜ	Datenfernübertragung
DiffServ	Differentiated Services (siehe auch RFC 2474)
DIX V2	Ethernet Standard der DIX-Gruppe: DEC, Intel, Xerox
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service, Auflösung von Namen zu IP-Adressen
DS	DiffServ
DSL	Digital Subscriber Line
DSP	Digital Signal Processor
DSS1	Digital Subscriber Signalling System one (D-Kanal Protokoll)
DTMF	Dual Tone Multiple Frequency (Tonwahlverfahren)
EF	Expedited Forwarding (siehe auch RFC 2598)
EMV	Elektromechanische Verträglichkeit
GSM	Global System of Mobile communication
HVT	Hauptverteiler
HXGM	HiPath HG 1500 Gateway Medium
HXGS	HiPath HG 1500 Gateway Small
IEEE802.1p	Institute of Electrical and Electronic Engineers (hier Definition von Verkehrs-/Prioritätsklassen)
IP	Internet Protocol
IPX	Internetwork Packet eXchange (von Novell)
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider

KDS	Kundendatenspeicher
LAN	Local Area Network
LCR	Least Cost Routing
MAC	Medium Access Control
MODEM	Modulator/Demodulator
MSN	Multiple Subscriber Number
NAT	Network Address Translation
NCP	Netware Core Protocol (von Novell)
NDS	Netware Directory Services (von Novell)
NLSP	Netware Link Services Protocol (von Novell)
PAP	Password Authentication Protocol
PBX	Private Branch Exchange (Telefonanlage)
PING	Packet InterNet Groper
PPP	Point to Point Protocol
PPPoE	Point to Point Protocol over Ethernet
PPTP	Point to Point Tunneling Protocol
QoS	Quality of Service
RAS	Remote Access Service
RFC	Request for Comments
RIP	Routing Information Protocol
RTCP	RTP Control-Protocol
RTP	Real-Time Transport-Protocol
SAP	Service Advertising Protocol (von Novell)
SIC	Serial Interface Cable
SLA	Subscriber Line Analog (Hicom-BG)
SLIP	Serial Line Interface Protocol
SLU	Subscriber Line UP0/E (Hicom-BG)
SNMP	Simple Network Management Protocol
SPX	Sequenced Packet eXchange Protocol
STLS	Subscriber Trunk Line S0 (Hicom-BG)
STRG	Steuerung
SUA	Single User Access (in Verbindung mit NAT)
TAPI	Telephony Application Programming Interface

TCP	Transmission Control Protocol
T-DSL	Telekom Digital Subscriber Line
TLA	Trunk Line Analog (Hicom-BG)
ToS	Type of Service
TS2	Trunkmodul S2M (Hicom-BG)
vCAPI	virtuelle CAPI
WAN	Wide Area Network

Stichwortverzeichnis

A

Administration mit Assistant I	25
Administrationsprogramm einrichten	13
Administrierbare HiPath HG 1500	73
Admin-PC einrichten	13
AE/EF Codepoints	39
Aktive Netzwerkschnittstellen	41
Anmelderufnummer der HiPath HG 1500 ..	36
Anzahl genutzter B-Kanäle	36
APS+KDS-Transfer	74
APS-Transfer	74
arp	169
Assistant I	
Administration	25
Erklärung der Menüfunktionen	33
Erstgenerierung	29
Menüleiste	26
Netzwerkschnittstellen	40
Programmeinstellungen	73
Start	25
Symbolleiste	27
Aufbau des Handbuchs	2
Authentifizierung	
System-Client	69
Authentifizierung System-Client	77
Automatischer Rückruf	102
AVM NDIS WAN CAPI-Treiber	144
AVM Networks	141
AVM-Client einrichten	141

B

Benutzername	73
Berechtigung Community	72
B-Kanäle	
Anzahl	36
ISDN-Partner	53
Blocking-Filter	46
BNC-Netz	152

C

Call back	
ITK-Client	140
RAS	144
Call Signaling	39
Callback	107
CAPI	93
CAPI-Teilnehmer Identifizierung	93
CE-Kennzeichen	7
CHAP	56, 102, 108
Cisco-Router	148
Codierung	
HiPath HG 1500	36
Voice Clients	67
Voice over IP	76
Communities	72

D

Data Payload	39
Datenpaketlänge	44
Datenschutz	181
DFÜ-Netzwerk	139
DFÜ-Netzwerkinstallation	16, 18, 19, 21
DFÜ-Netzwerkconfiguration	
unter Win 95/98	16, 18, 19, 21
Diagnose von TCP/IP	156
Dienstprogramme	156
Digitale Daten	
vCAPI-Client	95
vCAPI-Teilnehmer	62
DNS-Anfragen	180
DSL	9, 10, 12, 41, 43, 44, 51, 58, 91, 92, 108, 109, 131, 133
Durchwahl	55

E

Echo	
Voice Clients	67
Echo (Voice over IP)	76
Einrichten	
Administrationsprogramm	13
Admin-PC	13
Fax	99
Filetransfer	100

H.323-Client	80
Hicom System-Client	77
Internetzugang	101
Smartset	96
vCAPI-Client	94
Einrichten des DFÜ-Netzwerks	23
Empfangen+Speichern des Fehlerspeichers	74
Empfangen+Speichern des Kunden-Trace	74
Erstgenerierung mit Assistant I	29
Erstinbetriebnahme über LAN-Anschluß	14
über serielle Schnittstelle	14
Erstinbetriebnahme von Remote (Service- zentrum)	14
ETSI-Fehlermeldungen	181
Externe IP-Adresse	52

F

Fax einrichten	99
Fax Gruppe3 TAPI-Client	98
vCAPI-Client	95
vCAPI-Teilnehmer	62
Faxabruf	98
Faxdurchwahlnummer	98
Faxweiterleitung	98
Filetransfer einrichten	100
Filtermode ISDN1	46
Filtermode ISDN2	46
Filtermode LAN	46
Firewall	102, 118
Frametyp Ethernet_II	146
FRITZ! 32vox/fon	151
FRITZ!fax und Rufweiterleitung	151
FRITZ!vox/fon	151
Fritzfax	151

G

Gatekeeper	122
Voice Clients	70
Gateway	139
AMV-Client	141

IP-Routing	51
ITK-Client	140
Gebührenzuordnung vCAPI-Client	95
Gebührenzuordnung/Callback	107

H

H.323-Client	69, 79
Hicom Integrated	143
HiPath HG 1500 Routerrufnummer	38
Software	38
hostname	161
Hostrouting	136
HUB, 3COM, Dual Speed	153

I

IEEE802.1p	37
Inbetriebnahme	11
Interne IP-Adresse	52
Internet	57, 101
Internet Provider	130
Internetzugang	108
Internetzugang einrichten	101, 111
IP Networking (PBX-Routing)	81
IP-Accounting	58
IP-Adresse	29
AMV-Client	141
Community	72
Gatekeeper	70
H.323 Clients	69
H.323-Client	80
Internet	58
IP-Firewall	49
IP-Routing	51
ISDN-Partner	52
ITK-Client	140
Netzwerkinterface	43
TrapCommunity	72
vCAPI-Client	95
vCAPI-Teilnehmer	62
IP-Adresse unterdrücken	54
IP-Adressierung	171
IP-Adressliste	38

IP-Adressmapping	55, 114	Kunden-Trace	181
ipconfig	158	löschen	74
IP-Firewall	48, 117	L	
IP-Mapping	52	LAN Interface	43
IP-Netzmaske		LAN Lösungsvorschläge	152
IP-Routing	51	LAN2	9, 10, 41, 43, 44, 51, 58, 91
Netzwerkinterface	43	LAN-LAN Routing einrichten	104
IP-Protokoll		LAN-LAN und Teleworking	102
IP-Firewall	49	LAN-LAN-Kopplung	102, 134
IP-Routing	51	Lizenzierte B-Kanäle	63
IPX Reconnect-Filter	57	Log-in an NT Domäne	145
IPX-Firewall	50, 117	M	
IPX-Netzwerknummer		MAC-Adresse	146
Netzwerkinterface	44	MAC-Überprüfung	50
IPX-Node	146	Mapping Netmask	37
Netzwerkinterface	44	Max. Anzahl gleichzeitiger Rufe	67
ISDN RAS Router	144	Maximal verwendbare B-Kanäle	63
ISDN1 Interface	43	Menüfunktionen des Assistent I	33
ISDN2 Interface	43	Menüleiste des Assistent I	26
ISDN3 Interface	44	Monitoring	
ISDN-Partner	52	System-Client	78
IPX Reconnect Filter	60	Multilink	54, 102, 108
Rufnummer	59	AMV-Client	141
ITK Columbus Client Pro	140	ITK-Client	140
ITK-Clients einrichten	140	RAS	144
I-View unter Windows 95	142	N	
K		Name	
KDS		Community	72
drucken	34	ISDN-Partner	52
neu anlegen	33	TrapCommunity	72
Öffnen	33	Namensauflösung	106
speichern	34	NAT/SUA	111, 112
Übertragen zum PC	34	nbtstat	165
KDS (Kundendatenspeicher)	33	netstat	161
KDS konvertieren	73	Network Control	39
KDS-Hub	74	Netzinterfaces	43
Kennung 1	39		
Kennung 2	39		
Kennwort	73		
Kundendatenspeicher (KDS)	33		

Netzwerkschnittstellen	40, 41
Netzwerktopologie	
Stern	12
Node-Adresse	
ISDN-Partner	52
nslookup	159

O

Obere Schwelle	47
----------------------	----

P

PAP	55, 102, 108
Passwort	
Script	39
System-Client	69, 78
Pause	46
PBX-Knoten	68
PBX-Routing (ab Hicom 150 H V1.0)	68
PBX-Routingtabelle importieren	74
pcANYWHERE	116
ping	156
PPP	111
PPP-Multilink	102, 108
PPPoE	108, 109
PPP-Verbindungen	102
PPTP	40, 41, 108
Präfix	
Gatekeeper	70
Programmeinstellungen des Assistant I	73
Protokollierungsfunktion	181

Q

QoS-Bandbreite für EF	55
QoS-Fähigkeiten	55
QoS-Prioritätsklassen	39
QoS-Verfahren	37
Quality of Service (QoS)	90

R

RAS (Remote Access Service)	137
RAS/Teleworking einrichten	138
RAS-Server-Konfiguration	
unter Win 95/98	19
Remote Access Service (RAS)	137

Remote Control	116
Reset der HiPath HG 1500	75
route	166
Routerrufnummer	38
Routing	51, 102, 134
Routing mit Cisco-Router	148
Routing Peer to Peer	106
Rückruf	53, 102, 140, 141
AMV-Client	141
RAS	144
Rufnummer	56
H.323 Client	69
H.323-Client	80
LAN-Client	77
System-Client	69
vCAPI-Client	95
vCAPI-Teilnehmer	61
Rufnummer für Routing Digital	29
Rufnummernauswahlbox	30
Rufnummernhaushalt	11, 78, 99
Rufnummerntabelle anfordern	74
Rufnummern-Überprüfung	48, 117
Rufnummernvergabe bei Telematik	150
Rufrichtung	
ISDN-Partner	56
Rufzuschaltung	96

S

S0-Adapter am optiset E	143
Schutzmechanismus ("Firewall")	117
Scriptbearbeitung	38, 54
Segmentierung	54
Seitenansicht	34
Seiteneinrichtung	34
selbsttätiger Verbindungsaufbau	140
Servename	
Blocking-Filter	46
Service	63
Blocking-Filter	46
Severity	71
Short Hold	139, 144
Short Hold Gebührentaktauswertung	53
Short Hold Modus	53
Short Hold Zeit	52
Short-Hold	139, 144
Sicherheit	48

SLIP	15	Traps	71
Netzwerkinterface	43	Twisted Pair	152
Smartset	96		
SNMP	71, 128	U	
Soundeinstellung für Voice over IP	184	Überschreitungsdauer	47
Soundkarten	184	Übertragen des KDS zu HiPath HG 1500	35
Statisches Channel Bundling	55	Übertragen des KDS zum PC	34
Statusmeldungen		Untere Schwelle	47
System-Client	78	Unterschreitungsdauer	47
Statusmeldungen übertragen	69	UUNET	130
Stern-Topologie mit Hub	12		
Subnetze	171	V	
Switch	154	V.110-Gegenstelle	54
Symbolleiste des Assistant I	27	V.34-Gegenstelle	54
System Clients	68	vCAPi (virtuelle CAPi)	61, 93, 94
Systemstart-Verhalten	53	vCAPi für Clients im Netzwerk	93
		vCAPi und Fax	98
T		vCAPi und Filetransfer	100
TAPI	97	vCAPi und Internet	101
TAPI-Clients	97	vCAPi und Smartset	96
T-DSL	9, 109, 131, 133	vCAPi und TAPI	97
Telematik	150	vCAPi-Clients	94
Telematik mit vCAPi-Client	93	vCAPi-Teilnehmer	61
Telematikfunktion		Verbindungssteuerung	46
AVM Netways	141	Virtuelle CAPi (vCAPi)	61, 93, 94
CTI-Anwendungen	150	Voice	
DFÜ Netzwerk	139	vCAPi-Client	95
ITK Columbus Client	140	vCAPi-Teilnehmer	62
Rufauswertung auf dem PC	150	Voice Clients	67
Teleworking	145	Voice over IP	76
Teleworking an Novell	146	Soundeinstellung	184
T-Online	131, 133	Voice Payload	39
Trace	181	Vorbereiten WindowsNT als RAS	144
Trace-Gruppen	63	Voreinstellung der Blocking-Filter	46
tracert	168	Voreinstellungen	
Traffic-Statistic		Blocking-Filter	46
Voice over IP	76	IP-Firewall	50
Traffic-Statistik		IP-Routing	59
Voice Clients	67	IPX-Firewall	50
Trap-Communities	72	ISDN-Partner	59

vCAPi-Teilnehmer 62, 70

W

Wahlwiederholungen 46

Z

Ziel-IP-Adresse

 IP-Firewall 49

Zurücksetzen der HiPath HG 1500 73

Zweites LAN 9, 10, 41, 43, 44



1P A31003-K5020-B811-7-19

Bestell-Nr.: A31003-K5020-B811-7-19 • Gedruckt in der Bundesrepublik Deutschland • BA 0800 1.0

© Siemens AG 2002 • Information and Communication Networks • Hofmannstr. 51 • D-81359 München •

Liefermöglichkeiten und technische Änderungen vorbehalten.

