VoIP-Gateways

IP 400

Administrator Handbuch

innovaphone

Pure IP-Telephony

Release 5.01, 2. Auflage, April 2005

PDF-Ausgabe zum Download erhältlich unter:
http://www.innovaphone.com

Böblinger Str. 76 71065 Sindelfingen

Tel +49 (70 31) 7 30 09-0 Fax +49 (70 31) 7 30 09-99

http://www.innovaphone.com

VoIP-Gateways

IP 400

Version 5.01

Handbuch

Inhaltsverzeichnis

1 Über dieses Handbuch

Das vorliegende Handbuch beschreibt das innovaphone VoIP Gateway IP 400.

Das Handbuch beschreibt den Betrieb des Gerätes als Gateway und Gatekeeper. Sofern Sie das Gerät auch als Telefonanlage betreiben wollen, beachten Sie bitte zusätzlich das Ihrer Lizenz beiliegende "innovaphone PBX - Administrator-Handbuch".

Dieses Handbuch ist integraler Bestandteil des Gerätes. Alle darin aufgeführten Hinweise sind sorgfältig zu beachten und das Gerät ist ausschließlich so wie beschrieben zu verwenden. Der Hersteller lehnt jede Verantwortung für Personen-, Sach- oder Folgeschäden ab, die auf unsachgemäße Verwendung des Gerätes zurückzuführen sind.

Einige Bildschirmfotos stammen von anderen innovaphone Produkten. Diese sind jedoch inhaltlich gleich mit der IP 400.

Achtung

Beachten Sie in jedem Fall die im jeweiligen Handbuch aufgeführten Sicherheitshinweise!

1.1 Hinweis, Tipp und Achtung

Hinweis

Mit dem Hinweis erhalten Sie Informationen, die Sie unter Umständen zunächst in Erfahrung bringen müssen, um die Gateways richtig konfigurieren zu können.

Tipp

Mit dem Tipp erhalten Sie Informationen, die den Umgang mit den Gateways besonders einfach oder komfortabel machen.

Achtung

Zur Vermeidung von Beschädigungen an den Gateways oder anderem Equipment sowie zur Gewährleistung Ihrer eigenen Sicherheit beachten Sie unbedingt diese Felder.

2 Einführung, Inbetriebnahme und Installation des VoIP Gateways

2.1 Anschlüsse und Bedienelemente IP 400

2.1.1 Anschlüsse an der Rückseite

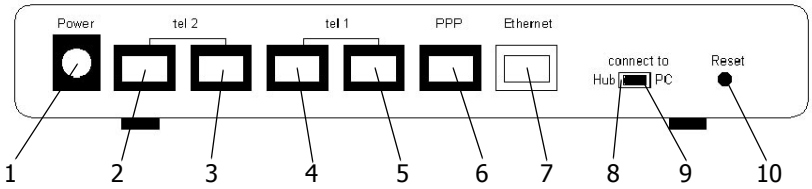

Abbildung 1 Anschlüsse der IP 400

Auf der Rückseite des Gateways sind (von links nach rechts) folgende Anschlüsse/ Schalter vorhanden:

Pos	Bezeichnung	Funktion
1	**Power**	für mitgeliefertes Steckernetzteil, 12V 900mA
2	**tel2 (erste Buchse)**	RJ 45-Buchse. Für ISDN -Telefon, -TK-Anlage oder -Amtsleitung
3	**tel2 (zweite Buchse)**	RJ 45-Buchse. Zum optionalen Anschluss eines zweiten Telefons an **tel2**
4	**tel1 (erste Buchse)**	RJ 45-Buchse. Für ISDN-Telefon, -TK-Anlage oder -Amtsleitung
5	**tel1 (zweite Buchse)**	RJ 45-Buchse. Zum optionalen Anschluss eines zweiten Telefons an **tel1**

Pos	Bezeichnung	Funktion
6	**PPP**	RJ 45. Zum Anschluss einer ISDN-Amtsleitung
7	**Ethernet**	RJ 45-Buchse. Zum Anschluss eines 10Mbit/s Ethernet (10_{BASE-T})
8	**connect to Hub**	Umschalter zum Anschluss des **Ethernet** Anschlusses der IP 400 an einen Hub (linke Schaltstellung).
9	**connect to PC**	Umschalter zum Anschluss des **Ethernet** Anschlusses der IP 400 direkt an einen PC (rechte Schaltstellung).
10	**Reset**	Taster zum Neustart des Gateways

Tabelle 1 Anschlüsse und Bedienelemente der IP 400

2.1.2 Anzeigen auf der Vorderseite

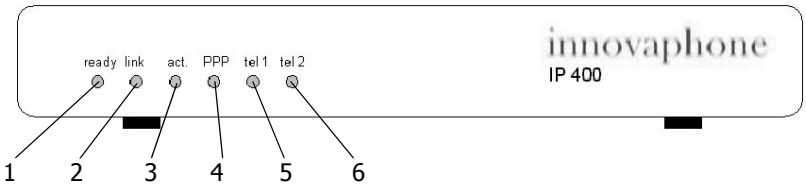

Abbildung 2 Kontrollanzeigen der IP 400

Auf der Vorderseite des Gateways sind (von links nach rechts) folgende LEDs zur Statusanzeige vorhanden:

Pos	Bezeichnung	Bedeutung
1	**ready**	LED leuchtet rot beim Booten, LED leuchtet grün, wenn betriebsbereit, LED blinkt während des Downloads.
2	**Ethernet link**	Der **Ethernet** Anschluss ist bereit zur Datenübertragung

Pos	Bezeichnung	Bedeutung
3	**Ethernet act.**	Es werden Daten auf dem **Ethernet** Anschluss gesendet oder empfangen
4	**PPP**	Amtsleitung an Anschluss **PPP** ist aktiv
5	**tel1**	Gerät oder Amtsleitung an Anschluss **tel1** ist aktiv
6	**tel2**	Gerät oder Amtsleitung an Anschluss **tel2** ist aktiv

Tabelle 2 Anzeigen der IP 400

Achtung

Blinkt die **ready**-LED während des Downloads, darf dieser Vorgang nicht unterbrochen werden. Das Gerät kann sonst beschädigt werden.

2.1.3 Das Seriennummernetikett der IP 400

Auf der Gehäuseunterseite befindet sich das Seriennummernetikett.

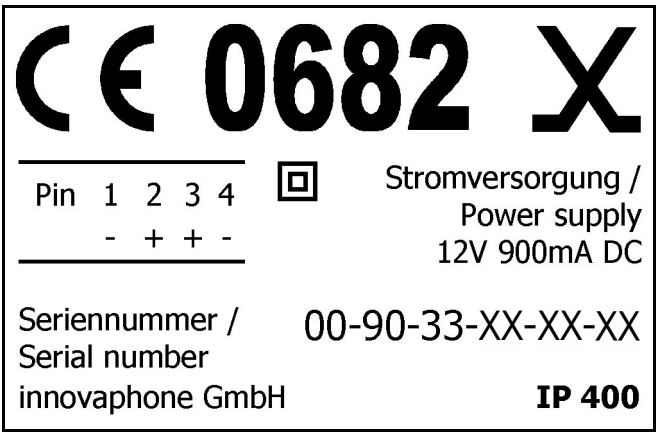

Abbildung 3 Das Seriennummernetikett

Die hinteren 3 durch einen Bindestrich (`-´) getrennten Hexadezimalzahlen (im Bild als `XX-XX-XX‘ gezeigt) stellen die fortlaufende Seriennummer Ihrer IP 400

dar, während die ersten 3 Hexadezimalzahlen als Herstellerkennung von innovaphone konstant sind.

Die Seriennummer ist gleichzeitig die MAC-Adresse Ihrer IP 400.

2.1.4 Inbetriebnahme und Installation der IP 400

Das Gateway wird mit den folgenden Schritten in Betrieb genommen:

- Installation der Anschlüsse wie zuvor beschrieben.
- Einstellen der IP-Schnittstellenparameter, siehe Kapitel 2.2 "Konfiguration des lokalen Netzzugangs" ab Seite 11.
- Festlegen der Betriebskonfiguration, siehe Kapitel 4 "Konfiguration der IP Schnittstellen" ab Seite 25.

Die folgenden Abschnitte gehen davon aus, dass sich das Gateway im Auslieferungszustand befindet und somit die Standardkonfiguration geladen ist. Sind Sie sich nicht sicher über den Stand der Konfiguration, so ist es zu empfehlen, zunächst die Standardkonfiguration wieder herzustellen (siehe Kapitel 2.2.1 "Herstellen der Standardkonfiguration" ab Seite 11).

Beachten Sie das Kapitel "Sicherheitshinweise für die IP 400" ab Seite 140.

Die IP 400 ist zur Wandmontage geeignet. Der Abstand der Aufhängungen beträgt horizontal 12 cm. Achten Sie bei der Montage darauf, die Platinenschutzfolie nicht zu beschädigen.

Die Geräte können gestapelt werden. Achten Sie bei Aufstellung in einem Schrank auf ausreichende Belüftung.

Für den Einbau in einen 19"-Schrank ist ein spezieller Einbaurahmen erhältlich, der zwei IP 400 Gateways aufnehmen kann.

2.2 Konfiguration des lokalen Netzzugangs

Im Auslieferungszustand ist das Gateway mit einer Standardkonfiguration versehen. In dieser Konfiguration wird das Gateway versuchen, die IP-Parameter per DHCP zu konfigurieren. Der eingebaute DHCP Client ist daher aktiviert und der ebenfalls enthaltene DHCP Server deaktiviert.

Erkundigen Sie sich bei Ihrem Netzwerkadministrator, ob Ihr Netz über einen DHCP Server verfügt.

Ist in Ihrem Netzwerk kein DHCP Server in Betrieb oder wollen Sie aus anderen Gründen keine automatische Konfiguration per DHCP vornehmen lassen, dann lesen Sie im Kapitel 2.2.4 "Einstellen der IP-Schnittstellenparameter ohne DHCP" ab Seite 16 nach. In diesem Fall muss Ihr PC zusätzlich über einen twisted-pair Ethernet Adapter verfügen (10Base-T für die IP 400).

Steht ein DHCP Server zur Verfügung, dann lesen Sie im Kapitel 2.2.3 "Einstellen der IP-Schnittstellenparameter per DHCP" ab Seite 13 nach.

In beiden Fällen können Sie auf das Gateway über Ethernet zugreifen.

2.2.1 Herstellen der Standardkonfiguration

Tipp

Sie können die Standardkonfiguration jederzeit wieder herstellen, indem Sie den Reset Taster einige Sekunden lang gedrückt halten. Die Zeitspanne beträgt bei der IP 400 ungefähr 5 Sekunden.

Das Gateway wird damit neu initialisiert und befindet sich in einem speziellen Reset-Modus. Nachfolgendes Ein- und wieder Ausschalten bringt sie wieder in den normalen Betriebsmodus.

Tipp

Nochmaliges kurzes Betätigen der Reset-Taste bringt das Gateway wieder in den normalen Betriebsmodus. Allerdings ist in diesem Fall der DHCP Server Modus (siehe ab Seite Seite 16) aktiviert, während nach einem Ein-/Ausschalten der DHCP Client Modus (siehe Seite 13) aktiviert ist.

Bedenken Sie jedoch, dass sie durch diese Prozedur alle vorangegangenen Konfigurationsdaten verlieren. Bei Bedarf können Sie die aktuelle Konfiguration jedoch vorher in eine Datei sichern.

2.2.2 Einschalten des Gateways

Achtung

Schließen Sie das Gateway mit dem mitgelieferten Netzteil (IP 400 100-240V) an die nächste Steckdose an.

Verwenden Sie ausschließlich das mitgelieferte Steckernetzteil bzw. Netzanschlusskabel. Andere Netzteile könnten das Gateway beschädigen.

Die Netzsteckdose muss in der Nähe des Gerätes und leicht zugänglich sein. Die Stromversorgung des Gerätes kann nur durch Herausziehen des Gerätenetzkabels beziehungsweise des Steckernetzteils aus der Netzsteckdose unterbrochen werden.

Das Gerät ist nun eingeschaltet und die **READY LED** leuchtet.

2.2.3 Einstellen der IP-Schnittstellenparameter per DHCP

... für Experten

- Grundsätzlich gibt es zwei Möglichkeiten, um für Ihr Gateway eine IP Adresse zu konfigurieren.
- Im Auslieferungszustand befindet sich der DHCP in einem automatischen Modus. Sie können den automatischen Modus mit einem langen Reset (mind. 3 Sekunden) erzwingen.
- Mit einem kurzen Reset wird der DHCP Server Modus eingestellt und das Gateway bekommt die IP Adresse 192.168.0.1.
- Besser ist auf jeden Fall, wenn Sie den DHCP Client Modus des Gateways benutzen. Dazu benötigen Sie einen DHCP Server im Netz.
- Wenn das Gateway im automatischen Modus kurz von der Stromzufuhr getrennt wird, schaltet sich der DHCP Client Modus ein. Jetzt wird Ihnen eine IP Adresse vom DHCP Server im Netz zugeteilt.
- Sie können die zugewiesene IP Adresse wie folgt anzeigen lassen.
  Geben Sie auf der Kommandozeile `C:>` folgende Befehle ein:
  ```
  nbtstat -R
  nbtstat -a ip400-YY-YY-YY
  ```
  Wobei die Zeichen `Y` mit der MAC-Adresse Ihres Gateways ersetzt werden müssen.
- Starten Sie jetzt die Web-basierende Konfiguration mit der neuen IP Adresse.

Tipp

Verfügt Ihr Netz über einen DHCP-Server, so ist die Konfiguration der IP-Schnittstellenparameter per DHCP die bequemste Methode.

Sie können Ihren Netzadministrator bitten, eine feste IP-Adresse für das Gateway über DHCP zu reservieren. Teilen Sie ihm dazu bitte die Hardwareadresse Ihres Gateways mit. Lesen Sie hierzu bitte das entsprechende Kapitel zu dem jeweiligen Seriennummernetikett Ihres Gateways.

In der Standardkonfiguration versucht das Gateway nach jedem Einschalten die Konfiguration per DHCP. Nach jedem Drücken der Reset-Taste (nicht per Aus-/

Einschalten und auch nicht mit dem Reset-Kommando) wird jedoch der Konfigurationsmodus ohne DHCP aktiviert (siehe hierzu Kapitel 2.2.4 "Einstellen der IP-Schnittstellenparameter ohne DHCP" ab Seite 16).

Gehen Sie nun wie folgt vor:

- Bringen Sie den **Ethernet Umschalter** auf der Rückseite in die Stellung "**connect to Hub**".
- Verbinden Sie den **Ethernet RJ 45**-Anschluss des Gateways und den RJ 45-Anschluss Ihres Ethernet Hub oder Switch mit einem **twisted pair** Kabel.
- Schalten Sie das Gateway einmal aus und wieder an, um den DHCP Klienten zu aktivieren.

Dem Gateway wird nun eine IP-Adresse zugewiesen. Hat Ihnen Ihr Netzadministrator keine feste IP-Adresse eingerichtet, so müssen Sie jetzt feststellen, welche IP-Adresse zugewiesen wurde. Dazu gibt es zwei Möglichkeiten:

- Die einfachste Möglichkeit ist, Ihren Netzadministrator zu befragen. Er kann die vergebene IP-Adresse im Verwaltungsprogramm des DHCP Servers feststellen.
- Die andere Möglichkeit besteht darin, das Gateway selbst zu befragen. Das Gateway registriert nach erfolgter Konfiguration den NetBIOS Namen "`ip400-XX-XX-XX`". "`XX-XX-XX`" ist durch die letzten 6 Hexadezimalziffern der Seriennummer zu ersetzen. Lesen Sie hierzu bitte das entsprechende Kapitel zu dem jeweiligen Seriennummernetikett Ihres Gateways.
  Sie können nun mit dem Kommando "`nbtstat`" auf einem Windows-PC die vergebene IP-Adresse feststellen.

```
C:> nbtstat –

C:> nbtstat –a ip400-XX-XX-XX

NetBIOS Remote Machine Name Table

Name                 Type         Status

---------------------------------------------

IP400-XX-XX-XX<00>  UNIQUE      Registered

195-226-104-217<00>  UNIQUE      Registered

IP400-XX-XX-XX<00>  UNIQUE      Registered

MAC Address = 00-90-33-XX-XX-XX
```

Tipp

Die Anzeige der IP-Adresse mit nbtstat funktioniert nicht, wenn Ihre NetBIOS Umgebung ausschließlich für die Namensauflösung über WINS konfiguriert ist. Findet das nbtstat Kommando Ihr Gateway nicht, sprechen Sie mit Ihrem Netzwerkadministrator, um die NetBIOS Namensauflösung entsprechend zu konfigurieren.

Das Gateway im obigen Beispiel hat die IP-Adresse 195.226.104.217.

Unter Linux können Sie hierzu das Kommando "`nmblookup`" verwenden, sofern das "SAMBA" Package installiert ist:

```
[dvl@cobalt ~ 2] $. nmblookup ip400-XX-XX-XX
Got a positive name query response from 195.226.104.220 (
195.226.104.220 )
195.226.104.220 ip400-XX-XX-XX<00>
[dvl@cobalt ~ 3] $.
```

Tipp

Der Abschluss der Installation kann durch Ihren **Web-Browser** oder kommandoorientiert mit Hilfe des Programms **telnet** erfolgen. In diesem Handbuch wird die Vorgehensweise bei Verwendung des **Web-Browsers** beschrieben, die für die üblichen Einsatzszenarien am komfortabelsten ist.

So schließen Sie die Festlegung der Schnittstellenparameter mit dem Web-Browser ab:

- Starten Sie Ihren Web-Browser und verbinden Sie ihn mit der Adresse `http://`***`ipaddr.`***
- Starten Sie das Konfigurationsapplet über den Menüeintrag **Config** im Menü **Gateway** (siehe Kapitel 3 "Allgemeines zur Konfiguration" ab Seite 20). Dazu müssen Sie sich am Gerät anmelden. In der Standardkonfiguration ist der Benutzername `admin` und das Kennwort `ip400`.
- Zur Vermeidung unbefugten Zugriffs sollten Sie im Bereich **General settings** unter **Change login parameters** Benutzername und Kennwort sofort

ändern (siehe Kapitel 8.1.2 "Festlegen des Administrationsbenutzers und -Kennworts" ab Seite 112).

- Legen Sie im Bereich **IP Interfaces / Ethernet Interface** unter **DHCP** den **DHCP Mode "Client"** fest (siehe Kapitel 4.1 "Konfiguration der Ethernet Schnittstelle" ab Seite 25).
- Sichern Sie die Konfiguration dauerhaft mit den Schaltflächen **Save** und **Activate** (siehe Kapitel 3.2 "Testen und Speichern der Konfiguration" ab Seite 22).

2.2.4 Einstellen der IP-Schnittstellenparameter ohne DHCP

Verfügt Ihr Netz nicht über einen DHCP Server, so müssen Sie die IP-Schnittstellenparameter des Gateways selbst einstellen.

... für Experten

- Konfigurieren Sie wenn möglich Ihren PC per DHCP!
- Der DHCP-Server des Gateways ist in der Standardkonfiguration nur nach einem Reset eingeschaltet.
- Verbinden Sie die Ethernet Anschlüsse des Gateways und des PC "back to back" (Schiebeschalter auf "**connect to PC**").
- Ist Ihr PC per DHCP konfiguriert, dann aktualisieren Sie die IP-Adresse mit `winipcfg` bzw. `ipconfig`. Anderenfalls stellen Sie die IP-Adresse des PC fest auf 192.168.0.2 ein.
- Das Gateway hat die Adresse 192.168.0.1.

Hinweis

Wenn Sie nicht sicher sind, welche IP-Adresse und welche Subnetzmaske Sie für das Gateway vergeben können sowie ob und wenn ja welches Default-Gateway Sie verwenden sollten, fragen Sie ihren Netzwerkadministrator.

Sie müssen den in das Gateway eingebauten DHCP Klienten deaktivieren und den eingebauten DHCP Server aktivieren. Beides geschieht, indem Sie nach einem Kaltstart kurz die **Reset** Taste betätigen.

Zur Konfiguration wird das Gateway zunächst direkt an ihren Computer angeschlossen.

- Ist Ihr Computer an das lokale Netzwerk angeschlossen, trennen Sie ihn für die Zeit der ersten Konfiguration des Gateways vom Netzwerk.

Achtung

Falls der Computer durch ein BNC-Kabel (**thin Ethernet**) an das Netzwerk angeschlossen ist, entfernen Sie das BNC-T-Stück vom Ethernet Adapter. Achten Sie darauf, dass das Netzwerkkabel dabei nicht aufgetrennt wird, da ihr Netzwerk sonst nicht mehr funktioniert.

Ist der Computer durch ein **twisted pair** Kabel mit RJ45-Steckern an das Netzwerk angeschlossen, trennen Sie das Kabel vom **Hub** oder **Switch** bzw. entfernen Sie es aus der Wanddose, je nachdem wo Ihr Computer angeschlossen ist.

- Bringen Sie den **Ethernet Umschalter** auf der Rückseite in die Stellung "**connect to PC**". Hierdurch funktioniert das Gateway als **Ethernet Hub** für Ihren Computer.
- Verbinden Sie den **Ethernet** RJ45-Anschluss und den RJ45-Anschluss Ihres Ethernet Adapters mit einem **twisted pair** Kabel.

Nun wird der Ethernet Adapter Ihres Computers so konfiguriert, dass er mit dem Gateway im Auslieferungszustand kommunizieren kann. Dies geschieht am bequemsten, indem Ihr Computer seine IP-Konfiguration über das DHCP-Protokoll bezieht.

Beherrscht Ihr Computer das DHCP-Protokoll, sollten Sie dies auf jeden Fall verwenden. Ist dies nicht der Fall, kann die Konfiguration manuell erfolgen.

- Ist Ihr Computer für die Verwendung des DHCP-Protokolls konfiguriert, wird nun die Zuweisung einer zur Kommunikation mit des Gateways geeigneten IP-Adresse veranlasst.

Tipp

Nun muss Ihrem PC eine für die Erstkonfiguration des Gateways geeignete IP-Adresse zugewiesen werden.

- Unter Windows 95/98 geschieht dies, indem Sie den Befehl
  `winipcfg`
  ausführen und die Optionen "**Alles freigeben**" und "**Alles aktualisieren**" auswählen
  Unter Windows NT/2000/ME/XP führen Sie folgende Befehle aus:

```
ipconfig /release /all
ipconfig /renew /all
```

- Wahlweise können Sie Ihren Computer auch neu starten.
- Ist Ihr Computer mit festen IP-Adressen konfiguriert, so ändern Sie die Einstellungen gemäß nachfolgender Tabelle:

Adresse	192.168.0.2
Netzmaske	255.255.255.0

Tabelle 3 IP-Konfiguration zur Inbetriebnahme

Unter Windows geschieht dies, indem Sie in der **Systemsteuerung** im Bereich **Netzwerk** die Einstellungen für das TCP/IP-Protokoll entsprechend anpassen. In diesem Fall muss der Rechner neu gestartet werden.

Tipp

Der Abschluss der Installation kann durch Ihren **Web-Browser** erfolgen. In diesem Handbuch wird die Vorgehensweise bei Verwendung des **Web-Browsers** beschrieben, die für die üblichen Einsatzszenarien am komfortabelsten ist.

So schließen Sie die Festlegung der Schnittstellenparameter mit dem Web-Browser ab:

- Starten Sie Ihren Web-Browser und verbinden Sie ihn mit der Adresse `http://192.168.0.1`.
- Starten Sie das Konfigurationsapplet über den Menüeintrag **Config** im Menü **Gateway** (siehe Kapitel 3 "Allgemeines zur Konfiguration" ab Seite 20). Dazu müssen Sie sich am Gerät anmelden. In der Standardkonfiguration ist der Benutzername `admin` und das Kennwort `ip400`.
- Zur Vermeidung unbefugten Zugriffs sollten Sie im Bereich **General settings** unter **Change login parameters** Benutzername und Kennwort sofort ändern (siehe Kapitel 8.1.2 "Festlegen des Administrationsbenutzers und -Kennworts" ab Seite 112).
- Legen Sie im Bereich **IP Interfaces** / **Ethernet Interface** unter DHCP den **DHCP Mode** "**off**" fest (siehe Kapitel 4.1 "Konfiguration der Ethernet Schnittstelle" ab Seite 25).
- Legen Sie an der gleichen Stelle die Parameter unter **Ethernet interface**

address fest.

- Legen Sie an der gleichen Stelle Ihren **Default IP router** fest.
- Sichern Sie die Konfiguration dauerhaft mit den Schaltflächen **Save** und **Activate** (siehe Kapitel 3.2 "Testen und Speichern der Konfiguration" ab Seite 22).

Das Gateway ist nun bereit zum Anschluss an Ihr lokales Netzwerk.

- Bringen Sie den **Ethernet Umschalter** auf der Rückseite in die Stellung "**connect to Hub**". Hierdurch verhält sich das Gateway wie ein normales Ethernet Endgerät und kann an einen **Hub** oder **Switch** angeschlossen werden.
- Verbinden Sie die **Ethernet** Buchse des Gateways mit Ihrem **Hub** oder **Switch** bzw. mit der entsprechenden Wanddose.

Vergessen Sie nicht, Ihren Computer wieder an Ihr eigenes Netzwerk anzuschließen und seine ursprüngliche IP-Konfiguration wieder herzustellen.

Wollen Sie auf diese Art und Weise weitere Gateways konfigurieren, müssen Sie vor Anschluss des nächsten Gerätes an Ihren PC zunächst einmal die Zuordnung der IP-Adresse zur Hardwareadresse löschen.

Tipp

Dies ist erforderlich, da ja das neue Gerät eine andere Hardwareadresse hat, jedoch auf die gleiche IP-Adresse reagieren soll.

Unter Windows- und Unix-Systemen geschieht dies, indem Sie das `arp` Kommando benutzen:

```
C> arp -d 192.168.0.1
```

Sie können nun die Konfiguration des Gateways gemäß Ihren eigenen Gegebenheiten durchführen. Das Vorgehen ist in Kapitel 3 "Allgemeines zur Konfiguration" ab Seite 20 beschrieben.

3 Allgemeines zur Konfiguration

Tipp

Die Betriebskonfiguration kann durch Ihren **Web-Browser** erfolgen. In diesem Handbuch wird die Vorgehensweise bei Verwendung des **Web-Browsers** beschrieben, die für die üblichen Einsatzszenarien am komfortabelsten ist.

Beachten Sie bitte, dass Ihr Browser HTML 4.0, HTTP 1.1 und Java Applets unterstützen muss. Getestet wird das Konfigurationsapplet mit dem Microsoft Internet Explorer 6.x. Einige Funktionen, wie das Sortieren von Listen, setzen die Funktion von XML und XML Stylesheets voraus. Die Geräte lassen sich jedoch auch ohne diese Funktionen vollständig bedienen.

Hinweis

Ist der Zugriff auf das Gateway durch eine Firewall geschützt, so müssen die Dienste `tcp/80` (http) freigegeben sein. Beachten Sie bitte, dass hierdurch nur der Konfigurationszugriff freigegeben wird. Sollen auch Gespräche über die Firewall hinweg möglich sein, lesen Sie bitte im Kapitel "NAT und Firewalls" ab Seite 146 nach.

Die Festlegung der Betriebskonfiguration geschieht durch die folgenden Schritte:

- Konfiguration der ISDN- bzw. Analog-Schnittstellen.
  Hierdurch legen Sie die Anschlussart der ISDN bzw. Analog-Schnittstellen des Gateways fest.
- Definition weiterer VoIP Gateways und VoIP Endgeräte.
  Hierdurch geben Sie dem Gateway bekannt, welche weiteren innovaphone Gateways, VoIP-Gateways von Drittherstellern und VoIP Endgeräte oder PC-Programme sie benutzen wollen.
- Ggf. Konfiguration der WAN Schnittstellen.
  Hierdurch legen Sie die Parameter Ihres Internet- beziehungsweise Intranet-Zugangs fest, falls Sie das Gateway zusätzlich als ISDN-Router oder VPN-Router verwenden wollen.

Tipp

Das innovaphone VoIP-Gateway IP 400 kann als ISDN Router aber auch als VPN-Router (PPPoE) arbeiten.

- Konfiguration der Rufbehandlung.
  Hierdurch legen Sie fest, welche Endgeräte letztlich unter welcher Nummer erreicht werden sollen.

Die Konfiguration der optionalen innovaphone PBX Komponente ist in einem separaten Handbuch erläutert, das Sie zusammen mit Ihrer innovaphone PBX Lizenz erhalten.

Starten Sie zunächst Ihren **Web-Browser** und öffnen Sie die URL `http://`***`Adresse`***`/`, wobei ***`Adresse`*** die IP-Adresse des Gateways ist, das Sie konfigurieren wollen. Sie wird im Format *x.x.x.x* angegeben. Sollten Sie für das Gateway einen Hostnamen im DNS-Namensverzeichnis eingetragen haben, so können Sie selbstverständlich auch diesen benutzen, etwa `http://h323gw.ih-redomaene.de`.

Klicken Sie nun auf **Config**, um das Konfigurationsapplet zu starten. Sie werden aufgefordert, die korrekte Nutzerkennung und das Kennwort einzugeben, das bei der Inbetriebnahme festgelegt wurde (siehe Seite 10).

3.1 Allgemeines zur Konfigurationsoberfläche

Die Konfigurationsoberfläche des Gateways besteht aus 2 Teilen. Der erste Teil besteht aus reinen HTML Seiten und dient hauptsächlich zum Abrufen von Laufzeitinformationen. Die Bedienung erfolgt wie von anderen Webseiten her gewohnt. Die einzelnen Funktionen sind in Kapitel 9 "Die Browser Administrationsoberfläche" ab Seite 121 näher beschrieben.

Die eigentliche Konfiguration erfolgt über ein eigenes Konfigurationsapplet, eine JAVA Anwendung. Sie starten das Applet, indem Sie den Punkt **Config** der Administrationsoberfläche aufrufen.

Das Applet läuft in einem eigenen Fenster ab. So können Sie während der Konfiguration des Gateways auf die verschiedenen Funktionen der Administrationsoberfläche zugreifen, ohne das Konfigurationsapplet zu schließen oder ein zweites Browserfenster öffnen zu müssen.

Im Applet finden sich zwei Bereiche. Auf der linken Seite ist die gesamte Konfiguration des Gateways als Baum dargestellt, ähnlich wie Sie es aus einem Datei-

browser gewöhnt sind. Wenn Sie in diesem Baum ein Objekt durch Anklicken selektieren, werden seine näheren Details auf der rechten Seite dargestellt. Das linke Fenster wird zur Navigation durch die Konfiguration benutzt. Eingaben können nur im rechten Fenster gemacht werden.

Am oberen Rand des Appletfensters befindet sich eine Schaltflächenleiste. Die **Save**, **Activate**, **Reset**, **Reset when idle** und **Cancel** Schaltflächen beziehen sich auf die gesamte Konfiguration. Zur Erläuterung der Funktionen dieser Schaltflächen siehe Kapitel 3.2 "Testen und Speichern der Konfiguration" ab Seite 22.

Die weiteren Schaltflächen (**Add**, **Remove,** etc.), wirken auf das jeweils im linken Fenster selektierte Objekt.

Tipp

Sie können für die meisten Elemente der Konfiguration eigene Bezeichnungen im Feld **Description** vorgeben. Diese erscheinen dann jeweils auf der linken Seite in der Baumdarstellung. Machen Sie von dieser Möglichkeit regen Gebrauch, es erleichtert ihnen später, die Übersicht zu bewahren.

Verschiedene Konfigurationsformulare enthalten die Option **Disable**. Damit können Sie das dort zu konfigurierende Objekt vorübergehend außer Betrieb nehmen, ohne die Konfigurationseinstellungen zu verlieren. Das Objekt ist sozusagen "auskommentiert".

3.2 Testen und Speichern der Konfiguration

Ihr Gateway speichert die Konfigurationsinformationen permanent in einem nichtflüchtigen Speicher, so dass sie auch nach einem Systemneustart noch verfügbar ist. Bei einem solchen Systemstart wird die Konfiguration aus dem nichtflüchtigen Speicher in den Arbeitsspeicher des Gateways kopiert. Diese Kopie wird beim Start ausgewertet und die gewonnenen Konfigurationsinformationen dann während des Betriebes benutzt.

Wird die Konfiguration verändert, so wirkt dies zunächst auf die Konfigurationsinformationen im Arbeitsspeicher. Soll die neue Konfiguration wirksam werden, muss sie analog zu dem Vorgang beim Systemstart neu ausgewertet werden.

Dies geschieht über die Konfigurationsoberfläche durch Betätigen der Schaltfläche **Activate**. Damit wird die neue Konfiguration wirksam und kann getestet werden. Sie ist jedoch noch nicht in den nichtflüchtigen Speicher übernommen, geht also

bei einem Kaltstart des Gateways verloren.

Tipp

Unter Kaltstart wird hier der Neustart durch das Unterbrechen der Stromversorgung verstanden, nicht der Neustart durch Betätigen des **Reset** Tasters.

Sind Sie nach Prüfung der neuen Konfiguration zufrieden, muss sie noch permanent gesichert werden. Dies erfolgt mit der Schaltfläche **Save**.

Die meisten Konfigurationsänderungen – beispielsweise die Änderung der Routinginformationen – führt Ihr Gateway ohne Unterbrechung des laufenden Betriebes durch. Einige Änderungen erfordern jedoch einen Neustart, bei dem laufende Gespräche unterbrochen werden.

Ihr Gateway weist Sie auf einen notwendigen Neustart hin, um zu verhindern, dass versehentlich Gespräche unterbrochen werden. Falls Sie den Neustart ablehnen (Schaltfläche **Later**), können Sie ihn zu einem späteren Zeitpunkt mit der Schaltfläche **Reset** oder **Reset when idle** erzwingen.

Während mit **Reset** ein sofortiger Neustart erfolgt, wird durch **Reset when idle** ein Neustart erst dann durchgeführt, wenn keine Gespräche mehr aktiv sind. Damit wird das Trennen bestehender Gespräche durch den Neustart vermieden.

Bei unsachgemäßer Konfiguration kann es vorkommen, dass das Gateway nach der Aktivierung einer neuen Konfiguration nicht mehr erreichbar ist. Dies ist zum Beispiel dann der Fall, wenn die Parameter der Ethernet Schnittstelle, wie IP-Adresse oder Subnetzmaske falsch eingestellt werden. In einem solchen Fall könnte der Fehler mit der Konfigurationsoberfläche nicht mehr behoben werden.

Daher verwirft das Gateway die aktivierte Konfiguration und restauriert die Konfiguration aus dem nicht-flüchtigen Speicher, falls nicht innerhalb von 60 Sekunden ein Zugriff von der Konfigurationsoberfläche oder über **telnet** erfolgt. Das Konfigurationsapplet verbindet sich nach einem **Save**, **Activate** oder **Reset** automatisch erneut mit dem Gateway, so dass im Erfolgsfall die neue Konfiguration automatisch erhalten bleibt.

Achtung

Bedenken Sie bitte, dass nach einem **Save** im Zweifel keine funktionstüchtige Konfiguration mehr rekonstruiert werden kann. Insbesondere im Fernwartungsfall ist dann unter Umständen kein Zugriff auf das Gerät mehr möglich. Es wird daher dringend empfohlen, jede Konfigurationsänderung zunächst per **Activate** zu testen.

Wollen Sie Ihre Änderungen seit dem letzten Betätigen von **Save** verwerfen, können Sie dies mit der Schaltfläche **Cancel** tun. Hierbei wird die aktuelle Konfiguration durch die zuletzt im nichtflüchtigen Speicher gesicherte Konfiguration ersetzt.

4 Konfiguration der IP Schnittstellen

4.1 Konfiguration der Ethernet Schnittstelle

Die Ethernet IP Schnittstelle wird normalerweise während der Inbetriebnahme konfiguriert und muss später meist nicht mehr verändert werden. Sollte dies doch der Fall sein, können Sie die Einstellungen im Konfigurationsapplet **IP Interfaces > Ethernet Interface** vornehmen.

Die DHCP Funktion des Gateways hat insgesamt vier Betriebsmodi:

Modus	Funktion	Anwendung
Off	keine DHCP Funktion	Wenn Sie die IP-Parameter fest konfigurieren.
Server	DHCP Server[1] aktiv	Angeschlossene Geräte bekommen eine IP-Adresse vom Gateway zugewiesen.
Client	DHCP Client aktiv	Das Gateway erhält seine IP-Konfiguration von einem DHCP Server im Netz. Kapitel 4.1.1 "DHCP Konfigurationsoptionen" ab Seite 27 listet die ausgewerteten DHCP Optionen auf.
Automatic	Nach Einschalten ist der DHCP Client aktiv, nach einem Reset der DHCP Server	Das Gateway ist im Auslieferungszustand (und damit auch nach einem langen Reset [siehe Kapitel 2.2.1 "Herstellen der Standardkonfiguration" ab Seite 11]) in diesem Zustand[2].

1.Diese Einstellung ist nur in Ausnahmefällen sinnvoll, da die Gateways keinen vollständigen DHCP Server enthalten. Sie wird hauptsächlich in Test- oder Demoaufbauten verwendet.
2.Diese Einstellung ist nur anfänglich sinnvoll. Sie sollte während der Inbetriebnahme auf jeden Fall durch die Einstellung "off" oder "Client" ersetzt werden.

Tabelle 4

- Zur vollständigen Konfiguration der Ethernet Schnittstelle muss gegebenenfalls noch das Standardgateway Ihres Netzwerkes als **Default IP Router** eingetragen werden.
- Müssen jenseits des Standard-Gateways noch weitere Routen eingefügt werden, kann dies über die Schaltfläche **Add IP route** erfolgen.

  Geben Sie für Netzwerkrouten die **Network address** mit dem Hostanteil zu 0 sowie die korrekte **Network mask** an.

  Geben Sie für Hostrouten die komplette IP-Adresse des Hosts und die **Network mask** `255.255.255.255` an.

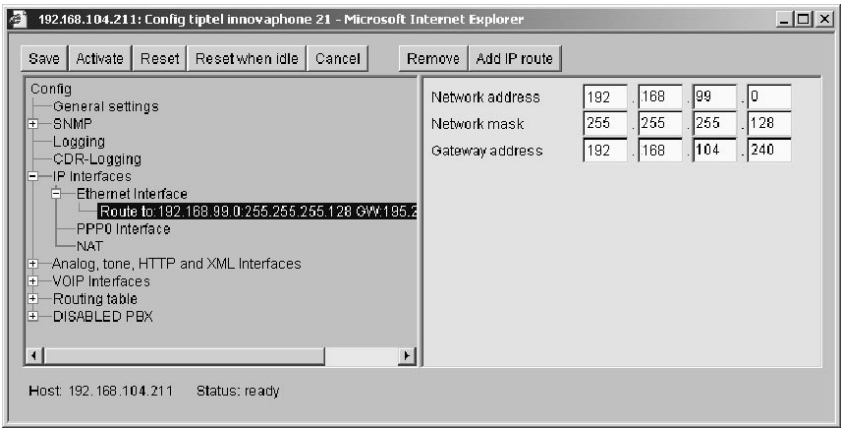

Abbildung 4 Anfügen von Routen zum Ethernet Interface

- Falls Ihr Gateway nicht zusätzlich noch die Funktion eines WAN-Routers übernehmen soll, lassen Sie den Eintrag **DNS server address** leer und deaktivieren Sie das Kontrollkästchen **Do proxy-ARP.**
- Normalerweise aktivieren Sie das Kontrollkästchen **Full duplex** nicht.

Tipp

Diese Option ist nur bei der IP 400 notwendig. Die IP 3000, IP 3000DD, IP 800, IP 202 und die IP 21 handeln den Vollduplex Modus automatisch mit dem Switch bzw. Hub aus.

- Aktivieren Sie das Kontrollkästchen 802.1p, wenn die Ethernet Pakete des

Gerätes im Switch priorisiert werden sollen.

4.1.1 DHCP Konfigurationsoptionen

Der DHCP Klient Ihres Gateways verarbeitet neben der eigentlich zugewiesenen IP-Adresse die in Tabelle 5 aufgeführten DHCP Optionen, sofern Sie bei der Erteilung des DHCP-Leases mitgeteilt werden.

Per DHCP mitgeteilte Optionen überschreiben immer eventuell in der Gatewaykonfiguration festgelegte Parameter.

DHCP #	DHCP Name	überschriebener Konfigurationsparameter	Beschreibung
001	Subnet mask	**IP address mask**	Die gemeldete Netzmaske wird verwendet.
002	Time offset	**Offset to UTC**	Der Abstand zur Weltzeit in Sekunden.
003	Routers	**Default Gateway**	Aus der Liste der gemeldeten Router wird der erste Eintrag als IP-Standardgateway verwendet.
006	Domain name servers	**DNS server address**	Aus der Liste der gemeldeten DNS Server werden die ersten beiden Einträge als DNS Server verwendet.
042	NTP servers	**SNTP server IP address**	Aus der Liste der gemeldeten NTP Server wird der erste Eintrag als NTP-Server verwendet.

Tabelle 5 DHCP Konfigurationsoptionen

4.1.2 Full duplex Ethernet

Der Ethernet controller der IP 400 kann in den Vollduplex Betriebsmodus gebracht werden. Im Normalfall wird die IP 400 im Halbduplex Modus betrieben.

Zum Vollduplexbetrieb:

- Navigieren Sie im Konfigurationsapplet zu **IP Interfaces > Ethernet Interface**.
- Markieren Sie **Full duplex** im Formular **Ethernet Interface**.
- Stellen Sie Ihren Ethernet Switch so ein, dass er für den Port, an dem die IP 400 angeschlossen ist, auf jeden Fall im Vollduplexbetrieb läuft. Dies ist notwendig, da der Betriebsmodus von der IP 400 nicht ausgehandelt wird. Stimmen die Einstellungen von IP 400 und Ethernet Switch nicht überein, kommt es zu Fehlfunktionen.

4.1.3 Priorisierung auf dem Ethernet

Die vom Gerät gesendeten Ethernet Pakete können im Switch auf Ebene 2 priorisiert werden. Dazu müssen die Pakete beim Senden entsprechend markiert werden. Diese Funktion muss vom verwendeten Switch unterstützt sein.

- Selektieren Sie im Konfigurationsapplet **IP Interfaces > Ethernet Interface**.
- Um die gesendeten Pakete mit der VLAN id 0 und der Priorität 7 zu markieren, markieren Sie **Use 802.1p for Quality of Service.**
- Die VLAN id mit dem Wert 0 schaltet die QoS nach 802.1Q ab. Ist das Editierfeld **802.1 Q VLAN id** leer, wird der Wert 0 angenommen. Sollte Ihr Switch auf dem Port zum innovaphone Gateway auf eine andere VLAN id konfiguriert sein, müssen Sie hier den gleichen Wert angeben, damit eine Priorisierung der Ethernet Pakete funktionieren kann.

Achtung

Zur Einstellung der **VLAN id** beachten Sie unbedingt die Konfiguration am Switch.

Der Zugriff der innovaphone Geräte auf die VLAN ID und die VLAN Priority kann auch über DHCP erfolgen. Für weitere Informationen zum DHCP-Client und VLAN -ID und -Priority siehe Anhang D: "Der innovaphone DHCP Client" ab Seite 155.

4.2 Konfiguration der WAN Schnittstellen

Ihr Gateway kann auch als ISDN- oder PPPoE- (PPP über Ethernet) Router eingesetzt werden. In diesem Fall übernimmt es den Transport der TCP/IP-Daten zwischen Ihrem lokalen Netzwerk und der WAN Verbindung, ganz gleich, ob es sich dabei um Sprache oder sonstige Daten handelt.

Die Geräte bieten verschiedene Möglichkeiten, um ins WAN zu routen. Die Nutzung von ISDN als WAN Schnittstelle ist bei der IP 400 serienmäßig gegeben. Die IP 400 unterstützt PPPoE als WAN Schnittstelle.

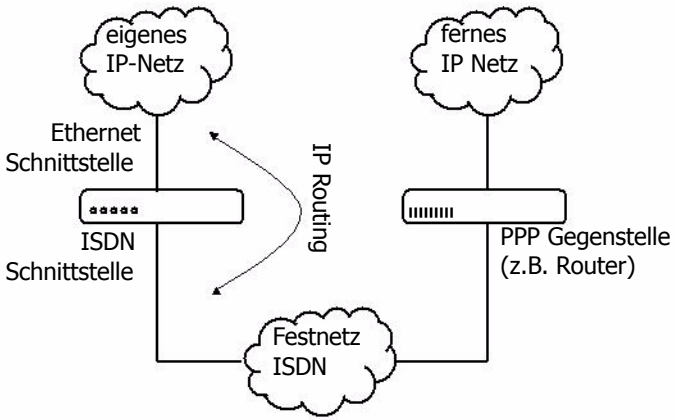

Abbildung 5 Einsatz des Gateways als ISDN Router

Als PPP Gegenstelle kommt jeder PPP fähige ISDN- oder PPPoE Router in Frage. Abbildung 5 auf Seite 29 zeigt den Zugriff auf ein entferntes IP-Netz mit einer IP 400 als ISDN Router. Abbildung 6 auf Seite 30 zeigt den Zugriff auf das Internet über einen DSL Anschluss.

Die IP 400 besitzt 4 konfigurierbare PPP-Interfaces.

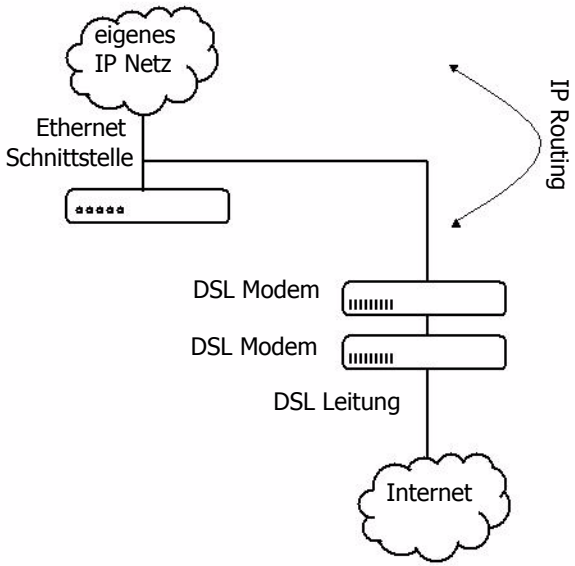

Abbildung 6 Anschluss an eine DSL Leitung über PPPoE

Die Verbindung kann auch direkt zwischen zwei Gateways hergestellt werden, beispielsweise im Rahmen einer TK-Anlagenkopplung zwischen zwei Standorten über eine ISDN Festverbindung. Abbildung 7 auf Seite 30 zeigt eine derartige Konfiguration.

Abbildung 7 Gatewaykopplung mit ISDN Festverbindung

Eine spezielle Anwendung der ISDN WAN Schnittstelle ist die Einwahl in das Gateway zu Wartungszwecken. Hierdurch kann die Fernwartbarkeit des Gateways gewährleistet werden, ohne Zugriff auf das lokale IP-Netz vorauszusetzen, wie Abbildung 8 auf Seite 31 zeigt.

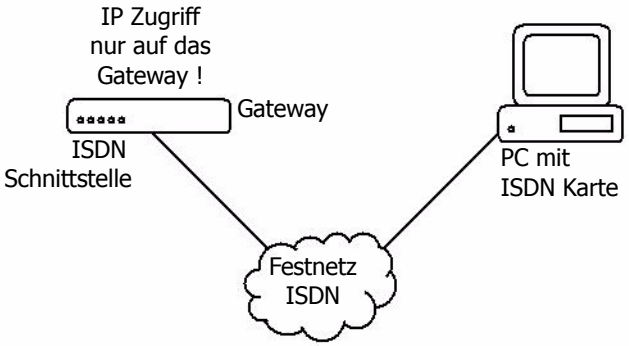

Abbildung 8 Fernwartungszugriff über ISDN

4.2.1 Generelle Überlegungen zur Konfiguration der PPP Verbindungen

Verbindungsaufbau

Die Gateways bauen normalerweise bei Verwendung von Wählleitungen keine Verbindungen selbsttätig auf. Eine PPPoE Verbindung wird dabei als Wählleitung verstanden. PPP Verbindungen kommen daher nur dann zustande, wenn ein eingehender Datenruf für eine konfigurierte PPP Schnittstelle empfangen wird oder wenn über die Administrationsoberfläche im Bereich **IP Interfaces** der Verbindungsaufbau explizit initiiert wird. Dadurch bleibt die volle Kontrolle über Kosten verursachende Datenverbindungen bestehen, insbesondere können Ereignisse im lokalen Netz keinen unerwünschten Verbindungsaufbau bewirken (kein **dial on demand**).

Achtung

In einigen Fällen kann es jedoch gewünscht sein, eine Wählleitung ständig offen zu halten. Dies wird erreicht durch die Einstellung Automatic dial after boot. Sie bewirkt, dass die entsprechende PPP Verbindung sofort nach dem Starten des Gateways aufgebaut und immer offen gehalten wird. Wenden Sie diese Einstellung mit der entsprechenden Vorsicht an.

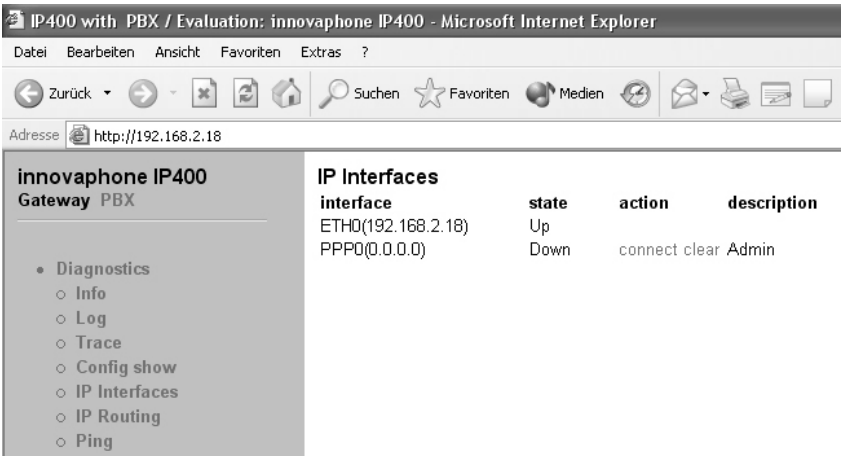

Abbildung 9 Verbindungskontrolle in der Administrationsoberfläche

Der Link **connect** veranlasst den Aufbau der ausgewählten Verbindung. Der Link **clear** veranlasst dagegen den Abbau der Verbindung.

Kanalbündelung (multi link)

Die Gateways unterstützen die Kanalbündelung auf 2 ISDN B-Kanälen (128 kbps).

Adressierung der WAN Schnittstellen

Normalerweise erhalten die WAN Schnittstellen eines Routers eigene IP-Adressen (normalerweise aus einem besonderen Transfernetz). Dies ist bei den Gateways nicht erforderlich, Sie benötigen also keine besonderen IP-Adressen außer der Ihres eigenen IP-Netzwerks.

Komprimierung von Sprachdaten auf der PPP Strecke

Die Gateways unterstützen die Kompression von Sprachdaten auf der PPP Strecke nach dem Verfahren **RTP Header Compression** (entsprechend RFC 2508 / 2509). Hierdurch wird die benötigte Bandbreite für VoIP Gespräche drastisch reduziert.

Ist die verwendete PPP Gegenstelle kein innovaphone Gateway, kann es in der Praxis zu Kompatibilitätsproblemen kommen. Wird auf der Gegenseite ein Cisco Router eingesetzt und kommt es zu Problemen bei der Übertragung von Sprachdaten, probieren Sie die Option **Adjust for Cisco's PPP implementation**.

Konfiguration der IP Routen

Zu jeder PPP Schnittstelle können Sie mit der Schaltfläche **Add IP route** separate IP Routen hinzufügen. Die Konfiguration erfolgt wie bei den Routen der Ethernet Schnittstelle (siehe Kapitel 4.1 "Konfiguration der Ethernet Schnittstelle" ab Seite 25). Alle IP Routen müssen explizit definiert werden. Über eine PPP Schnittstelle, für die keine IP Routen definiert sind, werden keinerlei Daten gerouted.

Beachten Sie jedoch bitte, dass die konfigurierten IP Routen statische Routen sind, die immer aktiv sind. Dies auch dann, wenn die entsprechende PPP Schnittstelle nicht verbunden ist. Einander überlagernde IP Routen auf verschiedenen PPP Schnittstellen (zum Beispiel mehrere **Default Routes**) sind daher nicht möglich.

4.2.2 Einstellungen für ausgehende ISDN PPP Wahlverbindungen

Hierdurch konfigurieren Sie Ihr Gateway für eine ausgehende PPP Datenverbindung:

- Selektieren Sie im Konfigurationsapplet den Pfad **IP Interfaces > PPPn Interface**, wobei n dem jeweiligen zu konfigurierenden PPP Interface entspricht.
- Entfernen Sie **Automatic dial after boot.**
- Entfernen Sie **Multilink.**
- Entfernen Sie **Permanent connection.**
- Wählen Sie im Auswahlfeld **Port** den oder die ISDN Schnittstellen, auf denen Sie den ausgehenden Ruf tätigen wollen.
- Das Auswahlfeld **Channel** hat nur für Festverbindungen eine Bedeutung und ist daher hier nicht veränderbar.
- Tragen Sie im Feld **Subscriber number** die für den Ruf zu verwendende rufende MSN ein. Diese kann in der Regel auch leer bleiben.
- Entfernen Sie **Allow incoming calls.**
- Entfernen Sie **Assign remote IP address**.

Tipp

Dadurch wird der gerufenen Seite keine IP-Adresse während des PPP Verbindungsaufbaus zugewiesen. Dies ist bei ausgehenden Rufen nicht üblich.

- Lassen Sie das Feld **Check remote number** leer.
- Soll sich die gerufene PPP Gegenstelle bei Ihrem Gateway selbst authentifizieren, tragen Sie in den Feldern **User** und **Password** im Bereich **Incoming calls** die entsprechenden Daten ein.
- Tragen Sie die Rufnummer der zu rufenden PPP Gegenstelle im Feld **Dial remote number** ein.
- Soll sich Ihr Gateway bei der gerufenen PPP Gegenstelle authentifizieren, tragen Sie in den Feldern **User** und **Password** im Bereich **Outgoing calls** die entsprechenden Daten ein.
- Konfigurieren Sie die IP-Routen, wie im Kapitel "Konfiguration der IP Routen" ab Seite 33 beschrieben.

Erweiterung auf Multilink

Sie können an Stelle einer Verbindung über einen B-Kanal auch eine **multilink** Verbindung über 2 gebündelte Kanäle konfigurieren.

- Selektieren Sie im Konfigurationsapplet den Pfad **IP Interfaces > PPPn Interface**, wobei **n** dem jeweiligen zu konfigurierenden PPP Interface entspricht.
- Markieren Sie **Multilink (128K ISDN) in der Gruppe Ports for PPP.**
- Muss für den zweiten Kanal der zu rufenden PPP Gegenstelle eine andere Rufnummer verwendet werden, tragen Sie diese im Feld **Dial remote number** im Bereich **Numbers for 2nd Multilink channel** ein. Kann die gleiche Rufnummer wie für den ersten Kanal verwendet werden, lassen Sie dieses Feld leer.
- Tragen Sie im Feld **Local subscriber number** die für den zweiten Kanal zu verwendende ausgehende Nummer ein. Diese kann in der Regel auch leer bleiben.

4.2.3 Einstellungen für eingehende ISDN PPP Wahlverbindungen

Hierdurch konfigurieren Sie Ihr Gateway für eine eingehende PPP Datenverbindung:

- Selektieren Sie im Konfigurationsapplet den Pfad **IP Interfaces > PPPn Interface** des zu konfigurierenden PPP Interface.
- Entfernen Sie **Automatic dial after boot.**
- Entfernen Sie **Multilink.**
- Entfernen Sie **Permanent connection.**

- Wählen Sie im Auswahlfeld **Port** den oder die ISDN Schnittstellen, auf denen Sie den eingehenden Ruf akzeptieren wollen.
- Das Auswahlfeld **Channel** hat nur für Festverbindungen eine Bedeutung und ist daher hier nicht veränderbar.
- Tragen Sie im Feld **Subscriber number** die Rufnummer ein, unter der eingehende Rufe akzeptiert werden sollen. Diese sollte nicht leer bleiben.

Tipp

Bleibt dieses Feld leer, so werden alle Datenrufe auf den gewählten ISDN Schnittstellen akzeptiert. Allerdings ist es in diesem Fall nicht möglich, diese Rufe den verschiedenen PPP Schnittstellen zuzuordnen. Derartige Konfigurationen sollten daher vermieden werden.

- Markieren Sie **Allow incoming calls.**
- Entfernen Sie **Assign remote IP address**, wenn die rufende PPP Gegenstelle über eine feste IP-Adresse verfügt. Dadurch wird der gerufenen Seite keine IP-Adresse während des PPP Verbindungsaufbaus zugewiesen. Dies ist bei ausgehenden Rufen nicht üblich. Markieren Sie **Assign remote IP address**, wenn es sich bei der rufenden PPP Gegenstelle um ein Gerät handelt, das eine dynamisch zugewiesene IP-Adresse benötigt. Dies ist z.B. bei einem Windows-PC der Fall, der über das DFÜ-Netzwerk in ein Gateway hineinruft. Tragen Sie in diesem Fall die IP-Adresse, die zugewiesen werden soll im Feld **IP address** ein und fügen Sie der PPP Schnittstelle eine IP-Route für genau diese IP-Adresse hinzu (siehe Kapitel "Konfiguration der IP Routen" ab Seite 33).
- Soll die Einwahl auf eine einzelne PPP Gegenstelle begrenzt werden, tragen Sie deren Rufnummer im Feld **Check remote number** ein. Das Ende der Rufnummer des Anrufers wird mit dem Inhalt dieses Feldes verglichen und muss übereinstimmen, sonst wird der Ruf abgewiesen. Ist im Feld beispielsweise die Nummer `7031730090` eingetragen, werden Rufe sowohl von `07031730090`, als auch von `004907031730090` akzeptiert.
- Soll sich die rufende PPP Gegenstelle bei Ihrem Gateway authentifizieren, tragen Sie in den Feldern **User** und **Password** im Bereich **Incoming calls** die entsprechenden Daten ein.
- Lassen Sie das Feld **Dial remote number** leer.
- Soll sich Ihr Gateway bei der rufenden PPP Gegenstelle authentifizieren, tragen Sie in den Feldern **User** und **Password** im Bereich **Outgoing calls** die

entsprechenden Daten ein.

- Konfigurieren Sie die IP-Routen, wie im Kapitel "Konfiguration der IP Routen" ab Seite 33 beschrieben.

Erweiterung auf Multilink

Sie können an Stelle einer Verbindung über einen B-Kanal auch eine **multilink** Verbindung über 2 gebündelte Kanäle akzeptieren.

- Markieren Sie **Multilink.**
- Lassen Sie die Felder **Dial remote number** und **Local subscriber number** im Bereich **Numbers for 2nd Multilink channel** leer. Ihr Gateway akzeptiert die Rufe für beide Kanäle auf der gleichen im Feld **Subscriber number** konfigurierten Nummer.

4.2.4 Einstellungen für ein- und ausgehende ISDN PPP Wahlverbindungen

Sie können eine PPP Schnittstelle auch für wahlweise ein- und ausgehende Rufe konfigurieren. Kombinieren Sie dazu die vorher für ein- und ausgehende Rufe beschriebenen Einstellungen.

4.2.5 Besonderheiten beim WAN Anschluss über Ethernet (PPPoE)

Der WAN-Anschluss über PPPoE, beispielsweise an einem DSL Modem, funktioniert denkbar einfach. Beachten Sie jedoch, dass in dieser Betriebsart nur ausgehende Rufe möglich sind.

Der PPPoE Anschluss – also beispielsweise das DSL Modem - muss am gleichen Ethernet Segment (bzw. –Switch) wie das Gateway angeschlossen sein.

PPPoE Verbindungen sind grundsätzlich Wahlverbindungen wie ISDN Verbindungen auch. Allerdings bieten verschiedene Provider so genannte **Flatrates** an, bei denen die anfallenden Gebühren unabhängig von der Verbindungsdauer sind. In solchen Fällen ist es möglich und sinnvoll, die PPPoE Verbindung ständig offen zu halten.

Falls die Verbindung mit inoffiziellen IP Adressen betrieben wird, die aber bekannt sind, wird die Network Address Translation (NAT) nicht benötigt. Zur Deaktivierung von NAT setzen Sie die Option **Exclude from NAT**. NAT muss nur bei einem Netz aktiviert sein, das offizielle IP Adressen benötigt.

- Markieren Sie **Automatic dial after boot**, wenn Sie die PPPoE Verbindung ständig offen halten wollen. Andernfalls, oder wenn Sie sich unsicher über die

anfallenden Gebühren sind, entfernen Sie diese Markierung.

- Entfernen Sie **Multilink.**
- Entfernen Sie **Permanent connection.**
- Wählen Sie im Auswahlfeld **Port** die Einstellung **PPPOE.**
- Das Auswahlfeld **Channel** hat nur für ISDN Festverbindungen eine Bedeutung und ist daher hier nicht veränderbar.
- Lassen Sie das Feld **Subscriber number** leer, es hat keine Bedeutung.
- PPPoE Verbindungen sind nur ausgehend möglich, entfernen Sie daher **Allow incoming calls.**
- Entfernen Sie **Assign remote IP address**.

Tipp

Dadurch wird der gerufenen Seite keine IP-Adresse während des PPP Verbindungsaufbaus zugewiesen. Dies ist bei ausgehenden Rufen nicht üblich.

- Lassen Sie das Feld **Check remote number** leer, es hat keine Bedeutung.
- Lassen Sie die Felder **User** und **Password** im Bereich **Incoming calls** leer, sie haben keine Bedeutung.
- Lassen Sie das Feld **Dial remote number** leer, es hat keine Bedeutung.
- Soll sich Ihr Gateway bei der gerufenen PPP Gegenstelle authentifizieren, tragen Sie in den Feldern **User** und **Password** im Bereich **Outgoing calls** die entsprechenden Daten ein.
- Konfigurieren Sie die IP-Routen, wie im Kapitel "Konfiguration der IP Routen" ab Seite 33 beschrieben.

4.2.6 Einstellungen für VPN Verbindungen mit PPTP

Das Point-to-Point Tunneling Protokoll (PPTP) realisiert virtuelle, private Verbindungen (VPN) über das Internet oder andere mit Internet Protokoll betriebene Netzwerke.

Die PPTP Verbindungen sind grundsätzlich Wählverbindungen. Gewählt wird eine IP Adresse. Die Authentifizierung erfolgt mittels Benutzername und Passwort. Zusätzlich können die übertragenen Sprachdaten mit der Microsoft Point-to-Point Encryption (MPPE) verschlüsselt werden. Voraussetzung ist jedoch, dass auch die Gegenstelle dieses Verfahren unterstützt.

Da jede Verschlüsselung und Entschlüsselung Zeit benötigt, kann es zur Verzöge-

rungen der Sprache kommen, wodurch die Qualität der Übertragung leidet. Sollten solche Qualitätsverluste auftreten, müssen Sie zwischen Sicherheit oder Sprachqualität selbst entscheiden.

Die innovaphone VoIP Gateways können sich sowohl als PPTP Client in einen fernen Server einwählen, als auch selbst einen Einwahlpunkt zur Verfügung stellen. Für die Kopplung von zwei innovaphone VoIP Gateways über das Internet kann das PPTP optimal eingesetzt werden.

Falls beide Seiten ein Netz mit inoffiziellen IP Adressen betreiben, die untereinander aber bekannt sind, wird die Network Address Translation (NAT) nicht benötigt. Zur Deaktivierung von NAT setzen Sie die Option **Exclude from NAT**. NAT wird nur benötigt, wenn der Tunnel zu einem Netz aufgebaut wird, das offizielle IP Adressen benötigt.

Einwahl des VoIP Gateways (Client) in einen PPTP Server

- Selektieren Sie im Konfigurationsapplet den Pfad **IP Interfaces > PPPn Interface** des zu konfigurierenden PPP Interface.
- Selektieren Sie in der Auswahl **Port** das Protokoll **PPTP**.
- Geben Sie unter **PPTP-IP address** die IP Adresse des fernen PPTP Servers an, mit dem Sie das VPN aufbauen wollen.
- Schalten Sie die Option **Allow incoming calls** aus.
- Setzten Sie **Enable Encryption**, **Exclude from NAT** und **No DNS on this port** entsprechend Ihren Erfordernissen.
- Geben Sie in der Gruppe **Outgoing calls** den **User** und das **Password** an, mit dem Sie sich beim fernen PPTP Server registrieren wollen.

Einrichten eines PPTP Server

- Selektieren Sie im Konfigurationsapplet den Pfad **IP Interfaces > PPPn Interface** des zu konfigurierenden PPP Interface.
- Selektieren Sie in der Auswahl **Port** das Protokoll **PPTP**.
- Geben Sie unter **PPTP-IP address** keine IP Adresse an.
- Schalten Sie die Option **Allow incoming calls** ein.
- Setzten Sie **Enable Encryption**, **Exclude from NAT** und **No DNS on this port** entsprechend Ihren Erfordernissen.
- Setzten Sie die Option **Assign remote IP address**, um der einwählenden Gegenstelle eine IP Adresse aus Ihrem Netz zuzuordnen. Geben Sie diese IP-Adresse im Feld **IP address** ein.
- Geben Sie in der Gruppe **Incoming calls** den **User** und das **Password** an,

mit dem sich der ferne PPTP Client registrieren soll.

4.2.7 Die Fernwartungseinrichtung in der Standardkonfiguration

In der Standardkonfiguration wird die **PPP** ISDN Schnittstelle zur Einwahl für Fernwartungszwecke konfiguriert. Damit kann das Gateway von jedem PC mit einer ISDN Karte und einem PPP DFÜ Programm (z.B. dem "DFÜ-Netzwerk" in Windows) aus fernkonfiguriert werden.

Tipp

Standardmäßig ist diese Voreinstellung disabled. Zum Aktivieren der voreingestellten Fernwartungseinrichtung deaktivieren Sie die Option Disable im Konfigurationsapplet unter **IP Interfaces > PPP0 Interface > Interface name and general config**.

Die Einstellungen für diesen Zugang sind in der logischen Schnittstelle PPP0 konfiguriert, die Sie unter **IP Interfaces > PPP0 Interface** ansehen und ggf. modifizieren können.

- Rufe werden auf der Schnittstelle **PPP** entgegengenommen (**ISDN Port** ist **PPP**, Kontrollkästchen A**llow incoming calls** ist markiert).
- Es werden Rufe an jede MSN angenommen (**Subscriber number** ist leer).
- Der rufenden Seite wird eine IP-Adresse (`192.168.0.253`) zugewiesen (Das Kontrollkästchen **Assign remote IP address** ist markiert).
- Es werden Rufe von allen Gegenstellen akzeptiert (**Check remote Number** ist leer).
- Als Nutzer (**User**) wird `admin` und als Kennwort (**Password**) wird `ip400` verwendet.
- Eine rückwärtige Authentifizierung findet nicht statt (die Felder unter **Outgoing calls** sind leer).
- Das gerufene Gateway selbst bekommt die IP-Adresse `192.168.0.254`.

Tipp

Diese IP-Adresse sollte sich unter normalen Umständen nicht mit der Adresse eines Gerätes am LAN überschneiden. Befindet sich ausnahmsweise doch ein Gerät mit der IP-Adresse `192.168.0.254` am Netz, so wird das Gateway selbst mit diesem Gerät nicht kommunizieren können. Diese Adresse ist fest in das Gateway einprogrammiert. Somit ist sicher gestellt, dass ein Gateway über die Fernwartungseinrichtung immer unter dieser IP-Adresse ansprechbar ist, unabhängig davon, welche IP-Adresse auf der Ethernet Schnittstelle des Gateways eingestellt ist.

Durch diese Konfiguration kann das Gateway durch Einstecken eines ISDN S_0 Mehrgeräteamtsanschlusses (also etwa eine S_0 Amtsleitung oder ein S_0 Teilnehmeranschluss einer TK-Anlage) in die **PPP** Schnittstelle von jedem PC mit PPP Einwahlapplikation konfiguriert werden.

Natürlich kann diese Konfiguration an die lokalen Gegebenheiten angepasst werden. Lesen Sie dazu die Hinweise in Kapitel 4.2.3 "Einstellungen für eingehende ISDN PPP Wahlverbindungen" ab Seite 34.

4.2.8 Einwahlzugriff auf das gesamte Netz erlauben

Bei IP-Paketen, die vom Ethernet über das Gateway auf logische PPP Schnittstellen geroutet werden sollen, kann sich das Gateway dem lokalen Netz gegenüber so darstellen, als ob es das angesprochene Endgerät selbst wäre. Damit können auch IP-Endgeräte am gleichen Ethernet Segment, die über keine korrekte Routingeinstellung verfügen, über das Gateway hinweg kommunizieren und die WAN Verbindung nutzen. Diese als **proxy arp** bezeichnete Funktion wird aktiviert, in dem im Bereich **Ethernet Interface** des Konfigurationsapplets das Kontrollkästchen **Do proxy-ARP** aktiviert wird.

Zu diesem Zweck muss der per ISDN verbundenen Gegenstelle eine IP-Adresse aus dem gleichen Subnetz zugewiesen werden, aus dem auch die IP-Adresse des Gateways stammt. Die geschieht durch einen entsprechenden Eintrag im Bereich **Remote IP address** und markieren des Kontrollkästchens **Assign remote IP address**.

Beachten Sie jedoch unbedingt, dass damit für den Einwählenden das gesamte eigene Netz zugreifbar wird, was unter Umständen ein Sicherheitsproblem darstellen kann.

4.2.9 Das ENUM-Protokoll

ENUM steht für ein Protokoll, dass sich mit der Abbildung von so genannten E.164-Nummern auf Uniform Resource Identifier (URI) befasst. Es definiert eine Vorschrift, mit der eine Telefonnummer in eindeutiger Weise auf eine Domain abgebildet wird. Diese Domain kann dann zur Identifizierung zum Beispiel von IP-Telefonie-Adressen herangezogen werden.

ENUM nutzt dazu das Domain Name System (DNS). Eine Aufgabe des DNS ist die Herstellung einer logischen Verbindung zwischen den Adressen der ans Internet angeschlossenen Rechner (die über rein numerische IP-Adressen identifiziert werden) und Domains, die den Vorteil haben, sich leichter merken zu lassen. Die meisten Internetnutzer kennen Domains bisher wahrscheinlich nur im Zusammenhang mit E-Mail-Adressen oder Web-Präsenzen. Die DNS-Infrastruktur und das ENUM-Protokoll ermöglichen aber, Telekommunikationsdienste mittels Domains abzufragen und anzusprechen. Im Gegensatz zu Web-Domains kann sich der Nutzer die ENUM-Domain allerdings nicht frei auswählen, da eine feste Vorschrift existiert, wie zu einer Telefonnummer die korrespondierende ENUM-Domain gebildet wird. Die entsprechende ENUM-Domain kann daher nur vom Inhaber der betreffenden Rufnummer angemeldet werden. Durch den Internet Service Provider (ISP) muss das ENUM-Protokoll unterstützt werden.

Durch die Verknüpfung von Telefonnummern und Internet-Ressourcen ergeben sich völlig neue Dienste. Ein Basisdienst ist das Auffinden eines telefoniefähigen Internet-Endgerätes von einem herkömmlichen Telefon aus. Optional liefert ENUM aber auch Hinweise auf zusätzliche Kommunikationsmöglichkeiten. Sollte ein telefoniefähiges Internet-Endgerät nicht erreichbar sein, kann aus der Liste weiterer Anwendungen eine entsprechende Alternative ausgewählt werden.

Ein Beispiel soll das Prinzip verdeutlichen: Nach Eingabe eine Rufnummer, für die ENUM-Informationen verfügbar sind, wird der Anruf zunächst auf einen Festnetzanschluss geschaltet. Sollte dort niemand abnehmen, wird auf die eingetragene Handynummer weitergeleitet. Sollte auch hier keine Verbindung zustande kommen, könnte die Nachricht aufgezeichnet und als Audio-Datei an eine E-Mail-Adresse gesandt werden. Denkbar wäre auch die Abfrage einer Webseite, die dann Auskunft über weitere Kommunikationsmöglichkeiten liefert.

Dieses Beispiel verdeutlicht auch den Vorteil des neuen Systems: Statt einer Vielzahl von Rufnummern für die verschiedenen Anwendungen reicht eine Rufnummer aus. Die Zuordnung zu den jeweils passenden Ausgabegeräten übernehmen die Einträge im ENUM-Nameserver. Ein eingehendes Fax wird somit automatisch auf das richtige Endgerät geleitet.

Die Verwendung von ENUM bietet für moderne Kommunikationsszenarien eine

Vielzahl an Möglichkeiten mit einem entsprechend großen Anwendungspotenzial in unterschiedlichen Bereichen. Beispielsweise beim Routing: hier können PSTN-Netzwerke und VoIP-Netzwerke miteinander verknüpft werden.

4.2.10 ENUM-Protokoll auf einem innovaphone Gateway einrichten

Um das ENUM-Protokoll nutzen zu können, ist die Einrichtung von drei VoIP Interfaces notwendig. Zum Übermitteln von ENUM-Rufen über die innovaphone PBX, zum Empfang eingehender ENUM-Rufe und um diese eingehenden ENUM-Rufe an die innovaphone PBX weiterzuleiten.

Zur Einrichtung des ENUM-Protokolls auf Ihrem innovaphone Gateway gehen Sie wie folgt vor:

- Starten Sie das Konfigurationsapplet Ihres innovaphone Gateways (siehe Kapitel 3.1 "Allgemeines zur Konfigurationsoberfläche" ab Seite 21).
- Selektieren Sie im Konfigurationsapplet den Pfad **Config > VoIP Interfaces > GWn**, wobei n dem jeweiligen zu konfigurierenden VoIP Interface entspricht, z. B. **GW1**.
- Geben Sie im Bereich **VoIP Interface name and general config** im Feld **Description** eine Kurzbezeichnung ein, z. B. `ENUM`.
- Selektieren Sie im Bereich **Mode** den zugehörigen Modus **Enum Gateway**.
- Im Bereich **Enum** können Sie im Feld **Suffix** einen Eintrag vornehmen. In der Regel ist kein Eintrag erforderlich. Bleibt das Feld leer, wird mit der internen Voreinstellung `e164.arpa` gearbeitet.

Somit ist das ENUM-Interface für ausgehende Rufe fertig konfiguriert. Auf die Einrichtung der Routen wird später eingegangen. Als nächster Schritt wird ein innovaphone PBX-Interface eingerichtet, sofern dieses noch nicht vorhanden ist. Im folgenden Beispiel gehen wir davon aus, dass **GW2** unser Gateway für das Amt der PBX ist und sich mit dem Alias `Amt` oder `PBX` und der Nummer `0` in der PBX `127.0.0.1` registriert:

- Selektieren Sie im Konfigurationsapplet den Pfad **Config > VoIP Interfaces > GWn**, wobei n dem jeweiligen zu konfigurierenden VoIP Interface entspricht, z. B. **GW2**.
- Geben Sie im Bereich **VoIP Interface name and general config** im Feld **Description** eine Kurzbezeichnung ein, z. B. `PBX`.
- Selektieren Sie im Bereich **Mode** den zugehörigen Modus **Registration at gatekeeper as gateway**.
- Geben Sie im Bereich **Remote gatekeeper address** im Feld **IP address**

die IP-Adresse `172.0.0.1` ein. Sollte eine **Gatekeeper ID** und ein **Password** notwendig sein, vervollständigen Sie bitte diese Angaben.

- Legen Sie einen zugehörigen **alias** Eintrag an. Dies geschieht, indem Sie die Schaltfläche **Add alias** betätigen. Für weitere Informationen zum **alias** Eintrag siehe Kapitel 6.2 "Verwaltung von VoIP Geräten per RAS (Gatekeeper)" ab Seite 83.

Somit ist das PBX-Interface fertig konfiguriert. Für weitere Informationen zum PBX-Interface siehe im "innovaphone PBX - Administrator-Handbuch".

Als nächster Schritt wird ein Interface für eingehende Rufe eingerichtet, sofern dieses noch nicht vorhanden ist. Das Interface muss die Annahme von beliebigen IP-Adressen ohne vorherige Registrierung erlauben:

- Selektieren Sie im Konfigurationsapplet den Pfad **Config > VoIP Interfaces > GWn**, wobei n dem jeweiligen zu konfigurierenden VoIP Interface entspricht, z. B. **GW3**.
- Geben Sie im Bereich **VoIP Interface name and general config** im Feld **Description** eine Kurzbezeichnung ein, z. B. `World`.
- Selektieren Sie im Bereich **Mode** den zugehörigen Modus **Gateway (w.o. registration)**.
- Geben Sie im Bereich **Remote gateway address** im Feld **IP address** die IP-Adresse `0.0.0.0` ein.

Mit der Angabe **Gateway (w.o. registration)** und der IP-Adresse `0.0.0.0` werden eigehende Rufe von unbekannt akzeptiert. Siehe auch Kapitel 6.3 "Statische Verwaltung von VoIP Geräten" ab Seite 86.

Somit ist das Interface für eingehende Rufe fertig konfiguriert.

Um einen Ruf über die ENUM-Abfrage aufzubauen, muss mindestens eine Route in das neu erstellte ENUM-Interface führen. Für Informationen zu den Routen siehe Kapitel 7.1 "Generelle Überlegungen zur Konfiguration der Rufbehandlung" ab Seite 89. Zum Erstellen einer Route in das ENUM-Interface gehen Sie wie folgt vor:

- Selektieren Sie im Konfigurationsapplet den Pfad **Config > Routing table**.
- Betätigen Sie die Schaltfläche **Add route**, um einen weiteren Eintrag in der Routingtabelle hinzuzufügen. Achten Sie dabei auf die Reihenfolge der Routen. Die neue Route wird immer hinter den aktuellen Eintrag eingefügt.
- Tragen Sie im Feld **Description** einen Namen für die Route ein, z. B. `to ENUM`.
- Selektieren Sie den Eintrag unterhalb der neuen Route `to ENUM` (den mit

dem "**->**").

- Markieren Sie im Bereich **Enable calls from interfaces** die Kontrollkästchen der Gateways und ISDN-Schnittstellen, die als Quelle dieser Route gültig sein soll. Es werden Ihnen nur die Schnittstellen angeboten, die auch konfiguriert sind. In unserem vorgenannten Beispiel ist dies **GW2**.
- Wählen Sie in der Auswahlliste **Default call destination** das Ziel, mit dem die Rufe verbunden werden sollen - also das neue ENUM-Interface. In unserem vorgenannten Beispiel ist dies **GW1**.

Nun ist die Route zum ENUM-Interface erstellt. Da ENUM-Abfragen als vollwertige E.164 Nummern übermittelt werden müssen, ist es notwendig, die zu wählenden Nummern entsprechend vorzubereiten, um die zur Telefonnummer korrespondierende ENUM-Domain zu bilden.

Daher wird im nächsten Schritt die Map zum **Tone Interface** konfiguriert, damit bei Wahl einer `0` der Wählton zu hören ist.

- Betätigen Sie die Schaltfläche **Add map**, während sich die Schreibmarke auf der zuvor eingerichteten Route `to ENUM` befindet.
- Tragen Sie im Feld **Called number in** die Rufnummer `0` ein.
- Wählen Sie im Feld **Destination:** den Eintrag **Tone** aus.

Mit diesen Einträgen ist gewährleistet, dass bei Wahl der Ziffer `0` der Wählton zu hören ist.

Im nächsten Schritt muss das Rufnummern-Mapping für internationale, nationale und lokale Rufe konfiguriert werden. Dazu sind drei weitere Maps notwendig, mit denen erreicht wird, dass jede Teilnehmernummer, die zum ENUM-Interface übermittelt wird, garantiert in der international genormten Form (ohne jegliche Prefixes) vorliegt.

Tipp

Beachten sie bitte, dass die Reihenfolge der konfigurierten Maps von großer Wichtigkeit ist. Die längsten Einträge müssen zuerst aufgeführt werden, da die Einträge nach Ihrer Reihenfolge abgearbeitet werden.

- Betätigen Sie die Schaltfläche **Add map.**
- Tragen Sie im Feld **Called number in** die Ziffern `000` ein.

Mit diesem Eintrag wird der Prefix `000` für die internationale Wahl erkannt und entfernt.

- Betätigen Sie die Schaltfläche **Add map.**

- Tragen Sie im Feld **Called number in** die Ziffern `00` ein.
- Tragen Sie im Feld **Called number out** den Landesprefix ein. Für Deutschland tragen Sie z. B. die Ziffern `49` ein.

Mit diesem Eintrag wird der Prefix `00` für die nationale Wahl erkannt und in das internationale Format transferiert.

- Betätigen Sie die Schaltfläche **Add map.**
- Tragen Sie im Feld **Called number in** die Ziffer `0` ein.
- Tragen Sie im Feld **Called number out** den Landesprefix gefolgt von der Ortsvorwahl (ohne die führende `0`) ein. Am Beispiel der Stadt Berlin (Ortsvorwahl `030`) in Deutschland (Landesprefix `49`) lautet der Eintrag `4930`.

Mit diesem Eintrag wird der Prefix `0` für die lokale Wahl erkannt und in das internationale Format transferiert.

Diese drei zuvor eingerichteten Maps ermöglichen es nun, dass alle gewählten Rufnummern in die für das ENUM-Protokoll notwendige internationale Syntax gebracht werden. Wenn also jemand die Zentrale der innovaphone® AG durch Wahl der Rufnummer +49 7031 73009-0 anrufen würde, würde die zugehörige, zum ENUM-Interface übertragene Nummer 497031730090 lauten. Egal, von wo in der Welt diese Nummer gewählt worden wäre.

- Aktivieren Sie bei den zuvor eingerichteten drei Routen für die internationale, nationale und lokale Vorwahl die Option **Final map**, damit im Falle eines Rerouting die nächste Map der nachfolgenden Route abgearbeitet wird.

Um die ausgehende Teilnehmernummer in eine voll qualifizierte E.164 Nummer zu wandeln, ist es sinnvoll, die zuvor eingerichteten drei Routen für die internationale, nationale und lokale Vorwahl um eine **CGPN map** zu erweitern. Damit wird ermöglicht, dass ein Teilnehmer, den Sie mittels ENUM anrufen, gegebenenfalls einen Rückruf zu Ihnen einleiten kann. Gehen Sie dazu wie folgt vor:

- Betätigen Sie die Schaltfläche **Add CGPN map**, nachdem Sie die Option **Final map** aktiviert haben und fügen Sie einen **CGPN map** Eintrag hinzu.
- Tragen Sie im Feld **Calling number out** die Ziffernfolge ein, durch den die ausgehende Rufnummer ersetzt werden soll. Also den Landesprefix gefolgt von der Ortsvorwahl (ohne die führende `0`) und die Rufnummer. Am Beispiel der Stadt Berlin (Ortsvorwahl `030`) in Deutschland (Landesprefix `49`) mit der Rufnummer `1234567` lautet der Eintrag `49301234567`.

4.2.11 Rerouting ausgehender Rufe

Das Rerouting wird unterstützt. Sollte der Rufaufbau zu einem ENUM-Interface fehlschlagen, würde durch das Rerouting eine weitere nachfolgende Route gesucht und abgearbeitet werden.

Tipp

Damit das Rerouting korrekt funktioniert, muss die Option **Final map** bei den zuvor eingerichteten drei Routen für die internationale, nationale und lokale Vorwahl aktiviert worden sein.

Wenn die ENUM-Funktion mit dem Rerouting kombiniert wird, haben Sie eine einfache Form des Least-Cost-Routings eingerichtet. Im ersten Versuch wird versucht, eine kostengünstige Verbindung durch Nutzung des ENUM-Interfaces aufzubauen. Schlägt dies fehl, wird der Ruf auf die herkömmliche Weise unter Nutzung einer ISDN-Leitung aufgebaut.

5 Konfiguration der ISDN-Schnittstellen

Die IP 400 verfügt über zwei "virtuelle" Schnittstellen, deren Konfiguration in Kapitel 5.3 "Überlegungen zur Konfiguration der virtuellen Schnittstellen" ab Seite 68 beschrieben ist.

Die IP 400 verfügt über ISDN Schnittstellen.

Zur Konfiguration der ISDN Schnittstellen müssen Sie sich zunächst über folgendes klar werden:

- Welche Geräte Sie mit dem Gateway verbinden wollen. Das können Telefone, TK-Anlagen, Netzabschlüsse Ihres ISDN Netzbetreibers oder andere ISDN Endgeräte sein.
- Ob die ISDN Anschlüsse ausschließlich für Sprachverbindungen genutzt werden sollen oder ob über einen davon auch eine ISDN/PPP Verbindung für das Datenrouting realisiert werden soll.

Die Konfiguration erfolgt im Bereich "ISDN Interfaces" des Konfigurationsapplets.

... für Experten

S_0

- **tel1** und **tel2** können im TE und NT Modus mit und ohne Speisung und Terminierung betrieben werden.
- **PPP** und **S/T** können nur im TE Modus betrieben werden.
- **tel1**, **tel2**, **PPP** und **S/T** können im Anlagenanschluss- und Mehrgerätemodus betrieben werden.
- **tel1**, **tel2**, **PPP** und **S/T** können im DSS1 und QSIG Signalisierungsmodus betrieben werden (auch gemischt).
- **NT** (**Line Emulation**) schaltet den NT Modus für Schicht 1, 2 und 3 ein.
- **Power** schaltet die Stromversorgung für Endgeräte am Bus ein (nur im NT Modus, maximal 4W).
- 100 Ohm **Termination** schaltet die Busterminierung ein.
- **Permanent activation** (nur im TE Modus) aktiviert die Leitung immer (Takt).
- **Point to Point** schaltet den Anlagenanschlussmodus ein.

S_0

- **Disable overlap receive** unterdrückt ein SETUP_ACK bei eingehender Einzelzifferwahl auf einem Mehrgeräteanschluss im TE Modus.
- **Suppress sending of HLC** unterdrückt das Aussenden von **high laye**r compatibility information elements auf dem Interface.
- **Suppress sending of FTY** unterdrückt das Aussenden von **facility information elements** auf dem Interface.
- **Provide inband progress tones** (nur im TE Modus) erzwingt die Generierung von Tönen (Wahlton, Rufton, Besetztton) auch im TE Modus (passiert im NT Modus immer).
- **Generate connected time** fügt die lokale Gatewayzeit in jede ausgehende CONNECT Nachricht ein.
- Die **D-Channel Protocol** bedeuten: **EDSS1** = Euro-ISDN, **QSIG** = ECMA QSIG (**CR len**=1, **channel id** wie Basic Rate), **QSIG-PRI-ECMA1** = ECMA QSIG (**CR len**=2, **channel id** wie Primary Rate, B-Kanäle 1 bis 30), **QSIG-PRI-ECMA2** = ECMA QSIG (**CR len**=2, **channel id** wie Primary Rate, B-Kanäle 1 bis 15 und 17 bis 31).
- Die **Dialtone type** bedeuten (im NT Modus oder bei **Provide inband progress tones**): **German PBX** = wie deutsche TK Anlage, **German** = wie deutsches Amt, **US** = amerikanischer Wahlton, **UK** = britischer Wahlton.
- Per **ADD CGPN MAP** können Ersetzungen von rufenden Nummern (CLI) erfolgen, die nur für dieses Interface gelten (getrennt nach ein/ausgehenden Rufen).
- Per **ADD CDPN MAP** können Ersetzungen von gerufenden Nummern erfolgen, die nur für dieses Interface gelten (getrennt nach ein/ausgehenden Rufen).

5.1 ISDN Schnittstellen der IP 400

Die IP 400 verfügt über 3 ISDN S_0 Schnittstellen, die als **PPP**, **tel1** und **tel2** bezeichnet werden (siehe Seite 7).

- **tel1** und **tel2** können für eine Amtsleitung, für ein oder zwei Telefone oder für eine TK-Anlage verwendet werden.

Tipp

Technisch können an einer ISDN Schnittstelle bis zu acht Endgeräte angeschlossen werden. Dabei ist jedoch zu beachten, dass von allen diesen Geräten nur zwei Gespräche gleichzeitig geführt werden können. Ferner muss sichergestellt sein, dass die Stromaufnahme aller Endgeräte zusammen nicht über dem zulässigen Wert von 4 Watt liegt.

- **PPP** kann ausschließlich als Anschluss für eine Amtsleitung verwendet werden.

Alle drei Schnittstellen können zum Aufbau von ISDN Datenverbindungen (PPP) verwendet werden. Dies auf Festverbindungen oder als Wählleitungen.

Mit der **Remove** Schaltfläche können Sie alle Einstellungen der ausgewählten Schnittstelle löschen.

5.2 Überlegungen zur Konfiguration der ISDN Schnittstellen

Die TE- und NT Modi

Die Schnittstellen **tel1** und **tel2** können wahlweise im TE oder NT Modus betrieben werden. **PPP** ist im Modus festgelegt.

Der TE (**terminal equipment**) Modus besagt dabei, dass sich die Schnittstelle wie ein normales ISDN Endgerät verhält. Das bedeutet, dass

- Schicht 2 und 3 des ISDN Protokolls als Endgerät konfiguriert werden,
- die Anschlussleitungen entsprechend belegt sind und
- das Gateway sich auf den Takt des Netzes synchronisiert (**clock slave**).

Der NT (**network termination**) Modus dagegen besagt, dass sich die Schnittstelle wie ein ISDN Netzabschluss (**NTBA**) verhält. Das bedeutet, dass

- Schicht 2 und 3 des ISDN Protokolls als Netz konfiguriert werden,
- die Anschlussleitungen entsprechend gekreuzt belegt sind und
- das Gateway den Takt vorgibt (**clock master**).

Die Lautstärkeanpassung

In manchen Fällen ist es wünschenswert, den Pegel der Lautstärke einer Schnittstelle grundsätzlichen anpassen zu können. Die Lautstärke der ISDN-Schnittstellen kann im Konfigurationsapplet unter **Config > ISDN, tone and HTTP Interfaces > TEL** bzw. **PRI** im Bereich **Interface configuration** im Feld **Volume** im Bereich von `-31` bis `32` eingestellt werden. Die Einheit der Anpassungsschritte ist Dezibel. Kein Eintrag bzw. der Eintrag `0` entspricht der Werkseinstellung. Ein Eintrag in Richtung "-" verringert und ein Eintrag in Richtung "+" erhöht den Lautstärkepegel der jeweiligen Schnittstelle.

Die Signalisierungsprotokolle

Die Gateways unterstützen auf den ISDN Schnittstellen grundsätzlich zwei verschiedene D-Kanal Protokolle: Euro-ISDN (EDSS1) und QSIG.

Euro-ISDN ist die Signalisierungsart, die sich weltweit für ISDN Teilnehmerschnittstellen durchgesetzt hat und ist trotz des Namens auch außerhalb von Europa üblich. Die prominenteste Ausnahme stellen zur Zeit die Vereinigten Staaten dar, die generell andere digitale Signalisierungen verwenden.

QSIG ist ein standardisiertes Signalisierungsprotokoll, das hauptsächlich zur Vernetzung von TK-Anlagen verwendet wird. Hier wird von den Gateways **basic call** und **tunnelling** unterstützt. Dadurch lassen sich insbesondere homogene TK-Anlagenkopplungen mit QSIG realisieren, bei denen herstellerspezifische Eigenschaften per QSIG ausgetauscht werden.

Leider gibt es verschiedenen Varianten des QSIG Standards und verschiedene, mehr oder weniger konforme Implementierungen. Die Gateways unterstützen daher 3 verschiedene Varianten, die sich durch

- die Länge der **call reference**,
- die Kodierung der **channel id** und
- die Nummerierung der B-Kanäle

unterscheiden. Die folgende Tabelle gibt die Unterschiede an.

Variante	**Call reference** Länge	**Channel id** Kodierung	Nummerierung der B-Kanäle	Verwendung
QSIG	1 Byte	Wie bei basic rate		S0
QSIG-PRI-ECMA1	2 Bytes	Wie bei **primary rate**	1 bis 30	S0

Tabelle 6 Unterschiede der QSIG Varianten

Einzelzifferwahl auf Endgeräte am Mehrgeräteanschluss

Normalerweise werden Endgeräte (also Geräte im TE Modus) an einem Mehrgeräteanschluss nicht mit Einzelzifferwahl (**overlapped sending**) gerufen. Die Gateways können jedoch unter Umständen in genau diesem Modus an eine TK-Anlage angeschlossen werden und unterstützen dann auch die eingehende Einzelzifferwahl (**overlapped receive**). Dabei wird eine eingehende **SETUP** Meldung standardkonform mit einer **SETUP_ACK** Nachricht beantwortet. Manche TK-Anlagen erwarten jedoch von einem Endgerät keine solche Meldung und brechen den Ruf an dieser Stelle ab. In einem solchen Fall kann das Gateway mit der Einstellung **Disable overlap receive** dazu veranlasst werden, die eingehende **SETUP** Nachricht nicht mit einem **SETUP_ACK** zu beantworten.

Unterdrückung bestimmter Protokollelemente

Nicht alle ISDN Implementierungen sind darauf vorbereitet, bestimmte standardkonforme **information elements** (so genannte **IE**s) zu empfangen. Derartige IEs können zum Beispiel bei der Kopplung unterschiedlicher TK-Anlagen oder bei der Übertragung von H.323 Rufen zu einer ISDN Schnittstelle und umgekehrt entstehen.

Kommt es durch die Übertragung bestimmter IEs zu Störungen, können die Gateways veranlasst werden, solche IEs aus den übertragenen Nachrichten zu entfernen.

Einstellung	Wirkung
Suppress sending of HLC	Es werden keine **high layer compatibility information elements** übertragen.
Suppress sending of FTY	Es werden keine **facility information elements** übertragen.

Tabelle 7 Unterdrückung der Übertragung von **information elements**

Wahltöne

Die Gateways sind in der Lage, an den ISDN Schnittstellen Wahltöne (Freizeichen, Rufzeichen, Besetztzeichen) zu generieren.

Dies wird für aus dem Gateway ausgehende Rufe in Richtung des Rufenden immer dann gemacht, wenn die gerufene Seite keine eigenen Wahltöne generiert.

Tipp

Wahltöne werden daran erkannt, dass von der gerufenen Seite eine **inband information** signalisiert wird.

Für an der ISDN Schnittstelle eingehende Rufe wird dies in Richtung des Rufenden normalerweise nur gemacht, wenn die Schnittstelle sich im NT Modus befindet, nicht jedoch im TE Modus. In wenigen Fällen, insbesondere bei der Kopplung von TK-Anlagen über Querverbindungsleitungen kann es jedoch nützlich sein, diese Töne auch im TE Modus zu generieren. Dies kann durch die Einstellung **Provide inband call progress tones** erreicht werden.

Erzeugung von Zeitstempeln beim Verbindungsaufbau

Das ISDN Netz generiert normalerweise in der **connect** Nachricht einen Zeitstempel. Dieser wird zum Beispiel von Telefonen oder TK-Anlagen dazu benutzt, die eigene Uhr bei der ersten Verbindung zu stellen. Die Gateways reichen solche Zeitstempel normalerweise unverändert weiter.

Es kann jedoch gewünscht sein, die Zeitstempel konsistent in allen **connect** Nachrichten mit der aktuellen Systemzeit des gateways zu versehen. Dies kann durch die Einstellung **Generate connected time** erreicht werden. Hierzu sollte das Gateway immer über die korrekte Zeit verfügen. Da es selber nicht über eine Echtzeituhr verfügt, sollte dafür ein NTP Zeitserver konfiguriert sein (siehe Seite

112). Diese Einstellung ist normalerweise nur im NT Modus sinnvoll.

5.2.1 Verwendung an einer Amtsleitung (Wahl- oder Festverbindung)

Hierbei wird das Gateway an eine ISDN-Amtsleitung Ihres Netzbetreibers angeschlossen. Diese Verwendungsart ist für **tel1**, **tel2** und **PPP** möglich.

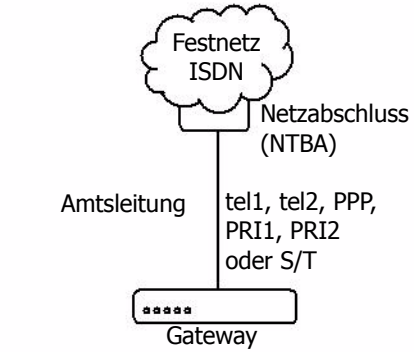

Abbildung 10 Gateway an einer Amtsleitung

Es gibt verschiedene Szenarien, in denen diese Anschlussart sinnvoll ist:

- Verwendung des Gateways als Gateway für H.323 Gespräche in das Festnetz. Hierdurch können H.323 Endgeräte normale Endgeräte im Telefonfestnetz erreichen und umgekehrt.
- Verwendung als IP-Router zur manuellen Einwahl beim ISP oder ins Firmennetz. Hierdurch ist das Gateway und das mit seinem Ethernetanschluss verbundene LAN an das IP (Inter- oder Intra-) Netz angeschlossen. Der Einsatz eines separaten IP-ISDN-Routers kann entfallen.
- Verwendung als IP-Router zum Betrieb an einer Festverbindung (nur IP 400). Hierdurch wird das Gateway über eine 64kbps oder 128kbps ISDN Festverbindung an eine PPP Gegenstelle (beim ISP oder im Firmennetz) angeschlossen.

Die Konfiguration unterscheidet sich je nachdem, ob die Amtsleitung als "Anlagenanschluss" (auch "**point to point**"), als "Mehrgeräteanschluss" (auch "**point to multipoint**") oder als "Festverbindung" geschaltet ist.

Ferner muss die Art der Signalisierung für Wählverbindungen korrekt eingestellt werden. An Amtsleitungen ist die Signalisierung immer EDSS1, an TK-Anlagenanschlüssen kann es sich auch um eine der QSIG Varianten handeln (siehe Kapitel

"Die Signalisierungsprotokolle" ab Seite 50). Für Festverbindungen spielt die Signalisierung keine Rolle.

Hinweis

Sind Sie nicht sicher, welche Anschlussart bei Ihnen vorliegt, erkunden Sie sich bei Ihrem Netzwerkadministrator oder Netzbetreiber.

- Navigieren Sie im Konfigurationsapplet zu **ISDN interfaces > TEL1** bzw. den Anschluss mit der Amtsleitung.
- Entfernen Sie **NT** (nur **tel1** und **tel2**).
- Entfernen Sie **Power** (nur **tel1** und **tel2**).
- Entfernen Sie **100 Ohm Termination** (nur **tel1** und **tel2**).
- Entfernen Sie **Permanent Activation** (nur **tel1**, **tel2** und **PPP**).
- Handelt es sich bei Ihrer Amtsleitung um einen Anlagenanschluss, Markieren Sie **Point to Point**. Handelt es sich um einen Mehrgeräteanschluss, Entfernen Sie **Point to Point**. Bei einer Festverbindung ist diese Einstellung irrelevant. Wird der Anschluss jedoch gemischt betrieben (ein B-Kanal fest auf einer Festverbindung, ein B-Kanal im Wahlbetrieb), dann hängt die Einstellung vom Betriebsmodus der Wählleitung ab (nur **tel1**, **tel2** und **PPP**).
- Entfernen Sie **Disable overlap receive.**
- Entfernen Sie **Suppress sending of HLC** und **Suppress sending of FTY** (siehe Kapitel "Unterdrückung bestimmter Protokollelemente" ab Seite 51).
- Entfernen Sie **Provide inband call progress tones** (siehe Kapitel "Wahltöne" ab Seite 52).
- Stellen sie im Auswahlfeld **D-Channel Protocol** das Protokoll **EDSS1** ein (siehe Kapitel "Die Signalisierungsprotokolle" ab Seite 50).
- Der **Dialtone type** spielt in dieser Konfiguration keine Rolle.
- Die besondere Modifikation der **called party** und **calling party number** ist in dieser Konfiguration normalerweise nicht nötig. Lesen Sie hierzu im Kapitel 5.2.7 "Behandlung der verschiedenen ISDN Adresstypen" ab Seite 64 nach.

Achtung

Ist die Amtsleitung als Anlagenanschluss geschaltet, darf dort außer dem Gateway kein weiteres ISDN-Gerät angeschlossen werden.

Handelt es sich um einen Mehrgeräteanschluss, so können weitere ISDN-Endgeräte dort angeschlossen werden. Bedenken Sie jedoch, dass eingehende Rufe dann prinzipiell von allen angeschlossenen Endgeräten angenommen werden können. Lesen Sie im Kapitel 7 "Konfiguration der Rufbehandlung" ab Seite 89 nach, wie das Gateway so konfiguriert wird, dass nur Rufe für die gewünschten Rufnummern angenommen werden.

Zur Konfiguration des IP-Routings über die ISDN Schnittstelle im Falle der Verwendung als IP Router lesen Sie bitte im Kapitel 4.2 "Konfiguration der WAN Schnittstellen" ab Seite 29 nach.

5.2.2 Verwendung als Anschluss für ein Telefon oder anderes ISDN-Endgerät

Hierbei werden ein oder mehrere ISDN-Endgeräte an die Schnittstelle angeschlossen. Sie verhält sich damit wie ein Mehrgeräteanschluss ("**point to multipoint**") Ihres Netzbetreibers. Diese Verwendungsart ist nur für die **tel1** und **tel2** Schnittstelle verfügbar.

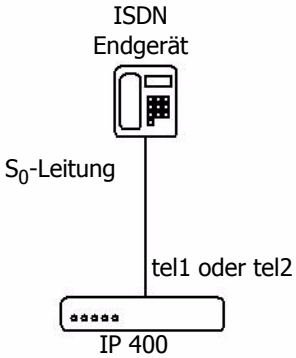

Abbildung 11 ISDN Endgerät an der IP 400

Die Konfiguration unterscheidet sich, je nachdem, ob die anzuschließenden Endgeräte über eine eigene Stromversorgung verfügen oder nicht. Telefone verfügen typischerweise über keine eigene Stromversorgung und werden daher aus der ISDN-Leitung gespeist.

Tipp

Sind Sie sich nicht sicher, ob Ihre Endgeräte eine Speisung benötigen, schalten Sie die Speisung einfach immer an.

- Rufen Sie im Konfigurationsapplet **ISDN interfaces > TEL1** auf bzw. den Anschluss mit dem ISDN Gerät.
- Markieren Sie **NT.**
- Markieren Sie **Power**, wenn ein anzuschließendes Endgerät aus der ISDN-Leitung gespeist werden muss.
- Markieren Sie **100 Ohm Termination.**
- Entfernen Sie **Permanent Activation.**
- Entfernen Sie **Point to Point**.
- Entfernen Sie **Disable overlap receive.**
- Entfernen Sie **Suppress sending of HLC** und **Suppress sending of FTY** (siehe Kapitel "Unterdrückung bestimmter Protokollelemente" ab Seite 51).
- Stellen Sie im Auswahlfeld **D-Channel Protocol** das Protokoll **EDSS1** ein (siehe Kapitel "Die Signalisierungsprotokolle" ab Seite 50).
- Wählen Sie im Auswahlfeld **Dialtone type** den gewünschten Wahlton ein.
- Die besondere Modifikation der **called party** und **calling party number** ist in dieser Konfiguration normalerweise nicht nötig. Lesen Sie hierzu im Kapitel 5.2.7 "Behandlung der verschiedenen ISDN Adresstypen" ab Seite 64 nach.

Tipp

An die ISDN-Schnittstellen **tel1** und **tel2** können bei dieser Verwendungsart bis zu vier Telefone oder andere ISDN-Endgeräte direkt angeschlossen werden, an eine IP 400 somit insgesamt maximal vier Geräte. Wird an **tel1** oder **tel2** eine ISDN Busverkabelung angeschlossen, können jeweils bis zu 8 Endgeräte angeschlossen werden. Handelt es sich allerdings um Endgeräte, die ihre Stromversorgung aus dem ISDN Netz beziehen, darf die Gesamtstromaufnahme aller angeschlossenen Geräte 4 Watt nicht überschreiten.

5.2.3 Verwendung als Amtsleitung für eine ISDN-TK-Anlage

Hierbei wird die Schnittstelle des Gateways an eine ISDN-TK-Anlage als einzige Amtsleitung oder als eine weitere Leitung innerhalb eines Amtsleitungsbündels angeschlossen. Sie verhält sich damit wie ein Anlagenanschluss ("**point to point**") Ihres Netzbetreibers.

Hierzu muss die Schnittstelle im NT Modus betrieben werden. Es kommen daher für diese Verwendungsart nur die Schnittstellen **tel1** und **tel2** in Frage.

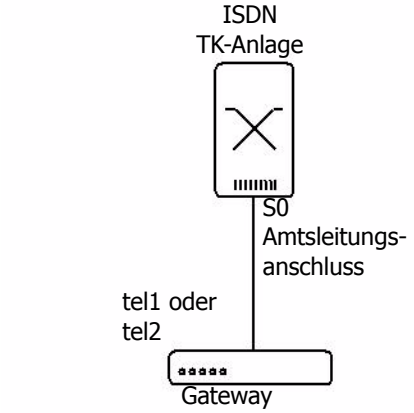

Abbildung 12 Gateway als Amtsleitung

Hinweis

Manche - vor allem kleinere – S_0 TK-Anlagen sind zum Anschluss an einen Mehrgeräteanschluss ("**point to multipoint**") vorgesehen. Die Konfiguration der ISDN-Schnittstelle muss dementsprechend erfolgen. Sind Sie nicht sicher, für welche Anschlussart Ihre TK-Anlage vorgesehen ist, ziehen Sie die Betriebsanleitung der Anlage zu Rate.

- Navigieren Sie im Konfigurationsapplet zu **ISDN interfaces > TEL1** bzw. den Anschluss mit der ISDN-TK-Anlage.
- Markieren Sie **NT** (nur **tel1** und **tel2**).
- Entfernen Sie **Power** (nur **tel1** und **tel2**).

Markieren Sie **100 Ohm Termination** (nur **tel1** und **tel2**).

- Ist Ihre TK-Anlage für den Betrieb an einem Anlagenanschluss vorgesehen, Markieren Sie **Point to Point**. Ist sie für den Betrieb am Mehrgeräteanschluss vorgesehen, entfernen Sie **Point to Point** (nur **tel1** und **tel2**).
- Entfernen Sie **Disable overlap receive.**
- Entfernen Sie **Suppress sending of HLC** und **Suppress sending of FTY** (siehe Kapitel "Unterdrückung bestimmter Protokollelemente" ab Seite 51).
- Entfernen Sie **Provide inband call progress tones** (siehe Kapitel "Wahltöne" ab Seite 52).
- Stellen Sie im Auswahlfeld **D-Channel Protocol** das Protokoll **EDSS1** ein (siehe Kapitel "Die Signalisierungsprotokolle" ab Seite 50).
- Stellen Sie im Auswahlfeld **Dialtone type** den gewünschten Wahlton ein.
- Die besondere Modifikation der **called party** und **calling party number** ist in dieser Konfiguration normalerweise nicht nötig. Lesen Sie hierzu im Kapitel 5.2.7 "Behandlung der verschiedenen ISDN Adresstypen" ab Seite 64 nach.

Die Schnittstelle PPP ist ausschließlich zum Anschluss einer Amtsleitung an das Gateway vorgesehen, daher ist der Anschluss einer ISDN TK-Anlage auf diese Weise hier nicht möglich (siehe jedoch Kapitel 5.2.4 "Verwendung als Teilnehmer an einer ISDN-TK-Anlage" ab Seite 60).

Ist die TK-Anlage außer an das Gateway noch an eine weitere Amtsleitung angeschlossen, so muss sichergestellt werden, dass beide Amtsleitungen einen synchronen Takt aufweisen. Dies wird erreicht, indem die **PPP** Schnittstelle bei der IP 400 mit einem normalen ISDN-Kabel parallel zur TK-Anlage an die direkte

Amtsleitung angeschlossen wird. Hierzu kann die normalerweise an einem Netzabschluss des Netzbetreibers (NTBA) vorhandene zweite Anschlussbuchse verwendet werden. Ist die TK-Anlage nicht über einen Basisanschluss an das ISDN Festnetz angeschlossen (also beispielsweise an einem Primärmultiplexanschluss), dann kann die Schnittstelle statt dessen mit einem ungenutzten S_0 Teilnehmeranschluss der TK-Anlage verbunden werden.

Achtung

In diesem Fall darf die Schnittstelle auf keinen Fall für ein- oder ausgehende Rufe verwendet werden (siehe Kapitel 7 "Konfiguration der Rufbehandlung" ab Seite 89). Die Markierung im Kontrollkästchen **Point to Point** der Schnittstelle muss entfernt werden und das Kontrollkästchen **permanent activation** muss markiert sein.

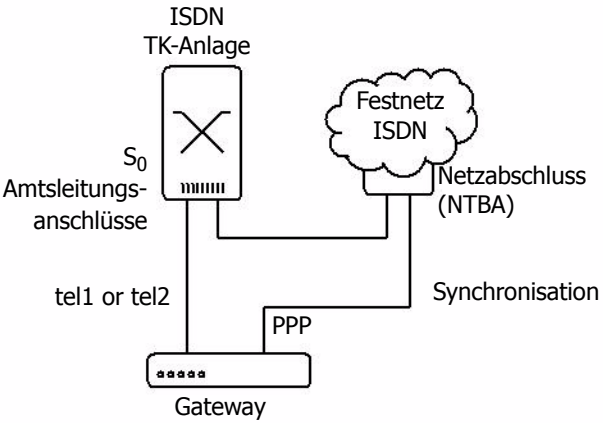

Abbildung 13 Synchronisation eines Gateway mit einem ISDN S_0 Anschluss

5.2.4 Verwendung als Teilnehmer an einer ISDN-TK-Anlage

In bestimmten Fällen kann es erforderlich sein, das Gateway als Teilnehmer an einen Endgeräteanschluss (und damit einem Mehrgeräteanschluss) der ISDN-TK-Anlage anzuschließen. Dies ist beispielsweise dann nötig, wenn die TK-Anlage keine zusätzliche Amtsleitung unterstützt, die vorhandene unverändert weiterbetrieben werden soll und auch keine Querverbindungsleitung (siehe Kapitel 5.2.5 "Verwendung an einer Querverbindungsleitung einer TK-Anlage" ab Seite 61) vorhanden ist.

Bedenken Sie jedoch, dass Sie in diesem Fall je nach TK-Anlage mit verschiedenen Einschränkungen rechnen müssen, da die TK-Anlage an diesem Anschluss ein einzelnes Endgerät erwartet und nicht ein vermittelndes Endgerät.

Diese Anschlussart kommt nur im Zusammenhang mit S_0 Schnittstellen vor und spielt daher normalerweise nur für die IP 400 eine Rolle.

In diesem Fall wird die TK-Anlage wie eine Amtsleitung an das Gateway angeschlossen, wie im Kapitel 5.2.1 "Verwendung an einer Amtsleitung (Wahl- oder Festverbindung)" ab Seite 53 beschrieben. Allerdings handelt es sich bei dem von der TK-Anlage bereitgestellten Anschluss in der Regel um einen Mehrgeräteanschluss. Die Markierung im Kontrollkästchen **Point to Point** ist dementsprechend zu entfernen. Falls die TK-Anlage keine Einzelzifferwahl zum Endgerät vorsieht, Markieren Sie **Disable overlap receive** (siehe Kapitel "Einzelzifferwahl auf Endgeräte am Mehrgeräteanschluss" ab Seite 51).

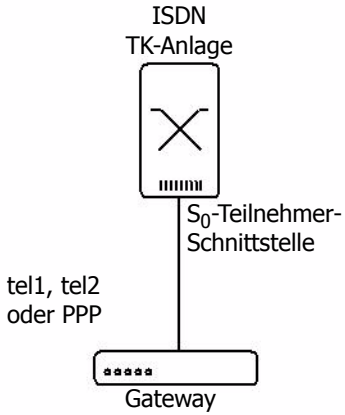

Abbildung 14 Gateway an TK-Anlagen Teilnehmerschnittstelle

Sollte die TK-Anlage eine Punkt-zu-Punkt Verbindung am Teilnehmeranschluss zur Verfügung stellen (dies wird oft auch als "Querverbindungsleitung" bezeichnet), so gelten die oben genannten Einschränkungen in der Regel nicht.

Beachten Sie jedoch, dass das Gateway keine proprietären Teilnehmerprotokolle zum Betrieb von Telefonen an TK-Anlagen unterstützt.

5.2.5 Verwendung an einer Querverbindungsleitung einer TK-Anlage

Der Anschluss des Gateways an eine Querverbindungsleitung einer TK-Anlage ist in der Regel die sinnvollste Methode, zwei oder mehrere TK-Anlagen zu koppeln.

Das Gateway kann dabei als **Clock-master** (NT) oder **Clock-slave** (TE) betrieben werden (siehe dazu Kapitel 5.2 "Überlegungen zur Konfiguration der ISDN Schnittstellen" ab Seite 49). Verfügt die TK-Anlage über einen eigenen Takt, kann das Gateway problemlos im TE-Modus betrieben werden. Dies ist auch auf beiden Enden der Verbindung möglich.

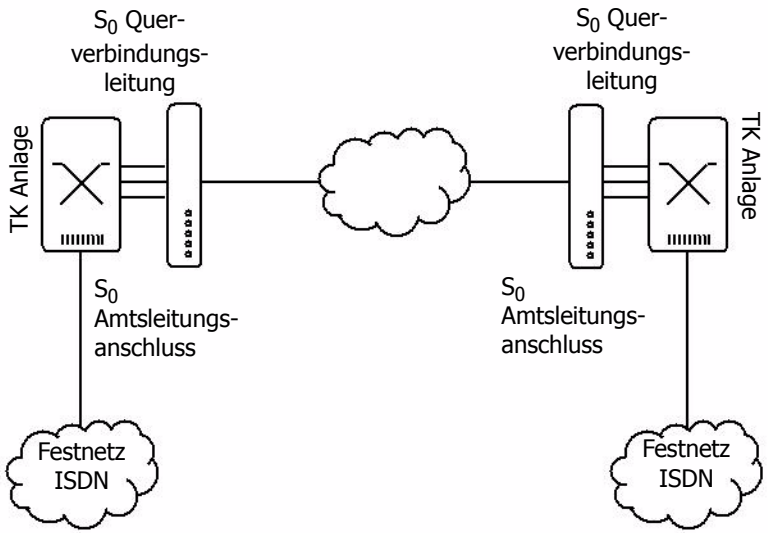

Abbildung 15 Gateway an Querverbindungsleitung

- Wählen Sie im Konfigurationsapplet **ISDN interfaces > TEL1** bzw. den

Anschluss mit der Querverbindungsleitung.

- Markieren Sie **NT**, wenn das Gateway den Takt vorgeben soll. Deaktivieren Sie das Kontrollkästchen, wenn die TK-Anlage den Takt vorgibt (nur **tel1**, **tel2**).
- Entfernen Sie **Power** (nur **tel1** und **tel2**).
- Entfernen Sie **100 Ohm Termination** (nur **tel1** und **tel2**).
- Entfernen Sie **Permanent Activation** (nur **tel1**, **tel2** und **PPP**).
- Markieren Sie **Point to Point.**
- Entfernen Sie **Disable overlap receive.**
- Entfernen Sie **Suppress sending of HLC** und **Suppress sending of FTY** (siehe Kapitel "Unterdrückung bestimmter Protokollelemente" ab Seite 51).
- Markieren Sie **Provide inband call progress tones** (siehe Kapitel "Wahltöne" ab Seite 52).

Tipp

Schalten Sie diese Option ab, wenn sie zu Fehlern bei der Rufvermittlung über die Querverbindungsleitung oder beim Rufabbau führt.

- Stellen sie im Auswahlfeld **D-Channel Protocol** die korrekte Signalisierung ein (siehe Kapitel "Die Signalisierungsprotokolle" ab Seite 50).
- Stellen Sie im Auswahlfeld **Dialtone type** den gewünschten Wahlton (siehe Kapitel "Wahltöne" ab Seite 52) ein.
- Werden auf der Querverbindungsleitung Rufnummern mit einem anderen **type of address** als **unknown** übertragen, so sind besondere Modifikationen der **called party** und **calling party number** nötig. Lesen Sie hierzu im Kapitel 5.2.7 "Behandlung der verschiedenen ISDN Adresstypen" ab Seite 64 nach.

5.2.6 Einschleifen des Gateways in eine vorhandene Amtsleitung

In einigen Fällen kann zum Anschluss der Gateways an die TK-Anlage keine weitere ISDN Schnittstelle genutzt werden. In einem solchen Fall ist es praktisch, das Gateway in die vorhandene Amtsleitung einzuschleifen.

Dazu wird je Amtsleitung eine ISDN Schnittstelle zum Amt (TE Modus) und eine zur TK-Anlage (NT Modus) im Gateway benötigt. Auch die IP 400 kann in eine Amtsleitung eingeschleift werden, allerdings können in diesem Betriebsmodus nicht alle 4 parallel möglichen Gespräche ausgenutzt werden, da die IP 400 zwar 2 NT Schnittstellen (**tel1** und **tel2**), jedoch nur eine TE Schnittstelle (**PPP**) besitzt.

Die Konfiguration der Schnittstellen erfolgt zum Amt hin wie im Kapitel 5.2.1 "Verwendung an einer Amtsleitung (Wahl- oder Festverbindung)" ab Seite 53 beschrieben und zur TK-Anlage hin wie im Abschnitt Kapitel 5.2.3 "Verwendung als Amtsleitung für eine ISDN-TK-Anlage" ab Seite 57 beschrieben. Allerdings werden auf einer Amtsleitung generell Rufnummern mit verschiedenen **type of address** übertragen, so dass besondere Modifikationen der **called party** und **calling party number** nötig sind. Lesen Sie daher unbedingt im Kapitel 5.2.7 "Behandlung der verschiedenen ISDN Adresstypen" ab Seite 64 nach.

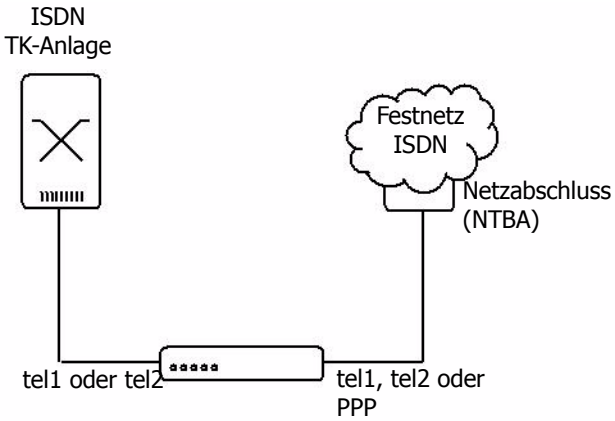

Abbildung 16 Einschleifen des Gateways in eine Amtsleitung

5.2.7 Behandlung der verschiedenen ISDN Adresstypen

Die Gateways behandeln Rufnummern intern grundsätzlich im Nummerntyp (**type of number**) **unknown**. Im ISDN gibt es jedoch verschiedene Rufnummerntypen (siehe Tabelle 8), so dass Rufnummern immer nur im Zusammenhang mit ihrem Nummerntyp zu interpretieren sind. So entspricht zum Beispiel an einem Amtsanschluss in Deutschland eine gerufene Nummer `0711654321` vom Nummerntyp **unknown** der gerufenen Nummer `711654321` vom Nummerntyp **national**. Dies deswegen, weil in Deutschland die Ausscheidungskennziffer für nationale Nummern die `0` ist. Dahingegen bezeichnet die rufende Nummer `41551234` vom Nummerntyp **unknown** einen Anschluss im eigenen Ortsnetz, während die gleiche Nummer `41551234` vom Nummerntyp **international** einen Anschluss im Ortsnetz Pfäffikon in der Schweiz bezeichnet.

Zur Auswertung von Rufnummern innerhalb der Gateways ist also eine Normalisierung in den Rufnummerntyp unknown erforderlich. Dies kann mit Hilfe der so genannten **CGPN (calling party number) map** und **CDPN (c**alle**d p**arty **n**umber) **map** Einträge erfolgen, die sowohl an den ISDN Schnittstellen, als auch an den einzelnen Gatewaydefinitionen festgelegt werden können.

Bezeichnung	Bedeutung	Typische Verwendung	Kürzel[1]	Kennziffer[2]
Unknown	Unspezifiziert	Gerufene Nummer beim ausgehenden Ruf.	u	
Subscriber	Rufnummer im Ortsnetz.	Gerufene Nummer beim eingehenden Ruf.	s	
National	Rufnummer mit Ortsnetzkennzahl.	Rufende Nummer vom Inland.	n	0
International	Anschlussnummer mit Landeskennziffer und Ortsnetzkennzahl.	Rufende Nummer vom Ausland.	i	00
Abbreviated		unüblich	a	

Bezeichnung	Bedeutung	Typische Verwendung	Kürzel[3]	Kennziffer[4]
Network specific		unüblich	x	

1. in den CGPN/CDPN Mappings
2. Äquivalente Ausscheidungskennziffer für ausgehende Rufe in Deutschland
3. in den CGPN/CDPN Mappings
4. Äquivalente Ausscheidungskennziffer für ausgehende Rufe in Deutschland

Tabelle 8 Nummerntypen

In der Standardkonfiguration sind für alle ISDN Schnittstellen und für die Gateways folgende Map-Einträge für die rufende Nummer enthalten (siehe Abbildung 17 auf Seite 66):

Art	Nummerntyp	Nummernanfang	Ersetzter Nummernanfang	Anwendung
eingehende rufende Nummer	National	Leer	0	Fügt die Ausscheidungskennziffer 0 vor nationalen CLI's ein.
eingehende rufende Nummer	International	Leer	00	Fügt die Ausscheidungskennziffer 00 vor internationalen CLI's ein.

Tabelle 9 CGPN Mappings in der Standardkonfiguration

Hierdurch wird sichergestellt, dass die Anzeige der rufenden Nummer bei eingehenden Rufen für alle Nummerntypen korrekt ist.

Eine typische Anwendung von CDPN Mappings ist die Behandlung der Stammnummer am Anlagenanschluss für eingehende Rufe. Hier wird bei der gerufenen Nummer, die meist als Nummer vom Typ **subscriber** eingeht, der Nummernstamm entfernt. Danach wird in der Routingtabelle der Gateways nur noch die Durchwahl behandelt. Abbildung 18 auf Seite 66 zeigt eine solche Konfiguration.

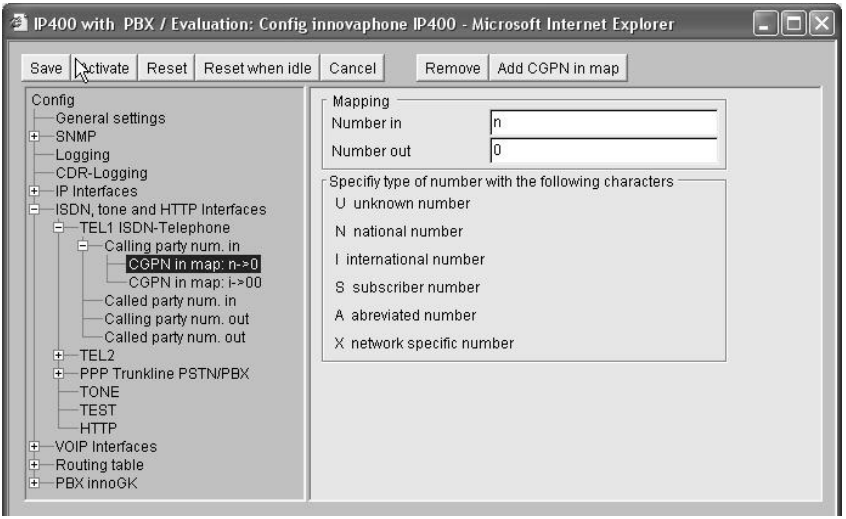

Abbildung 17 Standard CGPN/CDPN Mappings

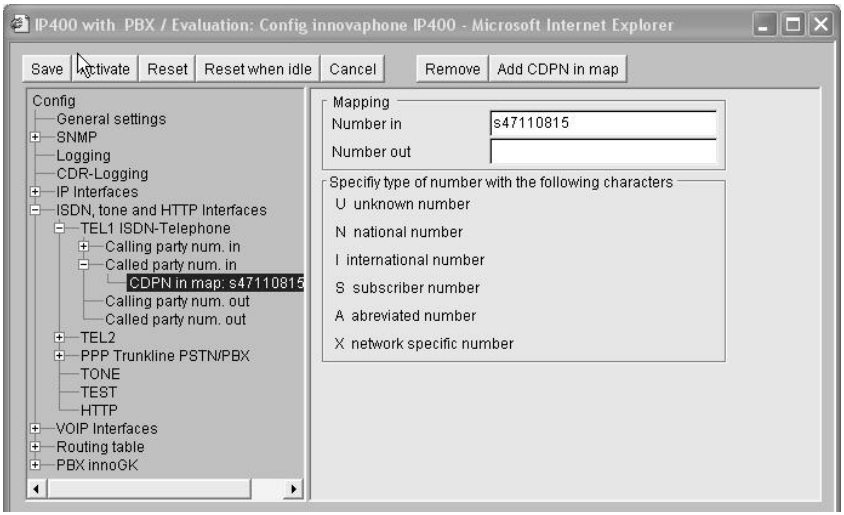

Abbildung 18 Behandlung der Stammnummer durch CDPN Mappings

- Wählen Sie in der linken Hälfte des Konfigurationsapplets die Schnittstelle aus, für die Sie Rufnummernmodifikationen einrichten wollen.
- Erweitern Sie nötigenfalls die Baumdarstellung durch Klicken des + Symbols im weißen Quadrat neben der Schnittstellenbezeichnung.
- Wählen Sie eine der folgenden Zeilen in der Darstellung auf der linken Seite.
    - **Calling party num. in** wenn Sie die rufende Nummer eingehender Rufe bearbeiten wollen.
    - **Calling party num. out** wenn Sie die rufende Nummer ausgehender Rufe bearbeiten wollen.
    - **Called party num. in** wenn Sie die gerufene Nummer eingehender Rufe bearbeiten wollen.
    - **Called party num. out** wenn Sie die gerufene Nummer ausgehender Rufe bearbeiten wollen.
- Fügen Sie Mappings ein, in dem Sie die Schaltfläche **Add CGPN/CDPN in/ out map** am oberen Rand klicken.
- Legen Sie unter **Number in** den Nummerntyp und –anfang fest, für den Sie eine Ersetzung wünschen. Der Nummerntyp wird dabei gemäß dem Kürzel aus Tabelle 8 auf Seite 65 bezeichnet.
- Legen Sie unter **Number out** die Ersetzung fest.

Das in Abbildung 18 auf Seite 66 gezeigte Beispiel bewirkt also, dass die gerufene Nummer eingehender Rufe (**CDPN in**) dann ersetzt wird, wenn der Rufnummerntyp **subscriber** (Kürzel `s`) ist und die Nummer mit den Ziffern `47110815` beginnt.

Beachten Sie, dass Rufnummern innerhalb des Gateways immer im **unknown** Format verarbeitet werden. Daher ist das Ergebnis einer Nummernersetzung für eingehende Rufe immer vom Typ **unknown** und der Rufnummerntyp zu ersetzender ausgehender Rufe ebenfalls immer **unknown**. Entsprechend können Sie für Ersetzungen eingehender Nummern im Feld **Number out** und für Ersetzungen ausgehender Nummern im Feld **Number in** keinen Nummerntyp angeben.

5.3 Überlegungen zur Konfiguration der virtuellen Schnittstellen

Das Gateway verfügt über die virtuellen Schnittstelle **TONE, TEST** und **HTTP**. Dabei handelt es sich nicht um physikalische Schnittstellen, sondern um im Gerät realisierte virtuelle Schnittstellen.

5.3.1 Die Amtstonschnittstelle TONE

Das Gateway verfügt über eine interne **TONE** Schnittstelle. Diese ist sinnvoll nur als Ziel eines Rufes verwendbar. Geht ein Ruf auf der TONE Schnittstelle ein, so wird er nicht verbunden, jedoch der für die Schnittstelle konfigurierte Amtston eingespielt (der eingehende Ruf wird mit einem **SETUP_ACK** quittiert und ein Medienkanal aufgebaut). Wird eine weitere Wahlziffer gewählt oder enthielt der ursprüngliche Ruf bereits gewählte Ziffern, so wird der Ruf abgelehnt.

Die Tone Schnittstelle kann verwendet werden, um einem Anrufer einen Amtston einzuspielen, obwohl sein Ruf noch nicht auf eine "echte" Amtsleitung verbunden wurde. Dies kommt insbesondere bei **least-cost-routing** Szenarien vor, bei denen die Vermittlung des Rufes erst nach Analyse einiger Rufziffern vorgenommen werden kann.

Das Tone Interface kann mehrere Rufe gleichzeitig verarbeiten. Der eingespielte Amtston wird im Bereich **Analog/ISDN Interfaces**, **Tone** unter **Tone provider interface configuration** eingestellt.

5.3.2 Die TEST Schnittstelle

Das Gateway verfügt über eine interne **TEST** Schnittstelle. Diese ist sinnvoll nur als Ziel eines Rufes verwendbar. Geht ein Ruf auf der **TEST** Schnittstelle ein, so wird er verbunden und die im nichtflüchtigen Speicher enthaltene Pausenmusik eingespielt. Nachwahlziffern werden ignoriert.

Bitte beachten Sie, dass die **TEST** Schnittstelle nur Rufe mit **G.729A** oder **G.723** bedienen kann. Gehen Rufe mit **G.711** ein, so wird keine Musik eingespielt.

Es ist keine Konfiguration der Schnittstelle möglich.

5.3.3 Die HTTP Schnittstelle

Die HTTP Schnittstelle ermöglicht das Einspielen von Musik, Announcements oder anderen Informationen über eine externe Datenquelle. Die Konfiguration ist nur sinnvoll in Zusammenarbeit mit der innovaphone PBX. Für weitere Informationen lesen Sie bitte im "Administrator Handbuch - innovaphone PBX" nach.

6 Konfiguration der VoIP Schnittstellen

So wie ISDN Schnittstellen in die Welt der klassischen Telefonie führen, sind "VoIP Schnittstellen" Wege in die **Voice over IP** Welt. Soll Ihr Gateway also mit anderen Geräten über VoIP kommunizieren, so muss der Zugriff auf diese Geräte als VoIP Schnittstelle konfiguriert sein.

Dabei kann es sich um verschiedene Arten von Geräten handeln:

- Weitere innovaphone Gateways,
- VoIP Endgeräte, zum Beispiel IP-Telefone wie das innovaphone IP 200,
- VoIP Terminal Adapter wie zum Beispiel das innovaphone IP 21 zum Anschluss analoger Endgeräte oder einer DECT Basisstationen,
- fremde VoIP Gateways, zum Beispiel als Übergang zu Telefonieswitches oder ins SS7 Netz,
- weitere Gatekeeper zur Rufkontrolle,
- VoIP PC Programme, wie beispielsweise innovaphone Softwarephone.

Jede VoIP Schnittstelle definiert den Zugriff zu einer Gruppe von Geräten, die in bestimmter Weise gleichartig behandelt werden. So lassen sich zum Beispiel alle IP-Telefone in einem Standort über nur eine VoIP Schnittstelle konfigurieren. Da Ihr Gateway die Definition von 12 verschiedenen Gruppen erlaubt, kann es insgesamt mit einigen hundert VoIP Geräten kommunizieren.

Die Konfiguration erfolgt im Bereich **VoIP Interfaces** des Konfigurationsapplets.

6.1 Generelle Überlegungen zur Konfiguration der VoIP Schnittstellen

Grundsätzlich setzt sich eine Telefonieinfrastruktur im VoIP Umfeld aus 3 verschiedenen Bausteinen zusammen:

- VoIP Endpunkte

  Dabei handelt es sich um Geräte, die den Endpunkt von Telefonaten realisieren. Zum Beispiel ein IP-Telefon wie das innovaphone IP 200 oder eine VoIP-Software wie innovaphone Softwarephone. Solche Endpunkte sind meist genau einem Benutzer zugeordnet.

- VoIP Gateways

  Dabei handelt es sich um Übergänge zu anderen Telefonienetzen oder -techniken. Dabei kann es sich um Übergänge ins ISDN-Netz oder ins analoge Telefonnetz handeln, aber auch um Adapter zum Anschluss von traditionellen, analogen Endgeräten oder zum Anschluss von vorhandenen TK-Anlagen.

Gateways bieten meist die Möglichkeit, mehrere Benutzer oder Endgeräte zu erreichen.

- Gatekeeper

  Gatekeeper übernehmen die Rufkontrolle und Rufvermittlung. Sie sind in der Lage, VoIP Endgeräte und Gateways zu verwalten, Rufnummern und Rufnamen zu interpretieren und somit die Rufvermittlung durchzuführen. Sie nehmen damit die Rolle der TK-Anlage beziehungsweise der Vermittlungsstelle in der klassischen Telefonie ein. Gatekeeper sind jedoch optional, Endpunkte und Gateways können wahlweise auch direkt miteinander kommunizieren.

Ihr innovaphone Gateway enthält immer auch einen Gatekeeper, den Sie wahlweise nutzen können. Gatekeeper und VoIP Endpunkte beziehungsweise VoIP Gateways kommunizieren normalerweise über das so genannte **RAS** Protokoll. Ihr Gateway kann wahlweise mit oder ohne **RAS** Protokoll eingesetzt werden. Bezüglich der Telefonieleistungsmerkmale ergeben sich beim Einsatz ohne **RAS** keine Nachteile. Auch die ausgefeilten Routingfunktionen Ihres Gateways können in dieser Betriebsart voll genutzt werden.

Der Einsatz mit **RAS** Protokoll bringt jedoch einige Vorteile mit sich:

- Der Gatekeeper kann die Übersetzung von logischen Gerätenamen (so genannten **Alias**en) in IP-Adressen durchführen. Dadurch lassen sich VoIP Geräte integrieren, deren IP-Adresse dynamisch ist. Nur so können per DHCP oder über eine PPP Einwählverbindung konfigurierte VoIP Geräte Verwendung finden.
- Der Gatekeeper kann ständig Buch führen über die Verfügbarkeit der ihm bekannten VoIP Geräte. Somit kann sich der Administrator jederzeit einen Überblick über den Status verschaffen. Darüber hinaus kann die Vermittlung der Gespräche von der Verfügbarkeit abhängig gemacht werden, ohne dass diese erst zum Rufzeitpunkt zeitaufwendig geprüft werden muss. Hiermit wird ein wesentlich besseres Verhalten im Fehlerfall erreicht.
- Viele fremde VoIP Geräte erfordern zum Betrieb zwingend das **RAS** Protokoll.

Es ist empfehlenswert, den in Ihrem Gateway enthaltenen Gatekeeper in Betrieb zu nehmen sowie nach Möglichkeit das **RAS** Protokoll zu nutzen. Sollten einzelne VoIP Geräte, mit denen Ihr Gateway kommunizieren soll, kein **RAS** Protokoll zulassen, können diese trotzdem problemlos direkt angesprochen werden.

Selbstverständlich können Sie Ihre Gateways auch im Zusammenhang einem bereits vorhandenen Gatekeeper betreiben.

Beachten Sie jedoch, dass viele Leistungsmerkmale in einem VoIP Netzwerk auch vom verwendeten Gatekeeper abhängig sind. Welche Leistungsmerkmale beim

Betrieb mit einem fremden Gatekeeper verfügbar sind, hängt daher vom jeweiligen Einzelfall ab.

6.1.1 Den Gatekeeper Ihres Gateways verstehen

Grundsätzlich kommen dem Gatekeeper zwei Aufgaben zu:

- Die Verwaltung der Endgeräte (Geräteverwaltung).
- Die Vermittlung von Sprachrufen (Rufvermittlung).

Beide Funktionen sind in Ihrem Gateway enthalten, die Geräteverwaltung ist jedoch optional.

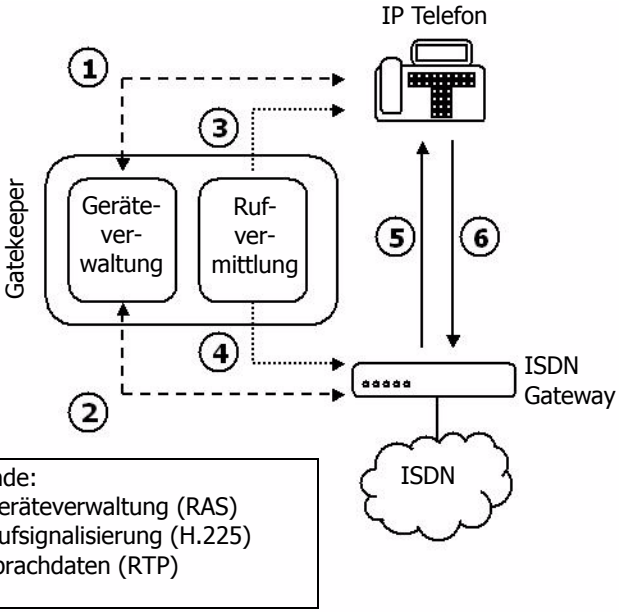

Abbildung 19 Rufablauf mit einem Gatekeeper und RAS

Abbildung 19 auf Seite 71 zeigt ein Szenario mit einem IP-Telefon, einem ISDN-Gateway und einem Gatekeeper. Bei dem Gatekeeper kann es sich um ein weiteres innovaphone Gateway handeln, es kann sich jedoch auch um den in jedem innovaphone Gateway enthaltenen Gatekeeper handeln. Zum besseren Verständnis sind Gatekeeper und ISDN-Gateway jedoch getrennt dargestellt.

Im Folgenden werden die einzelnen Schritte eines Rufes dargestellt, soweit sie in diesem Zusammenhang von Bedeutung sind. Tatsächlich können die Vorgänge weit komplexer sein.

- Sowohl das IP-Telefon (1.), als auch das ISDN-Gateway (2.) melden sich bei der Geräteverwaltung des Gatekeepers an. Dabei geben Sie eine Identifikation sowie ihre aktuelle IP-Adresse an. Dieser Schritt setzt das RAS Protokoll voraus und entfällt dementsprechend, wenn ohne RAS Protokoll gearbeitet wird.
- Das IP-Telefon initiiert einen Ruf (3.) und stellt eine Signalisierverbindung zum Gatekeeper her.
- Der Gatekeeper stellt das Rufziel fest und baut eine Signalisierverbindung zum Ziel auf (4.). IP-Telefon und Gateway tauschen ihre IP-Adressen aus. Die weitere Signalisierung zwischen beiden läuft über den Gatekeeper.
- Das IP-Telefon und das ISDN-Gateway bauen direkt untereinander die beiden Sprachkanäle (5. und 6.) auf.

Tatsächlich müssen Rufquelle und Rufziel nicht unbedingt den selben Gatekeeper verwenden. Abbildung 20 auf Seite 73 zeigt den Ablauf eines Rufes, der über 2 Gatekeeper vermittelt wird.

Für Ziel und Quelle des Rufes sieht der Ablauf ganz gleich aus wie in Abbildung 19 auf Seite 71, die komplexere Infrastruktur wird vollständig von den Gatekeepern verborgen. Lediglich die beiden Gatekeeper müssen nun untereinander bekannt sein. Dies kann wiederum über das RAS Protokoll erfolgen, in dem sich ein Gatekeeper bei dem anderen oder beide Gatekeeper gegenseitig anmeldet (Schritt 1). Der vom IP-Telefon eingehende Ruf wird nun vom ersten Gatekeeper an den zweiten vermittelt und von diesem wiederum an das Zielgateway. Auf diese Art und Weise lassen sich sehr komplexe Strukturen mit mehreren Gatekeepern aufbauen.

Die Geräteverwaltung wird im Konfigurationsapplet im Bereich **VoIP Interfaces** konfiguriert.

Die Geräteverwaltung erfolgt dynamisch über die so genannte **Registration** im **RAS** (**R**egistration, **A**dmission und **S**tatus) Protokoll. Hierbei ermittelt das sich anmeldende Gerät zunächst den zuständigen Gatekeeper. Bei dieser als **Gatekeeper discovery** bezeichneten Prozedur sucht das Endgerät im Netz einen Gatekeeper mit der gewünschten Gatekeeper ID, einem logischen Namen für den Gatekeeper.

Über die Gatekeeper Id lassen sich in einem Netz mehrere Gatekeeper betreiben und von jeweils "ihren" Geräten finden. Allerdings unterstützen viele Fremdgatekeeper die Gatekeeper Id nicht.

Tipp

Manche Gatekeeper und auch manche VoIP Geräte unterstützen die Discovery Prozedur nicht. In diesem Fall muss die IP-Adresse des Gatekeepers im anzumeldenden Gerät konfiguriert werden. Ebenso werden multicasts von Routern normalerweise nicht übertragen. Daher muss die IP-Adresse des Gatekeepers auch dann eingetragen werden, wenn er durch einen Router vom anmeldenden Gerät getrennt ist.

Ist der Gatekeeper ermittelt, übermittelt das Gerät seine Identifikation und seine IP-Adresse. Dabei kann es sich um einen logischen Namen oder eine Telefonnummer oder beides handeln. Ist die Identifikation in Ordnung, ist das Gerät nun betriebsbereit und erreichbar. Geräte, die sich per RAS Protokoll beim Gatekeeper anmelden, werden im Modus **Gatekeeper client group konfiguriert**.

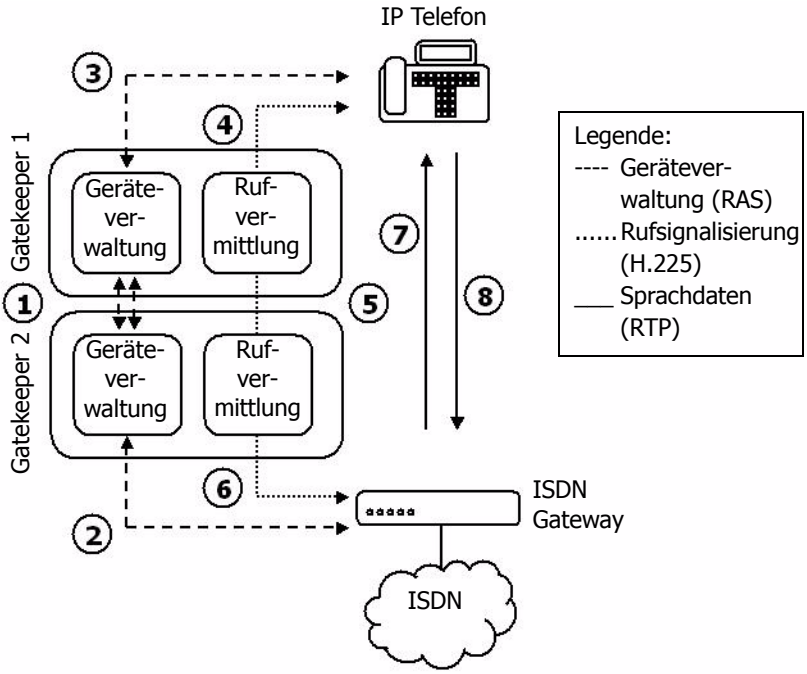

Abbildung 20 Rufablauf mit zwei Gatekeepern und RAS

Einige VoIP Geräte unterstützen das RAS Protokoll nicht. Solche Geräte können trotzdem verwaltet werden, indem sie statisch und damit mit festen IP-Adressen im Gatekeeper konfiguriert werden. Im Ablauf in Abbildung 19 auf Seite 71 entfallen dann die Schritte 1 und 2. Solche Geräte werden im Modus **Gateway** oder **Gateway group** konfiguriert.

Natürlich kann sich Ihr Gateway auch selbst bei einem anderen Gatekeeper mit RAS Protokoll anmelden, wie es in dem in Abbildung 20 auf Seite 73 der Fall ist. Diese Betriebsart wird im Modus **Registration at Gatekeeper as endpoint** oder **Registration at Gatekeeper as Gateway** konfiguriert.

6.1.2 Die Gatekeeper Discovery

Die **gatekeeper discovery** funktioniert über **IP multicast** Pakete, die ein Gatekeeper Klient aussendet, wenn er einen geeigneten Gatekeeper ermitteln will.

Im Normalfall werden solche Pakete nur im eigenen LAN Segment übertragen und insbesondere nicht in andere Netze geroutet. Daher werden Gatekeeper nur im eigenen LAN Segment gefunden. Allerdings können Router so konfiguriert werden, dass sie solche Pakete nach bestimmten Regeln weiter transportieren. Damit können auch Gatekeeper gefunden werden, die über WAN Strecken angebunden sind.

Die Unterscheidung basiert auf den so genannten **multicast addresses**. Die bei der **gatekeeper discovery** verwendete **multicast address** ist die `224.0.1.41`.

6.1.3 Die Gatekeeper-ID

Jeder Gatekeeper in einem Netz kann über eine eigene **Gatekeeper-ID** unterschieden werden. Diese ID ermöglicht es dem Administrator, mehrere Gatekeeper in einem Netz parallel zu betreiben, wobei jedes Endgerät bei der **gatekeeper discovery** trotzdem den "richtigen" Gatekeeper ermittelt. Die ID wird direkt im Konfigurationsapplet, Bereich **VoIP Interfaces** im Feld **Gatekeeper ID** festgelegt.

Haben Sie Ihrem Gateway eine Gatekeeper ID zugewiesen, wird der Gatekeeper nur solche **RAS Discovery** Anfragen beantworten, in denen entweder diese oder gar keine **Gatekeeper ID** aufgeführt ist. Auch wenn Ihre Endgeräte den Gatekeeper fest konfiguriert haben und daher keine **gatekeeper discovery** durchführen, werden die RAS Anmeldungen nur dann akzeptiert, wenn darin wiederum die richtige oder keine Gatekeeper ID konfiguriert ist.

Wird eine **Gatekeeper ID** konfiguriert, so gilt diese für das gesamte Gateway.

Wird in Ihrem Netz nur ein Gatekeeper betrieben oder verwenden Sie keine **gatekeeper discovery**, so genügt es, generell ohne **Gatekeeper ID** zu arbeiten.

6.1.4 H.323 Protokolloptionen

Ihr Gateway unterstützt bezüglich der Kommunikation mit anderen VoIP Geräten eine Reihe von Protokolloptionen, die bestimmte Details des Verhaltens beeinflussen. Diese Optionen sind unabhängig von dem verwendeten **Gateway mode** verfügbar.

Option	Bedeutung
Disable Faststart	In der Grundeinstellung ist die H245 Faststart Prozedur erlaubt. Ausgehende Rufe werden mit Faststart ausgeführt, eingehende Rufe mit Faststart werden mit Faststart beantwortet. Soll die H245 Faststart Prozedur unterbunden werden, muss die Option **Disable Faststart** aktiviert werden. Ist diese Option aktiviert, werden ausgehende Rufe ohne Faststart ausgeführt und eingehende Rufe mit und ohne Faststart ohne Faststart beantwortet. Die Aktivierung der Option **Disable Faststart** ist nur dann empfehlenswert, wenn Kompatibilitätsprobleme mit Fremdprodukten auftreten.

Tipp

Werden Verbindungen zu Endpunkten mit H.323 Version 2 aufgebaut, kann es sein, dass einige Ruftöne nicht mehr zu hören sind. In diesem Fall das Protokoll der Gegenseite aktualisieren.

Disable H245-tunneling	In der Grundeinstellung wird die Aushandlung der Sprachdatenverbindung in der bereits vorhanden TCP Signalisierverbindung[1] durchgeführt. Bei Aktivierung der Option **Disable H245-tunneling** wird eine eigene TCP Verbindung für diese Aushandlung aufgebaut. Dies gilt für die aus dem Gatekeeper hinausführende Signalisierverbindung. Ist die Option **Disable H245-tunneling** deaktiviert, wird eine separate Aushandlungsverbindung eingespart, was im Zusammenhang mit **NAT** und **Firewalls** von Vorteil sein kann. Forts. ...

Option	Bedeutung
Forts. ...	Die Aktivierung der Option **Disable H245-tunneling** ist nur dann empfehlenswert, wenn Kompatibilitätsprobleme mit Fremdprodukten auftreten.

Tipp

Werden Verbindungen zu Endpunkten mit H.323 Version 2 aufgebaut, kann es sein, dass einige Ruftöne nicht mehr zu hören sind. In diesem Fall das Protokoll der Gegenseite aktualisieren.

Enable T.38 fax protocol	Sprachverbindungen, über die ein Fax übertragen wird, werden mit dem speziellen **Fax over IP** Protokoll **T.38** übertragen. Anderenfalls werden Faxübertragungen nicht gesondert behandelt. Diese Option ist immer empfehlenswert, es sei denn, es treten Kompatibilitätsprobleme mit Fremdprodukten auf.
fake connect	Damit wird der rufenden Seite bereits ein Verbindungsaufbau signalisiert, sobald von der gerufenen Seite **in-band** Informationen erhalten werden, obwohl noch keine Verbindung zustande gekommen ist. Dabei kann es sich beispielsweise um Ruftöne oder um Fehleransagen des Netzes handeln. Einige VoIP Geräte schalten den Sprachkanal erst beim Zustandekommen einer Verbindung durch. In solchen Fällen können Ansagen, die vorher auftreten vom Anrufer nicht gehört werden. Diese Option behebt dieses Problem. Verwenden Sie diese Option nur für VoIP Geräte, die dieses Problem aufweisen.
Suppress sending of HLC	Verhindert das Senden von so genannten **high layer compatibility (HLC)** Informationselementen. Dies ist dann erforderlich, wenn das empfangende VoIP Gerät auf **HLCs** fehlerhaft reagiert. Anderenfalls werden die HLCs transparent durch den Gatekeeper weitergeleitet. Verwenden Sie diese Option nur dann, wenn ein derart fehlerhaftes VoIP Gerät betrieben werden muss. Verwenden Sie die Option insbesondere nicht bei der Koppelung von TK-Anlagen über innovaphone Gateways, da sonst unter Umständen wichtige Informationen verloren gehen.

Option	Bedeutung
Suppress sending of FTY	Verhindert das Senden von so genannten **facility (FTY)** Nachrichten. Dies ist dann erforderlich, wenn das empfangende VoIP Gerät auf **FTYs** fehlerhaft reagiert. Anderenfalls werden die **FTYs** transparent durch den Gatekeeper weitergeleitet. Verwenden Sie diese Option nur dann, wenn ein derart fehlerhaftes VoIP Gerät betrieben werden muss. Verwenden Sie die Option insbesondere nicht bei der Koppelung von TK-Anlagen über innovaphone Gateways, da sonst unter Umständen wichtige Informationen verloren gehen.
Generate connected time	Veranlasst den Gatekeeper, in ausgehenden **Connect messages** einen Zeitstempel mit der lokalen Gatewayzeit einzufügen. Verwenden Sie diese Option, wenn die gerufenen VoIP Geräte auf den Zeitstempel angewiesen sind und die Rufquellen (z.B. das ISDN Netz) keinen liefern

1. Technisch gesehen wird für das H.245 Protokoll keine eigene TCP Verbindung aufgebaut, sondern die TCP Verbindung der H.225 mitgenutzt.

Tabelle 10 H.323 Protokolloptionen

6.1.5 Einrichten eines Gatekeepers auf einem anderen Gateway

Soll der Gatekeeper nicht auf dem eigenen Gateway arbeiten, so kann im Konfigurationsapplet im Bereich **VoIP Interfaces** eine **Remote gatekeeper address** konfiguriert werden.

Ist im Feld **IP address** die IP-Adresse eines fernen Gatekeepers eingetragen, versucht das Gateway sich auf dem fernen Gatekeeper zu registrieren. Schlägt diese Registrierung fehl, wird die Registrierung auf einem alternativen Gatekeeper versucht, sofern im Feld **Alternate Gatekeeper** eine alternative Gatekeeper IP-Adresse angegeben ist.

Die Angabe einer alternativen Gatekeeper IP-Adresse ist besonders beim Einsatz von redundanten Systemen wichtig.

Arbeitet der Gatekeeper mit einer Gatekeeper ID, (siehe Kapitel 6.1.3 "Die Gatekeeper-ID" ab Seite 74) tragen Sie diese in das Feld **Gatekeeper ID** ein.

Das **Password** entspricht dem H.235 Password, das zum Anmelden auf dem fernen Gatekeeper benötigt wird.

Durch Aktivieren der Schaltfläche **Disable dynamic signaling port** kann ein fester **Signaling port** angegeben werden, der wiederum z. B. an Firewall-Sytemen konfiguriert werden kann.

6.1.6 Die Sprachübertragung

Ihr Gateway unterstützt verschiedene Methoden der Sprachübertragung im IP. Die entsprechenden Festlegungen für Gespräche zwischen einer ISDN Schnittstelle Ihres Gateways und einem VoIP Gerät, das durch diese VoIP Schnittstelle definiert wird, treffen Sie im Bereich **Codec configuration**. Beachten Sie, dass Gespräche zwischen zwei VoIP Geräten, also von IP zu IP, diese Einstellung nicht berücksichtigen, da die Aushandlung der Parameter direkt zwischen den Endgeräten erfolgt und damit deren Konfiguration maßgeblich ist.

Die Sprachkodierung

Sprache kann in verschiedenen Kodierungen übertragen werden. Einige der zur Verfügung stehenden Kodierungen komprimieren die Sprache, andere tun dies nicht. Ihr Gateway unterstützt verschiedene gebräuchliche Sprachkodierungsverfahren, deren Eigenschaften in der nachstehenden Tabelle beschrieben sind:

Kodierung	Bandbreite[1] je Gespräch	minimales Delay[2]	Eigenschaften
G.711A	64kbit/s	20 ms	Ohne Kompression, beste Sprachqualität (entspricht derjenigen von digitalen Telefonsystemen). Tondigitalisierung nach europäischem Verfahren.
G.711U	64kbit/s	20 ms	Wie oben, Tondigitalisierung nach amerikanischem Verfahren[3].

Kodierung	Bandbreite[1] je Gespräch	minimales Delay[2]	Eigenschaften
G.726-16 G.726-24 G.726-32 G.726-40	16,24,32, 40kbit/s	20 ms	Nur für Fax und Modem Daten in Ausnahmefällen vorgesehen.
G.723-53	5,3kbit/s	30 ms	Gute Sprachqualität (entspricht annähernd derjenigen von analogen Telefonsystemen).
G.723-63	6,3kbit/s	30 ms	Etwas bessere Sprachqualität als G.723-53 bei geringfügig größerer Bandbreite.
G.729A	8kbit/s	20 ms	Beste Sprachqualität der komprimierenden Kodierungsverfahren, geringstes minimales Delay.

1. Bei der angegebenen Bandbreite handelt es sich lediglich um die nominale Bandbreite des Kodierungsalgorithmus. Bei der Übertragung der komprimierten Daten im Netzwerk werden noch weitere Kontrollinformationen übertragen, so dass je nach Konfiguration die benötigte Gesamtbandbreite deutlich höher ausfallen kann.
2. Unter "Delay" wird hier die Verzögerung verstanden, die durch die Kodierung und Paketierung der Daten minimal entsteht. Im Rahmen der Übertragung der Daten in Netzwerken entstehen weitere Verzögerungen.
3. Sie können sowohl **µ–law**, als auch **A-law** Kodierung verwenden, ganz unabhängig davon, welche Kodierung auf Ihrem ISDN Anschluss verwendet wird. Die Kodierung wird jeweils am ISDN Anschluss korrekt angepasst.

Tabelle 11 Sprachkodierungsverfahren

Die Art der Komprimierung der Sprachdaten legen Sie im Feld **Standard** fest. Diese Einstellung wird bevorzugt verwendet. Unterstützt das entfernte VoIP Gerät die eingestellte Kodierung jedoch nicht, wird eine gemeinsam unterstützte Kodierung ausgehandelt. Aktivieren Sie das Kontrollkästchen **exclusive**, wenn Sie die Verwendung der eingestellten Kodierung erzwingen wollen. Was natürlich zu einem scheiternden Ruf führen kann, wenn Ihr Gateway und das entfernte VoIP Gerät keinen gemeinsamen **Coder** unterstützen.

Tipp

Den besten Kompromiss zwischen Sprachqualität und benötigter Bandbreite bietet G.729. Wählen Sie dieses Verfahren für entfernte Telefoniegateways, die Sie über das Internet, das Intranet oder stark belastete lokale Netzwerke erreichen. In leistungsfähigen lokalen Netzwerken benutzen Sie G.711, um die beste Sprachqualität zu erreichen. G.723.1 benötigen Sie für Verbindungen mit Telefoniegateways, die den G.729 Standard nicht unterstützen. G.726 Kodierungen sollten Sie nur in Fällen anwenden, wo auf einer Verbindung Faxdaten ohne T.38 übertragen werden sollen.

Die Paketierungsgröße

Unter **Packetsize** (**ms**) legen Sie die Größe der Pakete fest, in denen die kodierten Sprachdaten zwischen den Telefoniegateways ausgetauscht werden. Der Wert, den Sie hier einstellen, legt die Dauer fest, für die Sprachdaten gesammelt werden, bevor sie als ein Paket mit Sprachinformationen übertragen wird. Diese Dauer verursacht eine entsprechende Verzögerung in der Sprachübertragung. Ein Wert von 30ms wird vom menschlichen Ohr als praktisch verzögerungsfrei wahrgenommen, ein Wert von 100ms wird von den meisten Benutzern ebenfalls nicht als störend wahrgenommen.

Größere Pakete verursachen eine erhöhte Verzögerung in der Sprachdatenübertragung (**Delay**), verursachen jedoch eine geringere Netzwerkbelastung, da der beim Transport der Pakete im Netzwerk auftretende **Overhead** geringer wird.

Beachten Sie, dass der Overhead bei geringer **Packetsize** erheblich anwächst, da die zur Übertragung im IP-Protokoll (im LAN) und zusätzlich im PPP Protokoll (im WAN) notwendigen zusätzlichen Daten je Paket konstant bleiben, die Größe der Sprach- und damit eigentlichen Nutzdaten jedoch sinkt. Die tatsächlich erforderliche Bandbreite ist daher je nach Paketgröße erheblich größer, als die reine Sprachdatenbandbreite, wie sie in Tabelle 11 angegeben ist.

Können die Sprachdaten auf Grund fehlender Bandbreite oder zu großer Netzwerklaufzeiten nicht mehr ausreichend schnell übertragen werden, macht sich dies durch störende Fremdgeräusche (Knistern, Knacken) oder stark anwachsende Verzögerung bemerkbar. Erhöhen Sie in einem solchen Fall die Paketgröße für die betroffene Telefonieschnittstelle, um den Effekt zu mildern oder wechseln Sie zu einem effizienteren Kodierungsverfahren (beispielsweise von G.729 auf G.723-53). Tabelle 12 zeigt die benötigten Bandbreiten je nach Kodierung und Paketgröße.

Kodierverfahren	Effektiv benutzte Bandbreite (in kbit/s) je nach Paketlänge bei				
	20 ms	**30 ms**	**60 ms**	**90 ms**	**150 ms**
	mögliche Verbindungen je 64kbps				
G.711	83 kbit/s	77 kbit/s	70 kbit/s	68 kbit/s	67 kbit/s
G.723-53	24 kbit/s	18 kbit/s	12 kbit/s	9 kbit/s	8 kbit/s
	2	3	5	6	8
G.723-63	25 kbit/s	19 kbit/s	13 kbit/s	10 kbit/s	9 kbit/s
	2	3	5	6	7
G.729	27 kbit/s	21 kbit/s	14 kbit/s	12 kbit/s	11 kbit/s
	2	3	4	5	6
G.726-16	19 kbit/s bei 150 ms				
	3				
G.726-24	27 kbit/s bei 150ms				
	2				
G.726-32	35 kbit/s bei 150ms				
	1				
G.726-40	43 kbit/s bei 150ms				
	1				
T.38	14 kbit/s bei 120ms[1]				
	4				

1. Die Faxübertragung im T.38 Protokoll arbeitet fest mit einer Paketgröße von 150ms. Streng genommen werden die Fax Daten nicht komprimiert, es entfällt lediglich der bei der analogen Übertragung entstehende **Overhead**.

Tabelle 12 Benötigte Bandbreiten abhängig von der Paketgröße

Die hier angegebenen Werte sind Näherungswerte, da die genaue Bestimmung der benötigten Bandbreite von verschiedenen Faktoren abhängt.

Tipp

Die effektiv benötigte Bandbreite kann je nach Umgebungsbedingungen variieren. Zum einen können in der Übertragungsstrecke eingesetzte Router spezielle Komprimierungsverfahren (RTP Header Compression) verwenden und so die benötigte Bandbreite verringern. Zum anderen kommt es durch die Abschaltung der Sprachkanäle bei Sprachpausen ebenfalls zu verringertem Bandbreitenbedarf. Die in der Tabelle angegebenen Werte stellen den ungünstigsten Wert bei Übertragung über Weitverkehrsstrecken (PPP) dar.

Beachten Sie bitte, dass die angegebenen Werte pro Richtung gelten. Die Gesamtwerte für ein Gespräch ohne **Silence compression** sind damit doppelt so hoch. Allerdings werden die Bandbreiten von Kommunikationsmedien normalerweise auch je Richtung angegeben. So hat eine ISDN Verbindung 64kbps je Richtung, so dass die Angaben in der Tabelle intuitiv mit den bekannten Bandbreiten vergleichbar sind.

Eine weitere Möglichkeit, Bandbreite einzusparen besteht darin, in Sprachpausen keine Daten zu übertragen. Da bei einem Gespräch normalerweise nur jeweils eine Partei spricht, kann damit erheblich Bandbreite eingespart werden. Diese Funktion wird als **Silence compression** bezeichnet und kann normalerweise ohne Qualitätsverlust aktiviert werden.

Auf der sprachlich aktiven Seite würde eine absolute Stille von der anderen Seite irritierend wirken, oft nehmen Benutzer an, dass die Verbindung gestört ist, wenn sie nichts mehr von ihrem Gesprächspartner hören. Um dies zu vermeiden, wird auf dieser Seite ein künstliches Hintergrundgeräusch, so genannter **comfort noise** eingespielt. Um die Lautstärke dieser simulierten Hintergrundgeräusche regelmäßig an die tatsächlichen Hintergrundgeräusche der momentan stillen Seite anzupassen, werden regelmäßig Informationen darüber ausgetauscht. Diese so genannten **comfort noise updates** benötigen immer noch wesentlich weniger Bandbreite als die durch **silence compression** Eingesparte. **Silence compression** und **Send comfort noise updates** sollten daher zusammen aktiviert werden und nur dann deaktiviert sein, wenn es zu Kompatibilitätsproblemen durch Fremdgeräte kommt.

6.1.7 Festlegen der VoIP Tracing Level

Über die Einstellung der **tracing level** können Sie festlegen, zu welchen Themenbereichen Ihr Gateway **traces** schreibt. Dies geschieht auf der Grundseite im Bereich **VoIP Interfaces**.

Einstellung	Wirkung
RAS trace	Protokollierung des Geräteverwaltungsprotokolls
H.225 trace	Protokollierung des Rufsignalisierungsprotokolls
H.245 trace	Protokollierung des Medienkanalprotokolls
T.38 trace	Protokoll der Faxübertragung

Tabelle 13 VoIP **Tracing level**

Das Mitschreiben von Traces verursacht keine Performanceprobleme, da die Einträge lediglich in einen speziellen Puffer im Hauptspeicher Ihres Gerätes geschrieben werden. Allerdings handelt es sich dabei um einen Ringpuffer, so dass neue Meldungen ältere überschreiben. Es kann daher sinnvoll sein, bestimmte, nicht interessante Aspekte auszublenden, um von einer speziellen problematischen Situation einen vollständigen Trace zu erhalten.

6.2 Verwaltung von VoIP Geräten per RAS (Gatekeeper)

Die Verwaltung von VoIP Geräten in Ihrem Gateway mit Hilfe des RAS Protokolls stellt die empfohlene Methode der Geräteverwaltung dar.

- Wechseln Sie im Konfigurationsapplet **VOIP Interfaces** auf ein neues **Undefined GWn**.
- Legen Sie gegebenenfalls eine **Gatekeeper ID** fest (siehe Kapitel 6.1.3 "Die Gatekeeper-ID" ab Seite 74).
- Zur Festlegung der VoIP Geräte, die vom Gatekeeper verwaltet werden sollen, richten Sie im Bereich **VoIP Interfaces** unter **GW1** bis **GW12** eine Definition im Modus **Gatekeeper client group** ein.
  Schränken Sie bei Bedarf den Zugriff von VoIP Geräten auf Ihr Gateway ein. Tragen Sie dazu unter **IP address** die Netzwerkadresse des IP-Netzes ein, in dem sich die zugelassenen Geräte befinden. Unter **IP mask** stellen sie die Netzmaske des Netzes ein.
  Auf diese Art und Weise können Sie den Kreis der zugelassenen VoIP Geräte beliebig festlegen. Es ist dabei nicht erforderlich, dass es sich bei dem konfi-

gurierten Netz um ein tatsächlich existierendes Netz handelt.

- Legen Sie die H.323 Protokolloptionen für die zu verwaltenden VoIP Geräte fest (siehe Kapitel 6.1.4 "H.323 Protokolloptionen" ab Seite 75).
- Legen Sie für jedes VoIP Gerät einen **alias** Eintrag an. Dies geschieht, indem Sie die Schaltfläche **Add alias** betätigen.

  Für VoIP Endpunkte sollten Sie hier die zugewiesene Durchwahl oder MSN als **E.164 Adress** sowie den Namen als **H.323 Name** festlegen. Für VoIP Gateways genügt es, den Namen festzulegen.

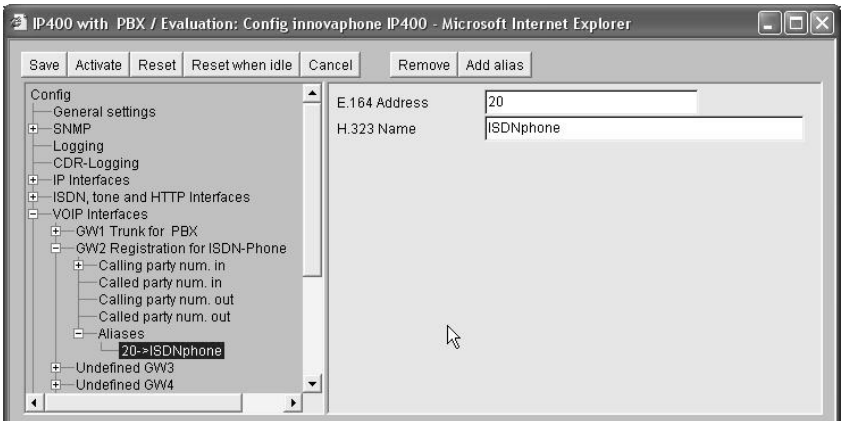

Abbildung 21 Eintragen eines VoIP Gerätes

Beachten Sie bitte, dass es in jedem Fall genügt, wenn sich das VoIP Gerät mit seinem Namen anmeldet. Generell wird bei der Anmeldung geprüft, ob Angaben, die in der Anmeldung enthalten sind mit einem konfigurierten Aliaseintrag übereinstimmen. Werden bei der Anmeldungen Angaben weggelassen (etwa die E.164 Adresse), dann wird diese auch nicht geprüft. Somit kann sich ein Endgerät allein mit seinem Namen anmelden und seine Durchwahl dadurch allein im Gatekeeper festgelegt werden, dass im Alias Eintrag mit dem passenden Namen die entsprechende Nummer eingetragen ist. Meldet sich das Endgerät jedoch mit Namen und Nummer an, so kann die Nummer nicht alleine im Gatekeeper geändert werden, da sich das Endgerät nach einer Änderung mit der falschen **E.164 Address** anmelden würde.

Meldet sich ein VoIP Gerät mit mehreren H.323 Aliasen gleichzeitig an, so wird jeder einzelne gegen die in Ihrem Gatekeeper definierten geprüft und die Anmeldung erfolgt nur, wenn alle Aliase definiert sind.

- Sollte eine Anpassung der Rufnummernbehandlung nötig sein (siehe Kapitel 5.2.7 "Behandlung der verschiedenen ISDN Adresstypen" ab Seite 64), so nehmen Sie die entsprechenden Eintragungen vor, indem Sie mit der Schaltfläche **Add CGPN** / **CDPN in** / **out map** in den Bereichen **Calling** / **Called party num. in** / **out** entsprechende Eintragungen hinzufügen.
- Sollen die konfigurierten VoIP Geräte auch Zugriff auf die ISDN Schnittstellen Ihres Gateways haben, legen Sie die Parameter der Sprachübertragung (siehe Kapitel 6.1.6 "Die Sprachübertragung" ab Seite 78) fest.

6.2.1 Besonderheiten bei der Konfiguration von innovaphone Geräten

Die innovaphone Geräte bieten die Möglichkeit, sich anhand ihrer Seriennummer zu registrieren. Dies geschieht immer dann, wenn Sie zum Betrieb an einem Gatekeeper konfiguriert sind, jedoch kein Aliasname im Profil konfiguriert ist. In diesem Fall versucht zum Beispiel das IP-Telefon tiptel innovaphone IP 200, sich mit dem **H.323 Name** `IP200-03-`***`xx-xx`*** zu registrieren, wobei sich ***`xx`***`-`***`xx`*** aus den letzten vier Ziffern der Seriennummer des IP-Telefons ergibt. Dadurch ist es möglich, alle IP-Telefone mit absolut identischer Konfiguration zu betreiben.

Tipp

Beachten Sie bitte, dass Endgeräte, die von der optionalen innovaphone PBX verwaltet werden, im Bereich **VoIP Interfaces** des Gateways nicht konfiguriert werden müssen.

- Wechseln Sie im Konfigurationsapplet zu **VOIP Interfaces** auf das **GWn**, das Sie für die Verwaltung der VoIP Geräte per RAS konfiguriert haben (siehe Kapitel 6.2 "Verwaltung von VoIP Geräten per RAS (Gatekeeper)" ab Seite 83).
- Legen Sie im Gatekeeper einen entsprechender Alias Eintrag an. Die Seriennummer wird im Feld **H.323 Name** eingetragen, die Durchwahl des Telefons wird im Feld **E.164 Address** festgelegt.
- Soll dem IP-Telefon zusätzlich noch ein "sprechender" Name zugewiesen werden, richten Sie einen weiteren Alias mit der gleichen Durchwahl als Text vor dem Seriennummernalias ein. Tragen Sie den gewünschten Namen als **H.323 Name** ein.

Zur Nutzung aller Leistungsmerkmale sollten Endgeräte jedoch mit der optionalen innovaphone PBX Komponente verwaltet werden.

6.3 Statische Verwaltung von VoIP Geräten

Arbeiten Sie mit VoIP Geräten, die keine dynamische Anmeldung mit Hilfe des RAS Protokolls unterstützen, so müssen Sie die Geräte statisch konfigurieren. Dadurch entfällt die ständige Kontrolle, ob die Geräte erreichbar sind und es besteht nicht die Möglichkeit, mit veränderlichen IP-Adressen (also z.B. mit DHCP) zu arbeiten. Andere Nachteile entstehen jedoch nicht.

Sie können die VoIP Geräte einzeln konfigurieren oder in Gruppen. Dies ist insbesondere dann praktisch, wenn eine größere Anzahl von VoIP Klienten benutzt wird, die kein RAS unterstützen.

- Zur Festlegung eines einzelnen VoIP Geräts, das statisch verwaltet werden soll, richten Sie im Bereich **VoIP Interfaces** unter **GW1** bis **GW12** eine Definition im Modus **Gateway** ein
  oder:
  Zur Festlegung einer Gruppe von VoIP Geräten, die statisch verwaltet werden sollen, richten Sie im Bereich **VoIP Interfaces** unter **GW1** bis **GW12** eine Definition im Modus **Gateway group** ein. Somit erlauben Sie allen VoIP Geräten, die sich in einem IP-Netzwerk befinden, den Zugriff. Gehen Sie bei der Einrichtung solcher Gatewaygruppen jedoch sorgfältig vor und stellen Sie sicher, dass Sie den Zugriff unerwünschter Geräte (z.B. solcher, die aus dem Internet versuchen, auf Ihr Gateway zuzugreifen) ausschließen.
- Für ein einzelnes VoIP Gerät tragen Sie unter **IP address** dessen IP-Adresse ein
  oder:
  Für eine Gruppe von VoIP Geräten tragen Sie unter **IP address** die Netzwerkadresse des IP-Netzes ein, in dem sich die zugelassenen Geräte befinden. Unter **IP mask** stellen Sie die Netzmaske des Netzes ein.
  Auf diese Art und Weise können Sie den Kreis der zugelassenen VoIP Geräte beliebig festlegen. Es ist dabei nicht erforderlich, dass es sich bei dem konfigurierten Netz um ein tatsächlich existierendes Netz handelt. Mit der Einstellung IP address auf `0.0.0.0` und IP mask `0.0.0.0` erlauben Sie allen VoIP Geräten den Zugriff.
- Legen Sie die H.323 Protokolloptionen für die zu verwaltenden VoIP Geräte fest (siehe ab Seite 75).
- Sollte eine Anpassung der Rufnummernbehandlung nötig sein (siehe ab Seite 64), so nehmen Sie die entsprechenden Eintragungen vor, indem Sie mit der Schaltfläche **Add CGPN** / **CDPN in** / **out map** in den Bereichen **Calling** / **Called party num. in** / **out** entsprechende Eintragungen hinzufügen.

- Sollen die konfigurierten VoIP Geräte auch Zugriff auf die ISDN Schnittstellen Ihres Gateways haben, legen Sie die Parameter der Sprachübertragung (siehe ab Seite 78) fest.

6.4 Anmelden des Gateways bei einem anderen Gatekeeper

Soll sich Ihr Gateway (bzw. der darin enthaltene Gatekeeper) bei einem anderen Gatekeeper anmelden, wie es etwa in dem in Abbildung 20 auf Seite 73 gezeigten Szenario der Fall ist, so kann dies durch eine Gatewaydefinition im Modus **Register at gatekeeper as gateway** erfolgen. Damit wird Ihr Gateway als VoIP Gateway (siehe Seite 69) angemeldet. Dies ist in den meisten Fällen der richtige Modus. Sollte der Gatekeeper, bei dem die Anmeldung erfolgen soll jedoch nur die Anmeldung eines VoIP Endpunktes zulassen, verwenden Sie den Modus **Register at gatekeeper as endpoint**. Handelt es sich bei dem fremden Gatekeeper wiederum um ein innovaphone Gateway, ist das Verhalten in beiden Modi gleich.

- Zur Anmeldung bei einem Gatekeeper, richten Sie im Bereich **VoIP Interfaces** unter **GW1** bis **GW12** eine Definition im Modus **Register at gatekeeper as gateway** oder **Register at gatekeeper as endpoint** ein.
- Soll die Ermittlung des Gatekeepers durch **Gatekeeper Discovery** erfolgen (siehe Kapitel 6.1.2 "Die Gatekeeper Discovery" ab Seite 74), können Sie das Feld **IP address** leer lassen. Anderenfalls tragen Sie dort die IP-Adresse des Gatekeepers ein.
- Arbeitet der Gatekeeper mit einer Gatekeeper ID, (siehe Kapitel 6.1.3 "Die Gatekeeper-ID" ab Seite 74) tragen Sie diese in das Feld **Gatekeeper ID** ein.
- Legen Sie durch Drücken der Schaltfläche **Add alias** den **H.323 Alias** fest, mit dem Sie sich beim Gatekeeper identifizieren müssen. Normalerweise ist es am sinnvollsten, wenn sich das Gateway nur mit einem H.323 Namen und nicht mit einer E.164 Adresse (also mit einer Telefonnummer) anmeldet. Manche Gatekeeper setzen dies allerdings zwingend voraus. Beachten Sie daher die Dokumentation des Gatekeepers, bei dem Sie sich anmelden wollen.
- Legen Sie die H.323 Protokolloptionen für die Kommunikation mit dem Gatekeeper fest (siehe Kapitel 6.1.4 "H.323 Protokolloptionen" ab Seite 75).
- Sollte eine Anpassung der Rufnummernbehandlung nötig sein (siehe ab Seite 64), so nehmen Sie die entsprechenden Eintragungen vor, indem Sie mit der Schaltfläche **Add CGPN** / **CDPN in** / **out map** in den Bereichen **Calling** / **Called party num. in** / **out** entsprechende Eintragungen hinzufügen.

- Sollen Rufe vom fremden Gatekeeper auch Zugriff auf die ISDN Schnittstellen Ihres Gateways haben, legen Sie die Parameter der Sprachübertragung (siehe Kapitel 6.1.6 "Die Sprachübertragung" ab Seite 78) fest.

6.5 Routing über das ENUM-Protokoll

Eine weitere Alternative für das Routing von Gesprächen ist das ENUM-Protokoll. ENUM steht für ein Protokoll, dass sich mit der Abbildung von so genannten E.164-Nummern auf Uniform Resource Identifier (URI) befasst. So ist es möglich, mit Hilfe des ENUM-Protokolls zu prüfen, ob eine zu wählende Rufnummer über eine kostengünstige Internetverbindung hergestellt werden kann oder eher doch über eine ISDN-Leitung gewählt werden muss. Für weitere Informationen zum Thema ENUM und wie ENUM auf Ihrem innovaphone Gateway konfiguriert werden kann siehe ab Kapitel 4.2.9 "Das ENUM-Protokoll" ab Seite 41.

7 Konfiguration der Rufbehandlung

Die Rufbehandlung ist das Herzstück des Gateways. Sie legt fest, welche Rufe von dem Gateway akzeptiert werden und wohin sie vermittelt werden.

7.1 Generelle Überlegungen zur Konfiguration der Rufbehandlung

Die Rufbehandlung erfolgt durch den Gatekeeper Ihres Gateways. Sie wird durch so genannte **Routen** kontrolliert.

Tipp

Es handelt sich hierbei um Sprachrouten, nicht zu verwechseln mit den im Kapitel "Konfiguration der IP Routen" ab Seite 33 beschriebenen Daten- bzw. IP-Routen.

Jede Route definiert dabei einen zulässigen Weg eines Rufes von einer Schnittstelle, an der der Ruf eingeht, zu einer Schnittstelle, an der der Ruf wieder hinausgeht. Bei der Schnittstelle kann es sich entweder um eine ISDN Schnittstelle (deren Konfiguration im Kapitel 5 "Konfiguration der ISDN-Schnittstellen" ab Seite 47 beschrieben wird) oder um eine VoIP Schnittstelle (siehe Kapitel 6 "Konfiguration der VoIP Schnittstellen" ab Seite 69) handeln.

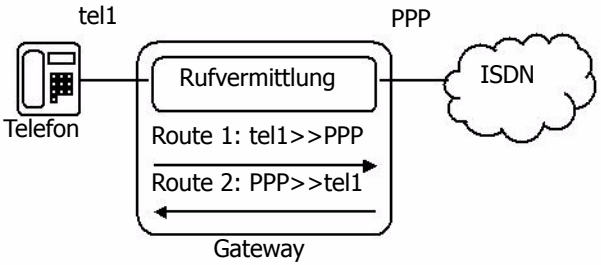

Abbildung 22 Unidirektionale Routen

Eine Route legt immer nur eine Rufrichtung fest. Sollen also Rufe zwischen zwei Schnittstellen in beide Richtungen möglich sein, so sind zwei Routen erforderlich. Eine für jede Richtung.

Routen legen die Rufbehandlung innerhalb eines einzelnen Gateways fest. Soll ein

Ruf über zwei Gateways hinweg vermittelt werden, so ist in jedem Gateway eine eigene Route erforderlich. Sollen die Rufe in beide Richtungen möglich sein, so sind insgesamt vier Routen erforderlich.

Abbildung 23 auf Seite 90 zeigt ein Szenario, in dem Rufe zwischen einem an Gateway A angeschlossenen Telefon und dem an Gateway B angeschlossene ISDN Netz über VoIP vermittelt werden.

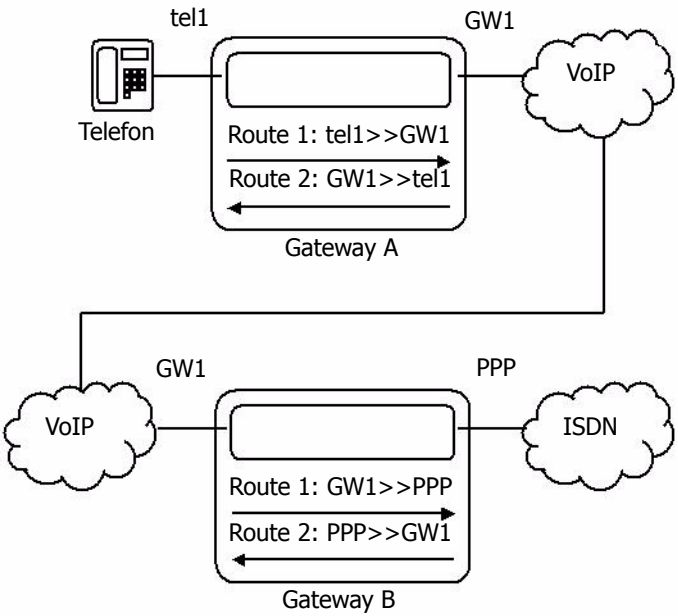

Abbildung 23 Routen über 2 Gateways

Für die Rufvermittlung spielt die Art der Rufe keine Rolle. Prinzipiell kann jeder Ruf an eine beliebige Schnittstelle vermittelt werden. So wird beispielsweise

- für ein Gespräch von Ihrem Telefonapparat über das Festnetz Ihres Netzanbieters ein Ruf von der ISDN-Schnittstelle des Gateways, an der Ihr ISDN-Telefon angeschlossen ist, auf die ISDN-Schnittstelle vermittelt, an der die entsprechende Amtsleitung angeschlossen ist bzw.
- für ein Gespräch von einem entfernten Gateway zu Ihrem ISDN-Telefon wird ein auf einer VoIP-Schnittstelle des Gateways eingehender Ruf auf die

ISDN-Schnittstelle verbunden, an der Ihr ISDN-Telefon angeschlossen ist.

Oftmals werden Rufe von verschiedenen Schnittstellen gleichartig behandelt. In dem in Abbildung 22 auf Seite 89 gezeigten Szenario kann es zum Beispiel erwünscht sein, Rufe sowohl von TEL1, als auch von TEL2 zuzulassen. Daher können für eine Route mehrere Schnittstellen als zulässige Quellen angegeben werden.

Natürlich hängt die Rufvermittlung oft auch von den gewählten Rufnummern ab. Daher ist es notwendig, die Gültigkeit von Routen für Rufe mit bestimmten Zielrufnummern festzulegen. Dazu wird an die Route für jeden gültigen Rufnummernanfang ein so genannter **Map** Eintrag gehängt. Jeder Map Eintrag legt also fest, dass Rufe von den in der Route angegebenen Quellschnittstellen, die mit der im Map angegebenen Ziffernkombination beginnen, auf die in der Route festgelegten Zielschnittstelle verbunden werden können. Abbildung 24 auf Seite 91 zeigt ein entsprechendes Szenario.

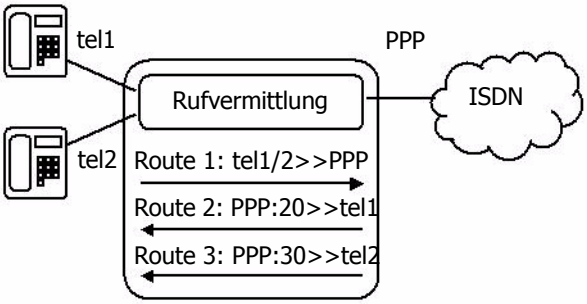

Abbildung 24 Rufnummernabhängige Routen

Manchmal ist es nützlich, die gerufene Nummer im Zuge der Rufvermittlung zu modifizieren. Abbildung 25 auf Seite 92 zeigt die Konfiguration eines solchen Szenarios im Konfigurationsapplet Ihres Gateways. Dort werden die einem Mehrgeräteanschluss zugeordneten MSN (`529969` und `529096`) auf die internen Durchwahlen `20` und `30` abgebildet.

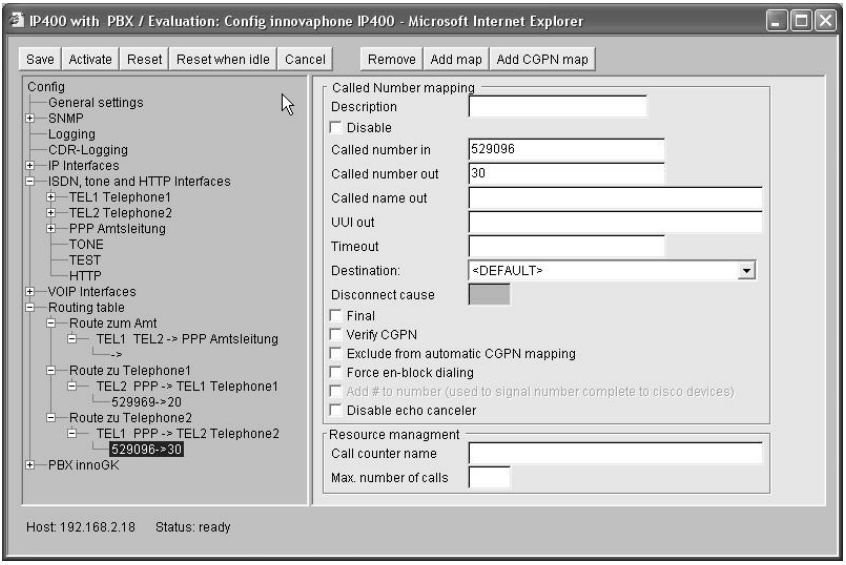

Abbildung 25 Routen mit Rufnummernersetzung

Schließlich ist es zuweilen nötig, Routen in Abhängigkeit von der rufenden Nummer festzulegen. Hierzu werden ganz ähnlich zu den **Maps**, die an die Routen angefügt werden, so genannte **CGPN Map**s an die **Maps** angehängt. Damit lassen sich sowohl die rufenden Nummern modifizieren, etwa um bei ausgehenden Rufen die Durchwahl zu unterdrücken, als auch das ganze **Map** von der rufenden Nummer abhängig zu machen.

Die Abbildung 26 auf Seite 93 zeigt die Konfiguration aus Abbildung 25 auf Seite 92 so verändert, dass der Zugang zur Amtsleitung nur für das Telefon mit der Nummer `20` besteht und bei ausgehenden Rufen abweichend von der eingehenden Abbildung die Rufnummer `529096` gesendet wird.

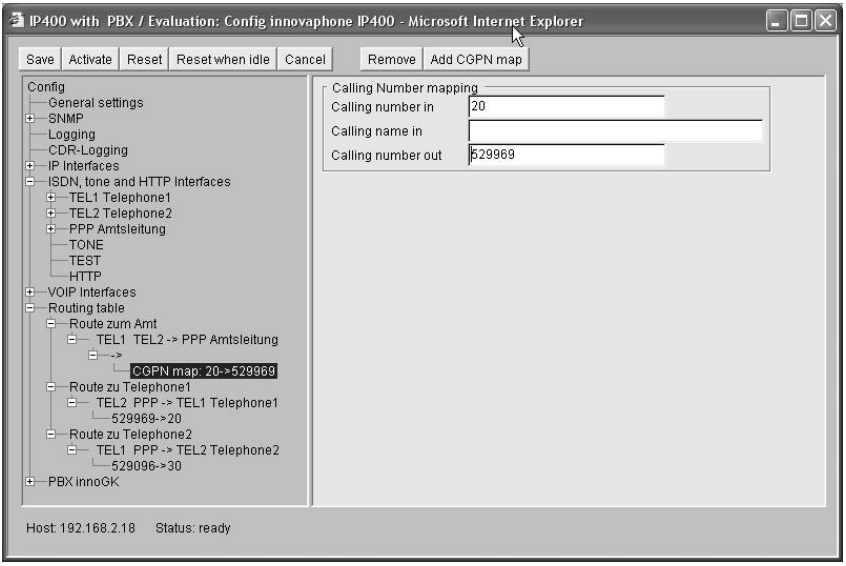

Abbildung 26 Abhängigkeit von der rufenden Nummer

Die Rufvermittlung wird von der **Routingtabelle** des Gateways (im Bereich **Routing table**) gesteuert.

Für jeden einzelnen Ruf wird die Routingtabelle von oben nach unten durchsucht. Wird ein **Map** gefunden,

- dessen Route die Quellschnittstelle des aktuellen Rufes als zulässige Schnittstelle in der Auflistung **Enable calls from interfaces** aufgeführt hat und
- dessen im Feld **Called number in** angegebener Rufnummernanfang mit der gerufenen Nummer des aktuellen Rufs übereinstimmt und

  dessen Kontrollkästchen **Verify CGPN** nicht gesetzt ist
  oder
  dessen Kontrollkästchen **Verify CGPN** gesetzt ist und die rufende Nummer des aktuellen Rufes mit dem **Calling number in** Eintrag eines der an das **Map** angefügten **CGPN maps** übereinstimmt,

dann wird der aktuelle Ruf auf die im Feld **Default call destination** der Route des **Maps** oder auf die im Feld **Destination** des **Maps** angegebene Schnittstelle vermittelt.

Dabei wird die gerufene Nummer so modifiziert, dass der im Feld **Called number**

in enthaltene Rufnummernanfang durch die im Feld **Called number out** enthaltene Ziffernfolge ersetzt wird. Entsprechend wird die rufende Nummer anhand der Felder **Calling number in** und **Calling number out** modifiziert, wenn am verwendeten Map Eintrag ein CGPN Map Eintrag besteht, dessen **Calling number in** Feld dem Beginn der rufenden Nummer des aktuellen Rufs entspricht.

Ist eine Vermittlung auf die ermittelte Schnittstelle jedoch nicht möglich, so wird der nächste **Map**-Eintrag in der Routingtabelle gesucht, der den oben angeführten Bedingungen genügt.

Tipp

Wird in der Routingtabelle kein passender **Map**-Eintrag gefunden, so ist der Ruf unzulässig und es findet keine Vermittlung statt. Auf diese Weise können Sie beispielsweise verhindern, dass von bestimmten Quellen eine Amtsholung erfolgt und damit Kosten verursacht werden.

7.2 Konfiguration der Routen

Die Konfiguration der Routingtabelle erfolgt im Bereich **Routing table** des Konfigurationsapplets.

Die Definition einer neuen Route geschieht in folgenden Schritten:

- Betätigen Sie die Schaltfläche **Add route**, um einen weiteren Eintrag in der Routingtabelle hinzuzufügen. Achten Sie dabei auf die Reihenfolge der Routen. Die neue Route wird immer hinter den aktuellen Eintrag eingefügt.
- Tragen Sie im Feld **Description** einen Namen für die Route ein. Dies erleichtert Ihnen später die Übersicht erheblich.
- Selektieren Sie den Eintrag unterhalb der neuen Route (den mit dem "**->**").
- Wählen Sie in der Auswahlliste **Default call destination** das Ziel, mit dem die Rufe verbunden werden sollen.
- Markieren Sie im Bereich **Enable calls from interface** die Kontrollkästchen der Gateways und ISDN-Schnittstellen, die als Quelle dieser Route gültig sein soll. Es werden Ihnen nur die Schnittstellen angeboten, die auch konfiguriert sind.
- Betätigen Sie die Schaltfläche **Add map.**
- Tragen Sie im Feld **Called number in** den Anfang der Rufnummern ein, für die die Route gelten soll.

- Tragen Sie im Feld **Called number out** die Ersetzung für den Anfang der Rufnummer ein, den Sie im Feld **Called number in** angegeben haben. Soll die Rufnummer unverändert übernommen werden, übernehmen Sie einfach den Nummernanfang in dieses Feld.
- Soll eine Route für eine bestimmte Nummer gelten und sollen alle Wahlziffern, die anschließend noch gewählt werden, ignoriert werden, so lassen Sie der Nummer ein "`!`" folgen.
- Sollen herstellerspezifische Daten im Signalisierungskanal übertragen werden, z. B. die URL für eine Ansage, so kann diese URL (z.B. "http://www. ...") im Feld **UUI out** eingetragen werden.
- Durch Setzen der Option **Add # to number** kann eine # als Kennzeichnung des Endes einer Rufnummer gesendet werden. Dies wird für Geräte benötigt, die das Ende der Nummer nicht ordnungsgemäß erkennen, wie z.B. bei Cisco-Geräten.

Wollen Sie mehrere Routen für einen Satz Quellen angeben, können Sie die Schaltfläche **Add map** mehrfach betätigen.

Abbildung 27 auf Seite 95 zeigt dazu ein Beispiel. Dort werden zwei MSN (`529096` und `529294`) auf eine ISDN Schnittstelle verbunden und dort auf die in den Telefonen eingestellten MSN (`30` und `31`) abgebildet. Beide Rufnummern mit Ersetzungen sind als **Map** zu einer Route konfiguriert.

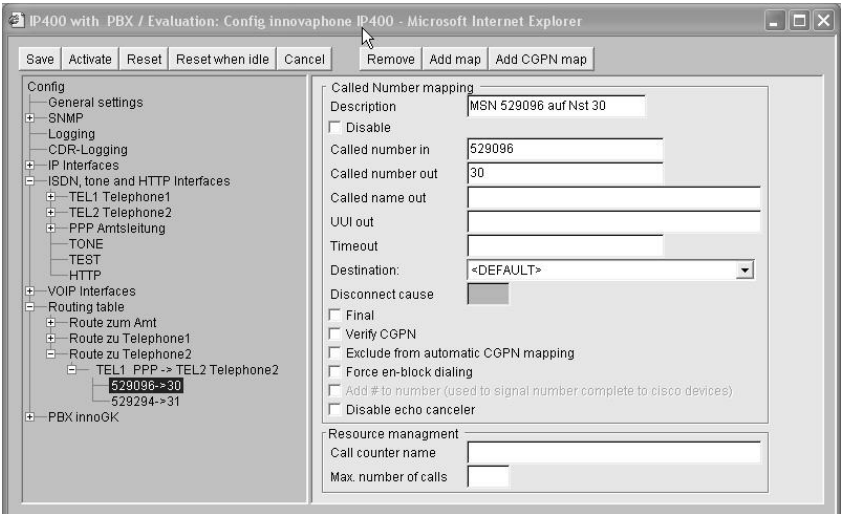

Abbildung 27 Routen mit mehrfachen Maps

- Soll für einen **Map** Eintrag der Route ausnahmsweise ein anderes Ziel konfiguriert werden, als im Feld **Default call destination** der Route angegeben, wählen Sie dies im Feld **Destination** des **Maps** aus.
- Lassen Sie alle weiteren Felder im Normalfall leer.
- Zur Konfiguration weiterer Routen markieren Sie die Route, hinter der die neue Route eingefügt werden soll und betätigen Sie die Schaltfläche **Add route.**

7.2.1 Beeinflussung der rufenden Nummer (CLI)

Bei der Vermittlung von Rufen kann es notwendig sein, die rufende Nummer zu beeinflussen, um beispielsweise den korrekten Rückruf zu gewährleisten.

Abbildung 28 auf Seite 96 zeigt die Konfiguration einer `0` als Amtsholung für eine Amtsleitung.

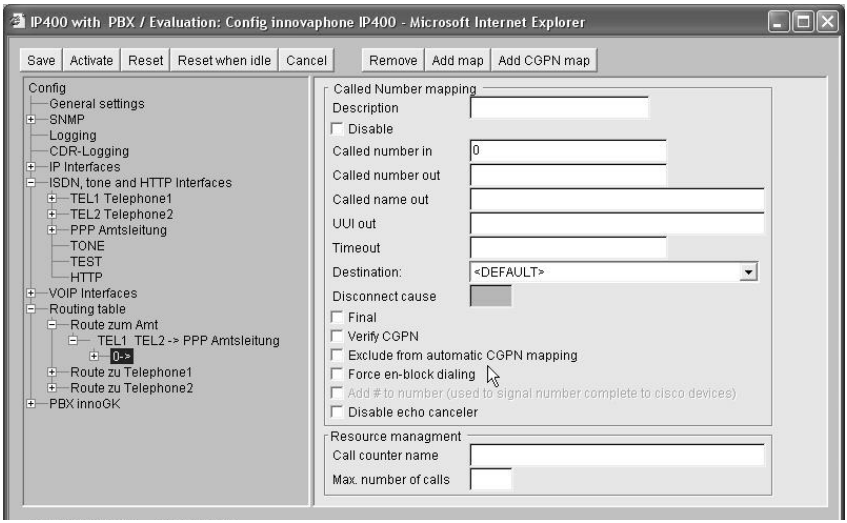

Abbildung 28 Konfiguration einer Amtsholung

Um hier zu erreichen, dass bei allen über die Amtsleitung eingehenden Rufen in der rufenden Nummer die Amtsholung `0` vorangestellt wird, müssen zu der entsprechenden Schnittstelle **CGPN** (**calling party number**) Mappings erstellt werden.

Die grundsätzliche Vorgehensweise hierzu ist im Abschnitt Kapitel 5.2.7 "Behand-

lung der verschiedenen ISDN Adresstypen" ab Seite 64 beschrieben.

Die Abbildung 29 auf Seite 97 zeigt, wie an der PPP Schnittstelle eine zusätzliche `0` als Amtsholungskennziffer eingefügt werden kann.

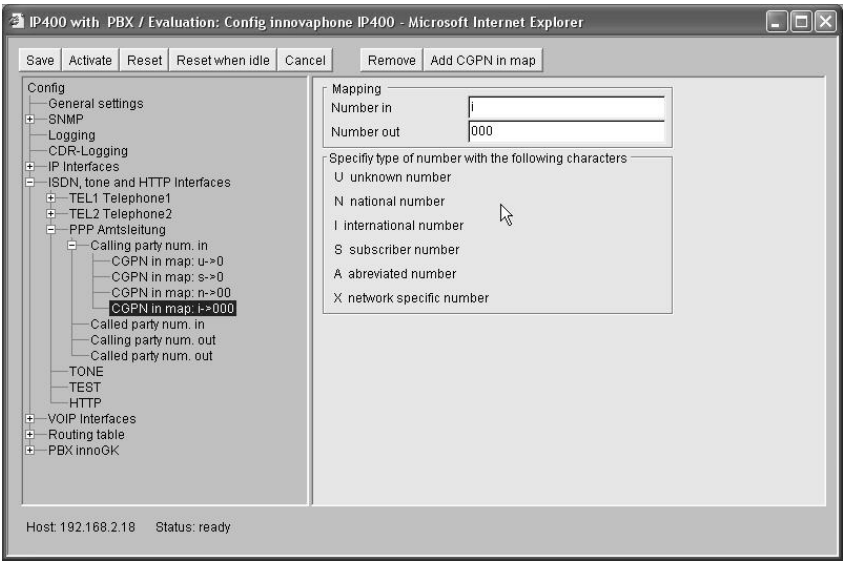

Abbildung 29 Manuelles Einfügen einer Amtsholung

7.2.2 Automatische Korrektur aller rufenden Nummern

Die oben beschriebene manuelle Korrektur kann bei komplexeren Routingtabellen sehr mühsam und fehlerträchtig sein. Daher besteht die Möglichkeit, alle rufenden Nummern automatisch richtig einstellen zu lassen. Dazu muss lediglich das Kontrollkästchen **Automatic CGPN mapping** im Bereich **Routing table** markiert werden.

Die entsprechenden Modifikationen der rufenden Nummern wird durch Analyse der Routingtabelle gesteuert. Es wird dabei quasi eine Route gesucht, die den Rückruf zum aktuellen Ruf ermöglichen würde. Die Nummernersetzungen dieser Route werden dann quasi verkehrt herum angewendet. Diese automatische Korrektur der rufenden Nummern wird nach gegebenenfalls eingestellten CGPN Mappings für ISDN-Schnittstellen oder Gateways durchgeführt.

Möchten Sie, dass bestimmte Routen bei diesem Vorgang nicht betrachtet wer-

den, so können Sie in der entsprechenden Route das Kontrollkästchen **Exclude from automatic CGPN mapping** markieren.

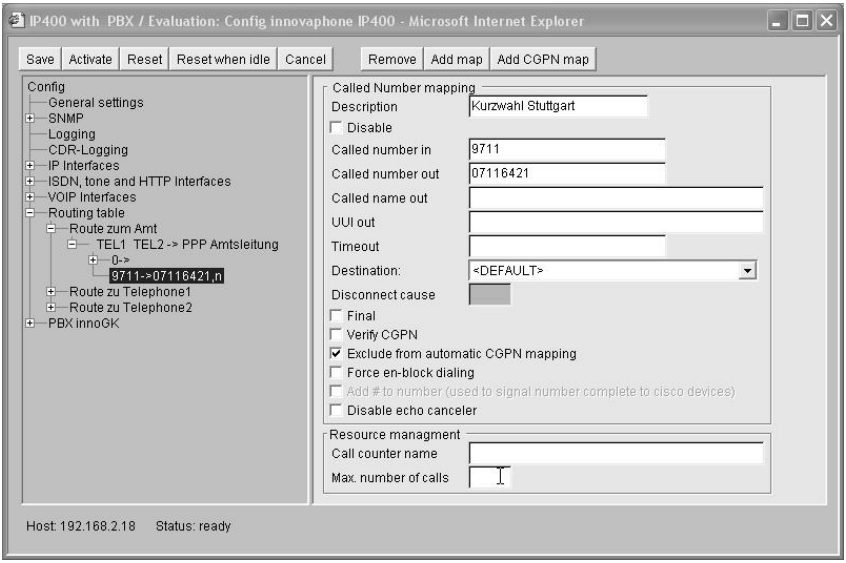

Abbildung 30 Ausschluss vom **automatic CGPN mapping**

Abbildung 30 auf Seite 98 zeigt zwei Kurzwahlrouten, die nicht zur Modifizierung der rufenden Nummer herangezogen werden sollen. Anderenfalls würden Rufe von der Berliner Filiale beginnend mit `930` an Stelle `0030926` angezeigt werden, was für die Benutzer verwirrend sein kann.

7.2.3 Selektive Routen in Abhängigkeit der rufenden Nummer

In bestimmtem Fällen kann es nützlich sein, einzelne Routen auf bestimmte rufende Nummern zu beschränken. Auf diese Art und Weise kann zum Beispiel der Zugang zu einer gebührenpflichtigen Amtsleitung auf bestimmte Nebenstellen beschränkt werden (**selektive Amtsberechtigung**).

Gehen Sie dazu wie folgt vor:

- Markieren Sie den Eintrag in der Routingtabelle, den Sie beschränken wollen.
- Markieren Sie **Verify CGPN.**
- Betätigen Sie die Schaltfläche **Add cgpn map** und fügen Sie einen oder mehrere Einträge hinzu.

- Tragen Sie unter **Calling number in** den Anfang der rufenden Nummern ein, die Sie für diese Route erlauben wollen. Es ist in diesem Falle nicht sinnvoll, nichts anzugeben.
- Tragen Sie unter **Calling number out** die Ziffernfolge ein, durch den der oben angegebene Anfang ersetzt werden soll. Es ist hier in der Regel sinnvoll, keine Ersetzung durchzuführen. Es wird dann die gleiche Ziffernfolge wie unter **Calling number in** angegeben.
- Lassen Sie die weiteren Felder leer.

Haben Sie die automatische Korrektur aller rufenden Nummern eingestellt (siehe Kapitel 7.2.2 "Automatische Korrektur aller rufenden Nummern" ab Seite 97), wirkt die Prüfung auf die bereits korrigierten Nummern.

Die Abbildung 26 auf Seite 93 zeigt eine solche Konfiguration.

Falls Sie die **CGPN Mappings** wieder löschen, achten Sie unbedingt darauf, das Kontrollkästchen **Verify CGPN** zu deaktivieren, da sonst keinerlei rufende Nummer mehr zugelassen und das **Map** somit wirkungslos wäre.

7.2.4 Änderung der rufenden Nummer für spezielle Routen

In einigen Fällen kann es nützlich sein, die rufenden Nummern für anhand bestimmter **Maps** vermittelte Rufe zu modifizieren. Gehen Sie hierzu entsprechend der Beschreibung unter Kapitel 7.2.1 "Beeinflussung der rufenden Nummer (CLI)" ab Seite 96 vor.

Achten Sie in diesem Fall darauf, dass das Kontrollkästchen **Verify CGPN** nicht aktiviert ist. Beachten Sie auch, dass die Rufnummern während der Ausführung einer Route immer unabhängig vom Adresstyp (siehe Kapitel 5.2.7 "Behandlung der verschiedenen ISDN Adresstypen" ab Seite 64) interpretiert werden, so dass hier keine Adresstypen angegeben werden können.

7.2.5 Festlegen von Rufnummernersetzungen

Häufig ist es sinnvoll Rufnummernanfänge generell und unabhängig von einzelnen Routen zu ersetzen. Beispielsweise, um Kurzwahlen zu realisieren. Dabei wird die Kurzwahl für eine Nummer durch die volle Rufnummer ersetzt und danach ein erneutes Routing für die nun vollständige Nummer durchgeführt.

Dies kann erreicht werden, indem eine Route zu dem Ziel **MAP** im Feld **Default call destination** angelegt wird. Nach der Nummernersetzung wird der Ruf nicht wie üblich verbunden, sondern mit der ersetzten Rufnummer weiter in der Routingtabelle nach einem passenden **Map** gesucht.

Beachten Sie bitte, dass zur Vermeidung von endlosen Ersetzungsvorgängen nur

Routen durchsucht werden, die sich textlich nach der MAP Route befinden. MAP Routen müssen daher immer vor den Routen aufgeführt werden, die die Behandlung der ersetzten Nummer festlegt.

7.2.6 Konfiguration mehrerer Routen für einen Nummernanfang

Sie können für verschiedene Rufquellen verschiedene Routen für ein und denselben Rufnummernanfang bestimmen, so dass der Vermittlungsvorgang von der Rufquelle abhängig ist, nicht nur von der gerufenen Nummer.

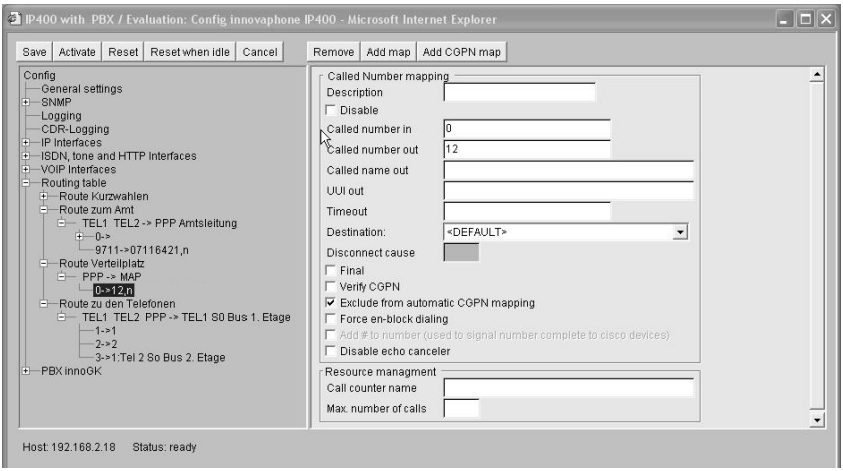

Abbildung 31 Unterschiedliche Rufbehandlung je nach rufender Schnittstelle

Abbildung 31 auf Seite 100 zeigt ein Beispiel für eine solche Konfiguration. Hier wird die Rufnummer `0` bei Rufen von der Amtsleitung auf die Nummer `12` verbunden (Verteilplatz), bei allen anderen Rufen jedoch auf die Amtsleitung.

7.2.7 Anrufweiterschaltungen

Es kann sinnvoll sein, mehrere Routen für Rufe mit ein und denselben Rufnummernanfang von der gleichen Rufquelle zu definieren.

Der Vermittlungsvorgang des Gateways verwendet immer die erste passende Route. Wird jedoch unter Verwendung dieser Route keine Verbindung hergestellt, so kann die Vermittlung mit einer weiteren Route versucht werden. Auf diese Weise lassen sich verschiedene Anrufweiterschaltungsarten realisieren.

- Wird anhand einer Route eine Vermittlung versucht und kann der Ruf auf Grund fehlender lokaler Ressourcen (etwa keine freie Amtsleitung, siehe Tabelle 14 auf Seite 102) nicht aufgebaut werden, so wird sofort eine weitere Route gesucht. Hiermit kann beispielsweise erreicht werden, dass die Rufe bei mehreren an ein Gateway angeschlossenen Amtsleitungen nacheinander auf diese Amtsleitungen verteilt werden (Abbildung 32 auf Seite 101 zeigt so eine Konfiguration).
- Wird anhand einer Route eine Vermittlung versucht und der Ruf konnte dem gerufenen Endgerät signalisiert werden (das Endgerät meldet ein **Alerting**) und ist für diese Route im Feld **Timeout** ein Wert größer 0 eingetragen, so wird nach Ablauf einer entsprechenden Anzahl von Sekunden eine weitere Route gesucht, falls der Ruf in der Zwischenzeit nicht angenommen wurde. Dies entspricht der Funktion "Anrufweiterschaltung bei fehlender Antwort (**CFNR**)". Tragen Sie eine **Timeout** von mehr als 120 Sekunden ein, so kann der Timeout nicht eintreten, da der globale Timeout für den Rufaufbau vorher ablaufen wird. Da aber bei eingetragenem Timeout nach einem gescheiterten Ruf vorhandene Alternativrouten immer ausgeführt werden, wirkt dies wie die Funktion "Anrufweiterschaltung bei belegt" (**CFB**).

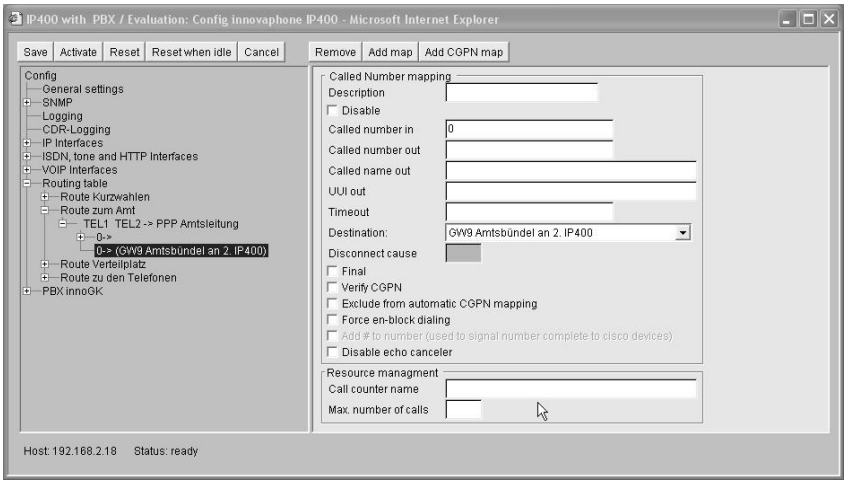

Abbildung 32 Konfiguration eines Amtsleitungsbündels

Möchten Sie nach der versuchten Vermittlung über einen Map Eintrag verhindern, dass weitere Routen versucht werden, können Sie das Kontrollkästchen **Final** im **Map** Eintrag markieren.

Ebenso können Sie für eine Route mit dem Ziel `MAP` das Kontrollkästchen **Final** in den **Map** Einträgen markieren. In diesem Fall werden keine weiteren `MAP` Einträge mehr ausgewertet, wohl aber noch passende andere Routen gesucht.

Fehlercode (dezimal)	Beschreibung
34	No circuit/channel available
38	Network out of order
41	Temporary failure
42	Switching equipment congestion
44	Requested circuit/channel not available
47	Resources unavailable, unspecified
49	Quality of service unavailable

Tabelle 14 "lokale Probleme" im Sinne der Anrufweiterschaltung

7.2.8 Rufsequenzen

Eine Besonderheit stellen Routen mit dem Rufziel `TRY` dar. Wird eine solche Route zur Vermittlung herangezogen, so wird die Rufnummernersetzung durchgeführt und anschließend werden mit dem Ergebnis normale Routen gesucht. Kann der Ruf auf diese Weise nicht erfolgreich vermittelt werden, wird anschließend eine weitere `TRY` Route gesucht.

Wird bei der `TRY` Route ein Timeout angegeben, so wirkt dieser auf die Routen, die zur Vermittlung versucht werden.

Ist im **Map** Eintrag das Kontrollkästchen **Final** markiert, werden gegebenenfalls keine weiteren `TRY` Routen mehr gesucht.

Abbildung 33 auf Seite 103 zeigt die Konfiguration eines Verteilplatzes, der von der Amtsleitung über die Durchwahl `0` erreichbar ist und intern nacheinander auf den Nebenstellen `12`, `13` und `22` versucht wird.

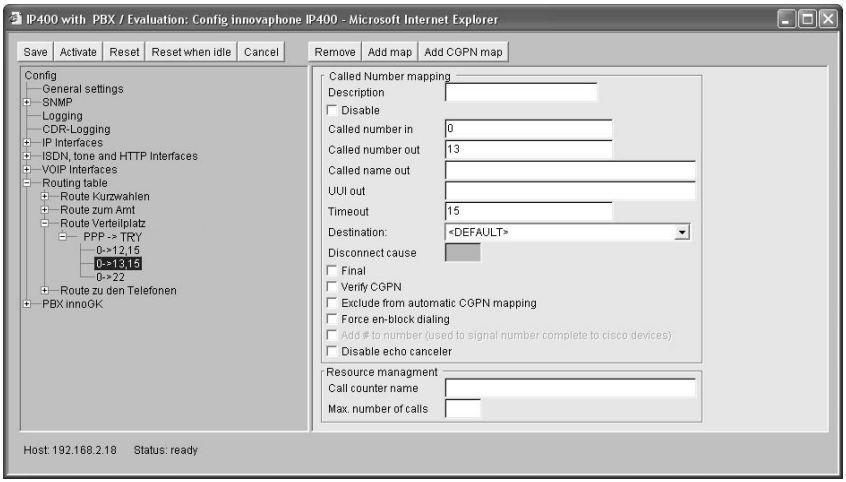

Abbildung 33 Rufsequenzen mit `TRY` Routen

7.2.9 Ablehnen von Rufen

Ihr Gateway wird bei jeder Behandlung eines Rufes versuchen, Routen mit passenden **Maps** zu finden und den Ruf entsprechend zu vermitteln. Wird in der Routingtabelle kein passender **Map** Eintrag gefunden oder scheitern alle Rufversuche, so wird der Ruf endgültig abgelehnt.

Manchmal ist es jedoch nützlich, bestimmte Rufe explizit durch einen Eintrag in der Routingtabelle abzulehnen. Dies ist möglich, indem eine Route mit dem Rufziel **DISC** eingerichtet wird. In Feld **Disconnect cause** kann dann der gewünschte Ablehnungsgrund angegeben werden.

Die Abbildung 34 auf Seite 104 zeigt eine Konfiguration, in der die Amtsholung so konfiguriert ist, dass bestimmte Rufnummern nicht angerufen werden können.

Eine Auflistung der definierten Ablehnungsgründe finden Sie in Tabelle 23 ab Seite 154. Es muss der in der Spalte "Fehlerwert (dezimal)" angegebene Wert verwendet werden.

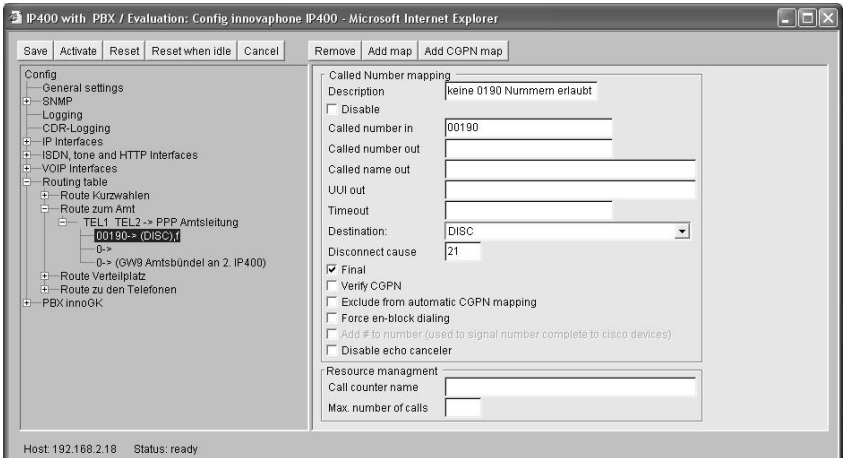

Abbildung 34 Ablehnen von Rufen

7.2.10 Erzwingen von Blockwahl

Ihr Gateway unterstützt die kontinuierliche Nachwahl von Einzelziffern, so dass es nicht erforderlich ist, die Rufnummer explizit mit einem besonderen Wahlzeichen abzuschließen. Dieses Verhalten entspricht auch dem von herkömmlichen TK-Anlagen.

Allerdings wird dieses so genannte **overlapped sending** nicht von allen H.323-kompatiblen Geräten unterstützt. Wird nun ein Ruf zu einem solchen Gateway aufgebaut, so kann dies die Nachwahlziffern nicht verarbeiten und der Ruf scheitert.

In einem solchen Fall kann dem Rufnummernanfang in einer Route eine Raute (#) angefügt werden. In diesem Fall wartet das Gateway mit dem Rufaufbau zum entfernten Gateway, bis vom Benutzer eine Raute gewählt wurde. Die Raute selbst und alle möglicherweise noch folgenden Wahlziffern werden nicht an das entfernte Gateway übertragen.

Ist die Anzahl der Ziffern, die zur Vervollständigung der Rufnummer erforderlich sind immer konstant für diese Route (z.B. immer 3-stellige Durchwahlen), so kann dem Rufnummernanfang auch eine entsprechende Anzahl von Punkten (.) angefügt werden. Das Gateway erwartet dann für jeden Punkt eine folgende Ziffer und führt anschließend den Ruf durch, ohne dass eine Raute gewählt werden muss. Alle möglicherweise noch folgenden Wahlziffern werden nicht an das entfernte

Gateway übertragen.

Ist die Anzahl der Ziffern, die zur Vervollständigung der Rufnummer erforderlich sind für diese Route nicht konstant und soll auch kein explizites Abschließen der Wahl durch eine Raute erfolgen, kann im entsprechenden **Map** Eintrag auch das Kontrollkästchen **Force en-bloc dialing** markiert werden. Greift ein solcher Map Eintrag, sammelt das Gateway so lange die folgenden Wahlziffern, bis seit dem letzten Tastendruck mehr als 4 Sekunden vergangen sind. Dann wird der Ruf vermittelt, weitere möglicherweise nachgewählte Ziffern gehen verloren.

7.2.11 Routen von und zu Fax Geräten

In der Version 2 der Firmware Ihres Gateways bestand die Möglichkeit, Faxverbindungen bestimmte Map Einträge zuzuordnen. Dadurch konnte die Verwendung des für die Übertragung von Gruppe 3 Faxen geeigneten Coder G.726 erzwungen werden.

Diese Funktion (**Fax** (**force G726 40Kbit/s coder**)) ist ab der Version 3 der Firmware nicht mehr verfügbar, da Faxe zuverlässig über das T.38 Protokoll übertragen werden können (siehe Kapitel 6.1.4 "H.323 Protokolloptionen" ab Seite 75).

Falls Sie eine derartige Version 2 Konfiguration auf Version 3 oder höher aktualisieren, müssen Sie lediglich in den betreffenden Gatewaydefinitionen im Bereich **VoIP Interfaces** das Kontrollkästchen **Enable T.38 fax protocol** markieren.

7.2.12 Unterdrücken der Echokompensierung

Ihr Gateway wird für alle Sprachverbindungen, die in einer lokalen ISDN Schnittstelle terminieren eine Echokompensierung (**echo cancellation**) ausführen. Für Daten- und Faxverbindungen wird die Echokompensierung automatisch nicht ausgeführt. In seltenen Fällen kann es jedoch sein, dass eine Verbindung als Sprachverbindung behandelt wird und doch keine Echokompensierung durchgeführt werden soll. Dies kann beispielsweise bei Modemverbindungen der Fall sein.

Sie können die Echokompensierung unterdrücken, indem Sie in dem entsprechenden **Map** Eintrag das Kontrollkästchen **Disable echo canceler** markieren.

7.2.13 Ressourcen-Management

Steht für eine Route z. B. wegen zu geringer Bandbreite der Datenverbindung nur eine begrenzte Ressource zur Verfügung, so kann mittels des Ressourcen-Managements eine Beschränkung der maximal zulässigen Rufe für eine Route eingerichtet werden.

Die Konfiguration des Ressourcen-Managements erfolgt über das Konfigurationsapplet im Feld **Resource Management** der Map der jeweiligen Route.

Hier kann ein **Call counter name** eingetragen werden und im Feld **Max. number of calls** kann die maximale Anzahl von Rufen festgelegt werden, die für diese Route zulässig sind.

Das System überprüft die Anzahl der Rufe über diese Route und lehnt Rufe, die über die eingetragene Anzahl von Rufen hinausgehen ab. Ist danach eine weitere Route zum Ziel konfiguriert, wird diese Route genutzt.

Im Bereich **Call counts** in der Bedienoberfläche des Gateways kann die Anzahl der aktuellen Rufe für den jeweiligen Namen des Rufnummernzählers angezeigt werden (siehe Kapitel 9.2.4 "Untermenü Call Counter" ab Seite 129).

7.3 Die Rufbehandlung in Abhängigkeit der Geräteverwaltung

Im Prinzip werden Rufe von und zu verschieden konfigurierten VoIP Geräten von Ihrem Gateway gleichartig behandelt. Es bestehen jedoch einige Unterschiede im Detail, die in den folgenden Abschnitten erläutert werden.

7.3.1 Rufe von und zu Gatewaygruppen

Im Abschnitt Kapitel 6.3 "Statische Verwaltung von VoIP Geräten" ab Seite 86 wurde erläutert wie dem Gateway Gruppen von VoIP Geräten bekannt gemacht werden.

Routen zu solchen Gruppen werden im Prinzip wie normale Routen konfiguriert. Der für die Route definierte Rufnummernanfang wird dann als passend zu einer gerufenen Nummer betrachtet, wenn die Nummer mit dem Rufnummernanfang vollständig übereinstimmt ***und*** die zur Vervollständigung der IP-Adresse des Zielgerätes fehlenden Ziffern gewählt wurden. Überschüssige weitere Ziffern werden gegebenenfalls an das Zielgerät weitergegeben.

Größe des Hostanteils in Bits	Anzahl Ziffern	Beispiel
1 bis 8	3	Class C Adresse
9 bis 16	6	Class B Adresse
17 bis 24	9	Class A Adresse
über 24	12	Unspezifizierte Gruppe (0.0.0.0)

Tabelle 15 Benötigte Ziffern zur Adressvervollständigung

Zur Vervollständigung der IP-Adresse sind 3, 6, 9 oder 12 Ziffern erforderlich. Dies hängt von der Größe des Hostanteils entsprechend der in der **VoIP Interfaces** Definition festgelegten Subnetzmaske ab. Die einzelnen Ziffern werden jeweils in Dreiergruppen zu einem Byte der Adresse konvertiert.

Tabelle 15 auf Seite 107 zeigt die erforderliche Anzahl Ziffern. Es müssen immer ganze Bytes der Adresse in Dreiergruppen gewählt werden, auch wenn gemäß der konfigurierten Subnetzmaske an sich weniger als 8 Bit zu vervollständigen sind. Führende Nullen müssen mitgewählt werden.

Angenommen, es wird eine Gruppe von VoIP Geräten mit der Netzwerkadresse `195.226.104.128` und der Subnetzmaske `255.255.255.128` definiert. Es sind also die Adressen `195.226.104.129` bis `195.226.104.254` erreichbar. Als Rufnummernanfang für die Route zu dieser Gruppe sei `91` konfiguriert. Um nun das Gerät mit der Adresse `195.226.104.135` zu rufen, muss die Nummer `91135` gewählt werden.

Ist die "Automatische Korrektur aller rufenden Nummern" (siehe Kapitel 7.2.2 "Automatische Korrektur aller rufenden Nummern" ab Seite 97) aktiviert und geht ein Ruf von einem in einer Gruppe von VoIP Geräten definiertem Gerät ein, so werden die zur Vervollständigung der IP-Adresse des rufenden Gerätes notwendigen Ziffern zusätzlich der rufenden Nummer vorangestellt. Somit ist ein Rückruf über die mitgelieferte Nummer möglich.

7.3.2 Rufe von und zu per RAS verwalteten Geräten

Rufe können an ein per RAS Protokoll am Gatekeeper angemeldetes Gerät (siehe Kapitel 6.2 "Verwaltung von VoIP Geräten per RAS (Gatekeeper)" ab Seite 83) per Rufnummer oder per Name vermittelt werden. Dabei werden Rufe an Gateways etwas anders behandelt, als Rufe zu Endgeräten (siehe Seite 69).

Prinzipiell wird die Rufvermittlung für einen Ruf an ein per RAS Protokoll verwaltetes VoIP Gerät ganz normal behandelt (siehe Kapitel 7.1 "Generelle Überlegungen zur Konfiguration der Rufbehandlung" ab Seite 89).

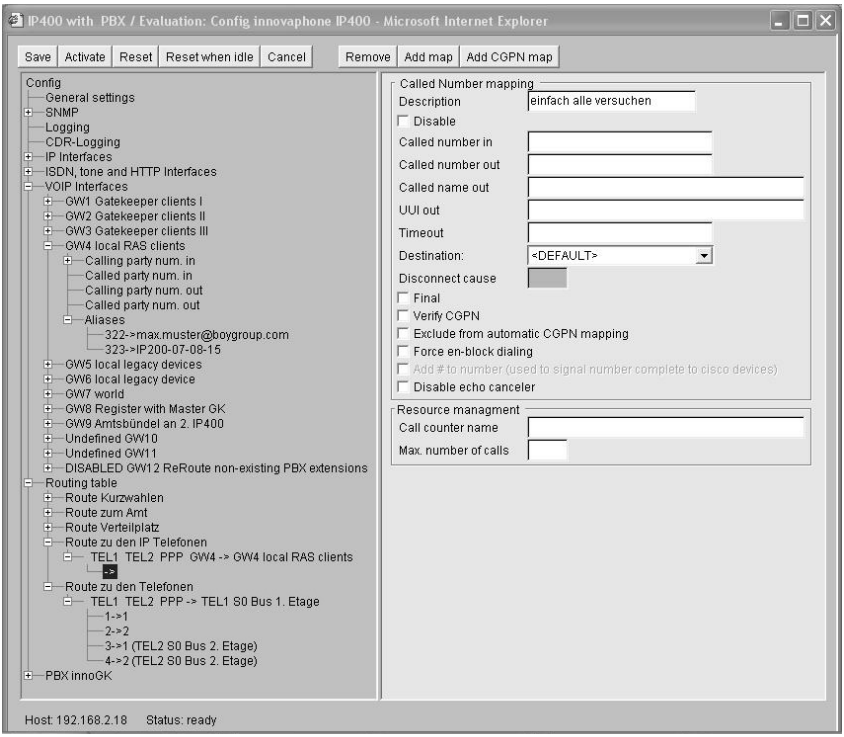

Abbildung 35 Routen zu per RAS angemeldeten Endgeräten

Wird ein für die gerufene Nummer passender **Map** Eintrag einer Route gefunden und hat dieser beziehungsweise die Route eine **VoIP Interfaces** Definition als Ziel, die als **Gatekeeper client group** konfiguriert ist, so werden in diesem Gateway alle Aliase durchsucht und ein Eintrag mit einer zur gerufenen Nummer pas-

senden **E.164 Address** gesucht. Wird ein solcher Eintrag gefunden und ist das zugehörige Gerät aktuell beim Gatekeeper registriert, wird der Ruf dorthin vermittelt, anderenfalls wird weiter nach passenden Aliasen gesucht. Gibt es keinen passenden Eintrag oder ist der Klient zum Zeitpunkt des Rufes nicht angemeldet, wird dieser Ruf scheitern und – sofern vorhanden – eine Alternativroute verwendet (siehe Kapitel 7.2.7 "Anrufweiterschaltungen" ab Seite 100).

Auf Grund dieses Vorgehens wird die gerufene Nummer eines Rufes bei der Rufvermittlung zweimal überprüft. Das erste mal, wenn eine zum Ruf passende Route gesucht wir und zum zweiten mal, wenn ein passender Alias innerhalb der **VoIP Interfaces** Definition gesucht wird. Es ist daher möglich und üblich, derartige Routen sehr einfach mittels leerer **Map** Einträge zu konfigurieren. Zwar wird dann versucht, alle Rufe zunächst an die per RAS angemeldeten Geräte zu vermitteln. Allerdings wird dies stillschweigend scheitern, wenn kein Gerät mit der richtigen Nummer angemeldet ist.

Abbildung 35 auf Seite 108 zeigt eine solche Konfiguration. Zwei IP-Telefone mit den Durchwahlen `22` und `36` sind in diesem Beispiel als per RAS angemeldete Geräte in der **VoIP Interfaces** Definition **GW2** konfiguriert. Der restliche Nummernkreis von `10` bis `49` ist auf 2 ISDN S_0 Busse verteilt.

Im Gegensatz zu VoIP Endgeräten, die mit Namen und Nummer im Gatekeeper eingetragen werden, wird für VoIP-Gateways normalerweise keine Nummer eingetragen. Dies wäre auch nicht sinnvoll, da die Gateways ja einen ganzen Nummernraum realisieren und nicht eine einzelne Nummer. Damit funktioniert aber die weiter oben beschriebene Ermittlung des Rufziels anhand der gerufenen Nummer nicht.

Sind in einer **VoIP Interfaces** Definition Gateways angemeldet und soll eine Route einen Ruf dorthin zustellen, so reicht die Angabe des Gateway-Eintrages **GWxx** zur Identifizierung des Zieles nicht. Hier ist es daher notwendig, zusätzlich auch noch den korrekten H.323 Namen im **Map** als **Called name** out anzugeben.

Abbildung 36 auf Seite 110 weiter oben zeigt eine Konfiguration, in der der Rufnummernplan von 10 bis 49 auf 2 ISDN S_0 Busse, von 50 bis 59 auf eine per VoIP Gateway angebundene Filiale und ansonsten auf IP-Telefone verweist.

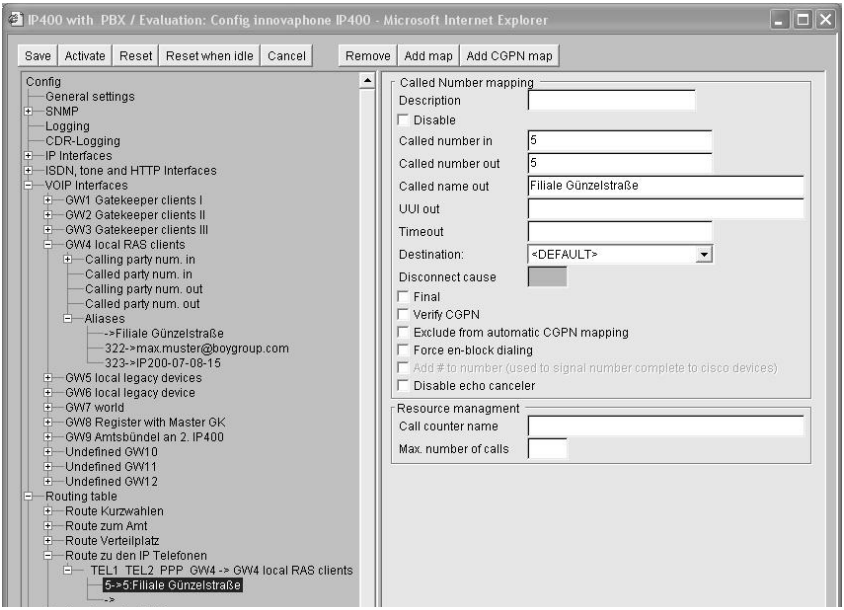

Abbildung 36 Routen zu per RAS angemeldeten Gateways

7.3.3 Rufe zu Gatekeeper Klienten per H.323 Name

Im VoIP Umfeld stellt die Wahl per Rufnummer nur eine Möglichkeit der Zieladressierung dar. Eine andere komfortable Möglichkeit besteht darin, als Rufziel einen Namen anzugeben.

Geht ein Ruf mit einem **H.323 name**, jedoch ohne E.164 Adresse (also ohne Telefonnummer) beim Gatekeeper ein, so wird zunächst die zu der ID gehörende Nummer ermittelt, indem nacheinander in allen **VoIP Interfaces** Definitionen vom Typ **Gatekeeper client group** nach einem Alias Eintrag mit einem entsprechenden **H.323 Name** gesucht wird. Die **E.164 Address** des ersten passenden Eintrags wird dann zur weiteren Rufvermittlung verwendet. Ganz so, als ob der Ruf von vornherein mit dieser Nummer als gerufener Nummer eingegangen wäre.

7.3.4 Abbilden von Rufnummern auf H.323 Namen

Sie können in der Routingtabelle Rufnummern auf H.323 Namen abbilden. Auf diese Weise können Sie dann auch mit Endgeräten, die keine H.323 Namen rufen können (z.B. ISDN Telefone) Rufe auf Namensbasis durchführen.

Tragen Sie dazu in den normalen Routen den H.323 Namen als **Called name out** ein.

Dieses Vorgehen ist nur dann sinnvoll, wenn das VoIP Endgerät nicht direkt bei Ihrem Gateway als Gatekeeper angemeldet ist, da dann ja die normalen Methoden ausreichen würden.

7.4 Konfiguration der PBX Komponente im Gateway

Durch Aufruf des Menüs **DISABLED PBX** und setzen der Option **ENABLE PBX** wandelt sich der Menüpunkt **DISABLED PBX** zu **PBX** und die Untermenüs **LDAP Server**, **LDAP Replication** und **Licenses** können konfiguriert werden.

Das LDAP-Protokoll wird beim Einsatz von redundanten Systemen benötigt, in denen Server und replizierender Client auf eine gemeinsame Benutzerdatenbank zurückgreifen.

Zur Konfiguration des Menüs **PBX** - insbesondere zur Einrichtung und Verwaltung der Lizenzen - beachten Sie bitte die Hinweise im "Administrator Handbuch - innovaphone PBX".

8 Festlegen verschiedener Betriebsparameter

8.1 Generelle Einstellungen

Im Bereich **General settings** des Konfigurationsapplets können allgemeine Parameter eingestellt werden.

8.1.1 Festlegen des Gatewaynamens

Sie können Ihrem Gateway einen sprechenden Namen vergeben und im Feld **Name** eintragen. Dieser Name erscheint im Fenstertitel der Homepage und des Konfigurationsapplets, was die Übersicht bei der Konfiguration mehrerer Geräte sehr erleichtert.

8.1.2 Festlegen des Administrationsbenutzers und -Kennworts

Im Bereich **Change login parameters** können Sie die Nutzerkennung und das zugehörige Kennwort festlegen, das die Konfiguration des Gateways absichert.

Beim Speichern oder Aktivieren der Konfiguration wird geprüft, ob das neu definierte Kennwort gültig ist. Wie jede andere Konfigurationsänderung muss jedoch auch die Kennwortänderung wie im Kapitel 3.2 "Testen und Speichern der Konfiguration" ab Seite 22 beschrieben, aktiviert und gesichert werden.

8.1.3 Festlegen der Zeit- und Datumsquelle

Ihr Gateway verfügt nicht über eine batteriegepufferte Echtzeituhr. Die interne Uhrzeit wird daher nach jedem Neustart auf den 1.1.1970, 0:00 Uhr zurückgesetzt.

Zum normalen Betrieb ist keine korrekte Uhrzeit erforderlich. Legen Sie jedoch Wert darauf – zum Beispiel um zeitlich korrekte **Call Detail Records** zu erhalten – können Sie im Bereich **Get time from SNTP Server** die IP-Adresse einer Zeit- und Datumsquelle angeben. Ihr Gateway wird dann im unter **Update interval** angegebenen Rhythmus seine interne Uhr mit der Zeitquelle synchronisieren.

Falls Sie in Ihrem eigenen Netzwerk über keinen NTP Server verfügen, können Sie einen öffentlichen Server verwenden. So bietet beispielsweise die TU Berlin unter der IP Adresse `130.149.17.21` einen Zeitdienst an. Bedenken Sie, dass dieser Service freiwillig ist und kein Anspruch auf dessen Verfügbarkeit besteht.

Tipp

Bedenken Sie, dass jeder Windows 2000 Server als SNTP Server fungieren kann. Ebenso gibt es verschiedene frei verfügbare SNTP Softwarepakete für Windows und Unix/Linux Plattformen.

Ihr Gateway arbeitet gleichzeitig auch als NTP Server. Betreiben Sie noch weitere IP 400 Gateways oder IP 200 Telefone, so können Sie eines mit einem – gegebenenfalls externen – Zeitserver synchronisieren und alle anderen wiederum mit diesem.

Tipp

IP 200 Telefone verwenden automatisch ihren Gatekeeper als SNTP Server, sofern kein anderer konfiguriert wurde.

Weitere öffentliche Zeitdienste weltweit finden Sie im Internet unter http://www.eecis.udel.edu/~mills/ntp/.

Sollten Sie in Ihrem Netzwerk weitere Geräte betreiben, die einen Zeitserver benötigen (zum Beispiel weitere Gateways oder IP-Telefone), so tragen Sie dort bitte die IP-Adresse Ihrer IP 400 ein. Ihr Gateway arbeitet dann selbst als Zeitdienst und wird dann die korrekte Zeit an die anderen Geräte melden. Vermeiden Sie es, alle Geräte mit einem externen Zeitdienst zu synchronisieren, da dies zu unnötig hoher Last auf diesen Servern führt.

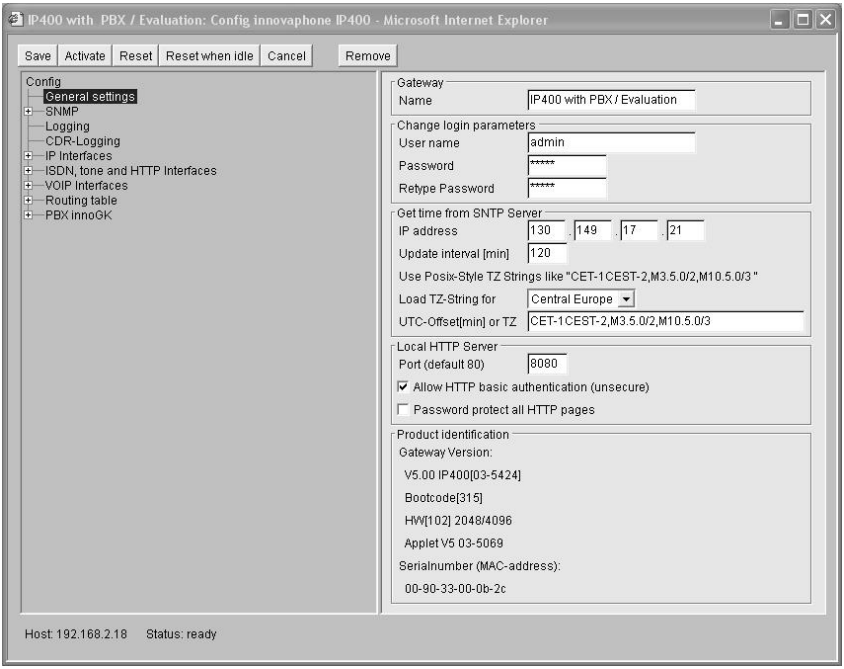

Abbildung 37 Die "General settings"

Zeitdienste liefern immer die koordinierte Weltzeit (**U**niversal **T**ime **C**oordinated [UTC], dies entspricht der **G**reenwich **M**ean **T**ime [GMT]), nicht jedoch die korrekte Zeitzone und auch nicht die Sommerzeit. Sie können daher die Distanz Ihrer Zeitzone zur Weltzeit im **Feld UTC Offset**[**min**] **or TZ** angeben. In der Zeitzone `GMT+1` (das ist die mitteleuropäische Zeitzone) beträgt diese Distanz 60 Minuten. In der Sommerzeit kommen noch weiter 60 Minuten hinzu, so dass der Abstand insgesamt 120 Minuten beträgt. In diesem Fall müssen Sie jedoch bei Umstellung von Winter- auf Sommerzeit und umgekehrt die Distanz manuell entsprechend anpassen.

Diese Anpassung kann das Gerät automatisch vornehmen, wenn sie den so genannten **TZ-String** (**T**ime **Z**one) im Feld **UTC Offset**[**min**] **or TZ** angeben. In diesem Wert wird der Name der Zeitzone, der Name der Sommerzeitzone, ihre jeweiligen Distanzen zu **UTC** und die Umschaltzeitpunkte kodiert.

Da die Werte etwas kompliziert sind, bietet Ihnen das Konfigurationsapplet eine

Editierhilfe für die korrekten Eintragungen für Mitteleuropa und Großbritannien zur Auswahl an:

- Wählen Sie im Feld **Load TZ-String for** den Wert `Central Europe` aus, so wird der **TZ-String** für die mitteleuropäische Zeitzone ins Feld **UTC Offset[min] or TZ** eingetragen.
- Wählen Sie im Feld Load TZ-String for den Wert UK aus, so wird der **TZ-String** für die britische Zeitzone ins Feld **UTC Offset**[**min**] **or TZ** eingetragen.
- Wählen Sie im Feld **Load TZ-String for** den Wert UK aus, so wird der **TZ-String** gelöscht und Sie können einen beliebigen Wert eintragen. Es gibt verschiedene Formate, die durch den IEEE POSIX Standard definiert wird.

Der Zugriff der innovaphone Geräte auf die POSIX Time Zone kann auch über DHCP erfolgen. Für weitere Informationen zum DHCP-Client und POSIX TZ siehe Anhang D: "Der innovaphone DHCP Client" ab Seite 155.

Tipp

Weitere Informationen zu diesem Standard finden Sie unter der Web Adresse http://standards.ieee.org/catalog/olis/posix.html.

Für die meisten praktischen Zwecke reicht jedoch die folgende Beschreibung aus (diese Beschreibung basiert auf einer Übersetzung aus der FAQ Liste des Linux Samba Paketes):
Posix TZ Strings haben folgende Form (optionale Teile in eckigen Klammern):

StdOffset[Dst[Offset],Date/Time,Date/Time]

- ***Std*** ist der Bezeichner der Zeitzone (z.B. `CET` für **central european time** oder `MEZ` für **mitteleuropäische Zeit**).
- ***Offset*** gibt die Distanz der Zeitzone zur **UTC** an, z.B. `-1` für die mitteleuropäische Zeit. Die Distanz ist negativ, wenn die Zeitzone der UTC voraus ist, also beispielsweise `-1` für die mitteleuropäische Zeit. Falls die Distanz nicht ganze Sunden umfasst, kann die Anzahl von Minuten angehängt werden, beispielsweise `-1:30`.

  Wenn Sie keine Sommerzeit verwenden, ist der TZ-String an dieser Stelle zu Ende.

- ***Dst*** ist der Bezeichner der Sommerzeitzone (z.B. `CEST` für **central european summer time** oder `MES` für **mitteleuropäische Sommerzeit**).
- Der optionale zweite ***Offset*** gibt die Distanz der Sommerzeit zu UTC an. Wird sie nicht angegeben, wird eine Stunde vor der Normalzeit angenommen.
- ***Date*/*Time*,*Date*/*Time*** legen Start und Ende der Sommerzeit fest. Das Format für einen Zeitpunkt ist `M`***m*.*n*.*d***, was den ***d***-ten Tag der ***n***-ten Woche im ***m***-ten Monat bezeichnet. Der Tag `0` ist der Sonntag. Wird die fünfte Woche angegeben, ist immer der letzte Tag (gemäß ***d***) im Monat gemeint. Das Format für den Zeitpunkt ist ***hh***[`:`***mm***[`:`***ss***]], im 24-Stunden Format.

Die in Deutschland gültige mitteleuropäische Zeitzone ist wie folgt angegeben:

```
CET-1CEST-2,M3.5.0/2,M10.5.0/3
```

Abbildung 37 auf Seite 114 zeigt die Konfiguration eines SNTP Servers, der alle 2 Stunden abgefragt wird. Das Gateway interpretiert die Zeit in der mitteleuropäischen Zeitzone.

8.1.4 Festlegen des Ports für den lokalen HTTP Server

Die Administration Ihres Gateways über das Netzwerk erfolgt über den TCP Port `80` (`http`). Falls aus irgendwelchen Gründen der Port 80 nicht verwendet werden soll, können Sie einen anderen Port im Feld **Local HTTP Server Port** der Grundeinstellungsseite **General settings** einstellen. Sie können dann über diesen Port zugreifen.

Für die Webadministration über den Browser müssen Sie den Link beispielsweise für einen Port `8080` wie folgt angeben: `http://192.168.0.3:8080`. Beachten Sie, dass alle Applikationen wie der Vermittlungsplatz **innovaphone PBX Operator** und die **TAPI** auf den Port des HTTP Servers eingestellt werden müssen.

8.2 Überwachung des Gateways per SNMP

Das Gateway bietet die Möglichkeit der Überwachung des Betriebszustandes per SNMP. Unterstützt wird die Standard MIB-II sowie eine herstellerspezifische MIB. Für Details über diese MIB wenden Sie sich an Ihren Händler oder laden Sie die MIB-Datei vom Download-Bereich des innovaphone Web (http://www.innovaphone.com).

Um per SNMP auf das Gateway zugreifen zu können, gehen Sie wie folgt vor:

- Öffnen Sie den Bereich **SNMP** des Konfigurationsapplets.
- Stellen Sie sicher, dass der Parameter **Access** entweder auf `read-only` oder auf `read-write` eingestellt ist. Ist `read-write` eingestellt, können bestimmte MIB-Variablen auch geschrieben werden.
- Falls Sie nicht den Standard **Community-Namen** `public` verwenden, tragen Sie den Namen im Feld **Community** ein.
- Die Einträge **Name**, **Contact** und **Location** sind rein informativ und daher optional.

Das Gateway kann jetzt per SNMP überwacht werden.

Soll das Gateway die in der herstellerspezifischen innovaphone-MIB definierten Traps auslösen, so müssen zusätzlich noch Ziele für Trap-Meldungen definiert werden.

- Selektieren Sie den Bereich **Trap Dest.**
- Fügen Sie mit der Schaltfläche **Add trap dest** ein neues Ziel hinzu. Sie können maximal 5 Ziele definieren.

Sie können zur Erhöhung der Sicherheit den Zugriff auf das Gateway beschränken, indem Sie den Zugriff per SNMP auf eine feste Liste von Rechnern beschränken.

- Selektieren Sie den Bereich **Accepted Hosts.**
- Fügen Sie mit der Schaltfläche **Add Host** die IP-Adresse eines autorisierten Rechner hinzu. Sie können maximal 5 autorisierte Rechner definieren.

Der Zugriff per SNMP ist nur möglich unter der Angabe des richtigen **Community-Namen**. Falls sie **Authentication Trap** im Bereich **SNMP** markiert haben, wird bei einem Zugriff mit falschem **Community-Namen** ein Trap generiert.

8.3 Festlegen der Syslog Parameter

Ihr Gateway kann wesentliche Ereignisse im Betrieb in einem Systemlog dokumentieren.

Die Art der Ereignisse, die festgehalten werden, kann im Feld **Log sources** im Bereich **Logging** des Konfigurationsapplets wie folgt konfiguriert werden:

Einstellung	Bedeutung
Log TCP	Alle TCP Verbindungsaufbauten im H.225 / H.245 Protokoll werden notiert.
Log PPP	Alle PPP Verbindungsaktivitäten werden notiert.

Einstellung	Bedeutung
Log calls	Alle Rufvermittlungen werden notiert.
Log RAS messages	Die auf die An- und Abmeldung von H.323 Endgeräten bezogenen Gatekeepernachrichten werden notiert.
Log gateway routing	Die einzelnen Schritte zur Rufvermittlung bei der Abarbeitung der Routing Tabelle werden notiert.
Log configuration changes	Alle Änderungen der Konfiguration werden notiert.

Tabelle 16

Die jeweils aktuellen Syslog Einträge können im Webinterface jederzeit über den Link **Log** kontrolliert werden, wie in Abbildung 38 auf Seite 118 gezeigt wird.

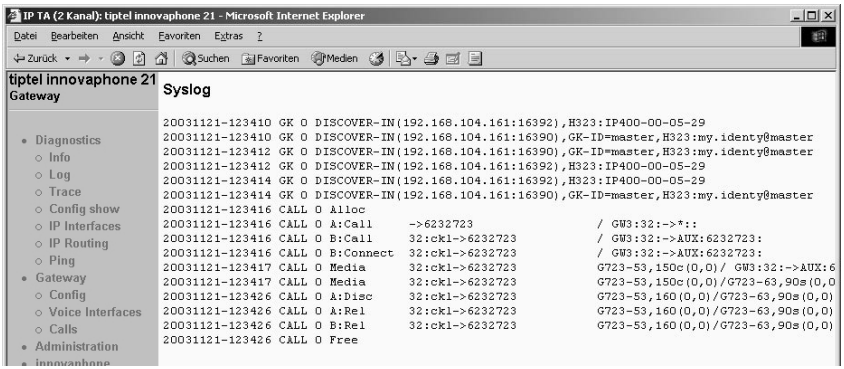

Abbildung 38 Die Syslog Einträge im Webinterface

Syslog Einträge werden nur dann angezeigt, wenn ein Webbrowser die **Log** Seite anzeigt. Anderenfalls gehen sie verloren.

Soll das Syslog dauerhaft gespeichert werden, stehen darüber hinaus wahlweise 3 Mechanismen zur Verfügung.

- Ablage der Syslog Einträge in einem `syslogd`.
  Hierbei werden die Einträge einem `syslogd` Server im Netz gemeldet. Die-

ser ist dann für die weitere Auswertung oder Abspeicherung zuständig.

- Wählen Sie als **Syslog mode** `SYSLOG` aus.
- Tragen Sie die IP-Adresse Ihres `syslogd` unter **Address** im Bereich **Syslog parameter** ein.
- Wählen Sie die gewünschte `syslogd` Meldungsklasse unter **Syslog class** aus.

- Ablage der Syslog Einträge in einem Web Server.
  Hierbei werden die Syslog Einträge an einen Web Server übertragen und können dort weiter verarbeitet werden. Jeder einzelne Syslog Eintrag wird als Formulardaten im HTTP GET Format an den Web Server übertragen.
  - Wählen Sie als **Syslog mode** `HTTP` aus.
  - Tragen Sie die IP-Adresse Ihres Web Servers unter **Address** im Bereich **HTTP parameter** ein.
  - Tragen Sie die relative URL des Formularprogramms auf Ihrem Web Server unter **URL-Path** ein.

Tipp

Ihr Gateway wird zum Webserver einen HTTP GET Request auf die eingetragene URL gefolgt vom url-encodeten Log Eintrag stellen. Haben Sie beispielsweise auf Ihrem Web Server eine Seite namens `/cdr/cdrwrite.asp` mit einem Formular, das die Logmeldung im Parameter `msg` erwartet, so tragen Sie in das Feld **URL-Path** den Wert `/cdr/cdrwrite.asp` ein. Ihr Gateway wird dann einen `GET /cdr/cdrwrite.asp?event=syslog&msg=`***`logmsg`*** Request zum Server stellen.

- Übermittlung der Syslog Einträge an ein TCP-Programm.
  Hierbei schreibt das Gateway die Syslog Einträge auf eine TCP-Verbindung. Das andere Ende der TCP Verbindung ist dann für die weitere Auswertung der Einträge zuständig.
  - Wählen Sie als **Syslog mode** `RAW-TCP` aus.
  - Tragen Sie die TCP Portnummer der Verbindung unter **TCP port number** im Bereich **Raw TCP parameter** ein.

- Soll das Gateway die TCP Verbindung selbsttätig aufbauen, tragen Sie die Ziel IP-Adresse unter **Address** ein.
- Soll das Gateway auf eine eingehende TCP Verbindung warten, tragen Sie die IP-Adresse, von der die Verbindung kommt, unter **Address** ein und Markieren Sie **Wait for incoming connections.**

8.4 Übermittlung von Call Detail Records (CDR)

Das Gateway kann detaillierte Informationen über jedes geführte Gespräch übermitteln. Die Informationen stehen in den Call Detail Records zur Verfügung und können mit geeigneter Software ausgewertet werden.

Zur Übermittlung der CDR-Daten stehen zwei Möglichkeiten zur Verfügung, die im Menüpunkt **CDR0-Logging** und **CDR1-Logging** des Konfigurationsapplets ausgewählt werden können. Somit können z. B. über **SYSLOG** CDR-Daten an den Administrator und die gleichen Daten z. B. über **HTTP** an die Abteilung Finance gesendet werden.

Zur Übersendung der Log-Datei stehen die Protokolle **SYSLOG**, **RAW TCP** und **HTTP** zur Verfügung. Die Auswahl **off** deaktiviert die Übertragung der Call Detail Records.

Je nach Art des gewählten Protokolls müssen die zugehörigen Parameter wie z. B. die IP-Adresse des Servers, etc. eingetragen werden.

Wird im Bereich **CDR Format** die Option **Send only billing CDR´s** aktiviert, erfolgt die Übermittlung von nur einem Call Detail Record am Ende eines ausgehenden Rufes, der über das Telefonnetz initiiert wurde. Dadurch werden nur ausgehende, externe und somit kostenpflichtige Gespräche erfasst.

Für weitere Informationen sehen Sie bitte in die Beschreibung auf der innovaphone Website im Downloadbereich oder wenden Sie sich an Ihren Händler für weitere Informationen.

9 Die Browser Administrationsoberfläche

Die Administration über den Web-Browser erlaubt Ihnen

- den Betriebszustand des Gerätes zu überwachen (Bereich **Diagnostics**),
- das Gateway und den Gatekeeper zu konfigurieren (Bereich **Gateway**),
- die Konfiguration zu sichern und zu laden sowie aktualisierte Firmware in Betrieb zu nehmen (Bereich **Administration**),
- falls installiert, die optionale innovaphone PBX Komponente zu konfigurieren und zu überwachen (Bereich **PBX pbx**).

Um die Administrationsoberfläche korrekt nutzen zu können, muss Ihr Web-Browser folgende Anforderungen erfüllen:

- HTTP1.1 Protokoll,
- HTML4.0 Protokoll,
- Frames,
- Java Applets,
- XML/XSL (XML/XSL ist nur für erweiterte Funktionen, wie das Sortieren von Listen erforderlich. Die Gateways lassen sich auch ohne diese Funktionen vollständig konfigurieren und administrieren.).

Die Administrationsoberfläche ist mit dem Internet Explorer 6.x getestet worden, lässt sich aber auch mit dem Netscape Browser bedienen.

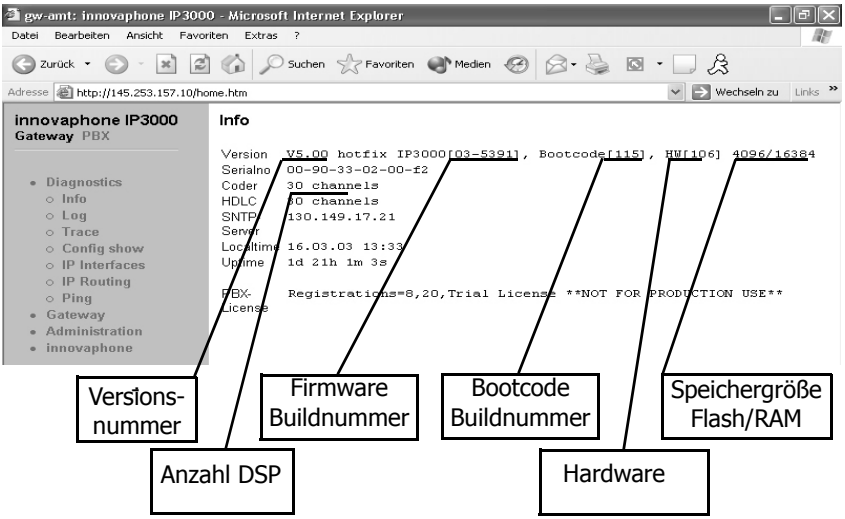

Abbildung 39 Die Browser Administrationsoberfläche

Wenn Sie Ihren Web-Browser mit der IP-Adresse Ihres Gateways verbinden, sehen Sie zunächst den Begrüßungsbildschirm. Die **URL** lautet

`http://`***xxx.xxx.xxx.xxx***

wobei ***xxx.xxx.xxx.xxx*** durch die IP-Adresse des Gateways zu ersetzen ist.

Über die Hyperlinks im oberen Rahmen des Browserfensters können Sie durch die verschiedenen Funktionsbereiche navigieren.

Verschiedene Bereiche verlangen die Eingabe der Administrator Nutzerkennung und des Kennwortes (siehe Seite 122).

9.1 Menü Diagnostics

9.1.1 Untermenü Info

Die Homepage Ihres Gateways (siehe Abbildung 39 auf Seite 122) zeigt Ihnen Informationen über

- die Hard- und Softwareversion des Gerätes,
- die Seriennummer,
- die Anzahl der Sprachkanäle,

- eine ggf. installierte innovaphone PBX Lizenz,
- die Adresse des benutzten SNTP Servers (sofern konfiguriert),
- die lokale Zeit des Gateways gemäß der Angaben des SNTP Servers und der Zeitzone,
- die Betriebsdauer seit dem letzten Kalt- oder Warmstart.

9.1.2 Untermenü Log

In diesem Bereich können Sie Logmeldungen Ihres Gateways direkt im laufenden Betrieb ansehen. Die Meldungen werden ständig selbsttätig aktualisiert und scrollen nach oben aus dem Fenster heraus.

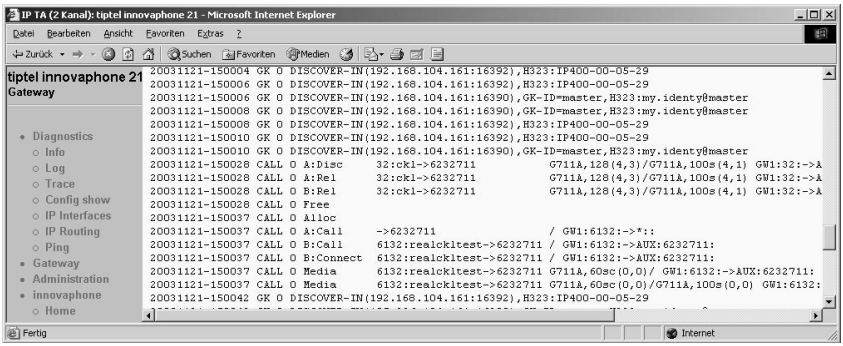

Abbildung 40 Anzeigen der Logmeldungen im Web-Browser

Es werden nur Meldungen angezeigt, die im Bereich **Logging** des Konfigurationsapplets konfiguriert sind. Die Logmeldungen erscheinen hier unabhängig davon, welches **Protocol** unter **Syslog mode** eingestellt ist.

9.1.3 Untermenü Trace

Dieser Bereich ermöglicht es Ihnen, Trace-Dateien aus Ihrem Gateway herunterzuladen. Analog zu dem im Kapitel 9.1.4 "Untermenü Config show" ab Seite 124 beschriebenen Vorgehen, können Sie den Trace in Dateien abspeichern.

Beachten Sie bitte, dass sich die Trace-Information ständig erweitert. Um einen fortlaufenden Trace zu bekommen, muss die Seite jeweils aktualisiert werden. Je nach Einstellung des Browsers reicht es dazu, den **Trace** Link erneut anzuklicken oder den Frame im Kontextmenü zu aktualisieren. Klicken Sie dazu mit der rechten Maustaste in das Arbeitsfeld und wählen Sie **Aktualisieren** im Kontextmenü.

9.1.4 Untermenü Config show

Das Menü **Config show** ermöglicht Ihnen, die aktuelle Konfiguration Ihres Gateways in Textform auszugeben.

Sie können die aktuelle Konfiguration auch in einer Datei abspeichern, in dem Sie – je nach verwendetem Browser – die **Ziel Speichern unter**... Funktion verwenden. Sie können auch den ganzen Text markieren (Ctrl-A) und mit der rechten Maustaste über das Kontextmenü in die Zwischenablage kopieren. Jetzt können Sie die Konfiguration in jeden Texteditor kopieren und abspeichern.

Eine solcherart gesicherte Konfiguration kann ganz oder teilweise mit Link **Config update** wieder geladen werden (siehe Kapitel 9.3.3 "Untermenü Config update" ab Seite 134). Auf diese Art und Weise können Sie Konfigurationen sichern und wieder herstellen oder auch Referenzkonfigurationen erstellen und auf eine Vielzahl von Geräten laden.

9.1.5 Untermenü IP Interfaces

Dieser Bereich listet Ihnen alle für Ihr Gateway konfigurierten IP-Schnittstellen mit dem jeweils aktuellen Status auf. Tabelle 17 erläutert die Bedeutung der Einträge.

Spalte	Bedeutung	Werte
interface	Die Art der Schnittstelle. • **ETH0**: Ethernet Schnittstelle • **PPP*x***: konfigurierte logische PPP Schnittstelle	**ETH0, PPP0, PPP1, PPP2, PPP3**

state	Zustand
	• **Up**:
	  • **ETH0**: der Ethernet Link ist in Ordnung
	  • **PPP*x***: die Verbindung ist hergestellt und das **IPCP** Protokoll ist erfolgreich abgelaufen
	• **Down**: Fehler am Ethernet Link bzw. PPP Verbindung nicht hergestellt
		Up, Down
		
		Down

Spalte	Bedeutung	Werte
action	Ändert den Verbindungsstatus • **connect**: initiiert einen Verbindungsaufbau • **clear**: schließt die Verbindung • **disconnect**: hat zur Zeit keine Bedeutung, bitte verwenden Sie **clear**	**connect, disconnect clear**
description	Zeigt die angegebene Beschreibung aus dem Konfigurationsapplet **IP Interfaces** an.	`Text`

Tabelle 17 Die Einträge der IP Interfaces Tabelle

9.1.6 Untermenü IP Routing

Dieser Bereich zeigt Ihnen die aktuelle IP-Routingtabelle an.

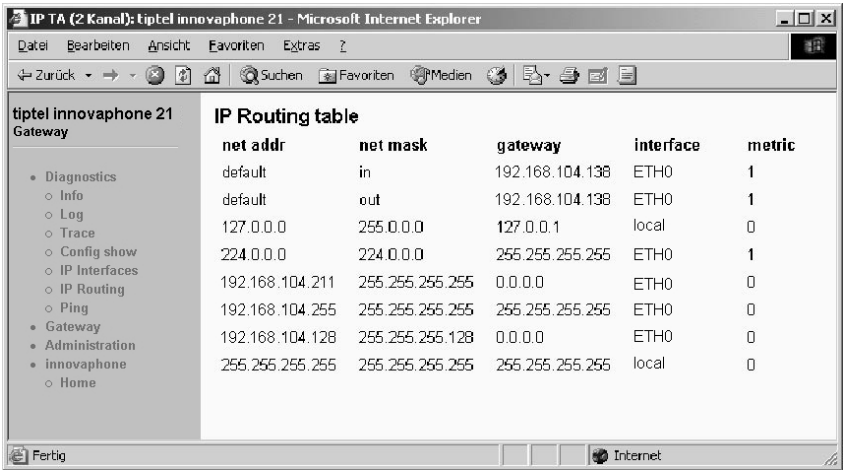

Abbildung 41 Die IP-Routing Tabelle

9.1.7 Untermenü Ping

Oft ist es notwendig, dass für Testzwecke von den VoIP Gateways aus ein Ping Kommando abgesetzt wird. In dem Editierfeld kann eine beliebige IP Adresse angegeben werden. Der Befehl wird mit der Enter-Taste abgeschlossen. Der Ping-

befehl wird auf dem verbundenen Gateway ausgeführt. Das Ergebnis wird wiederum im gleichen Fenster angezeigt.

9.2 Menü Gateway

9.2.1 Untermenü Config

Hiermit erreichen Sie das in Kapitel 3 "Allgemeines zur Konfiguration" ab Seite 20 vorgestellte Konfigurationsapplet.

9.2.2 Untermenü Voice Interfaces

Dieser Bereich listet Ihnen alle für Ihr Gateway konfigurierten Sprachschnittstellen mit dem jeweils aktuellen Status auf.

Die nachfolgende Tabelle erläutert die Bedeutung der Einträge.

Spalte	Bedeutung	Werte
Type	Die Art der Schnittstelle. • **IF**: ISDN Schnittstelle • **GW**: per RAS angemeldetes Gateway • **EP**: per RAS angemeldeter Endpunkt • **GK**: eigene Registrierung bei einem Gatekeeper	**IF, GW, EP, GK**
Addr	IP-Adresse • IP-Adresse des RAS Klienten für **EP** und **GW** • IP-Adresse des Gatekeepers für **GK**	`xxx.xxx.xxx.xxx`

State	Zustand der Schnittstelle
	• **Up**:
	  • **IF** Mehrgeräteanschlüsse: Schicht 1 ist aufgebaut
	  • **IF** Anlagenanschlüsse: Schicht 2 ist aufgebaut
	  • **GW**/**EP**: das Gerät ist angemeldet
	  • **GK**: Anmeld. am Gatekeeper erfolgt
	• **Down**: sonst
		Up, Down

Spalte	Bedeutung	Werte
Number	Die E.164 Adresse (Durchwahl) der Registrierung • **GW/EP:** die konfigurierte Durchwahl des Gerätes • **GK**: die bei der Registrierung mitgesendete E.164 Adresse • **IF**: ohne Bedeutung	`nnn`
Name	Der Schnittstellenname **IF**: die Beschriftung der Schnittstelle **GW**/**EP**/**GK**: der H.323 Alias der Registrierung	**TEL1, TEL2, TEL, PPP, TEST, TONE,** `Text`
Product	Herstellerbezeichnung • **GW**/**EP**: bei der Registrierung mitgelieferte Herstellerbezeichnung des angemeldeten Geräts • Sonst ohne Bedeutung	

Tabelle 18 Die Einträge der **Voice Interfaces** Tabelle

9.2.3 Untermenü Calls

In diesem Bereich können Sie die aktuell aktiven Rufe von und zu Ihrem Gateway beobachten. Falls Sie die optionale innovaphone PBX Komponente installiert haben, beachten Sie jedoch bitte, dass interne Gespräche zwischen innovaphone PBX Teilnehmern nicht angezeigt werden.

Die Bedeutung der einzelnen Spalten können Sie der nachfolgenden Tabelle entnehmen.

Spalte	Format	Werte	Bedeutung

State		`Dialing`
		
		`Alerting`
		
		`Connected`
		
		`Clearing`
			Es wird gewählt.
			
			Die gewählte Gegenstelle wird gerufen.
			
			Der Ruf ist verbunden.
			
			Der Ruf ist von einer der beiden Seiten getrennt worden.

Numbers	`Caller->Called`	`Caller`
		
		`Called`
			Die Rufnummer des Rufenden, so wie sie zum Rufziel übermittelt wird.
			
			Die gewählte Rufnummer.

Coders	`ACoders/BCoders`
	
	`Coder,ms(round, jitter)`
			Verwendeter Coder in Richtung A->B bzw. B->:
			Coder: verwendete Sprachkomprimierung.
			ms: verwendete Paketierung.
			round Laufzeit in ms
			jitter: Varianz der Laufzeit in ms.

Spalte	Format	Werte	Bedeutung
Inter-faces	`sif:cgpn:cgnm ->dif:cdpn:cdnm/ ccn`		Sif: Schnittstelle, auf der der Ruf einging. Cgpn: rufende Nummer vor dem Routen. Cgnm: rufender Name vor dem Routen. Dif: Schnittstelle, auf der der Ruf ausgeht. Cdpn: gerufene Nummer nach dem Routen. Cdnm: gerufener Name nach dem Routen. ccn: Name des für diese Route verwendeten Rufzählers (call counter name).

Tabelle 19 Einträge in der **Calls** Liste

9.2.4 Untermenü Call Counter

In diesem Bereich bekommen Sie den Namen des Rufzählers (**name**) und die Anzahl der aktuellen Rufe (**calls**) angezeigt, sofern für die jeweilige Route ein Rufzähler mit Rufbeschränkung im Resource Management eingerichtet worden ist (siehe Kapitel 7.2.13 "Ressourcen-Management" ab Seite 106).

9.3 Menü Administration

In diesem Bereich können Sie die Konfiguration sichern und laden sowie aktualisierte Firmware in Betrieb nehmen.

9.3.1 Untermenü Licenses

In diesem Bereich werden die installierten Lizenzen angezeigt. Ebenso können über dieses Menü weitere Lizenzen installiert werden.

Bei den Lizenzen werden zwei Gruppen unterschieden. Die hardwarebasierenden Lizenzen (Relay) und die softwarebasierenden Lizenzen (PBX).

Lizenz-Typ	Lizenz-Name
Relay - Registrations	Lizenz(en) für die Registrierungen am Gatekeeper
Relay - PRIs	Lizenz(en) für das S_2M Hardware-Interface
Relay - BRIs	Lizenz(en) für das S_0 Hardware-Interface

Tabelle 20 hardwarebasierende Lizenztypen

Die hardwarebasierenden Lizenztypen (siehe Tabelle 20) sind zwingend erforderlich, um die Hardware betreiben zu können. Zum Einen müssen Lizenzen für den Amtsanschluss (PRI bzw. BRI) des Gateways vorliegen, zum Anderen muss für jede Registrierung am Gatekeeper eine Lizenz vorliegen.

Lizenz-Typ	Lizenz-Name
PBX - Registrations	Lizenz(en) für die Registrierungen an der PBX
PBX - Operators	Lizenz(en) für die Registrierungen am Vermittlungsplatz PBX Operator
PBX - SoftwarePhones	Lizenz(en) für die SoftwarePhone-Registrierungen

Tabelle 21 PBX-bezogene Lizenztypen

Die Lizenzen werden mit einem Textfile in das Gateway geladen.

Die hardwarebasierenden Lizenzen müssen an Hand der Seriennummer Ihres innovaphone Gateways über das Web erstellt und heruntergeladen werden.

Die softwarebasierenden Lizenzen sind notwendig, um die innovaphone PBX und

die zugehörigen Applikationen nutzen zu können. Für jede Registrierung an der PBX ist eine Lizenz notwendig. Die Aktivierung der softwarebasierenden Lizenzen erfolgt über einen **Licensekey** bzw. **Activationkey**.

Lizenzen zum Gateway übertragen

Im Menü Licenses auf der Administrationsoberfläche Ihres Gateways befindet sich im oberen Bereich eine Übersicht der bereits installierten Lizenzen. Tabelle 20 und 21 zeigen die verschiedenen Lizenztypen.

Um weitere Lizenzen zum Gateway zu übertragen ist ein Textfile notwendig, das Sie über den **License Manager** erstellen können. Die Vorgehensweise für hardwarebasierende Lizenzen ist im Kapitel "Hardwarebasierende Lizenzen erstellen" ab Seite 132 beschrieben. Die Vorgehensweise für softwarebasierende Lizenzen ist im Kapitel "Softwarebasierende Lizenzen mit dem License Manager erstellen" ab Seite 133 beschrieben.

Um ein Lizenz-Textfile in das Gateway zu übertragen, gehen Sie wie folgt vor:

- Geben Sie im Eingabefeld **File:** den Speicherort der oben beschriebenen Lizenz-Textfiles an oder wählen Sie den Speicherort des **license files** mittels der Schaltfläche **Durchsuchen...**.
- Drücken Sie die Schaltfläche **Upload license file**, um die Lizenzdatei in das Gateway zu laden.

Mit diesem Upload sind die Lizenzen in der Konfiguration des Gateways gespeichert und stehen zur Verfügung. Die installierte Lizenz wird angezeigt. In der Spalte **type** wird der Lizenztyp und in der Spalte **name** wird der Lizenzname, gefolgt von der Seriennummer angegeben.

Sie können die zusätzlich installierten Lizenzen auch wieder aus dem Gateway laden, um sie auf ein anderes innovaphone Gerät zu übertragen oder aber auch, um sie vor dem Löschen der Konfiguration zu sichern.

Wollen Sie eine zusätzlich installierte Lizenz aus dem Gateway laden, gehen Sie wie folgt vor:

- Drücken Sie in der Spalte **action** die Schaltfläche **download** neben dem zu sichernden Lizenzeintrag, um die zusätzlich installierte Lizenz als Textfile zu sichern. Folgen Sie den weiteren Anweisungen.

Wollen Sie die zusätzlich installierte Lizenz aus dem Gateway löschen, gehen Sie wie folgt vor:

Achtung

Vor dem Löschen der zusätzlich installierten Lizenzen sollten Sie diese wie zuvor beschrieben sichern. Oder stellen Sie sicher, dass Sie das original Textfile, das Sie zur Installation der zusätzlichen Lizenzen verwendet haben, noch besitzen.

- Drücken Sie in der Spalte **action** die Schaltfläche **delete** neben dem zu löschenden Lizenzeintrag, um die zusätzlich installierte Lizenz zu löschen. Folgen Sie den weiteren Anweisungen.

Die Schaltflächen **download all** und **delete all** haben die gleiche Funktionalität wie die Schaltflächen **download** und **delete**, beziehen sich aber auf alle angezeigten Lizenzen.

Hardwarebasierende Lizenzen erstellen

- Verbinden Sie Ihren Web-Browser mit der folgenden Website: `http://www.innovaphone.com/license/license.php`
- Bestätigen Sie nach Anerkennung die Lizenzvereinbarung mit "ja".
- Sie werden aufgefordert, sich mit Ihren Account-Daten einzuloggen. Geben Sie diese ein und klicken Sie **Login**.

Tipp

Sollten Sie noch keinen Account eingerichtet haben, klicken Sie auf **register** und legen Sie Ihren Account durch Eingabe Ihrer Email-Adresse und eines Kennwortes an.

- Geben Sie im Feld **Serialnumber** die Seriennummer (`00-90-33-xx-xx-xx`) Ihres Gateways ein und klicken Sie auf die Schaltfläche **Download License**.
- Bestätigen Sie die Seriennummer mit **confirm**. Nach erfolgreicher Bestätigung wird Ihnen die fertige Lizenz zum Download angeboten.
- Klicken Sie auf **download**, um die Lizenz auf Ihren Rechner herunterzuladen.
- Klicken Sie auf **Logout**, um den Bereich zu verlassen.

Die hardwarebasierenden Lizenzen werden ebenfalls im Lizenzmanager verwaltet

und können von dort jederzeit wieder heruntergeladen werden. Diese Lizenzen werden von innovaphone mit eingetragener MAC-Adresse erstellt, so dass diese nicht auf einer anderen Hardware als der vorgesehenen eingesetzt werden können.

Softwarebasierende Lizenzen mit dem License Manager erstellen

Sollen mehr Registrierungen erfolgen als vorhanden sind, müssen Sie zusätzliche Lizenzen erwerben und installieren. Lizenzen können Sie bei Ihrem Fachhändler oder bei innovaphone direkt beziehen. Lizenzen werden über einen **Licensekey** aktiviert, der wiederum mit einem **Activationkey** erstellt wird.

- Verbinden Sie Ihren Web-Browser mit der folgenden Website: `http://www.innovaphone.com/license/license.php`
- Bestätigen Sie nach Anerkennung die Lizenzvereinbarung mit "ja".
- Sie werden aufgefordert, sich mit Ihren Account-Daten einzuloggen. Geben Sie diese ein und klicken Sie **Login**.

Tipp

Sollten Sie noch keinen Account eingerichtet haben, klicken Sie auf **register** und legen Sie Ihren Account durch Eingabe Ihrer Email-Adresse und eines Kennwortes an.

- Klicken Sie auf der Willkommensseite auf die Schaltfläche **License manager**.
- Selektieren Sie das Menü **Activationkeys**.
- Geben Sie im Feld **Activationkey** den erhaltenen Activationkey ein und betätigen Sie die Schaltfläche **Add**.

Nachdem Sie den Activationkey hinzugefügt haben, erscheint die Bildschirmanzeige des Menüpunktes **Balance**, in dem Sie jederzeit ersehen können, wie viele Lizenzen Sie erworben, verbraucht oder noch zur Verfügung haben. Aus diesem Pool können Sie nun frei verfügen.

- Um nun aus diesem Pool Lizenz-Textfiles zu kreieren, die auf einfache Weise auf die Geräte hochgeladen werden können, selektieren Sie das Menü **Licensekeys**.
- Hier können Sie nun mittels drop-down-Menüs die entsprechenden Lizenzen und die benötigte Anzahl eingeben. Für eine gute Übersichtlichkeit empfiehlt es sich beim ersten Mal die Seriennummer und den Endkunden einzutragen.

- Bei jeder einzelnen Lizenz bekommen Sie noch einmal angezeigt, was Sie soeben als Lizenz erstellen wollen. Falls Sie einen Fehler gemacht haben, besteht hier die Möglichkeit, den jeweiligen Schritt rückgängig zu machen.
- Sobald der Vorgang abgeschlossen ist, gelangen Sie auf eine Übersichtsseite, auf der alle Ihnen zugeordneten Lizenzen übersichtlich angeordnet sind und auf einfache Weise als Lizenz-Textfile heruntergeladen werden können.

9.3.2 Untermenü Config save

Das Menü **Config save (all)** ermöglicht Ihnen, die gesamte Konfiguration Ihres Gateways als txt-Datei zu öffnen und zu speichern.

Das Menü **Config save (config)** ermöglicht Ihnen, die Konfiguration Ihres Gateways ohne die Benutzerdaten als txt-Datei zu öffnen und zu speichern.

Das Menü **Config save (LDAP)** ermöglicht Ihnen, die Benutzerdaten aus der Konfiguration Ihres Gateways als txt-Datei zu öffnen und zu speichern.

9.3.3 Untermenü Config update

Im Menü **Config update** wird eine mit **Untermenü Config show** (siehe Kapitel 9.1.4 "Untermenü Config show" ab Seite 124) gespeicherte Konfiguration auf Ihr Gateway geladen.

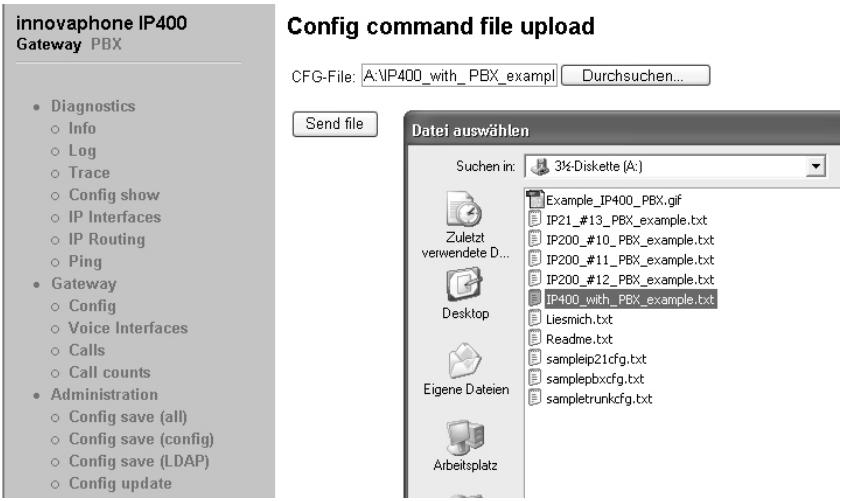

Abbildung 42 Laden einer Konfiguration im Web-Browser

Tragen Sie den Pfad und Dateinamen der zu ladenden Konfigurationsdatei im Feld **CFG-File** ein und klicken Sie auf die Schaltfläche **Send file**.

Abbildung 43 Aktivieren der geladenen Konfiguration

Beachten Sie bitte, dass die Konfigurationsdatei in den flüchtigen Speicher Ihres Gateways geladen wird. Sie ist damit weder permanent gesichert, noch sofort wirksam. Daher wird Ihnen nach erfolgtem Upload die in Abbildung 43 auf Seite 135 gezeigte Auswahl angeboten.

Lesen Sie im Kapitel 3.2 "Testen und Speichern der Konfiguration" ab Seite 22 nach, wie die neue Konfiguration getestet und gesichert werden kann.

9.3.4 Untermenü Firmware update

Diese Funktion ermöglicht es, eine neue Firmware Version auf Ihr Gateway aufzuspielen. Neue Firmware Versionen können Sie von Ihrem Händler erhalten.

Abbildung 44 Aktualisieren der Firmware im Web-Browser

Tragen Sie den Pfad und Dateinamen der zu ladenden Firmwaredatei im Feld **Protocol-File** ein und klicken Sie auf die Schaltfläche **Send file**.

Während des Ladens der neuen Firmware werden Sie darauf hingewiesen, den Ladevorgang auf keinen Fall zu unterbrechen.

Achtung

Blinkt die **Ready**-LED während des Downloads, darf dieser Vorgang nicht unterbrochen werden. Das Gerät kann sonst beschädigt werden.

Wird der Ladevorgang trotzdem unterbrochen, schalten Sie Ihr Gateway danach auf keinen Fall aus. Wiederholen Sie die Prozedur vielmehr noch einmal, nachdem Sie das Problem beseitigt haben.

Beachten Sie die den neuen Versionen beiliegenden Unterlagen, um festzustellen, ob auch eine neue Boot-Firmware geladen werden muss. Ist dies der Fall, beachten Sie falls angegeben auch die geforderte Reihenfolge von Bootcode und Firmware Update.

Die neue Firmware wird nicht direkt aktiv. Sie müssen einen Reset ausführen, um die neue Version zu aktivieren. Dazu werden Ihnen die Links **immediate reset** und **reset when idle** angeboten.

Nach erfolgreicher Aktualisierung der Firmware müssen Sie auf jeden Fall alle Browser und Appletfenster schließen und den Browser neu starten. Dies ist notwendig, da die neue Firmware auch neue Oberflächenelemente enthalten kann, die nur auf diese Weise aktiviert werden.

9.3.5 Update Server

Eine spezielle Funktion zum automatischen Update der Firmware Ihrer innovaphone Gateways steht Ihnen im Konfigurationsapplet im Bereich **Config > General settings > Update Server** zur Verfügung. Im Feld **URL** haben Sie die Möglichkeit eine URL mit einem Verweis auf den Speicherort einer Skripdatei innerhalb Ihres Netzwerkes zu setzen. Diese Skriptdatei muss einer definierten Syntax folgen, die Sie im Dokument "How to use the Update Server" der innovaphone Support-Dateien finden. Im Feld **Poll interval [min]** kann eine Zeit eingetragen werden, mit welchem Intervall diese Skriptdatei nach Änderungen durchsucht werden soll. Wird der Verweis auf eine neue Firmware-Version in dieser Skriptdatei gefunden, erfolgt das Firmware-Update automatisch. Sie müssen lediglich zuvor die neue Firmware-Version in ein entsprechendes Verzeichnis auf einen internen Webserver kopieren.

Es wird ein Web-Server benötigt, der von allen upzudatenden Geräten erreicht werden kann. Des weiteren müssen HTTP-PUT Schreibrechte (zum Speichern der Informationen zur Gerätekonfiguration) und HTTP-GET Leserechte (für alle darauf zugreifenden innovaphone Geräte) auf diesem internen Web-Server eingerichtet werden. Zudem muss der Web Server den simultanen Zugriff der Geräte erlauben.

Der Zugriff der innovaphone Geräte erfolgt über DHCP. Für weitere Informationen zum DHCP-Client und dem Update Server siehe Anhang D: "Der innovaphone DHCP Client" ab Seite 155.

9.3.6 Untermenü Boot update

Diese Funktion ermöglicht es, eine neue Bootcode Version auf Ihr Gateway aufzuspielen. Neue Bootcode Versionen erhalten Sie von Ihrem Händler.

Tragen Sie den Pfad und Dateinamen der zu ladenden Bootcodedatei im Feld **Boot-File** ein und klicken Sie auf die Schaltfläche **Send file**.

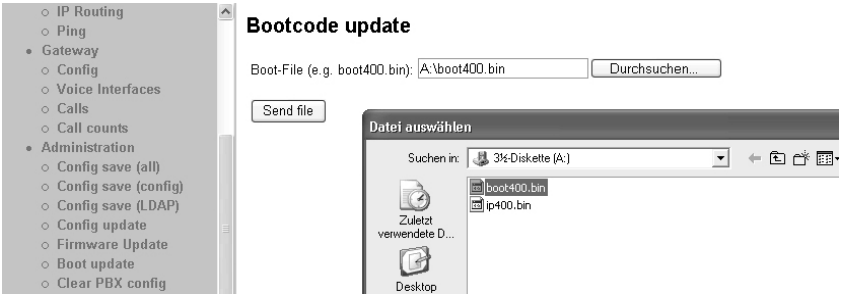

Abbildung 45 Aktualisieren des Bootcode im Web-Browser

Während des Ladens von neuem Bootcode werden Sie darauf hingewiesen, den Ladevorgang auf keinen Fall zu unterbrechen.

Achtung

Blinkt die **Ready**-LED während des Downloads, darf dieser Vorgang nicht unterbrochen werden. Ihr Gateway kann sonst beschädigt werden.

Wird der Ladevorgang trotzdem unterbrochen, schalten Sie Ihr Gateway danach auf keinen Fall aus. Wiederholen Sie die Prozedur vielmehr noch einmal, nachdem Sie das Problem beseitigt haben.

Der neue Bootcode wird nicht direkt aktiv. Sie müssen Ihr Gateway aus- und wieder einschalten, um die neue Version zu aktivieren.

Beachten Sie die den neuen Versionen beiliegenden Unterlagen, um festzustellen, ob auch eine neue Protocol-Firmware geladen werden muss.

9.3.7 Untermenü Clear PBX config

Diese Funktion ermöglicht es Ihnen, die gesamte Konfiguration einer gegebenenfalls installierten innovaphone PBX Komponente zu löschen. Dies ist z.B. nach einer Wiederherstellung der Standardkonfiguration (siehe Kapitel 2.2.1 "Herstellen der Standardkonfiguration" ab Seite 11) nützlich, da hierbei die Konfiguration der innovaphone PBX Komponente nicht zurückgesetzt wird.

Es empfiehlt sich, vor dem Löschen der Daten eine Sicherung der Konfiguration (siehe Kapitel 9.1.4 "Untermenü Config show" ab Seite 124) durchzuführen.

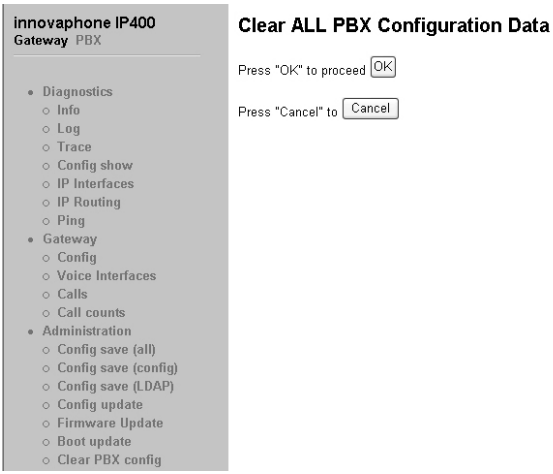

Abbildung 46 Löschen der innovaphone PBX Daten

Bei Betätigen von **Clear PBX config** werden Sie zunächst gefragt, ob tatsächlich die gesamte Konfiguration gelöscht werden soll. Wird dies bestätigt, wird die innovaphone PBX Konfiguration vollständig gelöscht. Danach ist ein Reset erforderlich. Sie können wählen, ob dieser sofort erfolgen soll, oder erst wenn das Gateway im Ruhezustand ist.

Abbildung 47 Reset nach Löschen der innovaphone PBX Konfiguration

9.4 Menü innovaphone

9.4.1 Untermenü Home

Durch Anwahl dieses Bereiches wird die innovaphone Website aufgerufen.

Anhang A:Sicherheitshinweise

Der Hersteller lehnt jede Verantwortung für Personen-, Sach- oder Folgeschäden ab, die auf unsachgemäße Verwendung des Gerätes zurückzuführen sind.

Dieses Gerät entspricht bei bestimmungsgemäßer Verwendung den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen des FTEG und der Richtlinie 1999/5/EG (Artikel 3 der R&TTE).

Die Konformitätserklärung liegt dem Gerät auf der mitgelieferten CD bei.

Zur Konfiguration der VoIP Endgeräte ist das Handbuch "VoIP-Endgeräte - Bedienungsanleitung" und das "Administrator Handbuch - innovaphone PBX" mit zu beachten. Alle darin aufgeführten Hinweise sind sorgfältig zu berücksichtigen und die Geräte sind ausschließlich so wie beschrieben zu verwenden.

Sicherheitshinweise für die IP 400

Achtung

Beachten Sie bitte zu Ihrer eigenen Sicherheit folgende Hinweise:

Stromversorgung

Betreiben Sie das Gerät ausschließlich mit dem mitgelieferten Steckernetzteil.

Das Steckernetzteil des Gerätes ist zum Betrieb an einem 100V-240V, 50Hz Wechselstromnetz ausgelegt. Versuchen Sie niemals, das Netzteil an andere Stromnetze anzuschließen!

- Stromversorgung durch Steckernetzteil, Primär: 110V-240V AC +10%-15%, 50/60Hz, 250mA, Sekundär: 12V DC 800mA.

Während eines Netzausfalls ist das Gerät nicht betriebsbereit. Die Einstellungen des Gerätes bleiben jedoch erhalten.

Die Netzsteckdose muss sich in der Nähe des Gerätes befinden und leicht zugänglich sein. Die Stromversorgung des Gerätes kann nur durch Herausziehen des Gerätenetzkabels aus der Netzsteckdose unterbrochen werden.

Aufstellung und Anschluss

Installation und ggf. Einbau des Gerätes darf nur durch geeignetes Personal erfolgen.

Achten Sie bei der Installation auf ausreichende Belüftung des Gerätes während des Betriebes, insbesondere bei Einbau in geschlossene Schränke.

Verlegen Sie die Anschlussleitungen stolperfrei. Alle angeschlossenen Kabel dürfen nicht übermäßig geknickt, gezogen oder mechanisch beansprucht werden.

Das Gerät ist nur zur Verwendung in trockenen Räumen bestimmt.

- Betriebstemperatur: 0° C bis 40° C, 10% bis 90% relative Luftfeuchtigkeit, nicht kondensierend
- Lagertemperatur: -10° C bis 70° C

Das Gerät darf nicht in folgender Umgebung aufgestellt und betrieben werden:

- In feuchten, staubigen oder explosionsgefährdeten Räumen,
- bei Temperaturen über 40°C oder unter 0°C,
- bei starken Erschütterungen oder Vibrationen.

Reinigung

Verwenden Sie ein weiches, leicht feuchtes Tuch zur Reinigung der Gehäuseoberfläche. Keine Chemikalien oder Scheuermittel verwenden. Das Gerät ist wartungsfrei.

Funktionsstörung

Unter bestimmungsgemäßen Betriebs- und Wartungsbedingungen ist es nicht erforderlich das Gerät zu öffnen. Sollten Sie das Gerät jedoch aus irgendwelchen Gründen öffnen, stellen Sie sicher, dass vorher alle Anschlusskabel entfernt wurden. Vor Öffnen des Gerätes die Verbindung zur Stromversorgung durch Ziehen des Netzsteckers trennen.

Ein defektes Gerät nicht öffnen und nicht mehr anschließen. Bringen Sie in diesem Fall das Gerät zu Ihrem Händler oder Service-Center. Verwahren Sie bitte die Original-Verpackung für eine evtl. Rücksendung auf, da sie Ihr Gerät optimal schützt. Sichern Sie vorher alle Einträge (z.B. auf einem PC), um sich gegen Datenverlust zu schützen.

Anhang B:Problembehebung

Typische Probleme

Bestimmte Probleme treten unserer Erfahrung nach häufiger auf. Die nachstehende Tabelle 22 listet diese Probleme und gibt Hinweise zu deren Behebung.

Symptom	Erläuterung	Maßnahme
Das Gateway reagiert nicht. **ready**, **link** und **act**. LED (bei der IP 400) leuchten ununterbrochen.	Das Gateway wartet auf einen Firmware Download.	• Führen Sie ein kurzes Reset durch Betätigen der **Reset** Taste durch.
Das Gateway reagiert nicht. **ready** LED leuchtet, **link** LED ist dunkel.	Die Ethernet Verbindung funktioniert nicht.	• Prüfen Sie die Stellung des "**connect to** ..." Schalters. • Überprüfen Sie die Ethernet Verkabelung.
Das Gateway reagiert nicht. **ready** und **link** LEDs leuchten, **act**. LED blinkt bei Zugriffsversuch.	Das Gateway hat eine falsche IP-Adresse konfiguriert.	• Stellen Sie die IP-Parameter korrekt ein (siehe Seite 27).
Im Auslieferungszustand weist das Gateway dem PC keine IP-Adresse zu.	Nach dem Einschalten ist der DHCP Klient aktiv.	• Betätigen Sie kurz die Reset Taste. • Lassen Sie dem PC erneut eine IP-Adresse zuweisen.
Ein an **tel1** oder **tel2** angeschlossenes Telefon funktioniert nicht (nur IP 400). Ein vorhandenes Display zeigt nichts an.	Dem Telefon fehlt die Stromversorgung.	• Markieren Sie **Power** in der Konfiguration der Schnittstelle.

Symptom	Erläuterung	Maßnahme
Ein an **tel1** oder **tel2** angeschlossenes Endgerät funktioniert unzuverlässig (nur IP 400).	Die Busterminierung fehlt.	• Prüfen Sie, ob die an der Schnittstelle angeschlossene ISDN Verkabelung ordnungsgemäß terminiert ist. • Fehlt die Terminierung, aktivieren Sie das Kontrollkästchen **100 Ohm Termination** in der Konfiguration der Schnittstelle (siehe Seite 55). • Ist die Terminierung korrekt, deaktivieren Sie das Kontrollkästchen 1**00 Ohm Termination** in der Konfiguration der Schnittstelle (siehe Seite 55).
Eingehende Rufe werden korrekt angenommen, jedoch ist kein Rückruf aus der Anrufliste der verwendeten Telefone möglich.	Die **Calling Line** ID ist unvollständig, da die Amtsholung fehlt.	• Fügen Sie die Amtsholungsziffer für die Leitung, auf der der Ruf eingeht in der Konfiguration der Schnittstelle ein (siehe Seite 96) oder aktivieren sie die automatische CLI Korrektur (siehe Seite 97).
Es können Rufe zu einem entfernten VoIP Gerät aufgebaut werden, es ist jedoch keine Verständigung möglich.	Die erforderliche Bandbreite für die Übertragung der Gesprächsdaten ist nicht verfügbar.	• Konfigurieren Sie in der Konfiguration für das entfernte Gateway eine effizientere Sprachkodierung (siehe Seite 80).

Symptom	Erläuterung	Maßnahme
Es können Rufe zu einem entfernten VoIP Gerät aufgebaut werden, es kommt jedoch keine Sprachverbindung zustanden.	Der Medienkanal kann nicht aufgebaut werden, da die beiden VoIP Geräte über keinen gemeinsamen Sprachkodierer verfügen.	• Stellen Sie sicher, dass das Kontrollkästchen **exclusive** deaktiviert ist (siehe ab Seite 78).
Es können Rufe zu einem entfernten VoIP Gerät aufgebaut werden, es kommt jedoch keine Sprachverbindung zustande.	Der Medienkanal kann nicht aufgebaut werden, da die beiden VoIP Geräte über keinen gemeinsamen Sprachkodierer verfügen.	• Nur der Medienkanal wird direkt zwischen den beiden VoIP Geräten aufgebaut, alle Signalisierverbindungen laufen über den Gatekeeper. • Stellen Sie sicher, dass beide VoIP Geräte über eine korrekte IP-Routingkonfiguration verfügen, insbesondere Subnetzmaske und Standardgateway.
Rufe zu einem entfernten Telefoniegateway werden von diesem immer abgelehnt.	Das Gateway unterstützt keine Einzelziffernachwahl.	• Fügen Sie im Rufnummernpräfix der zu diesem Gateway führenden Route eine Raute (#) ein, um Blockwahl zu erzwingen (siehe Seite 102).
Das Gateway verliert ihre Konfiguration nach dem Trennen von der Stromversorgung.	Die Konfiguration wurde nicht in den nichtflüchtigen Speicher gesichert.	• Sichern Sie die Konfiguration nach erfolgreichen Änderungen in den nichtflüchtigen Speicher (siehe Seiten 22).

Symptom	Erläuterung	Maßnahme
Ein an **tel1** oder **tel2** angeschlossenes Telefon funktioniert, bekommt jedoch keinen Wahlton (nur IP 400)	Es ist keine Route für diese Schnittstelle definiert.	• Definieren Sie mindestens eine Route, die für diese Schnittstelle gültig ist.
Das Gateway ist hinter einer "Firewall" ans Netz angeschlossen und die Konfiguration funktioniert nicht.	Die Firewall lässt den Zugriff auf die das Gateway nicht zu.	• Schalten Sie in der Firewall den Zugriff zum Gateway für den Dienst tcp/80 (http) frei.
Das Gateway ist hinter einer "Firewall" ans Netz angeschlossen und es kommen keine Verbindungen zu anderen VoIP Geräten zustande.	Die Firewall unterstützt das H.323 Protokoll nicht.	• Aktivieren Sie in Ihrer Firewall-Software das "H.323 Firewalling" und ggf. auch "H.323 NAT". Konsultieren Sie zu diesem Zweck die Dokumentation Ihrer Firewall. • Lesen Sie im Kapitel "NAT und Firewalls" ab Seite 146 nach.
Sie benutzen die `gwload.exe` Utility. Das Gateway wird zwar gefunden, der upload neuer Firmware scheitert jedoch.	Der arp-cache Ihres Rechners enthält falsche Informationen.	• Löschen Sie den arp-cache des Rechners. Benutzen Sie dazu auf einem Windows-PC das Kommando `arp -d` *`ip-addr`*.
Faxübertragungen brechen ab	T.38 ist nicht erlaubt in der Gatewaydefinition.	• Aktivieren Sie das T.38 Protokoll (siehe ab Seite 75).

Symptom	Erläuterung	Maßnahme
Faxübertragungen brechen ab, insbesondere bei längeren Faxen	Das Gateway und die TK-Anlage, an dem das Fax angeschlossen ist, verfügen über nicht-synchronen ISDN Takt.	• Sorgen Sie für korrekte Taktsynchronisierung (siehe Seite 54).

Tabelle 22 Fehlerbehebung

NAT und Firewalls

Ist Ihr Netzwerk durch eine Firewall zum Internet hin geschützt und wollen Sie mit Ihrem Gateway Verbindungen zu Gegenstellen über das Internet aufbauen, so müssen Sie für geeignete Konfiguration der Firewall sorgen.

Firewalls haben meist zwei Aufgaben. Sie kontrollieren den Zugriff auf Geräte und Netzbereiche innerhalb Ihres Netzes und sie realisieren die IP-Adressumsetzung in Netzen, die keine eigene reguläre Netzwerkadresse besitzen (so genanntes "NAT", network address translation). "NAT" kann auch von Routern realisiert werden.

Im Zusammenhang mit "Voice over IP" erfordern beide Funktionen zu Ihrer Umsetzung eine detaillierte Analyse des Datenstroms. Dies muss von Ihrer Firewall bzw. Router Firmware geleistet werden. Konsultieren Sie bitte die entsprechende Dokumentation des von Ihnen genutzten Produktes.

Sollte das von Ihnen verwendete Produkt kein "H.323 Firewalling" aufweisen, so gibt es vier mögliche Vorgehensweisen:

- Sie schalten in Ihrer Firewall den Weg für ***alle*** benötigten Daten von und zum Gateway frei.

  Diese Lösung wird von Netzwerkadministratoren meist nicht gern gesehen, ist jedoch risikolos, da das Gateway als dediziertes Gerät keine anderen Dienste außer "voice over IP" abwickelt. Ein Öffnen des Weges von und zum Gateway eröffnet daher keine Sicherheitslücken in Ihrem Netz.
- Soll kein RAS-Protokoll verwendet werden und handelt es sich bei den H.323 Geräten, deren Daten die Firewall passieren sollen, ausschließlich um innovaphone Geräte, so lässt sich die Anzahl der freizuschaltenden Ports eingrenzen. Dazu darf allerdings in den Gatewaydefinitionen aller Geräte nicht das

Kontrollkästchen **Disable H.245-tunneling** aktiviert sein (siehe Kapitel 6.1.4 "H.323 Protokolloptionen" ab Seite 75).

In beide Richtungen müssen folgende Ports freigeschaltet werden:

- Tcp: Zielport `80` (http), Quellport beliebig (zur Konfiguration)
- Tcp: Zielport `1720` (h.225), Quellport beliebig (für VoIP Gespräche) Die Freischaltung der Ports `1721`, `1722`, `1723`, etc. wird empfohlen. Die Anzahl der freizuschaltenden Ports ergibt sich aus der Anzahl der Verbindungen und ist vom Administrator nach Bedarf vorzunehmen.
- Udp: Zielport >= `2050`, Quellport `5004` und `5005` (RTP) (für VoIP Gespräche)

Tipp

Wird das RAS-Protokoll nicht verwendet, ist kein QSIG-Tunneling mehr möglich. Dies kann z. B. beim Szenario der Standortverbindung mit zwei verbundenen Telefonanlagen zu Performance-Einbußen führen, da keine Übertragung von zusätzlichen Leistungsmerkmalen stattfindet.

Muss Ihr Gateway mit Fremdprodukten kommunizieren, lässt sich die Anzahl der freizuschaltenden Ports nicht eingrenzen. Es ist daher erforderlich, alle Ports von und zum Gateway freizugeben.

- Soll das RAS-Protokoll verwendet werden (Empfehlung) und handelt es sich bei den H.323 Geräten, deren Daten die Firewall passieren sollen, ebenfalls ausschließlich um innovaphone Geräte, so lässt sich die Anzahl der freizuschaltenden Ports wie folgt gezeigt eingrenzen. Dazu darf allerdings in den Gatewaydefinitionen aller Geräte nicht das Kontrollkästchen **Disable H.245-tunneling** aktiviert sein (siehe Kapitel 6.1.4 "H.323 Protokolloptionen" ab Seite 75).
  - Tcp: Zielport `80` (http), Quellport beliebig (zur Konfiguration)

- Im Konfigurationsapplet muss für alle RAS-Gateways (Bereich **VOIP-Interfaces > GWnn**) der **mode > Registration at gatekeeper as gateway** eingestellt, die **Remote gatekeeper address > IP-address** eingetragen und die Option **Disable dynamic signaling port** aktiviert sein. Im Feld **Signaling Port** muss dann der zugehörige Port (`1720`, `1721`, `1722`, `1723`, etc.) für das GWnn Interface eingetragen werden.

- Tcp: Zielport `1720` (h.225), Quellport beliebig (für VoIP Gespräche)
  Die Freischaltung der Ports `1721`, `1722`, `1723`, etc. wird empfohlen. Die Anzahl der freizuschaltenden Ports ergibt sich aus der Anzahl der Verbindungen und ist vom Administrator nach Bedarf vorzunehmen.

- Udp: Zielport >= `2050`, Quellport `5004` und `5005` (RTP) (für VoIP Gespräche)

- Udp: Zielport `1718` und `1719`

- Udp: Quellport `1719` (für RAS und h.225)

- Udp: Quellport `5004` und `5005` (für RTP)

- Wird der Faxdienst genutzt, muss ebenfalls Udp: Quellport `5006` freigeschaltet werden, da nach dem Verbindungsaufbau auf T.38 umgeschaltet wird.

  Muss Ihr Gateway mit Fremdprodukten kommunizieren, lässt sich die Anzahl der freizuschaltenden Ports nicht eingrenzen. Es ist daher erforderlich, alle Ports von und zum Gateway freizugeben.

- Sie platzieren Ihr Gateway ***vor*** die Firewall, so dass der Datenstrom die Firewall nicht passieren muss. Bedenken Sie jedoch, dass Sie in diesem Fall keine Sprachverbindungen von innerhalb Ihres Netzes aus zum Gateway aufbauen können (z.B. mit innovaphone Softwarephone-PC´s).

Wird ihr Netzwerk im NAT Modus betrieben und das von Ihnen verwendete Produkt unterstützt kein "H.323 NAT", dann ist ein Betrieb über die Firewall hinweg nicht möglich.

VoIP und stark belastete WAN Strecken

Werden Gesprächsdaten über stark belastete, schmalbandige WAN Strecken übertragen, so kann es zu Einbußen in der Sprachqualität kommen, wenn die jeweiligen Strecken keine ausreichende Übertragungsqualität mehr sicherstellen können (siehe Tabelle 11 auf Seite Seite 79 sowie Tabelle 12 auf Seite Seite 81).

Abhilfe bringt hier die Priorisierung von Sprachdaten auf den WAN Strecken. Dies kann in der Regel durch die verwendeten Router erreicht werden.

Unterstützt Ihr Router die Funktion "Priorisierung von Sprachdaten nach H.323", so kann diese direkt genutzt werden.

Kann Ihr Router anhand des IP **type of service** (TOS) Feldes priorisieren, können Sie diese Funktion verwenden. Ihr Gateway setzt in allen IP-Paketen, die es sendet, das TOS Feld auf `0x10`. Sie können diesen Wert bei Bedarf im Konfigurationsapplet im Bereich **IP Interfaces** im Feld **TOS Value** verändern.

Tipp

Sie können den Wert hexadezimal, oktal oder dezimal angeben, die Eingaben `0x10`, `020` und `16` sind gleichwertig. Bedenken Sie, dass der Wert für das TOS Feld auf allen Geräten gleich gesetzt sein sollte.

Ist dies nicht der Fall, können Sie sich durch die Funktion "Priorisierung nach Quell- / Ziel- Adresse" behelfen, wenn vorhanden. Damit werden Datenpakete von und zum Gateway priorisiert. Dies entspricht im Effekt der Priorisierung von Sprachdaten, wie oben.

In jedem Fall sollte die Größe der auf der WAN Strecke übertragenen Pakete (oft als **MTU Size** bezeichnet) auf einen Wert kleiner 800 Bytes begrenzt werden. Damit wird sichergestellt, dass nicht größere Datenpakete trotz Priorisierung die Sprachdaten für längere Zeit während der Übertragung blockieren.

Manche Router können zwar priorisieren, können jedoch die einmal begonnene Übertragung großer Pakete nicht unterbrechen. Dies kann trotz Priorisierung zu schlechter Qualität führen. Prüfen Sie in einem solchen Fall, ob sich diese Unterbrechung gesondert anschalten lässt. Manche Router bezeichnen diese Funktion etwas verwirrend als **interleaving**.

Wenn Sie den Support in Anspruch nehmen müssen

Wenn Sie den Support Ihres Händlers in Anspruch nehmen müssen, sollten Sie folgende Informationen bereithalten:

- Die gesamte Konfiguration wie durch **Config show** angezeigt (siehe Kapitel 9.1.4 "Untermenü Config show" ab Seite 124),
- einen Trace, der die Fehlersituation zeigt (siehe Kapitel 9.1.3 "Untermenü Trace" ab Seite 123),
- die komplette Versionsbezeichnung des Gateways. Sie finden diese auf der Begrüßungsseite des Gateways (siehe Abbildung 39 auf Seite 122),
- die Seriennummer. Sie finden diese auf dem Seriennummernetikett auf der Unterseite des Gerätes oder auf der Begrüßungsseite des Gateways (siehe Abbildung 39 auf Seite 122).

Anhang C:ISDN Fehlerwerte

Die folgende Tabelle gibt die im Q.931 Standard definierten Fehlerwerte (**ISDN cause codes**) an.

Fehlerwert (hex)	Fehlerwert, Bit 8 zu 1 gesetzt (hex)	Fehlerwert (dezimal)	Bedeutung
0x1	0x81	1	Unallocated number
0x2	0x82	2	No route to specified transit network
0x3	0x83	3	No route to destination
0x6	0x86	6	Channel unacceptable
0x7	0x87	7	Call awarded and being delivered in an established channel
0x10	0x90	16	Normal call clearing
0x11	0x91	17	User busy
0x12	0x92	18	No user responding
0x13	0x93	19	No answer from user (user alerted)
0x15	0x95	21	Call rejected
0x16	0x96	22	Number changed
0x1A	0x9A	26	Non-selected user clearing
0x1B	0x9B	27	Destination out of order
0x1C	0x9C	28	Invalid number format
0x1D	0x9D	29	Facility rejected
0x1E	0x9E	30	Response to STATUS ENQUIRY
0x1F	0x9F	31	Normal, unspecified

Fehlerwert (hex)	Fehlerwert, Bit 8 zu 1 gesetzt (hex)	Fehlerwert (dezimal)	Bedeutung
0x22	0xA2	34	No circuit/channel available
0x26	0xA6	38	Network out of order
0x29	0xA9	41	Temporary failure
0x2A	0xAA	42	Switching equipment congestion
0x2B	0xAB	43	Access information discarded
0x2C	0xAC	44	Requested circuit/channel not available
0x2D	0xAD	47	Resources unavailable, unspecified
0x31	0xB1	49	Quality of service unavailable
0x32	0xB2	50	Requested facility not subscribed
0x39	0xB9	57	Bearer capability not authorised
0x3A	0xBA	58	Bearer capability not presently available
0x3F	0xBF	63	Service or option not available, unspecified
0x41	0xC1	65	Bearer capability not implemented
0x42	0xC2	66	Channel type not implemented
0x45	0xC5	69	Requested facility not implemented
0x46	0xC6	70	Only restricted digital information bearer capability is available

Fehlerwert (hex).	Fehlerwert, Bit 8 zu 1 gesetzt (hex).	Fehlerwert (dezimal).	Bedeutung.
0x4F	0xCF	79	Service or option not implemented, unspecified
0x51	0xD1	81	Invalid call reference value
0x52	0xD2	82	Identified channel does not exist
0x53	0xD3	83	A suspended call exists, but this call identity does not
0x54	0xD4	84	Call identity in use
0x55	0xD5	85	No call suspended
0x56	0xD6	86	Call having the requested call identity has been cleared
0x58	0xD8	88	Incompatible destination
0x5B	0xDB	91	Invalid transit network selection
0x5F	0xDF	95	Invalid message, unspecified
0x60	0xE0	96	Mandatory information element missing
0x61	0xE1	97	Message type non-existent or not implemented
0x62	0xE2	98	Message not compatible with call state
0x63	0xE3	99	Information element non-existent or nor implemented
0x64	0xE4	100	Invalid information element contents

Fehlerwert (hex)	Fehlerwert, Bit 8 zu 1 gesetzt (hex)	Fehlerwert (dezimal)	Bedeutung
0x65	0xE5	101	Message not compatible with call state
0x66	0xE6	102	Recovery on timer expiry
0x6F	0xEF	111	Protocol error, unspecified
0x7F	0xFF	127	Interworking, unspecified

Tabelle 23 ISDN Fehlerwerte

Anhang D:Der innovaphone DHCP Client

Die innovaphone Geräte unterstützen die automatische Konfiguration über Standard DHCP-Optionen. Zusätzlich unterstützen Sie einige anbieterspezifische innovaphone Optionen, die einige VoIP-spezifische Konfigurationen bewirken.

Diese Konfigurationen beinhalten:

- **POSIX Time Zone** (zur Definition der Zeitzone, in der das Gerät beheimatet ist),
- **VLAN ID** (die VLAN Identität für den Sprachverkehr),
- **VLAN Priority** (die VLAN Priorität für den Sprachverkehr),
- **TOS Bits** (der Wert des IP TOS Feldes im VoIP-Verkehr),
- **Enbloc dialling** (erzwungene Blockwahl) und
- Konfigurationsparameter für den **Update Server**.

Für Informationen bezüglich der DHCP Standardoptionen siehe Kapitel 4.1.1 "DHCP Konfigurationsoptionen" ab Seite 27.

Systemvoraussetzungen

Um die anbieterspezifischen DHCP Optionen nutzen zu können, ist ein DHCP Server notwendig, der diese Optionen unterstützt. Die gängigsten DHCP Server Implementierungen sind z. B. Microsoft Windows DHCP Service und Linux dhcpd.

Installation

Um für den DHCP Server die anbieterspezifischen DHCP Optionen nutzbar machen zu können, müssen diese Optionen dem Server bekannt gemacht werden. Die Begleitdokumentation Ihres DHCP Servers gibt Ihnen Auskunft, wie dies zu geschehen hat.

Im Nachfolgenden demonstrieren wir die Installation der innovaphone anbieterspezifischen DHCP Optionen am Beispiel von Windows 2000 DHCP Server.

- Starten Die den Windows 2000 DHCP Server (Start > Programme > DHCP).
- Zuerst müssen Sie eine neue Herstellerklasse definieren. Wählen Sie **Herstellerklasse definieren...** (**Define Vendor Class...**) im Menüeintrag des DHCP Server Kontextmenüs.
- Das Fenster **Neue Klasse** (**New class**) erscheint. Geben Sie im Feld **Anzeigename** (**Display name**) die Bezeichnung `innovaphone` ein.

- Im Feld **Beschreibung** (**Description**) tragen Sie `innovaphone VoIP Options` ein.
- Im Feld **ASCII:** tragen Sie den Wert `1.3.6.1.4.1.6666` ein. Dieser wird bei der Eingabe ebenso im Bereich **Binär:** dargestellt.
- Bestätigen Sie Ihre Eingabe durch Drücken der Schaltfläche **ok**.
- Schließen Sie das Fenster der **DHCP Herstellerklassen** (**DHCP vendor class**) durch Drücken der Schaltfläche **Schließen** (**close**).
- Wählen Sie **Vordefinierte Optionen einstellen** (**Configure predefined options**) im Menüeintrag des DHCP Server Kontextmenüs.
- Wählen Sie die **Optionsklasse innovaphone** (**option class innovaphone**), fügen Sie die innovaphone-spezifischen Optionen hinzu (siehe Tabelle 24) und übernehmen Sie die Werte durch Drücken der Schaltfläche **ok**.

Name	Data type	Array	Code
POSIX TZ	String	No	202
VLAN ID	Word (16bit)	No	206
VLAN Priority	Byte (8bit)	No	207
TOS Bits	String	No	208
Enbloc dialling	Byte (8bit)	No	209
Update URL	String	No	215
Update Poll Intervall	Word (16bit)	No	216

Tabelle 24 innovaphone-spezifische Optionen

Konfiguration

Um die innovaphone anbieterspezifischen DHCP Optionen für einen bestimmten Bereich zu konfigurieren, gehen Sie wie folgt vor:

- Wählen Sie den Eintrag **Optionen konfigurieren** (**Configure options**) im Kontextmenü der **Bereichsoptionen** (**Scope options**).
- Selektieren Sie die Registerkarte **Erweitert** (**Advanced**) und wählen Sie die **Herstellerklasse** (**DHCP vendor class**) `innovaphone`.

- Aktivieren Sie die Optionen, die Sie unterstützen wollen, vervollständigen Sie die entsprechenden Werte und übernehmen Sie diese.

Tabelle 25 zeigt die verfügbaren Optionen und ihre Bedeutung.

Option	Bedeutung	How to code
POSIX TZ	Definiert die Zeitzone und den Zeitpunkt der Zeitumstellung (Sommerzeit).	Tragen Sie die korrekte TZ Zeichenkette in das Feld, so wie Sie es im Konfigurationsapplet des Gerätes vornehmen würden. Siehe auch Kapitel 8.1.3 "Festlegen der Zeit- und Datumsquelle" ab Seite 112.
VLAN ID	Die 802.1q VLAN ID für vom Gerät gesendete und empfangene Daten.	Geben Sie die numerische ID in das 16bit Editierfeld ein.
VLAN Priority	Die 802.1p VLAN Priorität für vom Gerät gesendete Daten.	Geben Sie die numerische Priorität in das 8bit Editierfeld ein.
TOS Bits	Der Wert des IP TOS Feldes im IP-Header der vom Gerät gesendeten Gesprächsdaten.	Geben Sie die numerische Priorität in das Zeichenketten-Feld ein. Stellen Sie das Prefix `0x` vorn an, wenn Sie hexadezimale Zahlen eingeben bzw. beginnen Sie mit dem Prefix `0`, um oktale Nummern zu spezifizieren.

Option	Bedeutung	How to code
Enbloc dialling	Die Anzahl von Sekunden, die gewählte Ziffern in der IP 200 behalten werden, bevor Sie als Blockwahl zum Gatekeeper gesendet werden.	Tragen Sie die Anzahl Sekunden in das 8bit Editierfeld ein. Beim Wert `0` ist die Blockwahl deaktiviert und die gewählten Ziffern werden direkt bei der Eingabe zum Gatekeeper übermittelt.
Update URL	Speicherort der URL, von der Update-Kommandos abgerufen werden können. Diese ist identisch mit dem `/url` Optionsparameter des UP1-Modules.	Komplette URl wie z. B. `http://192.168.0.10/file.txt`. Es werden keine symbolischen Hostnamen unterstützt.
Update Poll Intervall	Standard Poll-Intervall in Minuten. Dies ist identisch mit dem `/poll` Optionsparameter des UP1-Modules.	Intervall in Minuten.

Tabelle 25 Verfügbare Optionen und Ihre Bedeutung

Stichwortverzeichnis

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z

innovaphone® AG
Böblinger Strasse 76
D-71065 Sindelfingen
Tel: +49 (70 31) 730 09-0
Fax: +49 (70 31) 730 09-99
www.innovaphone.com
info@innovaphone.com

CE