

# ***IP-Gateway***

***IP22***

***Administrator  
Handbuch***

**innovaphone**

***P u r e I P - T e l e p h o n y***

Warennamen werden ohne Gewährleistung der freien Verwendbarkeit benutzt. Fast alle Hardware- und Softwarebezeichnungen in diesem Handbuch sind gleichzeitig eingetragene Warenzeichen oder sollten als solche betrachtet werden.

Alle Rechte vorbehalten. Kein Teil dieses Handbuchs darf in irgendeiner Form (Druck, Fotokopie, Mikrofilm oder in einem anderen Verfahren) ohne ausdrückliche Genehmigung reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

Bei der Zusammenstellung von Texten und Abbildungen sowie bei der Erstellung der Software wurde mit größter Sorgfalt vorgegangen. Trotzdem lassen sich Fehler nicht vollständig ausschließen. Diese Dokumentation wird daher unter Ausschluss jedweder Gewährleistung oder Zusicherung der Eignung für bestimmte Zwecke geliefert. innovaphone behält sich das Recht vor, diese Dokumentation ohne vorherige Ankündigung zu verbessern oder zu verändern.

Copyright © 2001-2007 innovaphone® AG

# IP-Gateway

## IP22

### Handbuch Version 6.0

**Release 6.0, 3. Auflage, April 2007**

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

---

Copyright © 2001-2007 innovaphone® AG  
Böblinger Str. 76 71065 Sindelfingen  
Tel +49 (7031) 73009-0 Fax +49 (7031) 73009-99  
<http://www.innovaphone.com>

---

## Sicherheitshinweise

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

### Stromversorgung

Das Netzteil des Gerätes ist zum Betrieb an einem 100-240V, 50Hz Wechselstromnetz ausgelegt. Manche Geräte können auch durch PoE ( **P**ower-**o**ver-**E**thernet) nach IEEE 802.3af betrieben werden. Es sollte niemals versucht werden, das Gerät an andere Stromnetze anzuschließen! Bei Stromausfall bleiben die Einstellungen des Gerätes erhalten.

### Aufstellung und Anschluss

Die Anschlussleitungen sollten stolperfrei verlegt werden. Alle angeschlossenen Kabel dürfen nicht übermäßig geknickt 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, vibrierenden oder explosionsgefährdeten Räumen.
- bei Temperaturen über 40°C oder unter 0°C.

### Funktionsstörung

Unter bestimmungsgemäßen Betriebs- und Wartungsbedingungen ist es nicht erforderlich das Gerät zu öffnen. Sollte das Gerät jedoch aus irgendwelchen Gründen geöffnet werden, muss sicher gestellt werden, dass vorher alle Anschlusskabel entfernt wurden. Vor dem Öffnen des Gerätes, die Verbindung zur Stromversorgung durch Ziehen des Strom- oder Ethernetkabels trennen.

Ein defektes Gerät nicht öffnen und auch nicht mehr anschließen. Die Original-Verpackung für eine evtl. Rücksendung sollte gut aufbewahrt werden, da sie das Gerät optimal schützt. Zuvor sollten alle Einträge (z.B. auf einem PC) gesichert werden, um sich gegen Datenverlust zu schützen.

### Entsorgung

Soll das Gerät entsorgt werden, so muss dieses gemäß WEEE-Richtlinien (**W**aste-**E**lectrical-and-**E**lectronic-**E**quipment) direkt an den Hersteller die innovaphone-AG zurückgesendet werden. Die Kosten für die Rücksendung übernimmt dabei die innovaphone-AG.

# Inhaltsverzeichnis

<b>Sicherheitshinweise .....</b>	<b>4</b>
<b>Inhaltsverzeichnis .....</b>	<b>5</b>
<b>1 Einführung .....</b>	<b>9</b>
<b>1.1 Fax-Einbindung .....</b>	<b>9</b>
<b>1.2 Leistungsmerkmale für Telefonie .....</b>	<b>9</b>
<b>1.3 Leistungsmerkmale.....</b>	<b>9</b>
<b>2 Inbetriebnahme .....</b>	<b>10</b>
<b>2.1 Administratorzugang herstellen .....</b>	<b>10</b>
<b>3 Benutzeroberfläche.....</b>	<b>12</b>
<b>3.1 Aufbau der Benutzeroberfläche .....</b>	<b>12</b>
<b>3.2 Geschützte Bereiche .....</b>	<b>13</b>
<b>3.3 Speichern der Einstellungen .....</b>	<b>13</b>
<b>4 Konfiguration und Administration .....</b>	<b>14</b>
<b>4.1 Configuration .....</b>	<b>14</b>
4.1.1 Configuration/General.....	14
4.1.1.1 Configuration/General/Info .....	14
4.1.1.2 Configuration/General/Admin .....	15
4.1.1.3 Configuration/General/License .....	15
4.1.1.4 Configuration/General/Update.....	17
4.1.1.5 Configuration/General/NTP .....	17
4.1.1.6 Configuration/General/HTTP-Server.....	18
4.1.1.7 Configuration/General/HTTP-Client.....	19
4.1.1.8 Configuration/General/Logging.....	20
4.1.1.9 Configuration/General/SNMP.....	21
4.1.1.10 Configuration/General/Telnet .....	22
4.1.2 Configuration/IP .....	22
4.1.2.1 Configuration/IP/Settings.....	22
4.1.2.2 Configuration/IP/NAT .....	23
4.1.2.3 Configuration/IP/H.323-NAT .....	24
4.1.2.4 Configuration/IP/PPP-Config .....	25

4.1.2.5	Configuration/IP/PPP-State.....	29
4.1.2.6	Configuration/IP/Routing.....	30
4.1.3	Configuration/ETH0.....	30
4.1.3.1	Configuration/ETH0/Link .....	31
4.1.3.2	Configuration/ETH0/DHCP .....	31
4.1.3.3	Configuration/ETH0/IP .....	32
4.1.3.4	Configuration/ETH0/NAT .....	33
4.1.3.5	Configuration/ETH0/VLAN .....	33
4.1.3.6	Configuration/ETH0/DHCP-Server .....	34
4.1.3.7	Configuration/ETH0/DHCP-Leases.....	37
4.1.3.8	Configuration/ETH0/Statistics .....	38
4.1.4	Configuration/LDAP.....	39
4.1.4.1	Configuration/LDAP/Server .....	40
4.1.4.2	Configuration/LDAP/Server-Status.....	40
4.1.4.3	Configuration/LDAP/Replicator.....	41
4.1.4.4	Configuration/LDAP/Replicator-Status .....	41
4.1.5	Configuration/TEL1-2 .....	42
4.1.5.1	Configuration/TEL1-2/Physical .....	42
4.1.5.2	Configuration/TEL1-2/Signaling .....	42
<b>4.2</b>	<b>Administration.....</b>	<b>43</b>
4.2.1	Administration/Gateway .....	44
4.2.1.1	Administration/Gateway/General.....	44
4.2.1.1.1	Feature Codes.....	45
4.2.1.2	Administration/Gateway/Interfaces .....	49
4.2.1.2.1	Interface (ISDN- SIP- & virtuelle-Schnittstellen).....	49
4.2.1.2.2	CGPN-CDPN-Mappings .....	56
4.2.1.3	Administration/Gateway/VOIP .....	57
4.2.1.3.1	Interface (VoIP-Schnittstellen).....	58
4.2.1.3.2	CGPN-CDPN-Mappings.....	61
4.2.1.4	Administration/Gateway/Routes.....	61
4.2.1.4.1	From - To .....	62
4.2.1.4.2	CGPN-Maps.....	66
4.2.1.5	Administration/Gateway/CDR0-1.....	66
4.2.1.6	Administration/Gateway/Calls .....	68
4.2.2	Administration/Download.....	68

4.2.2.1	Administration/Download/Config .....	68
4.2.3	Administration/Upload .....	68
4.2.3.1	Administration/Upload/Config .....	69
4.2.3.2	Administration/Upload/Firmware .....	69
4.2.3.3	Administration/Upload/Boot .....	70
4.2.4	Administration/Diagnostics .....	70
4.2.4.1	Administration/Diagnostics/Logging .....	71
4.2.4.2	Administration/Diagnostics/Tracing.....	72
4.2.4.3	Administration/Diagnostics/Config Show .....	73
4.2.4.4	Administration/Diagnostics/Ping .....	74
4.2.5	Administration/Reset .....	74
4.2.5.1	Administration/Idle Reset .....	75
4.2.5.2	Administration/Reset/Reset.....	75
4.2.5.3	Administration/Reset/TFTP .....	75
<b>Anhang A:</b>	<b>Anschlüsse und Bedienelemente .....</b>	<b>76</b>
	Anzeigen und Anschlüsse.....	76
	Das Seriennummernetikett.....	78
<b>Anhang B:</b>	<b>Problembehebung .....</b>	<b>79</b>
	Typische Probleme.....	79
	Port-Einstellungen bez. NAT und Firewalls .....	81
	VoIP und stark belastete WAN-Strecken.....	82
<b>Anhang C:</b>	<b>ISDN-Fehlerwerte.....</b>	<b>84</b>
<b>Anhang D:</b>	<b>Support.....</b>	<b>88</b>
	Firmware Upload.....	88
	innovaphone Homepage .....	88
<b>Anhang E:</b>	<b>Konfiguration des Update-Servers.....</b>	<b>89</b>
	System Voraussetzungen.....	89
	Installation .....	89
	Konfiguration.....	90
	Wartungsdurchführung.....	90
	Wartungskommandos.....	90
<b>Anhang F:</b>	<b>Konfiguration eines NTP-Servers/-Clients.....</b>	<b>96</b>

Timezone-Strings (TZ-String): .....	96
<b>Anhang G: Anleitung zum Herunterladen von Lizenzen.....</b>	<b>98</b>
Login .....	98
Download .....	99
Ergebniss bestätigen.....	99
Ergebnis downloaden.....	100
<b>Anhang H: Glossar .....</b>	<b>101</b>
<b>Stichwortverzeichnis.....</b>	<b>125</b>



## 1 Einführung

Das vorliegende Handbuch beschreibt das innovaphone-VoIP-Gerät IP22. Der IP-Adapter IP22 ist ein analoger Terminal-Adapter (ATA), über den zwei analoge Endgeräte in die Umgebung der innovaphone-VoIP-Geräte eingebunden werden können. Er unterstützt die Protokolle SIP und H.323 mit allen benötigten Leistungsmerkmalen.

### 1.1 Fax-Einbindung

Die analogen Faxgeräte scheinen von der Evolution ausgenommen zu sein. Sie haben das ISDN-Zeitalter in Europa überstanden, ohne sich der neuen Technologie anzupassen und werden sich voraussichtlich auch nicht der VoIP-Technologie anpassen müssen. Statt dessen werden sie über geeignete Adapter in die neuen Umgebungen eingebunden. Der innovaphone Adapter IP22 arbeitet mit der stabilen und bewährten Implementation des Fax-over-IP Protokolls T.38 und bietet eine Steuerung wahlweise über SIP oder H.323 an.

### 1.2 Leistungsmerkmale für Telefonie

Auch analoge Telefone und Spezialtelefone mit analoger Schnittstelle können über den IP-Adapter IP22 eingebunden werden. Damit die Leistungsmerkmale der innovaphone-PBX weiterhin zur Verfügung stehen, kann mit üblichen Kombinationen von Steuerzeichen gearbeitet werden. So sind Makeln, Vermitteln und Konferenzen auch mit einfachen Geräten möglich.

### 1.3 Leistungsmerkmale

- 2 analoge Schnittstellen, separat freischaltbar
- gesicherte Fax-Übertragung mit "Fax over IP" (T.38)
- DTMF-Sequenzen für erweiterte PBX Leistungsmerkmale
- SIP- und H.323-Protokoll gleichzeitig
- Steckernetzteil, 110-240V oder "Power over LAN"

#### **Achtung**

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

## 2 Inbetriebnahme

Das Gerät wird durch Anschließen der externen Stromversorgung bzw. durch Speisung über PoE ( **P**ower-**o**ver-**E**thernet) nach IEEE (**I**nstitute- of **E**lectrical- and **E**lectrical-**E**ngineers) 802.3af eingeschaltet. Das Gerät ist eingeschaltet und betriebsbereit, wenn die Ready-LED auf der Gehäuse-Außenseite grün leuchtet. Das Gerät ist nicht Betriebsbereit wenn die Ready-LED rot leuchtet. Leuchtet die Ready-LED orange, dann befindet sich das Gerät im TFTP-Modus.

Um auf das Gerät zugreifen zu können, muss dessen RJ45-Ethernet-Anschluss (**ETH0**) mit dem RJ45-Ethernet-Anschluss des Ethernet-Hub oder Switch, mittels Twisted-Pair-Kabel verbunden werden. Optional kann das Gerät auch direkt mit einem PC verbunden werden. Hierfür wird kein zusätzliches Crossover-Kabel benötigt, da eine *Auto-MDX*<sup>2</sup>-Unterstützung der Ethernet-Schnittstelle gegeben ist.

### 2.1 Administratorzugang herstellen

Es gibt zwei Möglichkeiten das Gerät in Betrieb zu nehmen. Im Auslieferungszustand befindet sich das Gerät im so genannten *DHCP-Automatic-Modus*. In diesem Modus versucht das Gerät nach dem Einschalten eine IP-Adresse von einem DHCP-Server zu beziehen. Um festzustellen welche IP-Adresse dem Gerät zugewiesen wurde, kann unter Windows der Befehl **nbtstat** mit einem Kommandozeileninterpreter (z.B. DOS-Box) abgesetzt werden:

```
c:/ nbtstat -R (Lädt Remote Cache Tabelle neu)
```

```
c:/ nbtstat -a ipxxx-xx-xx-xx (Zeigt die IP-Adresse des angegebenen Remotecomputers anhand der eingegebenen MAC-Adresse an, wobei ipxxx mit der Gerätebezeichnung wie z.B. ip800 oder ip1200 und xx-xx-xx mit den letzten 6 Hexadezimalziffern der Seriennummer zu ersetzen ist)
```

```
NetBIOS Remote Machine Name Table
```

Name	Type	Status
ipxxx-xx-xx-xx<00>	UNIQUE	Registered
195-226-104-217<00>	UNIQUE	Registered

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

## **Achtung**

Die Anzeige der IP-Adresse mit **nbtstat** funktioniert nicht, wenn die NetBIOS Umgebung ausschließlich für die Namensauflösung über WINS konfiguriert ist. Findet das Kommando **nbtstat** das Gerät nicht, dann muss die NetBIOS Namensauflösung entsprechend konfiguriert werden.

Unter Linux kann hierzu das Kommando **nmblookup** verwendet werden, insofern das „SAMBA“ Package installiert ist:

```
[dvl@cobalt ~ 2]$ nmblookup ipxxx-xx-xx-xx
```

```
got a positiv name query response from 195.226.104.217
```

Dem Gerät wurde die IP-Adresse **195.226.104.217** zugewiesen. Es kann nun von jedem PC im gleichen Netz **195.226.104.x** auf das Gerät zugegriffen werden und wie gewünscht konfiguriert werden.

Sollte kein DHCP-Server vorhanden sein, kann durch ein kurzes Drücken der Reset-Taste die **ETH0**-Schnittstelle auf die konfigurierte IP-Adresse umgestellt werden. Wurde nicht explizit eine IP-Adresse konfiguriert, dann ist standardmäßig die IP-Adresse **192.168.0.1** angegeben.

## **Achtung**

Der *DHCP-Automatic-Modus* sollte sofort nach Inbetriebnahme des Gerätes umgestellt werden, da ein Reset die Betriebsart ändert (siehe auch Kapitel: „*Configuration/ETH0-1/DHCP*“).

## **Hinweis**

Die Inbetriebnahme des Gerätes betrifft nur die **ETH0**-Schnittstelle. Die **ETH1**-Schnittstelle besitzt während der Inbetriebnahme die feste IP-Adresse **192.168.1.1**.

## **Hinweis**

Der Auslieferungszustand wird durch einen langen Reset wiederhergestellt.

## 3 Benutzeroberfläche

Die Benutzeroberfläche ist mit dem Internet-Explorer 5.x, 6.x und auch dem Firefox-Browser getestet worden, lässt sich aber auch mit Netscape bedienen.

Die Benutzeroberfläche des VoIP-Gerätes kann durch Aufrufen der zuvor ermittelten IP-Adresse mit einem Webbrowser erreicht werden.

### 3.1 Aufbau der Benutzeroberfläche

Die Benutzeroberfläche des VoIP-Gerätes ist in zwei Bereiche aufgeteilt:

- Der Navigationsbereich (linker und oberer Bildschirmrand), welcher aus Menü- und Untermenüpunkten besteht.
- Der Eingabebereich, in dem die Einstellungen des Gerätes vorgenommen werden.

Die Hauptmenüs im linken Bereich des Browsers sind in zwei Kategorien unterteilt:

- **Configuration**
- **Administration**

Ein Hauptmenü kann wiederum in mehrere Untermenüs aufgegliedert sein.

## innovaphone IP22

Configuration	Info	Admin	License	Update	NTP	HTTP Server	HTTP Client	Logging	SNMP	Telnet
<b>General</b>										
IP										
ETH0										
LDAP										
TEL1										
TEL2										
<b>Administration</b>										
Gateway										
Download										
Upload										
Diagnostics										
Reset										

In der Kategorie **Configuration** wird all das vorgenommen, was beim Erstbetrieb notwendig ist. Zum Beispiel das Einstellen der Netzwerk Schnittstellen ETH0 & ETH1.

In der Kategorie **Administration** können die Einstellungen des laufenden Betriebes vorgenommen werden. Dazu gehört zum Beispiel das Hinzufügen neuer Benutzer zur innovaphone-PBX.

Je nachdem, welcher Hauptmenü Eintrag gerade aktiv ist oder auch je nachdem, welche Einstellung in einem Untermenü vorgenommen wurde, kann sich der Aufbau bzw. der Inhalt des Untermenüs verändern.

## 3.2 Geschützte Bereiche

Bis auf die Startseite sind alle Bereiche des Gerätes passwortgeschützt. Bei Auslieferung besitzt das innovaphone-VoIP-Gerät

- den Standard-Benutzer-Namen **admin** und
- das Standard-Benutzer-Kennwort **ipxxx** (ipxxx steht für die Geräteart, wie z.B: ip800, ip1200 etc.).

### **Achtung**

Um die Sicherheit des VoIP-Gerätes zu erhöhen, sollte der Standard-Benutzer und das Standard-Passwort in jedem Falle geändert werden (siehe Kapitel: „*Configuration/General/Admin*“)!

## 3.3 Speichern der Einstellungen

Das Speichern der Einstellungen im jeweiligen Untermenü erfolgt immer über die Schaltfläche **OK**.

- Manche Einstellungsänderungen benötigen einen Neustart des Gerätes, um wirksam zu werden. In diesem Fall wird im jeweiligen Menü *reset required* eingeblendet. Nähere Informationen zum Neustarten des Gerätes sind im Kapitel: „*Administration/Reset*“ enthalten.

## 4 Konfiguration und Administration

Der Aufbau des Kapitel: 4 „*Konfiguration und Administration*“ ist entsprechend dem Aufbau der Benutzeroberfläche strukturiert (*Kategorie/Hauptmenü/Untermenü*).

### 4.1 Configuration

In der Kategorie **Configuration** wird all das vorgenommen, was beim initialen Betrieb des Gerätes notwendig ist.

#### 4.1.1 Configuration/General

Über das Menü **General** können die Grundeinstellungen für das VoIP-Gerät vorgenommen werden.

##### 4.1.1.1 Configuration/General/Info

Allgemeine Informationen über das VoIP-Gerät werden hier angezeigt:

<b>Version</b>	<ul style="list-style-type: none"><li>• Die Software-Version (6.00) &lt;Gateway&gt;[firmware].</li><li>• Die Bootcode-Version &lt;Bootcode&gt;[firmware].</li><li>• Die Hardware-Version &lt;HW&gt;[nr].</li><li>• Die Speichergröße &lt;Flash/Ram&gt;.</li></ul>
<b>Serialno</b>	Die Seriennummer bzw. die MAC-Adresse ( <b>M</b> edia- <b>A</b> ccess- <b>C</b> ontrol) des Gerätes (6-stellige Hexadezimalzahl).
<b>Coder</b>	Die Anzahl und Art der Sprachkanäle.
<b>HDLC</b>	Die Anzahl der HDLC- Kanäle ( <b>H</b> igh-level- <b>D</b> ata- <b>L</b> ink- <b>C</b> hannels).
<b>Sync</b>	Die für die Synchronisation verwendete physikalische Schnittstelle (TEL, PPP, BRI, PRI).
<b>SNTP-Server</b>	Die IP-Adresse des verwendeten SNTP-Servers ( <b>S</b> imple- <b>N</b> etwork- <b>T</b> ime- <b>P</b> rotocol), sofern konfiguriert.
<b>Time</b>	Die lokale Zeit des Gerätes, gemäß den Angaben des NTP-Servers ( <b>N</b> etwork- <b>T</b> ime- <b>P</b> rotocol) und der Zeitzone.
<b>Uptime</b>	Die Betriebsdauer seit dem letzten Kalt- oder Warmstart.

## 4.1.1.2 Configuration/General/Admin

Der Administrator-Zugang wird hier konfiguriert.

<b>Device-Name</b>	Der Name des Gerätes. Dieser Name wird im Browser als Titel angezeigt.
<b>User-Name</b>	Der Administrator-Name.
<b>Password</b>	Das Administrator-Passwort, welches für alle geschützten Bereiche verwendet wird. Siehe Kapitel: 3.2 „ <i>Geschützte Bereiche</i> “.

## 4.1.1.3 Configuration/General/License

Hier werden die installierten Lizenzen des Gerätes angezeigt. Genauso können über dieses Menü auch zusätzliche Lizenzen aufgespielt werden.

Folgende Lizenzarten gibt es:

- **BRI-LIC** - Ermöglicht die Freischaltung eines S<sub>0</sub>-ISDN Kanals.
- **PRI-LIC** - Ermöglicht die Freischaltung eines S<sub>2</sub>M-ISDN Kanals.
- **DSP-LIC** - Ermöglicht die Freischaltung eines Sprachkanals im Digitalen Signalprozessor (DSP). Dies wird immer dann notwendig, wenn ein Übergang von der traditionellen TK-Welt (analog oder digital) zu IP geschaffen werden soll.
- **a/b-LIC** - Ermöglicht die Freischaltung eines analogen Kanals.
- **Gatekeeper-LIC** - Ermöglicht die Freischaltung einer Gatekeeper-Funktion. Dies wird immer dann notwendig, wenn man einen zentralen Gatekeeper für das Trunking mit mehreren Mediagateways benutzen möchte. Sie wird nicht benötigt, wenn man nur eine innovaphone PBX mit Home Usern anschließt, die die Telefone IP110/IP200/IP230 benutzen, ist aber dann sinnvoll, wenn man externe User, die beispielsweise an einer IP302 registriert sind, zentral verwalten möchte.
- **Basic-LIC** - Ermöglicht die Installation der PBX- und Voicemail-LIC. Sie ist Grundvoraussetzung zum Betreiben des innovaphone Media-Gateways als TK-Anlage. Je nach Anzahl der notwendigen Registrierungen an der PBX wird die passende Lizenzgröße ausgewählt. Einen groben Richtwert kann man durch die Anzahl der User angeschlossenen Geräte incl. Fax/DECT Handsets etc. zuzüglich 10-15% errechnen.

- **PBX-LIC** - Ermöglicht den Anschluss / die Registrierung eines Endgerätes ander innovaphone PBX. Die Bestelleinheit ist immer 10 LIC.
- **Voicemail-LIC** - Ermöglicht die Freischaltung der innovaphone Voicemail. Die Bestelleinheit muss identisch sein mit der Anzahl der Basis-Lizenzen, die auf dem Gerät installiert sind.

Alle Lizenzen werden gebunden an die MAC-Adresse des Gerätes, auf dem sie installiert werden.

Im oberen Abschnitt werden die bereits installierten Lizenzen angezeigt:

<b>Type</b>	Der installierte Lizenztyp (PBX, Relay oder DECT bei IP-DECT-Subsystem).
<b>Name</b>	Eine genaue Bezeichnung der Linzenz mit Angabe der Anzahl an Registrierungen gefolgt von der MAC-Adresse.
<b>Action</b>	Mit einem Klick auf den Button <b>download</b> können die angezeigten Lizenzen aus dem Gerät geladen und als Textdatei gesichert werden. Mit einem Klick auf den Button <b>delete</b> kann die angezeigte Lizenz aus dem Gerät gelöscht werden. Die Schaltflächen <b>download all</b> und <b>delete all</b> haben die gleiche Funktionalität wie die Schaltflächen <b>download</b> und <b>delete</b> , beziehen sich aber auf alle angezeigten Lizenzen.

Im unteren Abschnitt können zusätzliche Lizenzen aufgespielt werden:

Durch Angabe des Speicherortes des oben beschriebenen Lizenz-Textdatei im Eingabefeld **File** oder durch Wahl des Speicherortes mittels der **Durchsuchen...** Schaltfläche und einem anschließenden Klick auf **Upload** können zusätzliche Lizenzen auf das Gerät aufgespielt werden.

Mit diesem Upload sind die Lizenzen in der Konfiguration des Gerätes gespeichert und stehen nach einem kurzen Neustart zur Verfügung. Die installierte Lizenz wird angezeigt.



#### 4.1.1.4 Configuration/General/Update

Der Update-Server dient der effizienten Verwaltung verschiedener VoIP-Geräte. Von einer konfigurierbaren URL (**Uniform-Resource-Locator**) liest der Update-Server periodisch eine Datei.

**Command File URL** Eine URL, zum Beispiel `http://192.168.1.2/update/script-ip800.txt`, die auf den Speicherort einer Datei verweist, deren Befehle ausgeführt werden sollen.

Endet die URL mit einem Schrägstrich, zum Beispiel `http://192.168.1.2/update/`, fügt das Gerät den von seiner Kurzbezeichnung abgeleiteten Dateinamen `update-ipxxx.htm` an (z.B. `update-ip800.htm`).

Weiterhin können in der URL die Platzhalter `#h` und `#m` verwendet werden:

- `#h` - wird durch die Geräte Kurzbezeichnung ersetzt (z.B. IP800).
- `#m` - wird durch die MAC-Adresse des Gerätes ersetzt (z.B. 00-90-33-01-02-03).

Mit diesen Platzhaltern können z.B. Dateien in einem geräte-spezifischen Verzeichnis adressiert (`http://192.168.1.2/update/#h/script.txt`) oder auch HTTP-GET Parameter (`http://192.168.1.2/update/script.php?mac=#m`) generiert werden.

Handelt es sich bei dem Speicherort der Datei um einen passwortgeschützten Bereich, so muss die URL mitsamt Benutzer und Passwort unter dem Kapitel: „*Configuration/General/HTTP Client*“, angegeben werden.

**Interval [min]** Ein Intervall in Minuten, in dem die Datei jeweils neu gelesen und ausgeführt wird.

Detailliertere Informationen zum Update-Server und zum Update-Script sind im Anhang E: „*Konfiguration des Update-Servers*“ enthalten.

#### 4.1.1.5 Configuration/General/NTP

Das VoIP-Gerät ist durch Angabe eines NTP- (Network-Time-Protocol) Server in der Lage, seine interne Uhr mit einer externen Zeitquelle zu synchronisieren. Die-

se wird benötigt, da ohne Angabe eines Zeitserverns nach jedem Reset die interne Uhrzeit auf den 01.01.1970 0:00 Uhr zurückgesetzt wird.

<b>Server</b>	Die IP-Adresse des Zeitserverns.
<b>Interval [min]</b>	Die Zeit in Minuten, mit welchem Intervall sich das Gerät mit dem Zeitserver synchronisieren soll.
<b>Timezone</b>	Eine Auswahlmöglichkeit der Zeitzone, in der sich das Gerät befindet.
<b>String</b>	Es können zusätzliche Zeitzonen gemäß IEEE- (Institute-of-Electrical-and-Electronics-Engineers) POSIX- (Portable-Operating-System-Interface-for-Unix) Standard hinzugefügt werden.
<b>Last sync</b>	Zeigt das Datum und die Zeit der letzten Synchronisierung an.

Detailliertere Informationen zum NTP-Server sind im Anhang F: „*Konfiguration eines NTP-Servers/-Clients*“ enthalten.

#### 4.1.1.6 Configuration/General/HTTP-Server

Es können erweiterte, sicherheitsrelevante Einstellungen des VoIP-Gerätes vorgenommen werden.

<b>Disable HTTP basic authentication</b>	Die Anmeldedaten werden standardmäßig im Klartext und somit protokollier- und abhörbar übermittelt. Um diese Schwachstelle zu vermeiden empfiehlt es sich, die Standard-Authentifizierung (mit Benutzername und Passwort) zu deaktivieren und statt dessen die Digest-Hash-Authentifizierung zu verwenden.
<b>Password protect all HTTP pages</b>	Bis auf die Startseite <i>Configuration/General/Info</i> erfordern alle Bereiche der Benutzeroberfläche die Eingabe der Administrator-Nutzerkennung. Durch Aktivierung dieses Kontrollkästchens werden alle Seiten des Gerätes passwortpflichtig.
<b>Port</b>	Standardmäßig ist hier der HTTP-Port 80 eingetragen. Dieser kann geändert werden (z.B: 8080). Das Gerät ist dann nur noch über diesen port erreichbar (z.B: <IP des Gerätes>:8080).

**Allowed stations** Der Zugriff auf das Gerät kann auf einen bestimmten Netzbe-  
reich (z.B: *192.168.0.0 / 255.255.0.0*) oder auf eine  
bestimmte Netzadresse (z.B: *192.168.0.23 / 255.255.255.255*)  
eingeschränkt werden.

Zusätzlich werden unter dem Abschnitt **Active HTTP sessions** alle aktiven  
HTTP-Sessions angezeigt.

Zum Beispiel: **From** 172.16.1.49 **To** /HTTP0/info.xml **No** 22.

### 4.1.1.7 Configuration/General/HTTP-Client

Manche Dateien, auf die das Gerät über HTTP zugreifen muss (MoH, Ansage,  
Voicemail, etc.), befinden sich evtl. in einem passwortgeschützten Bereich. Hier  
können die unterschiedlichen URL's (**U**niform-**R**esource-**L**ocator) mit den  
jeweiligen Benutzernamen und Passwörtern hinterlegt werden.

**URL** Eine URL, zum Beispiel `http://192.168.1.2/update/  
script-ip800.txt`, die auf den passwortgeschützten Spei-  
cherort einer Datei verweist, deren Befehle ausgeführt werden  
sollen.  
Endet die URL mit einem Schrägstrich, zum Beispiel `http://  
192.168.1.2/update/`, fügt das Gerät den von seiner Kurz-  
bezeichnung abgeleiteten Dateinamen `update-ipxxx.htm`  
an (z.B. `update-ip800.htm`).  
Auch hier können in der URL die Platzhalter `#h` und `#m` ver-  
wendet werden:

- `#h` - wird durch die Geräte Kurzbezeichnung ersetzt (z.B  
IP800).
- `#m` - wird durch die MAC-Adresse des Gerätes ersetzt (z.B.  
00-90-33-01-02-03).

Mit diesen Platzhaltern können z.B. Dateien in einem geräte-  
spezifischen Verzeichnis adressiert (`http://192.168.1.2/  
update/#h/script.txt`) oder auch HTTP-GET Parameter  
(`http://192.168.1.2/update/script.php?mac=#m`)  
generiert werden.

**User** Der berechtigte Benutzer der Zugriff auf das Verzeichnis hat.

**Password** Das zugehörige Passwort des Benutzers.

## 4.1.1.8 Configuration/General/Logging

Das externe Logging ist standardmäßig deaktiviert (**Off**). Nach Auswahl eines Log-Types wird das Logging aktiviert und die entsprechenden Eingabefelder freigeschaltet.

**Off** Logging ist deaktiviert.

**TCP** Das Gerät sendet die Syslog-Einträge über eine TCP- (**T**ransmission-**C**ontrol-**P**rotocol) Verbindung.

- In das Eingabefeld **Address** wird die IP-Adresse eingetragen, zu welcher die TCP-Verbindung aufgebaut werden soll.
- Im Eingabefeld **Port** wird der Port angegeben, zu dem die Verbindung aufgebaut wird.

**SYSLOG** Die Syslog-Einträge werden an einen Syslog-Empfänger übermittelt (wird auch als `syslogd`, `syslog-server` oder `syslog-daemon` bezeichnet). Dieser ist dann für die weitere Auswertung oder Abspeicherung zuständig.

- In das Eingabefeld **Address** wird die IP-Adresse des `syslogd`-Servers eingetragen.
- Im Eingabefeld **Class** wird die gewünschte Meldungs-klasse eingetragen, die für die weitere Verarbeitung der Syslog-Einträge zuständig sein soll. Die Syslog-Klasse ist ein numerischer Wert zwischen 0 und 7.

## HTTP

Die Syslog-Einträge werden an einen Webserver übertragen und können dort weiter verarbeitet werden. Jeder einzelne Syslog-Eintrag wird als Formulardaten im HTTP-GET-Format an den Webserver übertragen.

- In das Eingabefeld **Address** wird die IP-Adresse des Web-servers eingetragen, der die Weiterverarbeitung der über-mittelten Daten übernimmt.
- In das Eingabefeld **Path** wird die relative URL des Formu-larprogramms auf dem Webserver eingegeben.

Das Gerät wird zum Webserver einen HTTP-GET-Request auf die eingetragene URL, gefolgt vom url-encodeten Sys-log-Eintrag stellen. Besteht beispielsweise auf einem Web-server eine Seite namens `/cdr/cdrwrite.asp` mit einem Formular, das die Log-Meldung im Parameter `msg` erwartet, dann wird der Wert `/cdr/cdrwrite.asp` ein-getragen. Das Gerät wird dann einen `GET /cdr/cdr-write.asp?event=syslog&msg=logmsg` Request an den Webserver stellen.

### 4.1.1.9 Configuration/General/SNMP

Das VoIP-Gerät bietet die Möglichkeit der Überwachung des Betriebszustandes per SNMP (**S**imple-**N**etwork-**M**anagement-**P**rotocol mit Version 1.0). Unterstützt wird die Standard-MIB-II, sowie eine herstellerspezifische MIB (**M**anagement-**I**nformation-**B**ase). Detaillierte Informationen über diese MIB, können bei einem zertifizierten innovaphone-Händler bezogen werden oder direkt im Download-Bereich der innovaphone-Homepage (<http://www.innovaphone.com>) heruntergeladen werden.

**Community** Falls nicht der Standard-Community-Name *public* verwendet wird, kann ein anderer Community-Name in dieses Feld einge-tragen werden.

**Device Name** Zur detaillierteren Information kann hier dem SNMP-Agenten ein Geräte Name angegeben werden.

**Contact** Sowie auch eine Kontaktperson (**Contact**).

<b>Location</b>	Genauso einen Standort ( <b>Location</b> ).
<b>Authentication Trap</b>	Der Zugriff per SNMP ist nur möglich unter der Angabe des richtigen Community-Namen. Sollte dieses Kontrollkästchen markiert sein, wird bei einem Zugriff mit falschem Community-Namen ein Trap generiert.
<b>Trap Destinations</b>	Soll das Gerät die in der herstellerspezifischen innovaphone-MIB definierten Traps auslösen, so müssen zusätzlich noch Ziele für Trap-Meldungen definiert werden.
<b>Allowed Networks</b>	Zur Erhöhung der Sicherheit kann der Zugriff auf das Gerät beschränkt werden, indem der Zugriff per SNMP auf eine feste Liste von Rechnern oder IP-Adressbereichen beschränkt wird.

#### 4.1.1.10 Configuration/General/Telnet

Hier kann der Zugriff über das Telnet-Protokoll aktiviert werden.

<b>Enable Telnet</b>	Ein markiertes Kontrollkästchen aktiviert den Zugriff auf das Gerät mittels telnet. Mit Befehlen wie z.B: <i>reset</i> , <i>config change UP1 /url &lt;http url&gt; /poll &lt;secs&gt;</i> kann das Gerät konfiguriert werden.
----------------------	--

#### 4.1.2 Configuration/IP

Hier werden allgemeine IP-Protokoll-Einstellungen vorgenommen, sowie auch die Konfiguration des VPN-Protokolls PPTP, des DSL-Protokolls PPPOE und der Adressen-Umsetzung mit NAT.

##### 4.1.2.1 Configuration/IP/Settings

Die grundlegenden IP-Einstellungen werden hier vorgenommen.

<b>ToS Priority</b>	Konfiguration des ToS-Feldes ( <b>Type-of-Service</b> ) bei Sprachpaketen. Standardmäßig wird der Wert $0 \times 10$ verwendet. Damit werden Sprachdaten bevorzugt weitergeleitet.
---------------------	--

## **First UDP-RTP port / numbers of port**

Diese Angabe schränkt den Bereich an Ports ein, in welchem UDP-RTP-Sprachdaten (**U**ser-**D**atagram-**P**rotocol, **R**eal-time-**T**ransport-**P**rotocol) für H.323- oder SIP-Rufe empfangen werden. Standardmäßig wird der Port Bereich 16384 bis 32767 verwendet. Der kleinste Bereich sind 128 Ports. Für eine Sprachverbindung wird ein RTP-Port und ein RTCP-Port verwendet.

Siehe auch Hinweise im Anhang B: „*Problembhebung*“ Abschnitt „*Port-Einstellungen bez. NAT und Firewalls*“.

## **First UDP-NAT port / numbers of port**

Diese Angabe schränkt den Bereich an Ports ein, die UDP-NAT-Daten (**N**etwork-**A**ddress-**T**ranslation) verwenden dürfen.

## **Private Networks**

Durch Angabe eines privaten Netzwerkes, kann das Gerät die Media-Relay-Funktion steuern. Die Media-Relay-Funktion braucht man zum Beispiel um NAT-Probleme zu lösen. Die PBX und das RELAY verwenden bei einem Ruf immer dann automatisch die Media-Relay-Funktion, wenn sie feststellen, dass ein VoIP-Gespräch zwischen dem privaten und dem öffentlichen (public) Netz verläuft. Dabei wird immer in der Private-Network Konfiguration nachgeschaut, ob sich die Calling- und die Called-Party-Number im selben IP-Netz befindet.

Wird hier nichts eingetragen, dann wird angenommen, dass beide Parteien im öffentlichen (public) Netzwerk liegen, wodurch die Media-Relay-Funktion nicht verwendet wird und RTP-Pakete direkt zwischen den Endpunkten ausgetauscht werden. Durch Angabe eines privaten Netzwerkes werden RTP-Pakete zwischen den Endgeräten nicht direkt durchgereicht sondern zwischen dem internen und externen Netz über das Gerät geroutet.

### **4.1.2.2 Configuration/IP/NAT**

Das Telefon ist in der Lage IP-Endgeräte aus dem Netz mit einer nicht öffentlichen Adresse mit dem öffentlichen Internet zu verbinden. Dazu ist eine **Network-Address-Translation (NAT)** notwendig. NAT dient als Router und bedarf einer

Konfiguration des PPOoE Protokoll.

Die dafür notwendigen Parameter dieser Konfiguration können hier eingestellt werden:

- Enable NAT** Ein markiertes Kontrollkästchen aktiviert NAT generell. Diese Funktion wird nur benötigt, wenn das IP-Telefon gleichzeitig ein DSL-Router ist.
- Default forward destination** Sollen standardmäßig alle eingehenden Datenpakete an eine bestimmte IP-Adresse weitergeleitet werden, so muss hier die Ziel-IP-Adresse eingetragen werden.
- Port specific forwardings** Um mehrere interne Ziele ansprechen zu können, werden hier unterschiedliche Port-Nummern auf IP-Adressen des internen Netzwerkes zugeordnet.

#### 4.1.2.3 Configuration/IP/H.323-NAT

H.323-NAT ist ein add-on für die allgemeine NAT-Funktion. Diese Funktion wird nur gebraucht, wenn das Telefon das private mit dem öffentlichen Netz verbindet. Das Telefon muss demnach eine Verbindungsstelle zwischen dem öffentlichen und dem privaten Netz darstellen. Diese Funktion ermöglicht H.323-Gespräche zwischen privaten und öffentlichen Netzen.

- Enable H.323-NAT** Aktiviert NAT für H.323 VoIP-Gespräche.
- Require authentication** Ein markiertes Kontrollkästchen setzt die H.323-Authentifizierung voraus. Diese Option gilt als eine Sicherungsmaßnahme vor fremden Zugriffen auf das eigene private Netz. H.323-Nachrichten ohne Authentifizierung werden nicht in das private Netz geleitet.
- H.225/RAS destination** IP-Adresse des Servers im privaten Netz, an den eingehende H.225/RAS-Nachrichten geleitet werden.
- H.225/Signalling destination** IP-Adresse des Servers im privaten Netz, an den eingehende H.225/Signalling-Nachrichten geleitet werden.

Im Abschnitt **Status** erhält man eine kleine Übersicht über die registrierten Benutzer (**Registered Clients**) und die gerade aktiven Anrufe (**Active Calls**).



#### 4.1.2.4 Configuration/IP/PPP-Config

Hier werden die Parameter für die DSL- und VPN-Verbindungen eingestellt.

Ein Klick auf die Interface-ID (**PPPn**) öffnet die jeweilige Konfigurationsseite, in der die PPP-Schnittstellen-Konfiguration vorgenommen werden kann.

Abschnitt **PPP Interface PPPn:**

<b>Enable</b>	Aktiviert / Deaktiviert die Schnittstelle. Die PPP-Schnittstelle wird in der Übersichtsseite PPP-State nur dann angezeigt, wenn sie aktiviert (Enable) ist.
<b>Connection Port</b>	Für PPP-Verbindungen über ISDN-Kanäle wird hier eines der ISDN-Interfaces (PPP, TEL, BRI, PRI) gewählt. Dies betrifft nur Geräte mit einer ISDN-Schnittstelle. Es sind aber auch PPTP (VPN)- und PPPoE (DSL)- Verbindungen über die Ethernet-Schnittstelle (ETH) möglich.
<b>Descriptiv Name</b>	Hier kann ein beschreibender Name für die Schnittstelle eingegeben werden. Dieser Name dient der Übersicht im Untermenü PPP-State (siehe Kapitel: „ <i>Configuration/IP/PPP-State</i> “).
<b>Bandwidth</b>	Durch Angabe einer bestimmten Bandbreite kann die Übertragungsrate bei einem connect eingegrenzt werden, womit gleichzeitig die verfügbare Netzwerk Bandbreite optimal aufgeteilt wird. Dies ist notwendig da bei einem Upstream eine geringere Bandbreite zur Verfügung stehen kann als benötigt. Pakete die über die maximal verfügbare Bandbreite hinaus gehen, würden verworfen. Durch Angabe einer Bandbreite werden Pakete die über die maximal verfügbare Bandbreite hinausgehen erst gar nicht abgeschickt.
<b>Maximum transfer unit (Bytes)</b>	Grenzt die Paketgröße bei einem Datenaustausch ein. Dies ist bei manchen Geräten nötig, die nur eine begrenzte Anzahl Bytes übertragen können. Nachfolgend ein paar typische MTU-Größen in Oktetts: <ul style="list-style-type: none"> <li>• X.25 - 576</li> <li>• PPoE (z.B: DSL) - 1492</li> <li>• ISDN, Ethernet - 1500</li> <li>• ATM - 4500</li> </ul>
<b>IP Address for Remote Party</b>	Weist der Gegenseite eine lokale IP-Adresse zu, um sie in das lokale Netz einzubinden.

<b>Auto dial after boot</b>	Bewirkt, dass die entsprechende PPP-Verbindung des Gerätes sofort nach dem Starten aufgebaut und offen gehalten wird.
<b>Allow inbound connections</b>	Als PPP-Server konfiguriert erlaubt ein markiertes Kontrollkästchen PPP-Wahlverbindungen, die auf dem Gerät eingehen (inbound).
<b>No DNS on this interface</b>	Bei einem PPP-Verbindungsaufbau zur Gegenseite wird standardmäßig immer versucht, den Namen der Gegenseite über DNS in eine IP-Adresse aufzulösen. Hier besteht jedoch die Gefahr, dass mehrere PPP-Verbindungen bestehen können, die die gleiche IP-Adresse (z.B: 192.168.1.2) verwenden. Somit würde nur einmal eine Namensauflösung stattfinden und die Datenpakete, die an einen anderen Namen mit der gleichen IP-Adresse gesendet wurden, gehen verloren.
<b>Exclude interface from NAT</b>	Mit dieser Option kann ein bestimmtes Interface von der NAT ( <b>Network-Address-Translation</b> ) ausgeschlossen werden, sollte NAT aktiviert sein (siehe Kapitel: „ <i>Configuration/IP/NAT</i> “).
<b>No IP Header compression</b>	Die VoIP-Geräte unterstützen die Kompression von Sprachdaten auf der PPP-Strecke nach dem Verfahren <b>RTP Header Compression</b> (RFC 2508, 2509). Dadurch wird die benötigte Bandbreite für VoIP-Gespräche drastisch reduziert. Um dies zu unterdrücken, muss das Kontrollkästchen <b>No IP Header compression</b> aktiviert werden.
<b>Adapt to Cisco PPP peers</b>	Wird auf der Gegenseite ein Cisco-Router eingesetzt und es kommt bei der Übertragung von Sprachdaten zu Problemen, dann könnte die Option <b>Adapt to Cisco PPP peers</b> Abhilfe schaffen.

## Abschnitt **Authentication**:

Das PPP-Protokoll erlaubt eine gegenseitige Authentifizierung (inbound/outbound). In der Regel wird bei eingehenden Verbindungen nur die **inbound**- und bei abgehenden nur die **Outbound**-Authentifizierung benötigt. Es kann aber auch vorkommen, dass sowohl vom Client als auch vom Server eine Authentifi-

zierung benötigt wird.

**Outbound User / Password** Bei ausgehenden Verbindungen benötigt. Zum Beispiel der Name des DSL-Providers bzw. der DSL-Benutzerkennung der Gegenseite (1564863maxmuster.1und1.de, 1564863maxmuster@t-online.de) oder der Inbound User / Password der Gegenseite.

**Inbound User / Password** Bei eingehenden Verbindungen benötigt. Zum Beispiel der Outbound User / Password eines anderen Gateways.

## Abschnitt **PPPOE**:

Hier kann die Schnittstelle als PPPoE-Client (z.B. für DSL) konfiguriert werden.

**DSL Provider (Access Concentrator)** Der DSL-Modem Name. Da mehrere Modems in einem Netz vorkommen können wird ein Broadcast zur Identifikation gesendet wird.

## Abschnitt **PPTP**:

Diese Betriebsart gilt für ein- und ausgehende Rufe. Das PPTP (Point-to-Point-Tunneling-Protokoll) realisiert private VPN-Verbindungen über das Internet oder andere mit dem IP-Protokoll betriebene Netzwerke.

PPTP-Verbindungen sind grundsätzlich Wählverbindungen. Gewählt wird eine IP-Adresse. Die Authentifizierung erfolgt über Benutzername und Passwort. Zusätzlich können die übertragenen Sprachdaten mit der MPPE (**M**icrosoft-**P**oint-to-**P**oint-**E**ncryption) verschlüsselt werden. Voraussetzung ist jedoch, dass auch die Gegenseite das Verfahren unterstützt. Wurde die MPPE aktiviert, kann es zur Verzögerung der Sprache führen. Treten derartige Qualitätsverluste auf, muss zwischen der Sicherheit oder der Sprachqualität selbst entschieden werden.

Die innovaphone Geräte können sich sowohl als PPTP-Client in einen fernen PPTP-Server einwählen als auch selbst einen Einwahlpunkt zur Verfügung stellen.

**Server Address** Die IP-Adresse des PPTP-Servers. Soll das Gerät selbst die Rolle eines PPTP-Servers spielen, dann muss hier keine IP-Adresse angegeben werden.

<b>Route to Interface</b>	Hier können Verbindungsaufbau-Anfragen direkt an ein bestimmtes Interface weitergeleitet werden. Zum Beispiel: ETH0-1, PPP0-31.
<b>Enable MPPE Encryption</b>	Aktiviert das Microsoft Point-To-Point-Encryption-Protocol. MPPE (RFC 3078) benutzt den RSA-RC4-Algorithmus.
<b>Stateless Operation</b>	Dabei wird der Schlüssel nach jedem übertragenem Paket geändert.
<b>40-Bit Encryption</b>	Aktiviert die Verschlüsselung mit einem 40Bit-Session-Key.
<b>128-Bit Encryption</b>	Aktiviert die Verschlüsselung mit einem 128Bit-Session-Key verwendet.

## Abschnitt **ISDN**:

<b>Link Configuration</b>	Hier kann die ISDN-Schnittstellenkonfiguration vorgenommen werden. Die PPP-Schnittstelle kann hier sowohl für eingehende als auch für ausgehende Rufe konfiguriert werden.
<b>Link type</b>	Es können vier verschiedenen Link-Typen gewählt werden. <b>Singlelink (64k)</b> - Eine Verbindung über einen B-Kanal. <b>Multilink (128k)</b> - Eine Verbindung über zwei gebündelte B-Kanäle. Stellt die doppelte Übertragungsgeschwindigkeit zur Verfügung. <b>Permanent B1</b> - Verwendet ausschließlich den B1-Kanal. <b>Permanent B2</b> - Verwendet ausschließlich den B2-Kanal.
<b>Local Subscriber Number</b>	Die <b>Local Subscriber Number</b> ist bei eingehenden Wahlverbindungen die Rufnummer (MSN), unter der eingehende Rufe akzeptiert werden sollen. Die <b>Local Subscriber Number</b> ist bei ausgehenden Wahlverbindungen die für den Ruf zu verwendende ausgehende Rufnummer (MSN).
<b>2nd Local Subscriber Number</b>	Wird <b>Multilink</b> verwendet, kann für den zweiten Kanal der zu rufenden PPP-Gegenstelle eine andere Rufnummer verwendet werden. Das Eingabefeld kann unausgefüllt bleiben, sollte die gleiche Rufnummer wie für den ersten Kanal verwendet werden können.

<b>Outbound Conne- ctions</b>	Hier kann die ISDN-Schnittstelle für ausgehende PPP-Wahlverbindungen konfiguriert werden.
<b>Called Party Num- ber</b>	Die für den ausgehenden Ruf zu verwendende Rufnummer (MSN).
<b>2nd Called Party Num- ber</b>	Die für den ausgehenden Ruf zu verwendende Rufnummer (MSN) auf dem zweiten B-Kanal.
<b>Inbound Conne- ctions</b>	Hier kann die ISDN-Schnittstelle für eingehende PPP-Wahlverbindungen konfiguriert werden.
<b>Calling Party Num- ber</b>	Mit Angabe der <b>Calling Party Number</b> kann die Annahme von eingehenden Rufen auf diese eine Rufnummer begrenzt werden. Sollte das Eingabefeld unausgefüllt bleiben, werden alle Datenrufe auf der/den gewählten ISDN-Schnittstelle/n akzeptiert.

#### Abschnitt **IP Routes**:

Hier können statische Routen für das PPP-Interface konfiguriert werden. Das ist erforderlich, da kein Routingprotokoll verwendet wird.

<b>Network Address</b>	Die Netzwerk-Adresse der neu hinzuzufügenden Route.
<b>Network Mask</b>	Die Netzwerk-Maske der neu hinzuzufügenden Route.
<b>Gateway</b>	Die Netzwerk-Adresse des default Gateways.

#### **4.1.2.5 Configuration/IP/PPP-State**

Es wird der Status für alle definierten und aktivierten PPP-Schnittstellen werden hier angezeigt. Zusätzlich besteht die Möglichkeit manuell die Verbindung zu schließen und wieder aufzubauen.

<b>Interface</b>	ID der PPP-Interfaces.
<b>Address</b>	Die lokale IP-Adresse des PPP-Interfaces.

<b>Type</b>	Der Typ des Interfaces. PPTP, PPPoE oder, falls es sich um PPP über einen ISDN-Kanal handelt, eine der ISDN-Schnittstellen.
<b>State</b>	Zeigt den aktuellen Zustand des Interfaces an. Mögliche Zustände: <i>Connecting</i> , <i>Up</i> oder <i>Down</i> .
<b>Since</b>	Hier wird die Zeit angegeben, seit wann die Verbindung besteht.
<b>Action</b>	<ul style="list-style-type: none"><li>• <b>connect</b> stellt eine Verbindung zum gewählten Interface her.</li><li>• <b>clear</b> löscht die aktuelle Verbindung zum gewählten Interface.</li><li>• <b>info</b> zeigt relevanten Verbindungsdaten des gewählten Interfaces an.</li></ul>
<b>Name</b>	Die Bezeichnung der Schnittstelle bzw. der Verbindung.

#### 4.1.2.6 Configuration/IP/Routing

Hier wird die Routing-Tabelle der aktuellen **IP-Konfiguration** des Gateways angezeigt. Die Tabelle dient der Fehleranalyse für den Administrator des Netzwerkes. Die Tabelle ist wie folgt aufgebaut:

<b>Destination Network</b>	Die Ziel-Netzwerk-Adresse.
<b>Network Mask</b>	Die zugehörige Netzwerk-Maske.
<b>Gateway</b>	Die IP-Adresse des Default Routers.
<b>Interface</b>	Zeigt die Schnittstelle an, auf der die Route angelegt wurde. Mögliche Schnittstellen sind: <i>ETH0</i> , <i>ETH1</i> , <i>PPP0-31</i> , <i>Local</i> und <i>ISDN</i> .
<b>State</b>	Mögliche Zustände sind: <i>Up</i> oder <i>Down</i> .

#### 4.1.3 Configuration/ETH0

Hier kann die Ethernet-Schnittstelle (**ETH0**) des Gerätes konfiguriert werden. Für die Ethernet-Schnittstelle werden *CAT5-STP*-Kabel empfohlen.

## 4.1.3.1 Configuration/ETH0/Link

Die Übertragungsart der Ethernet-Schnittstelle wird hier festgelegt.

Standardmäßig ist die Übertragungsart **auto** selektiert:

<b>auto</b>	Automatische Wahl der Übertragungsgeschwindigkeit.
<b>10m-hdx</b>	Entspricht 10-MBit-Half-Duplex.
<b>10m-fdx</b>	Entspricht 10-MBit Full-Duplex.
<b>100m-hdx</b>	Entspricht 100-MBit Half-Duplex.
<b>100m-fdx</b>	Entspricht 100-MBit Full-Duplex.

Zusätzlich wird noch der Status der Schnittstelle (*Up* bzw. *Down*) und die verwendete Autonegotiation (z.B.: *100m-fdx*) angezeigt.

## 4.1.3.2 Configuration/ETH0/DHCP

Die DHCP-Funktion kann entweder ausgeschaltet im *DHCP-Disabled*-Modus oder im *DHCP-Client*- bzw. im *DHCP-Server-Modus* betrieben werden. Die DHCP-Funktion der Ethernet-Schnittstelle hat insgesamt vier Betriebsmodi:

<b>Disabled</b>	Die IP-Adresse und andere Parameter werden manuell konfiguriert.
<b>Server</b>	Die IP-Parameter werden im <i>DHCP-Server-Modus</i> manuell konfiguriert (Standard-IP-Adresse <b>192 . 168 . 0 . 1</b> ). Der DHCP-Server ist an und sollte wie im Kapitel: „ <i>Configuration/ETH0-1/DHCP-Server</i> “ entsprechend konfiguriert werden.
<b>Client</b>	Im <i>DHCP-Client-Modus</i> erhält das Gerät seine IP-Konfiguration von einem DHCP-Server, an dessen Netzwerk das Gerät angeschlossen ist.
<b>Automatic</b>	Nach dem erstmaligen Einschalten des Gerätes (Power-Up) arbeitet <b>ETH0</b> als DHCP-Client. Nach einem Neustart durch kurzes Drücken der Reset-Taste, wird der <b>ETH0</b> -Schnittstelle die konfigurierte IP-Adresse vergeben. Wurde nicht explizit eine IP-Adresse konfiguriert (siehe Kapitel: „ <i>Configuration/ETH0-1/IP*</i> “), dann ist standardmäßig die IP-Adresse <b>192 . 168 . 0 . 1</b> angegeben.

Im Auslieferungszustand ist **ETH0** im *DHCP-Automatic-Modus* mit der IP-Adresse 192.168.0.1 und **ETH1** im *DHCP-Disabled-Modus* mit der IP-Adresse 192.168.1.1 konfiguriert.

## **Achtung**

Der *DHCP-Automatic-Mode* sollte **nicht** für den 'normalen' Betrieb verwendet werden, da ein versehentlicher Neustart die Betriebsart umschaltet.

### **4.1.3.3 Configuration/ETH0/IP**

Die manuellen Konfigurations-Einstellungen sind wirksam wenn der DHCP-Modus *Disabled* oder *Server* konfiguriert ist. Rechts neben den Eingabefeldern werden immer die aktuell gespeicherten Einstellungen angezeigt.

- IP Address** Die IP-Adresse des Netzwerkadapters.
- Network Mask** Die Subnet-Mask des Netzwerkadapters.
- Default Gateway** Der Standard-Router des LANs.
- DNS Server** Der DNS-Server des LANs.
- Proxy-ARP** Bei IP-Paketen, die vom Ethernet über das Gerät auf PPP-Schnittstellen geroutet werden, kann sich das Gerät 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 Routing-einstellung verfügen über das Gerät kommunizieren und die WAN-Verbindung nutzen. Um den Einwahlzugriff auf das gesamte Netz zu erlauben, muss die Proxy-ARP Funktion aktiviert werden.
- Multicast** Mit der Option Multicast besteht die Möglichkeit, die zu versendenden Datenpakete an alle Geräte in einem Netz zu senden. Standardmäßig werden Datenpakete an alle Geräte in einem Netz versendet. Das Kontrollkästchen Multicast ist somit markiert.

Im Abschnitt **Static IP Routes** können zusätzliche Netzwerkrouen definiert werden, sollten ausser dem lokalen Netz noch andere Netzbereiche benötigt



werden.

<b>Network Destination</b>	Die Netzwerkadresse der Zielroute.
<b>Network Mask</b>	Die entsprechende Subnet-Mask der Zielroute.
<b>Gateway</b>	Das Standard-Gateway des zu routenden Netzes.

#### 4.1.3.4 Configuration/ETH0/NAT

Hier läßt sich die Verwendung von NAT (**N**etwork-**A**ddress-**T**ranslation) für die entsprechende Schnittstelle aktivieren. Zusätzlich besteht die Möglichkeit, bestimmte Netzwerk-Adressen und Masken von der Übersetzung auszuschliessen.

<b>Include Interface in NAT</b>	Ein markiertes Kontrollkästchen aktiviert NAT für das Interface, sofern NAT unter dem Kapitel: „ <i>Configuration/IP/NAT</i> “ generell aktiviert wurde. D.h.: Das an <i>ETHn</i> angeschlossene Netz wird als extern betrachtet, es sei denn, es wurde unter <b>Exclude Adress</b> oder <b>Exclude Mask</b> exkludiert.
<b>Exclude Address</b>	IP-Netz, das nicht in die Network-Address-Translation inkludiert werden soll.
<b>Exclude Mask</b>	IP-Netzbereich, welcher nicht in die Network-Address-Translation inkludiert werden soll.

#### 4.1.3.5 Configuration/ETH0/VLAN

Verwendet ein Netzwerk mehrere VLANs (**V**irtual-**L**ocal-**A**rea-**N**etwork), so kann für jede Ethernet-Schnittstelle ein VLAN angegeben werden. Somit wird sichergestellt, dass die Datenpakete ausschließlich in das angegebene VLAN übermittelt werden.

<b>ID</b>	Die ID des VLANs. Ist das Eingabefeld <b>ID</b> leer, wird der Wert 0 angenommen. Die VLAN-ID mit dem Wert 0 schaltet die QoS ( <b>Q</b> uality- <b>o</b> f- <b>S</b> ervice) nach 802.1q ab.
-----------	---

**Priority** Sollte der Switch auf dem Port zum innovaphone Gateway auf eine andere ID konfiguriert sein, muss hier der gleiche Wert angegeben werden, damit eine Priorisierung der Ethernet Pakete funktionieren kann. Hier wird ein Priorisierungswert zwischen 0-7 (Konfiguration auf dem Ethernet Switch) angegeben.

#### 4.1.3.6 Configuration/ETH0/DHCP-Server

Wurde der DHCP-Server (siehe Kapitel: „*Configuration/ETH0-1/DHCP*“) aktiviert, kann dieser hier konfiguriert werden.

Alle Optionen, die mit einem „\*“ gekennzeichnet sind, sind innovaphone spezifische Optionen, die ausschließlich bei innovaphone Geräten zu finden sind.

**Lease Time [min]** Gibt die Gültigkeitsdauer des DHCP-Leases in Minuten an.

**Check interval [min]** Gibt das Interval in Minuten an, in dem überprüft wird, ob der DHCP-Lease noch gültig ist.

#### Address Ranges:

**First Address** Die IP-Adresse, die den Beginn des Adress-Bereichs darstellt (z.B.: 192.168.1.100).

**Last Address** Die IP-Adresse, die das Ende des Adress-Bereichs darstellt (z.B.: 192.168.1.110).

#### Offer Parameters:

**Network Mask** Die entsprechende Netzwerk-Maske bezüglich der IP-Adresse (z.B.: 192.168.1.100 entspricht der Netzwerkmaske 255.255.255.0).

**Default Gateway** Der Standard-Router (z.B.: 192.168.1.1).

**TOS Priority** Der ToS (**T**ype-**o**f-**S**ervice)- Wert für Sprachpakete (0x10).

<b>IP Routing</b>	Es besteht die Möglichkeit, statische IP-Routen hinzuzufügen. Diese müssen in Form von <i>Address:Mask:Gateway</i> eingegeben werden. Dabei muss jedes Element mit einem Doppelpunkt voneinander getrennt sein. Durch Abschluss einer Route mit „;“ können auch mehrere Routen hinzugefügt werden.
<b>DNS Server 1</b>	Die primäre DNS-Server-Adresse.
<b>DNS Server 2</b>	Die sekundäre DNS-Server-Adresse.
<b>Syslog Server</b>	Die Syslog-Server-Adresse.
<b>Time Server</b>	Die Zeit-Server-Adresse.
<b>Timezone String *</b>	Hier können den Geräten neue Zeitzonen gemäß IEEE-POSIX-Standard mittels einer bestimmten Zeichenkette (z.B: CET-1CEST-2,M3.5.0/2,M10.5.0/3) hinzugefügt werden.
<b>TFTP Server</b>	Die TFTP-Server-Adresse.
<b>WINS Server</b>	Die WINS-Server-Adresse.
<b>Primary Gatekeeper *</b>	Die primäre Gatekeeper-IP-Adresse.
<b>Secondary Gatekeeper *</b>	Die alternative Gatekeeper-IP-Adresse.
<b>Coder *</b>	Coder-Prefärenz für VoIP-Telefone.
<b>Gatekeeper Identifier *</b>	Der VoIP-Gatekeeper bzw. die Gatekeeper-Id für VoIP-Telefone.
<b>Dial Tones *</b>	Der Wahlton, der VoIP-Telefonen als Standard-Wahlton übermittelt wird (z.B: <i>German PBX</i> = wie deutsche TK Anlage, <i>US</i> = amerikanischer Wahlton, <i>UK</i> - englischer Wahlton).

<b>Enblock Dialing Timeout [s] *</b>	Schaltet Blockwahl für VoIP-Telefone ein.
<b>Faststart [0   1] *</b>	Mit der Option <b>Faststart[0   1]</b> kann man die H.323-Faststart Prozedur an/aus schalten.
<b>Tunneling [0   1] *</b>	Mit der Option <b>Tunneling[0   1]</b> kann man die H.245-Tunneling Prozedur an/aus schalten.
<b>Language *</b>	Alle VoIP-Telefone, die per DHCP ihre IP-Adresse erhalten, bekommen die hier festgelegte Sprache als Standard-Sprache eingerichtet.
<b>Dialing Location *</b>	Definiert die verschiedenen PBX-Zugriffsnummern auf VoIP-Telefonen für den Verzeichniszugriff. Diese Zeichenkette muß / cc-, /ac-, /ntp-, /itp-, /col- und /pbx-Optionen enthalten. Solch eine Zeichenkette kann wie folgt aussehen: „/cc 49 /ac 7031 /ntp 0 /itp 00 /col 0 /pbx 7“.
<b>AM/PM Clock [0   1]</b>	Aktiviert / deaktiviert das englische Zeitformat für VoIP-Telefone. Standardmäßig wird das deutsche Zeitformat angezeigt: „dd.mm.yy hh:mm, 24 Stunden Uhr“. Wird in dieses Feld eine 1 eingetragen, so wird das englische Zeitformat „mm/dd hh:mm xm, 12 Stunden am/pm Uhr“ angezeigt.
<b>LDAP Directory</b>	Um allen VoIP-Geräten die per DHCP eingebunden werden, eine funktionierende LDAP-Konfiguration zu zuweisen, kann im Feld <b>LDAP Directory</b> eine Konfigurationszeichenkette eingetragen werden. Diese Konfigurationszeichenkette erhält man, wenn man im Browser eines bereits konfigurierten Gerätes folgendes Kommando absetzt: „<IP-Adresse des VoIP-Gerät>/!mod cmd PHONEDIRO ldap-config“. Nach Absetzen dieses Befehls wird im Browser eine Konfigurationszeichenkette ausgegeben, welche man kopiert und in das Feld <b>LDAP Directory</b> des DHCP-Servers einfügt. Damit erhalten alle weiteren Geräte eine korrekte LDAP-Konfiguration.
<b>Update Interval [min]</b>	Alle per DHCP eingebundene Geräte erhalten den hier angegebenen Interval in das Feld <b>Interval [min]</b> des Update-Servers (siehe Kapitel: „Configuration/General/Update“) eingetragen.

**Update Server URL** Alle per DHCP eingebundenen Geräte erhalten die hier angegebenen URL (z.B.: `http://192.168.1.2/update/script.htm`) in das Feld **Command File URL** des Update-Servers (siehe Kapitel: „*Configuration/General/Update*“) eingetragen, womit eine automatisierte Aktualisierung der Geräte gewährleistet ist.

**802.1q VLAN ID** Zur Einstellung der VLAN-ID muss unbedingt die Konfiguration am Switch beachtet werden. Ein leeres Feld **802.1q VLAN-ID** (16Bit) nimmt den Wert 0 an. Die VLAN-ID mit dem Wert 0 schaltet QoS (**Quality-of-Service**) nach 802.1q ab. Sollte der Switch auf dem Port zum innovaphone Gerät auf eine andere VLAN-ID konfiguriert sein, muss hier der gleiche Wert angegeben werden, damit eine Priorisierung aus dem Ethernet stattfinden kann. Um zwischen den VLANs unterscheiden zu können wird das Ethernet-Paket um 4Byte erweitert, wovon 12Bit für die Aufnahme der VLAN-ID vorgesehen sind und somit 4094 VLANs möglich sind (die VLAN-ID 0 und 4095) sind reserviert bzw. nicht zulässig).

**802.1p VLAN Priority** Im Feld **802.1p VLAN-Priority** (3Bit) kann die zugehörige VLAN-Prioritätsstufe, ein Wert zwischen 0 und 7 angegeben werden um beispielsweise Sprachdaten bevorzugt weiterzuleiten.

#### 4.1.3.7 Configuration/ETH0/DHCP-Leases

VoIP-Geräte, die über diese Schnittstelle eine IP-Adresse des eingebauten DHCP-Server bezogen haben, werden hier angezeigt.

Im Abschnitt **Reserve IP Address** besteht zusätzlich die Möglichkeit, eine bestimmte IP-Adresse an eine bestimmte MAC-Adresse zu zuweisen.

Unter dem Abschnitt **Cleanup** können vergebene DHCP-Leases wieder gelöscht werden. Mit einem Klick auf **Clear dynamic leases** werde alle dynamisch vergebenen Leases gelöscht. Mit einem Klick auf **Clear reserved leases** werden alle reservierten Leases gelöscht. Und mit einem Klick auf **Clear all leases** werden alle vergebenen Leases gelöscht.

**IP Address** Die vergebene IP-Adresse des DHCP-Lease.

**MAC Address** Die MAC-Adresse des eingebundenen VoIP-Gerät.

<b>Acknowledged</b>	Das Datum, an dem der DHCP-Lease vergeben wurde.
<b>Expires</b>	Das Datum, an dem der DHCP-Lease ablaufen wird.
<b>Type</b>	Die Art des DHCP-Lease. <i>Dynamic</i> oder <i>Reserved</i> .
<b>Hostname</b>	Der Hostname des eingebundenen VoIP-Gerätes.

#### 4.1.3.8 Configuration/ETH0/Statistics

Über das Untermenü **Statistics** erhält man eine Übersicht über alle versendeten (tx) und empfangenen (rx) Datenpakete:

<b>tx-good</b>	Die Anzahl erfolgreich versendeter Pakete.
<b>tx-unicast</b>	Die Anzahl erfolgreich versendeter Unicast-Pakete.
<b>tx-broadcast</b>	Die Anzahl erfolgreich versendeter Broadcast-Pakete.
<b>tx-multicast</b>	Die Anzahl erfolgreich versendeter Multicast-Pakete.
<b>tx-lostcarrier</b>	Die Anzahl verlorener Trägersignale. Deutet auf ein defektes Medium (z.B.: Kabel) hin.
<b>tx-deferred</b>	Die Anzahl zurückgestellter Pakete.
<b>tx-collision</b>	Die Anzahl von kollidierenden Paketen (max. 16).
<b>tx-excesscol</b>	Die Anzahl der kollidierenden Pakete (wenn tx-collision > 16).
<b>tx-latecol</b>	Die Anzahl der kollidierenden Pakete, die zuviel Zeit benötigen, um übermittelt zu werden. Wurde eine Kollision erkannt, nachdem das 512.-Bit des zu übermittelnden Frames erreicht wurde, wird eine <i>late collision</i> ausgegeben.
<b>rx-good</b>	Die Anzahl der erfolgreich empfangenen Pakete.
<b>rx-unicast</b>	Die Anzahl erfolgreich empfangener Unicast-Pakete.
<b>rx-broadcast</b>	Die Anzahl der erfolgreich empfangener Broadcast-Pakete.

<b>rx-multi-cast</b>	Die Anzahl der erfolgreich empfangener Multicast-Pakete.
<b>rx-crc-err</b>	Die Anzahl der empfangenen CRC-Prüfsummenfehler.
<b>rx-align-err</b>	Die Anzahl der Alignment Error (falscher Treiber, Kabel defekt) beim Empfang von Datenpaketen.
<b>rx-too-short</b>	Die Anzahl der zu kleinen Datenpakete, während der Übermittlung.
<b>rx-too-long</b>	Die Anzahl der zu großen Datenpakete, während der Übermittlung.
<b>rx-collision</b>	Die Anzahl der kollidierenden Pakete (max. 16).
<b>rx-overflow-err</b>	Die Anzahl der Buffer-Overflow-Error beim Empfang von Datenpaketen.
<b>rx-queue-overflow</b>	Die Anzahl der Queue-Overflow-Error beim Empfang von Datenpaketen.
<b>rx-no-buffer</b>	Die Anzahl der No-Buffer beim Empfang von Datenpaketen.
<b>rx-tx-64</b>	Die Gesamtanzahl gesendeter und empfangener Pakete mit 64 Bytes.
<b>rx-tx-64-127</b>	Die Gesamtanzahl gesendeter und empfangener Pakete zwischen 64 und 127 Bytes.
<b>rx-tx-128-255</b>	Die Gesamtanzahl gesendeter und empfangener Pakete zwischen 128 und 255 Bytes.
<b>rx-tx-256-511</b>	Die Gesamtanzahl gesendeter und empfangener Pakete zwischen 256 und 511 Bytes.
<b>rx-tx-512-1023</b>	Die Gesamtanzahl gesendeter und empfangener Pakete zwischen 512 und 1023 Bytes.
<b>rx-tx-1024</b>	Die Gesamtanzahl gesendeter und empfangener Pakete mit 1024 Bytes.

#### 4.1.4 Configuration/LDAP

Die LDAP-Server und Replikator-Konfiguration kann hier vorgenommen werden.

Der LDAP-Server stellt die lokale LDAP-Datenbank externen Klienten zur Verfügung.

#### 4.1.4.1 Configuration/LDAP/Server

Hier können Zugangsdaten konfiguriert werden, die externen LDAP-Clients lesenden oder lesenden und schreibenden Zugriff auf die LDAP-Datenbank erlauben.

VoIP-Telefone benötigen lesenden Zugriff auf die LDAP-Datenbank. Replikationsverbindungen benötigen schreibenden Zugriff.

<b>Username</b>	Der LDAP-Benutzer-Name.
<b>Password</b>	Das zugehörige LDAP-Benutzer-Passwort.
<b>Write-Access</b>	Ein aktiviertes Kontrollkästchen erteilt eine Schreibberechtigung.

#### 4.1.4.2 Configuration/LDAP/Server-Status

Die angezeigten Server-Status-Daten werden automatisch periodisch aktualisiert:

<b>connec-tions</b>	Gesamtanzahl aller Verbindungen zum LDAP-Server.
<b>write-con-nections</b>	Anzahl der Verbindungen mit Schreibberechtigung.
<b>rx-search</b>	Anzahl der empfangenen Suchanfragen.
<b>rx-modify</b>	Anzahl der empfangenen Änderungsanforderungen.
<b>rx-add</b>	Anzahl der empfangenen Hinzufügearforderungen.
<b>rx-del</b>	Anzahl der empfangenen Löschanforderungen.
<b>rx-aban-don</b>	Anzahl der empfangenen Abbrucharforderungen.
<b>tx-notify</b>	Anzahl der gesendeten Benachrichtigungen.
<b>tx-error</b>	Anzahl der gesendeten Fehlerbenachrichtigungen.
<b>tx-error-49</b>	Anzahl der gesendeten Fehlerbenachrichtigungen aufgrund fehlerhafter Zugangsdaten.



**tx-error-50** Anzahl der gesendeten Fehlerbenachrichtungen aufgrund nicht ausreichender Rechte.

### 4.1.4.3 Configuration/LDAP/Replicator

Die LDAP-Replikation kann hier konfiguriert werden. Aufgabe der LDAP-Replikation ist es, den gesamten Inhalt oder Teile der Benutzerdatenbank einer entfernten innovaphone-PBX zu kopieren und aktuell zu halten.

Die Replikation wird in drei Anwendungsfällen benötigt:

1. Replikation der Benutzerdaten von der Master-PBX zu einer Standby-PBX. Die Replikator-Konfiguration findet auf der Standby-PBX statt.
2. Replikation der Benutzerdaten von der Master-PBX zu einem Slave. Die Replikator-Konfiguration findet auf dem Slave statt.
3. Replikation der Benutzerdaten von einem DECT-Master zu einem DECT-Radio. Die Replikator-Konfiguration findet auf dem DECT-Radio statt.

**Server** Die LDAP-Server IP-Adresse.

**Location** Um im Sinne einer Teilreplikation nur die Objekte eines bestimmten Standortes zu replizieren, kann hier der Name des Standortes (PBX-Name) angegeben werden.

**User & Password** Der LDAP-Benutzer und Passwort. Dieser ist auf dem LDAP-Server im Kapitel: „*Configuration/LDAP/Server*“ hinterlegt.

**Enable** Eine Replizierung findet nur dann statt, wenn das Kontrollkästchen Enable gesetzt ist.

### 4.1.4.4 Configuration/LDAP/Replicator-Status

Die angezeigten Replicator-Status-Daten werden automatisch periodisch aktualisiert. Es werden zusätzlich die letzten zehn Aktivitätsmeldungen der Replikation angezeigt:

**Server** IP-Adresse und Port des entfernten LDAP-Servers.

**Full Replication** Aktueller Zustand der Replikation. Es gibt vier Zustände: *Stop, Starting, Up, Down*.

**remote** Zeigt den Zustand der Replikation in Poll-Richtung an.

**notify** Anzahl der empfangenen Benachrichtigungen.

<b>modify</b>	Anzahl modifizierter Objekte.
<b>local</b>	Zeigt den Zustand der Replikation in Push-Richtung an.
<b>add</b>	Anzahl lokal hinzugefügter Objekte.
<b>del</b>	Anzahl lokal gelöschter Objekte.
<b>modify</b>	Anzahl lokal modifizierter Objekte.
<b>notify</b>	Anzahl der lokal entstandenen Benachrichtigungen.
<b>pending</b>	Anzahl lokal wartender Objekte.

## 4.1.5 Configuration/TEL1-2

Das Gerät verfügt über analoge TEL-Schnittstellen, sogenannte FXS-Schnittstellen, welche für den Anschluss von analogen-Telefonen oder Fax-Geräten der Gruppe 3 geeignet sind. Der Aufbau beider Menüs ist identisch und wurde deshalb zusammengefasst.

### 4.1.5.1 Configuration/TEL1-2/Physical

Die Physikalischen Einstellungen der analogen Schnittstellen können hier vorgenommen werden:

<b>Pulse</b>	Ein aktiviertes Kontrollkästchen erkennt Pulswahl an der entsprechenden Schnittstelle.
<b>Reverse</b>	Ein aktiviertes Kontrollkästchen invertiert die Verdrahtung der entsprechenden Schnittstelle. Dies ist nur bei einer Inkompatibilität der Endgeräte notwendig, da manche Endgeräte (z.B.: in den USA) genau anders verdrahtet sind.

### 4.1.5.2 Configuration/TEL1-2/Signaling

Die Rufsignalisierungseinstellungen der analogen TEL- Schnittstellen können hier angepasst werden:

<b>Disable</b>	Deaktiviert die entsprechende analoge Schnittstelle.
----------------	--

<b>Speech Bearer Capability</b>	Standardmäßig werden Rufe an der entsprechenden Schnittstelle mit Bearer-Capability <i>Audio</i> gesendet. Ein markiertes Kontrollkästchen sendet Rufe von der entsprechenden Schnittstelle mit Bearer-Capability <i>Speech</i> . Dies ist nur Sinnvoll sollten ausschliesslich Telefone an der entsprechenden Schnittstelle betrieben werden (kein Fax oder Modem).
<b>Create Metering Pulses</b>	Ein markiertes Kontrollkästchen erzeugt periodische Gebühren- bzw. Tarifimpulse an der entsprechenden Schnittstelle.
<b>No Call Waiting</b>	Ein markiertes Kontrollkästchen deaktiviert das Anklopfsignal bei wartenden Anrufen an der entsprechenden Schnittstelle. Der rufenden Seite wird stattdessen <i>Call busy</i> signalisiert. Dies ist zum Beispiel notwendig, sollte ein FAX-Gerät an der entsprechenden Schnittstelle betrieben werden, da ein Anklopfsignal die FAX-Übertragung stören würde.
<b>Passive</b>	Versetzt die entsprechende Schnittstelle in den passiven Modus. Dadurch wird das Flash/Hook-Signal (R-Taste) nicht ausgewertet.
<b>No Call Transfer on Hook-On</b>	Ein markiertes Kontrollkästchen deaktiviert die Vermittlungsfunktion. Ein gehaltenes Gespräch wird standardmäßig beim Auflegen des Hörers vermittelt. Nachdem ein Ruf aufgebaut wurde, kann durch drücken der R-Taste das aktive Gespräch gehalten werden und ein neuer Ruf initiiert werden. Wurde der neue Ruf aufgebaut, so kann durch Auflegen des Hörers der gehaltene, wartende Ruf mit dem neuen aktiven Ruf verbunden werden.
<b>Volume</b>	Stellt die Wiedergabe für die entsprechende Schnittstelle in Dezibel (db) zwischen -32db und +32db ein. Kein Eintrag bzw. der Eintrag 0 entspricht der Werkseinstellung.

## 4.2 Administration

Hier wird all das vorgenommen, was im laufenden Betrieb notwendig wird.

Dazu gehört zum Beispiel das Anmelden von VoIP-Telefonen an einem Gateway oder wenn vorhanden an einer innovaphone-PBX.

## 4.2.1 Administration/Gateway

Hier kann die Gateway-Konfiguration des Gerätes vorgenommen werden. Das Gateway-Menü stellt die Verbindung zum herkömmlichen Telefonnetz zum Beispiel über eine digitale ISDN-Schnittstelle oder eine VoIP-Schnittstelle her. Je nachdem welches Gerät verwendet wird, stehen verschiedene Schnittstellen zur Verfügung. Dazu gehören zum Beispiel die virtuellen TEST-, TONE- und HTTP-Schnittstellen, die analogen-Schnittstellen (TEL) sowie auch die ISDN-Schnittstellen (TEL, PPP, BRI oder PRI). Mittels zusätzlicher Lizenzen stehen auch sogenannte VoIP-Schnittstellen (GW1-12) bereit, mit welchen es z.B. möglich ist eine TK-Anlagen-Kopplung ohne Verwendung der innovaphone-PBX herzustellen.

### 4.2.1.1 Administration/Gateway/General

Generelle Gateway-Einstellungen können hier eingestellt werden:

- Gatekeeper ID** Der eindeutige Gatekeeper-Name. Sollten mehrere Gatekeeper in einem Netz verwendet werden, so müssen unterschiedliche Gatekeeper-IDs vergeben werden. Diese Gatekeeper-ID ist die ID für VoIP-Interfaces (siehe auch Kapitel: „*Administration/Gatekeeper/VoIP-Interfaces*“). Dieses Feld wird nur in Verbindung mit einer Gatekeeper-Lizenz angezeigt.
- Automatic CGPN Mapping** Ein markiertes Kontrollkästchen aktiviert die automatische Rufnummerbehandlung. Die entsprechende Modifikation der rufenden Nummer wird durch Analyse der Routingtabelle gesteuert. Es wird dabei eine Route gesucht, die den Rückruf zum aktuellen Ruf ermöglichen würde. Es besteht die Möglichkeit einzelne Routen von der automatischen Korrektur aller rufenden Nummern auszuschließen (siehe Kontrollkästchen *Exclude from Auto-CGPN* im Abschnitt **Settings** des Kapitels: „*Administration/Gateway/Routes*“).
- Call Logging** Ein markiertes Kontrollkästchen aktiviert die Ausgabe von Syslog-Informationen bezüglich der geführten Gespräche über das Gateway.
- Route Logging** Ein markiertes Kontrollkästchen aktiviert die Ausgabe von Syslog-Informationen bezüglich der verwendeten Sprachrouten des Gateways.

## Billing CDR's only

Wurde im Kapitel: „*Administration/Gateway/CDR0-1*“ eine Methode angegeben sogenannte **Call-Detail-Records (CDR)** zu übermitteln, werden bei einem markierten Kontrollkästchen ausschließlich Abrechnungsrelevante Informationen der geführten Gespräche übermittelt.

### 4.2.1.1.1 Feature Codes

Der Abschnitt **Feature Codes** wird aktiviert, sobald für eine Schnittstelle (siehe Kapitel: „*Administration/Gateway/Interfaces*“) explizit das Kontrollkästchen *Supplementary Services (with Feature Codes)* oder bei einem IP-DECT-Gerät (siehe Kapitel: „*Configuration/DECT/Features*“) das Kontrollkästchen *Enable* markiert wurde.

Mittels **Feature Codes** stehen den VoIP-Telefonen weitere Leistungsmerkmale zur Verfügung. Die Codes für diese Leistungsmerkmale können konfiguriert werden. Dabei ist zu beachten, dass allgemein:

- das „\$“-Zeichen für eine variable Anzahl an Zeichen (z.B. eine Telefonnummer) und
- das „(x)“-Zeichen für eine feste Anzahl an Zeichen steht.
- Vorwiegend werden Aktionen mit einem „\*“-Zeichen eingeleitet und
- mit der „#“-Taste rückgängig gemacht.

## Umleitungsoptionen

Die IP-Geräte unterstützen drei verschiedenen Arten von Anrufumleitungen.

Aktivität	Code	Beschreibung
<b>CFU</b>		Aktiviert, deaktiviert die permanente Anrufweiterleitung. Das \$-Zeichen steht für die Zielrufnummer.
<b>Activate</b> <b>Deactivate</b>	*21*\$# #21#	
<b>CFB</b>		Aktiviert, deaktiviert die Anrufweiterleitung wenn besetzt. Das \$-Zeichen steht für die Zielrufnummer.
<b>Activate</b> <b>Deactivate</b>	*67*\$# #67#	

<b>CFNR</b>		Aktiviert, deaktiviert die Anrufweiterleitung bei fehlender Antwort. Das \$-Zeichen steht für die Zielrufnummer.
<b>Activate</b>	*61*\$#	
<b>Deactivate</b>	#61#	

## Sperren

Die VoIP-Telefone können mit folgender Tastenkombination aus dem Grundzustand gesperrt werden.

Aktivität	Code	Beschreibung
<b>Lock Phone</b>	*33*\$#	Aktiviert, deaktiviert die Tastensperre des Telefons. Das \$-Zeichen steht für den PIN.
<b>Unlock</b>	#33*\$#	

## PIN

Die PIN dient dazu, den Zugang für unberechtigte Nutzer zu verhindern. Mit dieser Funktion kann der Schutz aktiviert und eine PIN festgelegt werden.

Aktivität	Code	Beschreibung
<b>Set PIN</b>	*99*\$*\$\$*#	Speichert einen PIN für das Telefon. Das erste \$-Zeichen ist der alte PIN (beim ersten setzen des PINs wird hier kein Zeichen ersetzt), die nächsten 2 \$-Zeichen ist der neue PIN.

## Anrufschutz

Mit dieser Funktion kann gesondert auf eingehende Anrufe reagiert werden.

Im Ruhezustand wird das Telefon stumm geschaltet. Dem Anrufenden wird dennoch ein Freizeichen vermittelt.

Aktivität	Code	Beschreibung
<b>Do not Disturb</b>		Aktiviert, deaktiviert die Stummschaltfunktion sowohl für eingehende <b>externe</b> und <b>interne</b> Rufe.
<b>On</b>	*42#	
<b>Off</b>	#42#	

<b>Do not Disturb Int.</b>		Aktiviert, deaktiviert die Stummschaltfunktion für eingehende <b>interne</b> Rufe.
<b>On</b>	*421#	
<b>Off</b>	#421#	
<b>Do not Disturb Ext.</b>		Aktiviert, deaktiviert die Stummschaltfunktion für eingehende <b>externe</b> Rufe.
<b>On</b>	*422#	
<b>Off</b>	#422#	

## Anklopfunktionen

Aktivität	Code	Beschreibung
<b>Call Waiting</b>		Aktiviert, deaktiviert die Anklopf-Funktion des Telefons
<b>On</b>	*43#	
<b>Off</b>	#43#	

## Lokale Einstellungen löschen

Aktivität	Code	Beschreibung
<b>Clear Local Settings</b>	*00#	Löscht alle getätigten Feature Codes Einstellungen.

## Pickup

Innerhalb einer Gruppe kann ein eingehender Ruf von einem Teilnehmer übernommen werden.

Aktivität	Code	Beschreibung
<b>Pickup Group</b>	*0#	<i>Pickup Group</i> holt ungezielt einen Ruf einer Pickup-Gruppe heran.
<b>Directed</b>	*0*\$#	Mit <i>Directed</i> kann ein bestimmter Ruf durch Angabe der Rufnummer herangeholt werden.

## Park

Mit dieser Funktion kann die Parkposition definiert werden. Diese wird an ein bestehendes Objekt der gleichen Gruppe gebunden. Das Objekt kann beispielsweise

se die Amtsleitung oder die Warteschleife sein.

Gespräche können auf diese Position geparkt und von beliebigen Mitgliedern der Gruppe wieder abgeholt werden.

Aktivität	Code	Beschreibung
<b>Park</b>	R*16\$(1)	Mit <i>Park</i> kann ein Ruf durch Drücken der R-Taste und anschließender Eingabe des Feature Codes (1 = Position in der eigenen Nebenstelle) geparkt werden.
<b>Unpark</b>	#16\$(1)	Mit <i>Unpark</i> holt man diesen wieder zurück.
<b>Park To</b>	*17\$(1)\$#	Genauso wie <i>Park</i> , nur mit Unterschied das der Ruf in einer anderen Nebenstelle z.B. dem Amt (0) geparkt wird.
<b>Unpark From</b>	#17\$(1)\$#	

## Join Group

Aktivität	Code	Beschreibung
<b>Group Join</b>	*31#	Mit <i>Group Join</i> tritt man einer Gruppe bei.
<b>Leave</b>	#31#	Mit <i>Leave</i> verlässt man diese wieder. Für IP-DECT nicht implementiert.

## Rückruf

Mit nachfolgendem Code besteht die Möglichkeit, einen Rückruf auf der gerufenen Seite zu initiieren, sollte diese belegt sein.

Aktivität	Code	Beschreibung
<b>Call Completion</b>	*37#	Mit <i>Call Completion</i> kann ein Rückruf initiiert werden, sollte der angerufene Teilnehmer belegt sein. Für IP-DECT implementiert.
<b>Cancel</b>	#37#	

Im Abschnitt **Licenses** erhält man Geräteabhängig eine kleine Übersicht über die verfügbaren und die bereits vergebenen Lizenzen:

<b>Gateway</b>	Gateway-Lizenzen.
<b>Gatekeeper6</b>	Gatekeeper-Lizenzen.
<b>BRIs</b>	BRI-Schnittstellen.
<b>PRIs</b>	PRI-Schnittstellen.



<b>Channels</b>	DSP-Kanäle.
<b>aBs</b>	AB-Schnittstellen.
<b>Registrations</b>	Registrierungs-Lizenzen.

## 4.2.1.2 Administration/Gateway/Interfaces

Die Anzeige der konfigurierbaren Schnittstellen des Gateways ist in folgende Spalten gegliedert:

<b>Interface</b>	Der Name der Schnittstelle. Ein Klick auf diesen Namen öffnet eine Popup-Seite, in der alle Einstellungen vorgenommen werden können. Diese werden im nachfolgenden Kapiteln: „ <i>Administration/Gateway/Interfaces/Interface (ISDN &amp; Virtuelle Schnittstellen)</i> “ genauer erläutert.
<b>CGPN-In, CDPN-In, CGPN-Out, CDPN-Out</b>	Genauer Details zu CGPN-In, CDPN-In, CGPN-Out und CDPN-Out-Mappings sind im Kapitel: „ <i>Administration/Gateway/Interfaces/CGPN-CDPN-Mappings</i> “ weiter unten im Text enthalten.
<b>State</b>	Der aktuelle Zustand der Schnittstelle auf Physikalischer- und auf Protokollebene. Mögliche Zustände sind: <i>Up, Down</i> .
<b>Registration</b>	Hat sich ein Endgerät erfolgreich an einer ISDN- SIP- oder virtuellen-Schnittstelle registriert, so wird dies in dieser Spalte durch Angabe der <i>IP-Adresse</i> angezeigt <i>&lt;Name der VoIP-Schnittstelle:Rufnummer:IP-Adresse&gt;</i> .

### 4.2.1.2.1 Interface (ISDN- SIP- & virtuelle-Schnittstellen)

Ein Klick auf den Namen der entsprechende Schnittstelle in der Spalte **Interface** öffnet eine Popup-Seite, in welcher die individuelle Schnittstellen-Konfiguration vorgenommen werden kann. Wie die PBX-Objekte enthält auch diese Popup-Seite Standard-Eingabefelder, die in allen Schnittstellen mehr oder minder vorkommen. Diese Standard-Felder sind:

<b>Name</b>	Der beschreibende Name der Schnittstelle.
-------------	---

<b>Disable</b>	Ein markiertes Kontrollkästchen deaktiviert die entsprechende Schnittstelle.
<b>Tones</b>	Die Standard-Ruftonart für die entsprechende Schnittstelle wird mit der Auswahlbox Tones eingestellt.
<b>Interface Maps</b>	Die Schnittstelle lässt sich als Anlagenanschluss ( <i>Point-To-Point</i> ) als auch als Mehrgeräteanschluss ( <i>Point-To-Multipoint</i> ) sowie auch manuell ( <i>Manual</i> ) über CGPN-, CDPN-Maps konfigurieren. Siehe Beschreibung weiter unten im Text.
<b>Registration</b>	Mit der Auswahlbox Registration kann für ISDN-Schnittstellen eine H.323-Registrierung oder eine SIP-Registrierung veranlasst werden. Die Routen wie ein- und ausgehende Rufe an der entsprechenden Schnittstelle behandelt werden sollen, werden dabei automatisch angelegt (siehe Kapitel: „ <i>Administration/Gateway/Routes</i> “).

## ISDN-Schnittstellen (PPP, TEL1-4, BRI1-4, PRI1-4)

Nach Auswahl eines **Interface Maps** wird der entsprechende Abschnitt eingeblendet. Bei Auswahl von *Point to Point* wird Abschnitt **Interface Maps Point to Point** eingeblendet:

<b>Area Code</b>	Die Landesvorwahl (z.B. 49).
<b>Subscriber Number</b>	Die Ortsnetznummer (z.B. 7031).
<b>National Prefix</b>	Der Nationale Prefix (z.B. 0).
<b>International Prefix</b>	Der Internationale Prefix (z.B. 00).

Bei Auswahl von *Trunk Point to Multipoint* wird der Abschnitt **Interface Maps**

**Point to Multipoint** eingeblendet:

**MSN1-3 / Ext.** Für jeden ISDN-Basisanschluss können mehrere Rufnummern konfiguriert werden. Die innovaphone-Gateways unterstützen bis zu drei MSN-Rufnummern (*MSNI-3*), gefolgt von der Extension (*Ext.*), welche die Nebenstelle darstellt, auf die die MSN gemapped werden soll.

**National Prefix** Der Nationale Prefix (z.B. 0).

**International Prefix** Der Internationale Prefix (z.B. 00).

Abschnitt **Coder Preferences**:

Nach Auswahl einer Registrierungsmethode wird der Abschnitt **Coder Preferences** wie auch der entsprechende **Registration** Abschnitt eingeblendet. Die Standard-Eingabefelder des **Coder Preferences** Abschnittes sind:

**Model** Über die Auswahlbox *Model* wird der zu verwendende Coder ausgewählt. Zur Auswahl stehen folgende Coder: *G711A*, *G711u*, *G723-53*, *G729A*, *G726-32* und *XPARENT*. Sollte das entfernte VoIP-Gerät den eingestellten Coder nicht unterstützen, wird ein gemeinsam unterstützter Coder verwendet, es sei denn das Kontrollkästchen *Exclusive* wurde aktiviert.

**Frame** Bestimmt die bei der Übertragung von Sprachdaten verwendete Paketgröße (in *ms*). Größere Pakete verursachen eine erhöhte Verzögerung in der Sprachdatenübertragung (*Delay*), verursachen jedoch eine geringere Netzwerkbelastung, da der beim Transport der Paket im Netzwerk auftretende *Overhead* geringer wird. Je höher also die verwendete Paketgröße, desto geringer die effektiv verwendete Bandbreite.

**Kodierverfahren | Paketgröße | Bandbreite**

G.711		30 <sub>ms</sub>		77 <sub>kb</sub>
G.711		90 <sub>ms</sub>		68 <sub>kb</sub>

-----

G.729		30 <sub>ms</sub>		21 <sub>kb</sub>
G.729		90 <sub>ms</sub>		12 <sub>kb</sub>

<b>Exclusive</b>	Ein markiertes Kontrollkästchen erzwingt die eingestellte Kodierung ( <i>Mode</i> ), egal ob diese vom entfernten VoIP-Gerät unterstützt wird oder nicht.
<b>SC</b>	Ein markiertes Kontrollkästchen aktiviert <b>SC (Silence-Compression)</b> . Bei einer SC werden in Gesprächspausen keine Daten übermittelt. Damit lässt sich zusätzlich Bandbreite (Bandwith) ohne Qualitätsverlust einsparen.
<b>Enable T.38</b>	Ein markiertes Kontrollkästchen aktiviert das Fax-Over-IP-Protokoll <i>T.38</i> . Wurde an die entsprechende Schnittstelle ein Fax-Gerät angeschlossen, dann muss dieses Kontrollkästchen aktiviert sein, andernfalls werden Faxübertragungen nicht behandelt.
<b>Enable PCM</b>	Ein markiertes Kontrollkästchen aktiviert den PCM-Switch ( <b>Pulse-Code-Manipulation</b> ). Damit werden Rufe von einer Schnittstelle zu einer anderen direkt über den ISDN-PCM-Bus abgewickelt, was wiederum DSP-Kanäle einspart. Dieses Eingabefeld ist optional und wird nur in bestimmten Geräten angezeigt.

## Abschnitt **Registration**:

Alle nicht virtuellen Schnittstellen besitzen nach Auswahl der Registrierungs-methode zusätzlich noch den Abschnitt **Registration**.

Die Eingabefelder bei einer **H.323**-Registrierung sind:

<b>Gatekeeper Address (primary)</b>	Die primäre Gatekeeper-IP-Adresse an der sich die Schnittstelle registrieren soll. Befindet sich der primäre Gatekeeper auf dem selber Gerät, so kann hier auch die lokale IP-Adresse <code>127.0.0.1</code> eingetragen werden.
<b>Gatekeeper Address (secondary)</b>	Die sekundäre Gatekeeper-IP-Adresse an der sich die Schnittstelle registrieren soll, sollte die Registrierung am primären Gatekeeper fehlschlagen. Befindet sich der sekundäre Gatekeeper auf dem selber Gerät, so kann hier ebenfalls die lokale IP-Adresse <code>127.0.0.1</code> eingetragen werden.

<b>Gatekeeper ID</b>	Es ist auch ausreichend nur die Gatekeeper-ID anzugeben (Siehe auch Kapitel: „ <i>Administration/Gateway/General</i> “).
<b>Name</b>	Der eindeutige, beschreibende H.323-Name der Schnittstelle bzw. der Registrierung.
<b>Number</b>	Die eindeutige E.164-Rufnummer der Schnittstelle bzw. Registrierung.
<b>Password / Retype</b>	Die Sicherheit der Registrierung lässt sich durch Angabe eines Passwortes ( <b>Password</b> ) erhöhen. Das Passwort muss bestätigt werden ( <b>Retype</b> ).
<b>Supplementary Services (with Feature Codes)</b>	Ein markiertes Kontrollkästchen aktiviert die Verwendung zusätzlicher Leistungsmerkmale ( <b>Feature Codes</b> ). Siehe Beschreibung in Kapitel: „ <i>Administration/Gateway/General</i> “.
<b>Dynamic Group</b>	Der H.323-Registrierung kann eine <i>Dynamic Group</i> angefügt werden. Gruppen können <i>statisch</i> , <i>dynamic-in</i> oder <i>dynamic-out</i> konfiguriert werden. Rufe werden bei Mitgliedern statischer Gruppen immer signalisiert. Anders verhält es sich bei Mitgliedern dynamischer Gruppen, welche sich über eine Funktionstaste (Join Group) dynamisch an einer Gruppe an- bzw. abmelden. Der Unterschied zwischen <i>dynamic-in</i> und <i>dynamic-out</i> besteht darin, ob das Objekt in der entsprechenden Gruppe standardmäßig enthalten sein soll ( <i>in</i> ) oder nicht ( <i>out</i> ). Siehe auch Beschreibung in Kapitel: „ <i>Administration/PBX/Objects</i> “.
<b>Direct Dial</b>	Mittels <i>Direct Dial</i> wird sofort nach Abnehmen des Hörers ein Rufaufbau zur angegebenen Rufnummer initiiert. Ein denkbare Szenario wäre z.B. ein Fahrstuhl-Not-Telefon, welches mit der Sicherheitszentrale verbunden ist.
<b>Locked White List</b>	Hier kann eine komma separierte Liste von Rufnummern angegeben werden, welche auch bei einem gesperrten Telefon gewählt werden dürfen (z.B.: Notdienstnummern wie 110, 911).

Die Eingabefelder bei einer **SIP**-Registrierung sind:

<b>Server Address (primary)</b>	Angabe der IP-Adresse oder der Proxy-Server-Adresse des SIP-Providers (z.B. sipgate.de: 217.10.79.9) , wohin die SIP-Nachrichten (z.B.: register) gesendet werden sollen.
<b>Server Address (secondary)</b>	Sollte der SIP-Provider eine alternative IP-Adresse oder Proxy-Server besitzen, so kann diese hier eingetragen werden, so dass im Falle eines Ausfalls (z.B.: bei einer Wartung) des primären Servers die Registrierung erhalten bleibt.
<b>STUN Server</b>	Der STUN-Server-Name oder IP-Adresse muss konfiguriert werden, wenn das Telefon eine private IP-Adresse nutzt, der SIP-Server jedoch unter einer öffentliche IP-Adresse zu erreichen ist. Der Wert wird vom SIP-Provider oder Administrator genannt (z.B.: stun.xten.com oder 64.69.76.23). Der STUN-Server kann beliebig gewählt werden und muss nicht zwingend dem des SIP-Provider entsprechen.
<b>ID @</b>	Die Benutzer-ID bzw. die Benutzerkennung, gefolgt vom SIP-Provider Domainnamen wird hier eingetragen (z.B.: 8111111e0@sipgate.de).
<b>Display Name</b>	Der hier einzugebende Name, welcher der Teil vor dem @ der URI entspricht, wird für die Registrierung nur benötigt, wenn die Nummer (Account) nicht angegeben wurde (z.B.: 8111111e0).
<b>Account</b>	Auch in diesem Protokoll ist für die Registrierung eine Rufnummer erforderlich, welche dem Teil vor dem @ der URI entspricht (z.B.: 8111111e0).
<b>Password / Retype</b>	Das Passwort (Password) des SIP-Accounts muss angegeben und bestätigt (Retype) werden.
<b>Supplementary Services (with Feature Codes)</b>	Siehe Eingabefelder bei einer <b>H.323</b> -Registrierung.
<b>Dynamic Group</b>	Siehe Eingabefelder bei einer <b>H.323</b> -Registrierung.
<b>Direct Dial</b>	Siehe Eingabefelder bei einer <b>H.323</b> -Registrierung.

**Locked White List**      Siehe Eingabefelder bei einer **H.323**-Registrierung.

## SIP-Schnittstellen (SIP1-4)

Zusätzlich zu den ISDN-Schnittstellen (PPP, TEL1-4, BRI1-4, PRI1-4) und Virtuellen-Schnittstellen (TEST, TONE, HTTP) gibt es auch noch vier SIP-Schnittstellen (SIP1-4), womit z.B. die Möglichkeit besteht, eine Amtsleitung von einem SIP-Provider zu erhalten. Die Beschreibung der Eingabefelder sind der obigen Beschreibung der SIP-Registrierung zu entnehmen. Es gibt aber noch drei weitere Eingabefelder:

<b>Name</b>	Ein beschreibender Name für die Schnittstelle.
<b>Disable</b>	Deaktiviert die entsprechende Schnittstelle.
<b>Registration</b>	Entspricht dem Eingabefeld <i>Registration</i> der ISDN-Schnittstellen. Nach Auswahl von H.323 wird der Abschnitt <i>Registration für H.323</i> eingeblendet, wodurch eine Registrierung eines SIP-Accounts an einer lokalen PBX (z.B. innovaphone-PBX) ermöglicht wird. Nach Auswahl von SIP wird Abschnitt <i>Registration für SIP</i> eingeblendet, wodurch wiederum eine Registrierung an einer lokalen SIP-PBX (z.B. innovaphone-PBX) ermöglicht wird.

Um eine Amtsleitung von einem SIP-Provider zu erhalten muss wie folgt vorgegangen werden:

1. Eine der vier SIP-Schnittstellen öffnen.
2. SIP-Account Daten (ID, STUN Server, Account, Passwort) eintragen.
3. Unter Registrations die SIP-Registrierung via H.323 an ein zuvor angelegtes PBX-Objekt vom Typ *Trunk* binden (Angabe der GK-ID oder der GK-Adresse und des H.323-Namens bzw. der E.164-Rufnummer genügen).
4. Mit OK bestätigen.

Eine erfolgreiche Registrierung wird in der Übersichtsseite *Administration/Gateway/Interfaces* wie folgt angezeigt:

State (IP des SIP-Providers)	Alias (PBX-Benutzer-Objekt)	Registration (IP der PBX)
---------------------------------	--------------------------------	------------------------------

z.B.: 217.10.79.9 (sipgate.de)	H.323-Name:E.164-Nr. SIPTrunk:8	--> 127.0.0.1
-----------------------------------	------------------------------------	---------------

Im obigen Beispiel wird die Amtsleitung des SIP-Carriers *sipgate.de* über das PBX-Objekt *Trunk* mit dem Namen *SIPTrunk* und der Rufnummer *8* herangeholt. Die Wahl der Rufnummer *807031730090* initiiert demnach einen Ruf bei der Firma innovaphone AG über den konfigurierten SIP-Carrier.

## Virtuelle Schnittstellen (TEST, TONE, HTTP)

Die nicht konfigurierbare, interne Schnittstelle **TEST** ist nur als Ziel eines Rufes verwendbar. Geht ein Ruf auf dieser Schnittstelle ein, so wird die im nichtflüchtigen Speicher enthaltene Pausenmusik eingespielt. Eingehende Rufe müssen im G.729A- oder im G.723-Format sein, andere Formate werden nicht unterstützt. Nachwahlziffern werden ignoriert.

Die interne Schnittstelle **TONE** ist nur als Ziel eines Rufes verwendbar. Geht ein Ruf auf dieser Schnittstelle ein, so wird dieser verbunden und der konfigurierte Amtston (**Tones**) eingespielt. Dies kommt insbesondere bei **least-cost-routing** Szenarien vor, bei denen die Vermittlung des Rufes erst nach Analyse einiger Rufziffern vorgenommen werden kann. Währenddessen wird über die TONE-Schnittstelle der Amtston eingespielt. Nachwahlziffern werden ignoriert. Die TONE-Schnittstelle kann mehrere Rufe verarbeiten.

Die nicht konfigurierbare, interne Schnittstelle **HTTP** ist nur als Ziel eines Rufes verwendbar. Geht ein Ruf auf dieser Schnittstelle ein, so wird eine Wartemusik, eine Ansage oder irgendeine andere gesprochene Information von einem Webserver abgespielt. Die Konfiguration ist nur im Zusammenhang mit der innovaphone-PBX sinnvoll.

### 4.2.1.2.2 CGPN-CDPN-Mappings

Es ist möglich für jedes Interface sogenannte CGPN-In, CDPN-In, CGPN-Out und CDPN-Out-Mappings (**Calling-Party-Number-In, Called-Party-Number-In, Calling-Party-Number-Out, Called-Party-Number-Out**) zu hinterlegen, womit Rufnummern und Rufnummernformate für ein- und ausgehende Rufe angepasst werden können. Folgenden Rufnummernformate gibt es:

<b>Unknown</b>	Unspezifiziert. Gerufene Nummer bei ausgehenden Rufen.	u
----------------	--	---



<b>Subscriber</b>	Rufnummer im Ortsnetz. Gerufene Nummer bei eingehenden Rufen.	s	
<b>National</b>	Rufnummer mit Ortsnetz-kennzahl. Rufende Nummer aus dem Inland.	n	0
<b>International</b>	Rufnummer mit Landes- und Ortsnetz-kennzahl. Rufende Nummer aus dem Ausland.	i	00
<b>Abbreviated</b>	Unüblich.	a	
<b>Network Specific</b>	Unüblich.	x	

Ein Klick auf den Link **+** oder auf einen bereits angelegtes Mapping (z.B.: **n->0**) öffnet eine Popup-Seite, in welcher die Einstellung für die CGPN-In, CDPN-In, CGPN-Out und CDPN-Out-Mappings getätigt werden:

<b>CGPN In</b>	Wird verwendet, um die rufende Nummer eingehender Rufe zu bearbeiten.
<b>CDPN In</b>	Wird verwendet, um die gerufene Nummer eingehender Rufe zu bearbeiten.
<b>CGPN Out</b>	Wird verwendet, um die rufende Nummer ausgehender Rufe zu bearbeiten.
<b>CDPN Out</b>	Wird verwendet, um die gerufene Nummer ausgehender Rufe zu bearbeiten.

Jedes Mapping kann auf einen bestimmten Rufnummertyp spezifiziert werden:

<b>Unknown</b>	Das entsprechende Mapping gilt für unbekannte, externe Rufe.
<b>ISDN</b>	Das entsprechende Mapping gilt für externe Rufe.
<b>Private</b>	Das entsprechende Mapping gilt für interne Rufe.

#### 4.2.1.3 Administration/Gateway/VOIP

Nachfolgend eine Übersicht über alle konfigurierbaren VoIP-Schnittstellen des

Gateways:

<b>Interface</b>	Der Name der Schnittstelle. Ein Klick auf diesen Namen öffnet eine Popup-Seite, in der alle Einstellungen vorgenommen werden können. Diese werden im nachfolgenden Kapitel: „ <i>Administration/Gateway/VOIP/Interface (VoIP-Schnittstellen)</i> “ genauer erläutert.
<b>CGPN-In, CDPN-In, CGPN-Out, CDPN-Out</b>	Genauer Details zu CGPN-In, CDPN-In, CGPN-Out und CDPN-Out-Mappings sind im Kapitel: „ <i>Administration/Gateway/Interfaces/CGPN-CDPN-Mappings</i> “ weiter oben im Text enthalten.
<b>Registration</b>	Hat sich ein Endgerät erfolgreich an einem Gateway registriert, so wird dies in dieser Spalte durch Angabe der IP-Adresse angezeigt < <i>Name der VoIP-Schnittstelle:Rufnummer:IP-Adresse</i> >.

#### 4.2.1.3.1 Interface (VoIP-Schnittstellen)

Ein Klick auf die entsprechende VoIP-Schnittstelle (*GW1-12 <Name der VoIP-Schnittstelle>*) in der Spalte **Interface** öffnet eine Popup-Seite, in welcher die individuelle VoIP-Schnittstellen-Konfiguration vorgenommen werden kann. Wie die PBX-Objekte enthält auch diese Popup-Seite Standard-Eingabefelder, die in allen VoIP-Schnittstellen mehr oder minder vorkommen.

Diese Standard-Felder sind:

<b>Name</b>	Der beschreibende Name der VoIP-Schnittstelle.
<b>Disable</b>	Ein markiertes Kontrollkästchen deaktiviert die entsprechende VoIP-Schnittstelle.
<b>Protokoll</b>	Das zu verwendende Protokoll, <i>H.323</i> oder <i>SIP</i> . Je nachdem welches Protokoll verwendet wird, ändert sich der Aufbau der Eingabefelder.

<b>Mode</b>	<p>Beschreibt die Art der Registrierung. Mögliche Registrierungsarten sind:</p> <ol style="list-style-type: none"><li>1. Gateway without Registration - Meldet die VoIP-Schnittstelle (Gateway) an dem konfigurierten Gatekeeper ohne eine Registrierung an.</li><li>2. Register as Endpoint - Registriert ein VoIP-Endgerät an dem konfigurierten Gatekeeper.</li><li>3. Register as Gateway - Registriert ein VoIP-Gateway an dem konfigurierten Gatekeeper.</li><li>4. Gatekeeper/Registrar - Wird benötigt um alle Gatekeeper-Registrierungen auf einem Gateway zu verwalten.</li><li>5. ENUM - Wird verwendet um einen ENUM-Anschluss an der entsprechenden Schnittstelle anzumelden.</li></ol>
<b>Gatekeeper Address (primary)</b>	<p>Die primäre Gatekeeper-IP-Adresse an der sich das Endgerät oder Gateway über die entsprechende Schnittstelle registrieren soll. Nur bei Mode 2 und 3 notwendig.</p>
<b>Gatekeeper Address (secondary)</b>	<p>Die alternative Gatekeeper-IP-Adresse an der sich das Endgerät oder Gateway über die entsprechende Schnittstelle registrieren soll, sollte die Registrierung am primären Gatekeeper fehlschlagen. Nur bei Mode 2 und 3 notwendig.</p>
<b>Mask</b>	<p>Eingehende Rufe können durch Angabe einer Netzwerk-Maske gefiltert werden. Die Angabe der Netzwerk-Maske <code>255.255.0.0</code> gestattet somit eingehende Rufe an der entsprechenden Schnittstelle für Endgeräte aus dem IP-Adressbereich <code>192.168.0.0 - 192.168.255.255</code>.</p>
<b>Gatekeeper Identifier</b>	<p>Es ist auch ausreichend nur die Gatekeeper-ID anzugeben. Jeder Gatekeeper in einem Netz kann über eine eigene Gatekeeper-ID unterschieden werden, sodass mehrere Gatekeeper in einem Netz betreiben werden können, wobei jedes Endgerät bei der <code>gatekeeper-discovery</code> (verwendet multicast adresse <code>224.0.1.41</code>) trotzdem den richtigen Gatekeeper ermittelt.</p>

Im Abschnitt **Authorization** kann ein Passwort für die VoIP-Schnittstelle hinter-

legt werden.

**Password /  
Retype**

Die Sicherheit der Registrierung lässt sich durch Angabe eines Passwortes (**Password**) erhöhen. Das Passwort muss bestätigt werden (**Retype**).

Im Abschnitt **Alias List** wird der Rufname (H.323) und die Rufnummer (E.164) der entsprechenden Registrierung angegeben. Für VoIP-Endpunkte sollte hier die zugewiesene Durchwahl oder MSN als E.164 Adresse sowie den Namen als H.323 Name festgelegt werden. Für VoIP-Gateways genügt es, den Namen festzulegen.

**Name**

Der H.323-Name.

**Number**

Die E.164-Rufnummer.

Die Standard-Eingabefelder des **Coder Preferences** Abschnittes sind bereits im Kapitel: „*Administration/Gateway/Interfaces/Interface (Physische und Virtuelle Schnittstellen)*“ beschrieben.

Zusätzlich stehen im Abschnitt **H.323 Interop Tweaks** erweiterte Einstellungsmöglichkeiten zur Verfügung. Sie sind im Normalfall nicht nötig, und dienen lediglich dazu Kompatibilitätsprobleme mit manchen TK-Anlagen zu lösen:

**No Faststart**

Die H.245-Faststart-Prozedur ist standardmäßig aktiviert. Ausgehende Rufe werden mit Faststart ausgeführt, eingehende Rufe mit Faststart werden mit Faststart beantwortet.

Ein markiertes Kontrollkästchen deaktiviert die H.245-Faststart-Prozedur womit ausgehende Rufe ohne Faststart ausgeführt werden und eingehende Rufe mit und ohne Faststart ohne Faststart beantwortet werden.

**No H.245 Tunneling** Die H.245-Tunneling Prozedur ist standardmäßig aktiviert. Die Aushandlung der Sprachdatenverbindung wird in der bereits vorhandenen TCP-Signalisierungsverbindung<sup>a</sup> durchgeführt. Dies kann im Zusammenhang mit NAT und Firewalls von Vorteil sein. Ein markiertes Kontrollkästchen deaktiviert die H.245-Tunneling-Prozedur, womit eine eigene TCP-Verbindung für diese Aushandlung aufgebaut wird. Dies gilt für die aus dem Gatekeeper hinausführende Signalisierungsverbindung.

**Suppress HLC** Ein markiertes Kontrollkästchen deaktiviert das Senden von HLC-Information-Elements (**H**igh-**L**ayer-**C**ompatibility).

**Suppress FTY** Ein markiertes Kontrollkästchen deaktiviert das Senden von FTY-Informationelementen (**F**acility).

**Suppress Sub-address** Ein markiertes Kontrollkästchen deaktiviert das Senden von Subaddress-Information-Elements.

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

#### 4.2.1.3.2 CGPN-CDPN-Mappings

Eine detailliertere Beschreibung ist unter dem Kapitel: „*Administration/Gateway/Interface/CGPN-CDPN-Mappings*“ zu finden.

#### 4.2.1.4 Administration/Gateway/Routes

Die wichtigste Aufgabe des Gateways ist die Rufbehandlung. Sie legt fest, welche Rufe akzeptiert werden und wohin sie vermittelt werden.

Die Rufbehandlung erfolgt durch den Gatekeeper des Gateways, welche durch Routen (für Sprache) kontrolliert wird. Für jede Rufrichtung muss eine Route definiert werden. Geht ein Ruf über mehrere Gateways, so muss in jedem Gateway eine entsprechende Route definiert werden. Eine Route definiert einen zulässigen Weg eines Rufes von einer Schnittstelle, an der der Ruf eingeht, zu einer Schnittstelle an der der Ruf wieder hinausgeht. Dabei werden oftmals Rufe von verschiedenen Schnittstellen gleichartig behandelt. So können beispielsweise Rufe von mehreren ISDN-Schnittstellen (z.B. TEL1 und TEL2) oder auch von

mehreren VoIP-Schnittstellen (GW1-12) zugelassen werden.

Die Rufvermittlung hängt oft auch von der gewählten Rufnummer ab. Dazu muss die Gültigkeit von Routen für Rufe mit bestimmter Zielrufnummer mittels eines Map-Eintrags festgelegt werden. Jeder Map-Eintrag legt fest, dass Rufe von den in der Route angegebenen Quellschnittstellen, die mit der im Map-Eintrag angegebenen Ziffernkombination beginnen, auf die in der Route festgelegten Zielschnittstelle verbunden werden können.

Alle definierten Routen werden zeilenweise in der Routing-Tabelle angezeigt. Für jeden einzelnen Ruf wird die Routing-Tabelle von oben nach unten nach einem passenden Map-Eintrag durchsucht. Ist die Vermittlung auf die ermittelte Schnittstelle nicht möglich, so wird der nächste Map-Eintrag in der Routing-Tabelle gesucht, der den angegebenen Bedingungen entspricht. Wurde ein Map-Eintrag gefunden, so wird der aktuelle Ruf an die Zielschnittstelle des angelegten Map-Eintrags weitervermittelt. Wurde kein passender Map-Eintrag gefunden, so ist der Ruf unzulässig und es findet keine Vermittlung statt.

#### 4.2.1.4.1 From - To

Die Routing-Tabelle ist wie folgt aufgebaut:

<b>From</b>	Die Quellschnittstelle von der ein Ruf akzeptiert werden soll. Das können sowohl ISDN-Schnittstellen (TEL, BRI, PRI etc.) sein oder aber auch VoIP-Schnittstellen (GW1-12).
<b>To</b>	Die Zielschnittstelle an welche ein Ruf weitervermittelt werden soll. Das können sowohl ISDN-Schnittstellen (TEL, BRI, PRI etc.) sein oder aber auch VoIP-Schnittstellen (GW1-12).
<b>CGPN Maps</b>	Das CGPN-Map ( <b>Calling-Party-Number</b> ) wird für das Ändern der rufenden Nummer verwendet. Damit kann beispielsweise bei ausgehenden Rufen die Durchwahl unterdrückt werden oder aber auch der gesamte Map-Eintrag von der rufenden Nummer abhängig gemacht werden.

Um einen neuen Routing-Eintrag zu erstellen muss die Schaltfläche *Insert Route below* angeklickt werden. Es öffnet sich eine Popup-Seite, in welcher die Routeneinstellung vorgenommen werden kann.



Diese Popup-Seite beinhaltet auch die Angabe der Map-Einträge. Ein Klick auf die Schaltflächen *Add Map above/below* öffnet die selbe Popup-Seite und fügt einen Map-Eintrag an entsprechender Stelle hinzu. Diese Popup-



Seite ist wie folgt aufgebaut:

- Description** Der beschreibende Name für die Route.
- Quell-schnitt-stelle** Hier wird die ISDN- oder VoIP-Schnittstelle selektiert, die für die entsprechende Route als Quelle gültig sein soll. Es können auch mehrere Quellen selektiert werden. Je nach Verfügbarkeit stehen folgende Quellschnittstellen zur Verfügung: *RT, RS, TEL, BRI, PRI, PPP, TEST, TONE, HTTP, SIP* und *GW*.
- Number In** Um die Routing Entscheidung abhängig von einem Map-Eintrag zu machen, muss hier die rufende Nummer eingetragen werden. Wurde hier keine Nummer angegeben, dann ist der Map-Eintrag für alle Rufe gültig.  
Es stehen zusätzliche Varianten der Rufnummernmanipulation zur Verfügung:  
Soll eine Route für eine bestimmte Nummer gelten und alle Wahlziffern, die anschliessend noch gewählt werden, ignoriert werden, muss der angegebenen Rufnummer der Operator „!“ folgen.  
Manche Geräte benötigen den Operator „#“ als Signalisierungszeichen für das Ende eines Rufes. Dafür kann das Kontrollkästchen *Add #* (siehe Beschreibung weiter unten im Text) markiert werden.  
Mit dem Operator „?“ besteht zusätzlich die Möglichkeit eine variable un- und bekannte Anzahl an Zeichen durch ein bestimmtes zu ersetzen. Zum Beispiel: „???” mit 1 ersetzen ergibt bei „1234“ -> „14“ oder aber auch „0????“ mit 1 ersetzen ergibt bei „01234“ -> „14“, da die bekannte Ziffer 0 ebenfalls ersetzt wird.  
Mit dem Operator „.“ kann an eine bestimmte Anzahl an Zeichen ersetzt werden. Zum Beispiel: „...“ mit „123“ ersetzen ergibt bei „321“ -> „123“.
- Number Out** Sofern gewünscht wird hier die zu ersetzenden Rufnummer der Route eingetragen. Soll die Rufnummer unverändert übernommen werden, muss hier die gleiche Rufnummer wie in *Number In* angegeben werden.  
**Achtung:** Wurde die rufende Nummer manipuliert, dann darf das Kontrollkästchen *Verify CGPN* nicht markiert sein, da die Überprüfung der rufenden Nummer fehlschlagen würde und der Map-Eintrag somit wirkungslos wäre.

- Zielschnittstelle** Hier wird die Schnittstelle selektiert, die für die entsprechende Route als Ziel gültig sein soll. Je nach Verfügbarkeit stehen folgende Zielschnittstellen zur Verfügung: *RT, RS, TEL, BRI, PRI, PPP, TEST, TONE, HTTP, SIP, GW, MAP und DISC*.
- Name Out** Soll der H.323-Rufname verändert werden, kann hier der neue Rufname eingetragen werden.
- Cause (DISC)** Wurde die Zielschnittstelle DISC gewählt kann zusätzlich noch ein sogenannter *disconnection-cause* (siehe Anhang C: „*ISDN-Fehlerwerte*“) angegeben werden, um auf dem Endgerät eine entsprechend passende Ausgabe zu erzielen.

Für jede Routendefinition lassen sich erweiterte Einstellungen tätigen:

- Add UUI** Sollen herstellerspezifische Daten im Signalisierungskanal übertragen werden, z.B. die URL für eine Ansage, so kann diese URL (<http://192.168.1.2/webdav>) hier angegeben werden.
- Final Route** Ein markiertes Kontrollkästchen simuliert das Ende der Routen. Sollten noch weitere Routen folgen, werden diese ignoriert.
- Final Map** Ein markiertes Kontrollkästchen simuliert das Ende der Map-Einträge. Sollten noch weitere Map-Einträge vorhanden sein, werden alle weiteren Map-Einträge ignoriert.
- Exclude from Auto-CGPN** Wurde im Kapitel: „Administration/Gateway/General“ das Kontrollkästchen *Automatic CGPN-Mapping* markiert, dann kann die entsprechende Route durch Markierung dieses Kontrollkästchens von der Automatischen Korrektur aller rufenden Nummern ausgeschlossen werden.



- Verify CGPN** Die Routing-Entscheidung findet normalerweise auf Basis der Routen selber und der in den Routen definierten Map-Einträge statt. Mit einem aktivierten Kontrollkästchen findet die Routing-Entscheidung auf Basis der CGPN-Maps statt. Was bedeutet das zuerst eine Überprüfung der rufenden Nummer stattfindet und nur bei einer Übereinstimmung der rufenden Nummer die Routing Tabelle weiter abgearbeitet wird und z.B. eine Rufvermittlung stattfindet.  
Da dies nur der Verifizierung und Einschränkung bestimmter Nummern gilt, wird hier sinnvollerweise keine Manipulation der Rufnummer vorgenommen. Auf diese Art kann zum Beispiel der Zugang zu einer gebührenpflichtigen Amtsleitung auf bestimmte Nebenstellen beschränkt werden (selektive Amtsberechtigung).  
Wurde im Kapitel: „*Administration/Gateway/General*“ das Kontrollkästchen *Automatic CGPN-Mapping* markiert, dann wirkt die Prüfung auf die bereits korrigierte Nummer.
- Interworking (QSIG)** Ein markiertes Kontrollkästchen übersetzt H.323 oder SIP nach QSIG. Wobei von QSIG nach H.323 oder SIP nicht übersetzt sondern transparent übertragen wird (findet Verwendung bei einer Kopplung gleichartiger TK-Anlagen über VoIP).
- Force enblock** Ein markiertes Kontrollkästchen erzwingt Blockwahl. D.h. sollte ein Map-Eintrag zutreffen, dann werden alle folgenden Wahlziffern gesammelt, bis seit dem letzten Tastendruck mehr als vier Sekunden vergangen sind.
- Add #** Ein markiertes Kontrollkästchen sendet das Raute (#)-Zeichen als Kennzeichnung des Endes einer Rufnummer. Dies wird nur bei Endgeräten benötigt, die das Ende der Rufnummer nicht erkennen (wie z.B. Cisco-Geräte).
- Disable Echo Canceller** Ein markiertes Kontrollkästchen unterdrückt die Echokompensation für den entsprechenden Map-Eintrag. Dies ist meistens nur notwendig, sollte eine Verbindung als Sprachverbindung verwendet werden die keine Echokompensierung durchführen soll wie das z.B. bei Modems der Fall ist.
- Call Counter max** Steht nicht ausreichend Bandbreite zur Verfügung kann über das Eingabefeld *Call Counter* ein Name und in das Eingabefeld *max* die maximale Anzahl von Rufen eingetragen werden, die für die entsprechenden Route zulässig ist.

Ein Klick auf den Namen einer Route (z.B. TEL1:Amt) filtert die Anzeige der Routen nach der eingestellten Schnittstelle. Ein erneuter Klick auf den Namen der Route blendet die nicht zugehörigen Routen wieder ein. Sollten zum Beispiel mehrere Routen für die TEL1-Schnittstelle angelegt sein, so blendet ein Klick auf eine der TEL1-Schnittstellen alle anderen Routen aus, die nicht TEL1 als Quell- oder Zielschnittstelle ausgewählt haben.

Mit der neben stehenden Pfeil-Schaltfläche (—>) können Routen editiert werden.

#### 4.2.1.4.2 CGPN-Maps

Es ist auch oftmals notwendig Routen in Abhängigkeit von der rufenden Nummer festzulegen. Um dies zu erreichen muss ähnlich wie Maps an Routen angefügt werden, sogenannte CGPN-Maps an die Maps angefügt werden. Damit lassen sich sowohl rufende Nummern manipulieren, um z.B. bei ausgehenden Rufen die Durchwahl zu unterdrücken, als auch das ganze Map von der rufenden Nummer abhängig zu machen.

Mit der Pfeil-Schaltfläche (—>) in der Spalte CGPN-Maps können solche definieren und editieren.

<b>Number In</b>	Die rufende Nummer. Das CGPN-Map ist gültig, sollte die eingehende E.164-Rufnummer mit der hier eingestellten Rufnummer oder Rufnummernanfang übereinstimmen.
<b>Name In</b>	Der rufende Name. Das CGPN-Map ist gültig, sollte der eingehende H.323-Rufname mit dem hier eingestellten Namen übereinstimmen.
<b>Number Out</b>	Hier wird die für die Vermittlung zu ersetzenden Rufnummer oder Rufnummernanfang eingetragen.

#### 4.2.1.5 Administration/Gateway/CDR0-1

Das Senden der sogenannten CDR (**Call-Detail-Records**) ist standardmäßig deaktiviert (**Off**). Nach Auswahl eines CDR-Types wird das Senden von detaillierten CDRs aktiviert und die entsprechenden Eingabefelder freigeschaltet. Das kein Datenverlust im Falle eines Ausfalls des ersten CDR-Servers (**CDR0**) entsteht, besteht die Möglichkeit einen zweiten CDR-Server (**CDR1**) anzugeben.

<b>Off</b>	CDR ist deaktiviert.
------------	----------------------

- TCP** Das Gerät sendet die CDR-Einträge über eine TCP-Verbindung.
- In das Eingabefeld **Address** wird die IP-Adresse eingetragen, zu welcher die TCP-Verbindung aufgebaut werden soll.
  - Im Eingabefeld **Port** wird der Port angegeben, zu dem die Verbindung aufgebaut wird.

- SYSLOG** Die CDR-Einträge werden an einen Syslog-Empfänger übermittelt (wird auch als `syslogd`, `syslog server` oder `syslog daemon` bezeichnet). Dieser ist dann für die weitere Auswertung oder Abspeicherung zuständig.
- In das Eingabefeld **Address** wird die IP-Adresse des `syslogd` servers eingetragen.
  - Im Eingabefeld **Class** wird die gewünschte Meldungs-kategorie eingetragen, die für die weitere Verarbeitung der CDR-Einträge zuständig sein soll.

- HTTP** Die CDR-Einträge werden an einen Webserver übertragen und können dort weiter verarbeitet werden. Jeder einzelne CDR-Eintrag wird als Formularaten im HTTP-GET-Format an den Webserver übertragen.
- In das Eingabefeld **Address** wird die IP-Adresse des Web-servers eingetragen, der die Weiterverarbeitung der über-mittelten Daten übernimmt.
  - In das Eingabefeld **Path** wird die relative URL des Formu-larprogramms auf dem Webserver eingegeben.

Das Gerät wird zum Webserver einen HTTP\_GET-Request auf die eingetragene URL, gefolgt vom url-encodeten CDR-Eintrag stellen. Besteht beispielsweise auf einem Webserver eine Seite namens `/cdr/cdrwrite.asp` mit einem Formular, das die Log-Meldung im Parameter `msg` erwartet, dann wird der Wert `/cdr/cdrwrite.asp` eingetragen. Das Gerät wird dann einen `GET /cdr/cdrwrite.asp?event=syslog&msg=logmsg` Request an den Webserver stellen.

## 4.2.1.6 Administration/Gateway/Calls

In der Gateway-Übersichtseite **Calls** können alle aktiv geführten Rufe beobachtet werden. Dies ist besonders für Diagnosezwecke von Vorteil, da z.B. sofort ersichtlich ist ob Netzprobleme vorhanden sind (siehe **Coder**):

<b>Interfaces</b>	Anzeige des rufenden interface.
<b>Protocol</b>	Anzeige des verwendeten Protokolls auf der rufenden Seite.
<b>Coders</b>	Anzeige des verwendeten Coders auf der rufenden Seite. Zum Beispiel <i>G711AB(2,0,0)</i> . Die Werte in Klammern bedeuten in Reihenfolge: <ul style="list-style-type: none"><li>• round-trip = Laufzeit eines Datenpaketes von A nach B und wieder zurück.</li><li>• jitter = Latenzzeit (Zeitintervall vom Ende eines Ereignisses bis zum Anfang der Reaktion).</li><li>• loss = Anzahl der verlorengegangener Pakete (package loss).</li></ul>
<b>Number</b>	Anzeige der gerufenen Nummer.
<b>State</b>	Mögliche Zustände: <i>Alerting, Calling, Connected, Disconnecting</i> .

## 4.2.2 Administration/Download

Die Konfiguration des VoIP-Gerätes kann über dieses Menü gesichert werden.

### 4.2.2.1 Administration/Download/Config

Hiermit kann die aktuelle Konfiguration des VoIP-Gerätes gespeichert werden. Nach Betätigung des Links **Download** erscheint eine Popup-Seite, in welcher angegeben werden kann, ob die Konfigurationsdatei als txt-Datei gespeichert, oder sofort mit einem Editor geöffnet werden soll.

## 4.2.3 Administration/Upload

Es gibt mehrere Möglichkeiten, das VoIP-Gerät zu aktualisieren.

## **Hinweis**

Detailliertere Informationen bezüglich der Statusanzeige (Ready LED) während des Aufspiels von Dateien auf das Gerät können dem innovaphone knowledgebase Artikel „*How to Reset IPxxx , factory default, led behaviour, tftp mode, clear config, gwload*“ (<http://www.innovaphone.com/innov-kb>) entnommen werden.

### **4.2.3.1 Administration/Upload/Config**

Mit dieser Funktion kann eine gespeicherte Konfiguration (siehe Kapitel: „*Administration/Diagnostics/Config Show*“) auf das Gerät geladen werden.

Durch Angabe von Pfad und Dateinamen der zu ladenden Konfigurationsdatei im Feld **File** und einem darauf folgenden Klick auf die Schaltfläche **Upload** wird die Konfigurationsdatei in das Gerät geladen.

Dabei ist zu beachten, dass die Konfigurationsdatei in den flüchtigen Speicher des Gerätes geladen wird. Sie ist damit weder permanent gesichert noch sofort wirksam. Das Gerät muss demnach noch kurz zurückgesetzt werden. Nähere Informationen zum Zurücksetzen des Gerätes sind im Kapitel: „*Administration/Reset*“ enthalten.

### **4.2.3.2 Administration/Upload/Firmware**

Diese Funktion ermöglicht es, manuell eine neue Firmware-Version auf das VoIP-Gerät aufzuspielen. Dies kann auch automatisiert werden, indem wie in Kapitel: „*Configuration/General/Update*“ beschrieben, ein Update-Server konfiguriert wird. Neue Firmware-Versionen können von einem zertifizierten innovaphone-Händler oder direkt über die innovaphone-Homepage (<http://www.innovaphone.com>) bezogen werden.

Durch Angabe von Pfad und Dateinamen der zu ladenden Konfigurationsdatei im Feld **Firmware-File** und einem darauf folgenden Klick auf die Schaltfläche **Upload** wird die Konfigurationsdatei in das Gerät geladen.

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

Wird der Ladevorgang trotzdem unterbrochen, sollte das Gerät danach auf keinen Fall ausgeschaltet werden. Die Prozedur sollte vielmehr wiederholt werden, nachdem das Problem beseitigt wurde.

Man beachte die den neuen Versionen beiliegenden Unterlagen, um festzustellen, ob auch eine neue Boot-Firmware geladen werden muss. Ist dies der Fall, dann muss, wenn angegeben, ebenfalls beachtet werden, ob auch die geforderte Reihenfolge von Bootcode und Firmware-Update eingehalten wird.

Die neue Firmware wird nicht direkt aktiv. Es muss ein Reset ausgeführt werden, um die neue Version zu aktivieren. Dazu werden die Links **immediate reset** und **reset when idle** angeboten. Nähere Informationen zum Zurücksetzen des Gateways sind im Kapitel: „*Administration/Reset*“ enthalten.

### 4.2.3.3 Administration/Upload/Boot

Eine neue Bootcode-Version kann mit dieser Funktion auf das VoIP-Gerät aufgespielt werden. Neue Bootcode-Versionen können von einem zertifizierten innovaphone-Händler bezogen werden.

Durch Angabe von Pfad und Dateinamen der zu ladenden Bootcode-Firmware im Feld **Boot-File** und einem darauffolgenden Klick auf die Schaltfläche **Upload** wird die Bootcode-Firmware in das Gerät geladen.

Während des Ladens der neuen Bootcode-Firmware wird darauf hingewiesen, den Ladevorgang auf keinen Fall zu unterbrechen.

Wird der Ladevorgang trotzdem unterbrochen, sollte das Gerät danach auf keinen Fall ausgeschaltet werden. Die Prozedur sollte vielmehr wiederholt werden, nachdem das Problem beseitigt wurde.

Der neue Bootcode wird nicht direkt aktiv. Es muss ein Reset ausgeführt werden, um die neue Version zu aktivieren. Dazu werden die Links **immediate reset** und **reset when idle** angeboten. Nähere Informationen zum Zurücksetzen des Gerätes sind im Kapitel: „*Administration/Reset*“ enthalten.

Dabei ist in den neuen Versionen beiliegenden Unterlagen zu beachten, ob auch eine neue Protocol-Firmware geladen werden muss.

### 4.2.4 Administration/Diagnostics

Mit Hilfe des Menüs **Diagnostics** kann der Betriebszustand des Gerätes überwacht werden.

## 4.2.4.1 Administration/Diagnostics/Logging

Über den Link **Syslog** können die Log-Meldungen des Gerätes direkt im laufenden Betrieb angesehen werden. Die Meldungen werden ständig selbsttätig aktualisiert und scrollen nach oben aus dem Fenster heraus.

Es werden nur Meldungen angezeigt, die im Untermenü **Logging** aktiviert wurden. Folgende Einstellungen können aktiviert werden:

<b>TCP</b>	Alle TCP-Verbindungen.
<b>PPP</b>	Alle PPP-Verbindungen.
<b>Relay-Calls</b>	Alle Rufe, die über das Relay gehen - nur bei Geräten mit S <sub>0</sub> oder S <sub>2m</sub> Schnittstelle sichtbar.
<b>Relay-Routing</b>	Alle Rufe, die über das Relay geroutet werden müssen - nur bei Geräten mit S <sub>0</sub> und S <sub>2m</sub> Schnittstelle sichtbar.
<b>DECT-Master</b>	Alle DECT-Master-Verbindungen - Nur bei IP-DECT-Systemen sichtbar.
<b>DECT-Radio</b>	Alle DECT-Radio-Verbindungen - Nur bei IP-DECT-Systemen sichtbar.
<b>H.323-Registrierungen</b>	Alle H.323-Registrierungen.
<b>SIP-Registrierungen</b>	Alle SIP-Registrierungen.
<b>Config-Changes</b>	Alle Konfigurations Änderungen.
<b>TEL1-n</b>	Alle TEL1-n-Verbindungen - Nur bei Geräten mit TEL-Schnittstelle sichtbar.
<b>PPP</b>	Alle PPP-Verbindungen - Nur bei Geräten mit PPP-Schnittstelle sichtbar.
<b>BRI1-n</b>	Alle BRI1-n-Verbindungen - Nur bei Geräten mit BRI-Schnittstelle sichtbar.
<b>PRI1-n</b>	Alle PRI1-n-Verbindungen - Nur bei Geräten mit PRI-Schnittstelle sichtbar.

Ein Klick auf *OK* speichert die gemachten Einstellungen.

## 4.2.4.2 Administration/Diagnostics/Tracing

Über den Link **trace (buffer)** können die Trace-Informationen des VoIP-Gerätes angesehen und abgespeichert werden. Dabei wird eine Textdatei *log.txt* generiert, welche den aktuellen Trace in einem neuen Browserfenster anzeigt.

Über den Link **trace (continous)** können die fortlaufenden Trace-Informationen des Gerätes angesehen und abgespeichert werden. Dabei wird eine Textdatei *c/log.txt* generiert, welche den aktuellen Trace in einem neuen Browserfenster anzeigt. Wie bereits erwähnt, werden die Meldungen ständig selbsttätig aktualisiert und scrollen nach oben aus dem Fenster heraus.

Für beide Trace-Varianten gilt, dass nur Meldungen angezeigt werden, die in diesem Menü aktiviert wurden. Je nachdem welches Gerät verwendet wird ist nicht jeder Abschnitt und nicht jede Einstellung ersichtlich:

### Abschnitt **DECT**:

<b>System</b>	Informationen zum DECT-System.
<b>Master</b>	Informationen zum DECT-Master.
<b>Radio</b>	Informationen zum DECT-Radio.

### Abschnitt **Interfaces**:

<b>PPP</b>	Informationen zum PPP-Interface.
<b>TEL1-n</b>	Informationen TEL1-n-Interface.
<b>BRI1-n</b>	Informationen zum BRI1-n-Interface.
<b>PRI1-n</b>	Informationen zum PRI1-n-Interface.
<b>prot</b>	Das Kontrollkästchen <b>prot</b> hinter den einzelnen Interface-Einstellungen geben Informationen zum verwendeten Protokoll.

### Abschnitt **VOIP**::

<b>H.323/ RAS</b>	Informationen zu H.323-RAS.
<b>H.323/ H.225</b>	Informationen zu H.323/H.225.



<b>H.323/ H.245</b>	Informationen zu H.323/H.245.
<b>H.323/ T.38</b>	Informationen zu H.323/T.38
<b>H.323/ T.30</b>	Informationen zu H.323/T.30
<b>SIP/Mes- sages</b>	Informationen zu SIP/Messages.
<b>SIP/ Events</b>	Informationen zu SIP/Events.
<b>SIP/T.38</b>	Informationen zu SIP/T.38.
<b>DSP</b>	Informationen zu DSP.
<b>DSP con- trol mes- sages</b>	Informationen zu DSP control messages.
<b>DSP data messages</b>	Informationen zu DSP data messages.

#### Abschnitt **IP**:

<b>PPP</b>	Informationen zum PPP-Protokoll.
<b>PPTP</b>	Informationen zum PPTP-Protokoll.
<b>PPoE0-1</b>	Informationen zum PPoE0/1-Protokoll.
<b>DHCP0-1</b>	Informationen zum DHCP0/1-Server.
<b>HTTPCLI- ENT</b>	Informationen zum HTTP-Client.
<b>HTTPCLI- ENT ver- bose</b>	Detaillierte Informationen zum HTTP-Client

Ein Klick auf *OK* speichert die gemachten Einstellungen.

#### **4.2.4.3 Administration/Diagnostics/Config Show**

**Config Show** ermöglicht, die aktuelle Konfiguration des VoIP-Gerätes in Text-

form auszugeben.

Die aktuelle Konfiguration kann auch in einer Datei abgespeichert werden, indem – je nach verwendetem Browser – die Funktion **Frame Speichern unter** verwendet wird. Man kann auch den gesamten Text markieren (Ctrl-A) und mit der rechten Maustaste (oder Ctrl+C) über das Kontextmenü in die Zwischenablage kopieren. Jetzt kann die Konfiguration in jeden Texteditor kopiert (Ctrl+V) und abgespeichert werden.

Eine auf diese Art gesicherte Konfiguration kann ganz oder teilweise wieder aufgespielt werden. Auf diese Art und Weise kann die Konfiguration gesichert und wieder hergestellt werden oder es können Referenzkonfigurationen erstellt und auf eine Vielzahl von Geräten geladen werden.

#### 4.2.4.4 Administration/Diagnostics/Ping

Es besteht die Möglichkeit, einen **Ping** auf einen bestimmten Zielhost (**IP-Adresse**) abzusetzen, da es oft für Testzwecke notwendig ist, direkt vom VoIP-Gerät aus ein Ping-Kommando abzusetzen. Damit kann überprüft werden, ob eine Netzwerkadresse (PC, Drucker, Telefon, etc.) erreichbar ist. Ist eine Adresse erreichbar, so wird dem Sender `Reply from <host>` angezeigt. Ist die Adresse nicht erreichbar, so wird `No Reply from <host>` angezeigt.

#### 4.2.5 Administration/Reset

Zusätzlich zu der Möglichkeit das Gerät über den Hardware Reset Schalter zurück zusetzen, gibt es mit Hilfe des Webbrowsers drei weitere Möglichkeiten, das VoIP-Gerät zurück zusetzen.

##### **Hinweis**

Informationen bezüglich der Reset Funktion über den Hardware Schalter am Gerät sind im Anang A: „Anschlüsse und Bedienelemente“ in der Tabelle 1 „Anzeigen und Anschlüsse der IP6000“ („Reset“) enthalten.

Weitere, detailliertere Information können dem innovaphone knowledgebase Artikel „How to Reset IPxxx , factory default, led behaviour, tftp mode,clear config,gwload“ (<http://www.innovaphone.com/innob-kb>) entnommen werden.

## 4.2.5.1 Administration/Idle Reset

Bei einem **Idle-Reset** wird das VoIP-Gerät zurückgesetzt, sobald keine aktiven Gespräche mehr geführt werden.

## 4.2.5.2 Administration/Reset/Reset

Bei einem normalen **Reset** wird das Gerät sofort zurückgesetzt. Alle aktiven Gespräche gehen verloren.

## 4.2.5.3 Administration/Reset/TFTP

Mit einem **TFTP-Reset** wird das VoIP-Gerät in den TFTP-Modus versetzt. Befindet sich das Gerät im TFTP-Modus, so kann dieses nur noch mit dem Tool GW-Load erreicht und somit eine IP-Adresse vergeben werden. Weitere Informationen zum Tool innovaphone-GWLoad können der innovaphone knowledgebase entnommen werden.

## Anhang A: Anschlüsse und Bedienelemente

### Anzeigen und Anschlüsse

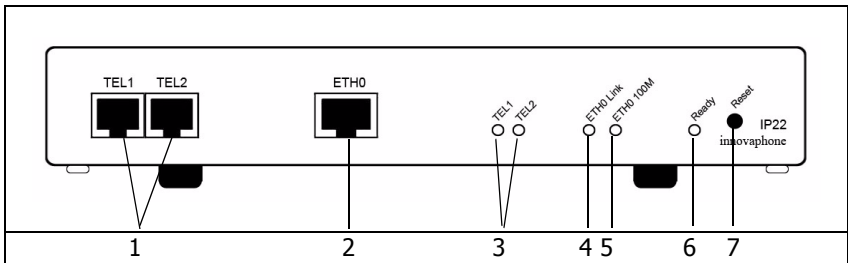


Abbildung 1 - Anzeigen und Anschlüsse der IP22

Pos.	Symbol	Beschreibung und Funktion
1	<b>TEL1-2</b>	RJ11-Buchse zum Anschluss eines analogen Telefons.
2	<b>ETH0</b>	RJ45-Buchse zum Anschluss eines 100 Mbit/s Ethernet (10/100 <sub>Base-T</sub> auto sense).
3	<b>TEL1-2 LED</b>	LED zur Anzeige, dass Daten auf der <b>TEL1</b> - oder der <b>TEL2</b> -Schnittstelle gesendet oder empfangen werden.
4	<b>ETH0 Link LED</b>	LED zur Anzeige, dass Daten auf der <b>ETH0</b> Schnittstelle gesendet oder empfangen werden.
5	<b>ETH0 100M LED</b>	LED zur Anzeige, dass das 100 Mbit/s Netz für die <b>ETH0</b> Schnittstelle aktiv ist.

6	<b>Ready LED</b>	<p>Drei-farbige LED zur Statusanzeige des Gerätes:          LED leuchtet grün, wenn betriebsbereit.          LED blinkt schnell in grün, wenn die config gelöscht wird oder Firmware/Bootcode Dateien aufgespielt werden.          LED leuchtet orange, wenn im TFTP-Modus.          LED leuchtet rot bei einem Neustart oder wenn Fehler aufgetreten sind.          LED blinkt schnell in rot, wenn Firmware/Bootcode Dateien aufgespielt werden.          Siehe auch Beschreibung zu „Reset“ in Tabelle 1 „Anzeigen und Anschlüsse der IP22“.</p>
7	<b>Reset</b>	<p>Zusätzlich zu der Möglichkeit das Gerät über den Webbrowser zurück zusetzen, gibt es mit Hilfe der Reset Taste drei bzw. vier weitere Möglichkeiten, das Gerät zurück zusetzen.</p> <p><b>Kurzer Reset:</b> Ein kurzer Reset startet das Gerät neu. Alle aktiven Rufe gehen verloren.</p> <p><b>Mittlerer Reset (TFTP-Reset):</b> Hält man die Reset-Taste solange gedrückt, bis die Ready LED ein bis zweimal grün blinkt und läßt dann los, so wird das Gerät in den TFTP-Modus versetzt. Alle alle ISDN-LEDs werden gelöscht und Ready leuchtet orange.</p> <p><b>Langer Reset (Factory-Reset):</b> Hält man die Reset Taste gedrückt, so blinkt die Ready LED 4-6 mal auf, wechselt dann aber nach rot. Läßt man die Reset Taste jetzt wieder los, so beginnt der Löschvorgang der Konfiguration. Die Ready-LED bleibt gut 5 Sekunden rot, beginnt dann aber sehr schnell für etwar 3 Sekunden rot-grün zu flackern und löscht anschließend alle ISDN-LEDs. Die Ready LED wird orange und das Gerät befindet sich im TFTP-Modus.</p> <p><b>Power-Cycle:</b> Bedeutet das Gerät kurz von der Stromzufuhr zu nehmen. Funktioniert sowohl technisch als auch optisch wie der kurze Reset.</p>

Abbildung 2 Anzeigen- und Anschlussbeschreibung der IP22

## Hinweis

Informationen bezüglich der Software-Reset Funktion über den Webbrowser sind im Kapitel: „*Administration/Reset*“ enthalten.

Weitere, detailliertere Information können dem innovaphone knowledgebase Artikel „*How to Reset IPxxx, factory default, led behaviour, tftp mode, clear config, gwload*“ (<http://www.innovaphone.com/innokb>) entnommen werden.

## Das Seriennummernetikett

Auf der Geräteverpackung und auf der Gehäuseunterseite befindet sich das Seriennummernetikett.

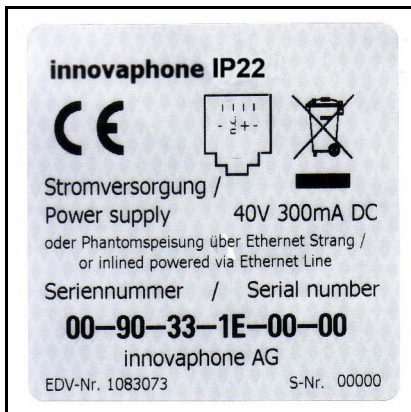


Abbildung 3 Das Seriennummernetikett der IP22

Die MAC-Adresse ist gleichzeitig die Seriennummer Ihrer IP22.

Die ersten drei durch einen Bindestrich (‘-’) getrennten konstanten Hexadezimalzahlen stellen die Herstellerkennung von innovaphone dar (009033 oder 00-90-33), während die letzten drei Hexadezimalzahlen (1E0000 oder 1E-00-00) die fortlaufende Seriennummer der IP22 darstellen.

## Anhang B: Problembhebung

Bestimmte Probleme treten unserer Erfahrung nach häufiger auf. Die nachstehende Tabelle 1 listet diese Probleme und gibt Hinweise zu deren Behebung.

### Typische Probleme

Symptom	Erläuterung	Maßnahme
Das VoIP-Gerät reagiert nicht. <b>Ready</b> , <b>Link</b> und <b>100M</b> . LED leuchten ununterbrochen.	Das VoIP-Gerät wartet auf einen Firmware-Download.	<ul style="list-style-type: none"> <li>Führen Sie einen Kurzen Reset durch Betätigen der <b>Reset</b>-Taste durch.</li> </ul>
Das VoIP-Gerät reagiert nicht. <b>Ready</b> LED leuchtet, <b>Link</b> LED blinkt unregelmäßig.	Die Ethernet-Verbindung funktioniert nicht.	<ul style="list-style-type: none"> <li>Überprüfen Sie die Ethernet-Verkabelung.</li> </ul>
Das VoIP-Gerät reagiert nicht. <b>Ready</b> und <b>Link</b> LEDs leuchten, <b>100M</b> . LED blinkt bei Zugriffsversuch.	Das VoIP-Gerät hat eine falsche IP-Adresse konfiguriert.	<ul style="list-style-type: none"> <li>Stellen Sie die IP-Parameter korrekt ein.</li> </ul>
Im Auslieferungszustand weist das VoIP-Gerät dem PC keine IP-Adresse zu.	Nach dem Einschalten ist der DHCP-Client aktiv.	<ul style="list-style-type: none"> <li>Betätigen Sie kurz die Reset-Taste.</li> <li>Lassen Sie dem PC erneut eine IP-Adresse zuweisen.</li> </ul>
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.	<ul style="list-style-type: none"> <li>Konfigurieren Sie in der Konfiguration für das entfernte VoIP-Gerät eine effizientere Sprachkodierung.</li> </ul>
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.	<ul style="list-style-type: none"> <li>Stellen Sie sicher, dass das Kontrollkästchen „<i>exclusive</i>“ deaktiviert ist.</li> </ul>

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 Sprachkoder verfügen.	Nur der Medienkanal wird direkt zwischen den beiden VoIP-Geräten aufgebaut, alle Signalisierungsverbindungen laufen über den Gatekeeper. <ul style="list-style-type: none"> <li>• Stellen Sie sicher, dass beide VoIP-Geräte über eine korrekte IP-Routerkonfiguration verfügen, insbesondere Subnetzmaske und Standardgateway.</li> </ul>
Rufe zu einem entfernten Telefoniegateway werden von diesem immer abgelehnt.	Das Gerät unterstützt keine Einzelziffernachwahl.	<ul style="list-style-type: none"> <li>• Fügen Sie im Rufnummernpräfix der zu diesem Gateway führenden Route eine Raute (#) ein, um Blockwahl zu erzwingen.</li> </ul>
Das VoIP-Gerät verliert seine Konfiguration nach dem Trennen von der Stromversorgung.	Die Konfiguration wurde nicht in den nichtflüchtigen Speicher gesichert.	<ul style="list-style-type: none"> <li>• Sichern Sie die Konfiguration nach erfolgreichen Änderungen in den nichtflüchtigen Speicher.</li> </ul>
Das VoIP-Gerät ist hinter einer Firewall ans Netz angeschlossen und die Konfiguration funktioniert nicht.	Die Firewall lässt den Zugriff auf das VoIP-Gerät nicht zu.	<ul style="list-style-type: none"> <li>• Schalten Sie in der Firewall den Zugriff des VoIP-Gerätes für den Dienst tcp/80 (http) frei.</li> </ul>
Das VoIP-Gerät 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.	<ul style="list-style-type: none"> <li>• 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.</li> <li>• Lesen Sie im Kapitel „NAT und Firewalls“ nach.</li> </ul>

Tabelle 1 Fehlerbehebung



## Port-Einstellungen bez. NAT und Firewalls

Ist ein Netzwerk durch eine Firewall zum Internet hin geschützt und soll eine Verbindung zu Gegenstellen über das Internet aufgebaut werden, so muss für eine geeignete Konfiguration der Firewall gesorgt werden.

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 (NAT). 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 der Firewall bzw. Router-Firmware geleistet werden.

Sollte das verwendete Produkt kein H.323-Firewalling aufweisen, so gibt es zwei Vorgehensweisen:

- In der Firewall den Weg für alle benötigten Daten von und zum VoIP-Gerät freischalten.

Diese Lösung wird von Netzwerkadministratoren meist nicht gern gesehen, ist jedoch risikolos, da das VoIP-Gerät als dediziertes Gerät keine anderen Dienste außer Voice-over-IP abwickelt. Ein Öffnen des Weges von und zum Gerät eröffnet daher keine Sicherheitslücken in einem Netzwerk.

Die Anzahl der freizuschaltenden Ports für H.323- oder SIP-Geräte lässt sich eingrenzen.

Bei H.323 müssen für beide Richtungen folgende Ports freigeschaltet werden:

- UDP:1718,1719 (H.225/RAS)
- TCP:1720 (H.225/Signaling)
- TCP: dynamic allocation (H.245/Control - optional)

Wird das SIP-Protokoll verwendet, sind zusätzlich abhängig vom interface typ freizuschalten:

- UDP:5060 (SIP Phone, Registrar, Without Registration)
- UDP:any free (Gateway mode)

Alle anderen Registrierungen verwenden keine Standard-Ports.

T.38 via H.323 oder SIP verwendet zwei Ports über den Standard RTP-Ports.

Für eine Sprachverbindung wird ein RTP-Port und ein RTCP-Port verwendet. Somit verwendet jeder Ruf zwei freie Ports aus dem RTP-Port-Bereich. Der RTP-Port-Bereich liegt standardmäßig zwischen 16384 und 32767. Dieser Port-Bereich, welcher für H.323- und SIP-Rufe gültig ist, kann unter dem Kapitel: „*Configuration/IP/Settings*“ eingestellt werden. Der kleinste Port-Bereich sind 128 Ports.

Die Config Option „Fixed RTP-Send Port xxx“ kann nicht in der Benutzeroberfläche konfiguriert werden. Diese muss direkt in die Konfigurationsdatei geschrieben werden. Für alle Verbindungen wird dieser eine konfigurierte RTP-Port verwendet. Dieser Fixed RTP-Send Port ist abgelöst vom RTCP-Port. Es wird nicht empfohlen einen Fixed RTP-Send Port einzustellen, da anschließend RTP nicht mehr symmetrisch arbeitet und es zu Interoperabilitäts Problemen mit Fremdprodukten führen kann.

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

- Das Gerät wird vor die Firewall plaziert, sodass der Datenstrom die Firewall nicht passieren muss. In diesem Fall wird man keine Sprachverbindungen innerhalb des Netzes aus zum Gerät aufbauen können (z.B. mit innovaphone Softphone-PC´s).

Wird das Netzwerk im NAT-Modus betrieben und das 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.

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

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

Kann der verwendete Router anhand des ToS-Feldes (**Type-of-Service**) priorisieren, kann diese Funktion verwendet werden. Das VoIP-Gerät setzt in allen IP-Paketen die es sendet das ToS-Priority-Feld auf den Wert  $0 \times 10$ . Dieser Wert

kann bei Bedarf unter dem Kapitel: „*Configuration/IP/Settings*“ verändert werden.

## **Tipp**

Dieser Wert kann hexadezimal, oktal oder dezimal angegeben werden, die Eingaben `0x10`, `020` und `16` sind gleichwertig. Der Wert für das ToS-Priority Feld sollte auf allen verwendeten Geräten gleich gesetzt sein.

Ist dies nicht der Fall, dann könnte, wenn vorhanden, die Funktion Priorisierung nach Quell- / Ziel-Adresse helfen. Damit werden Datenpakete von und zum Gerät 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. In einem solchen Fall sollte überprüft werden, ob sich diese Unterbrechung gesondert anschalten lässt. Manche Router bezeichnen diese Funktion etwas verwirrend als **interleaving**.

## Anhang C: ISDN-Fehlerwerte

Die folgende Tabelle gibt die im Q.931 Standard definierten ISDN-Fehlerwerte an:

<b>Fehlerwert (hex)</b>	<b>Fehlerwert, Bit 8 zu 1 gesetzt (hex)</b>	<b>Fehlerwert (dezimal)</b>	<b>Bedeutung</b>
0x1	0x81	1	Rufnummer nicht zugeordnete
0x2	0x82	2	Keine Route zum spezifizierten Übergangsnetzwerk
0x3	0x83	3	Keine Route zum angegebenen Ziel
0x6	0x86	6	Kanal unzulässig
0x7	0x87	7	Ruf wurde gewährt und in einem zulässigen Kanal durchgestellt
0x10	0x90	16	Normale Ruf freigabe
0x11	0x91	17	Benutzer belegt
0x12	0x92	18	Benutzer reagiert nicht (Ruf wird nicht signalisiert)
0x13	0x93	19	Benutzer reagiert nicht (Ruf wird signalisiert)
0x15	0x95	21	Ruf zurückgewiesen
0x16	0x96	22	Geänderte Rufnummer
0x1A	0x9A	26	Non-selected user clearing
0x1B	0x9B	27	Ziel gibt es nicht
0x1C	0x9C	28	Ungültiges Nummernformat

0x1D	0x9D	29	Informations Element zurückgewiesen
0x1E	0x9E	30	Rückantwort zu STATUS ENQUIRY
0x1F	0x9F	31	Normal, unspezifiziert
0x22	0xA2	34	Keine Verbindung/Kanal verfügbar
0x26	0xA6	38	Netzwerk nicht erreichbar
0x29	0xA9	41	Temporärer fehler
0x2A	0xAA	42	Überlastung des Switches
0x2B	0xAB	43	Zugriffsinformation verworfen
0x2C	0xAC	44	Angeforderte Verbindung/Kana nicht erreichbar
0x2D	0xAD	47	Ressourcen nicht erreichbar, unspezifiziert
0x31	0xB1	49	Quality of service nicht erreichbar
0x32	0xB2	50	Angefordertes Informations Element nicht bestellt
0x39	0xB9	57	Bearer capability nicht autorisiert
0x3A	0xBA	58	Bearer capability nicht erreichbar
0x3F	0xBF	63	Service oder Option nicht erreichbar, unspezifiziert
0x41	0xC1	65	Bearer capability nicht implementiert
0x42	0xC2	66	Kanal Typ nicht implementiert
0x45	0xC5	69	Angefordertes Informations Element nicht implementiert

0x46	0xC6	70	Nur eingeschränkte digitale bearer capability Informationen erreichbar
0x4F	0xCF	79	Service oder Option nicht implementiert, unspezifiziert
0x51	0xD1	81	Ungültiger Wert für die Ruf-Quellenangabe
0x52	0xD2	82	Identifizierter Kanal existiert nicht
0x53	0xD3	83	Ein unterdrückter Ruf existiert, jedoch ohne Ruf-Identität
0x54	0xD4	84	Ruf-Identität in gebrauch
0x55	0xD5	85	Kein Ruf unterdrückt
0x56	0xD6	86	Der Ruf mit der angeforderten Ruf-Identität wurde bereinigt
0x58	0xD8	88	Inkompatible Ziele
0x5B	0xDB	91	Ungültige Übergangsnetzwerk Selektion
0x5F	0xDF	95	Ungültige Nachricht, unspezifiziert
0x60	0xE0	96	Fehlendes Mandatory Informations Element
0x61	0xE1	97	Nachrichten Typ existiert nicht oder nicht implementiert
0x62	0xE2	98	Nachricht nicht kompatibel mit Ruf-Status
0x63	0xE3	99	Informations Element existiert nicht oder ist nicht implemented
0x64	0xE4	100	Ungültige Inhalte in den Informations Elementen

0x65	0xE5	101	Nachricht nicht kompatibel mit Ruf-Status
0x66	0xE6	102	Wiederherstellung verfällt zum Zeitpunkt
0x6F	0xEF	111	Protokoll fehler, unspezifiziert
0x7F	0xFF	127	Zusammenarbeit, unspezifiziert

## Anhang D: Support

Sollte der Support eines Händlers in Anspruch genommen werden, sollten folgende Informationen bereitgehalten werden:

- Die komplette Versionsbezeichnung des Gerätes. Diese ist auf der Begrüßungsseite des Gerätes zu finden (siehe Kapitel: „*Configuration/General/Info*“).
- Einen Trace, der die Fehlersituation zeigt (siehe Kapitel: „*Administration/Diagnostics/Tracing*“).
- Die gesamte Konfiguration wie durch **Config Show** angezeigt (siehe Kapitel: „*Administration/Diagnostics/Config Show*“).
- Die Seriennummer, welche auf dem Seriennummernetikett auf der Unterseite des Gehäuses oder auf der Begrüßungsseite des Gerätes (siehe Anhang A: „*Anschlüsse und Bedienelemente*“ oder auch Kapitel: „*Configuration/General/Info*“).

## Firmware Upload

Die innovaphone VoIP-Geräte werden nicht mit der aktuellsten Firmware ausgeliefert, sodass in der Regel ein Firmware-Upload notwendig ist.

Neue Firmware-Versionen können im Downloadbereich (<http://download.innovaphone.com>) der innovaphone-Homepage bezogen werden.

## innovaphone Homepage

Auf der innovaphone-Homepage (<http://www.innovaphone.com>) sind alle aktuellen Service-Packs, Bootcodes, Hotfixes, Firmware-Updates, Manuals, Datensheets etc. enthalten. Zudem besteht die Möglichkeit einen Newsletter zu beantragen, in diesem man ständig über aktuelle innovaphone-Neuigkeiten informiert wird.

In Zukunft wird es die Möglichkeit geben, Reklamationen online über die innovaphone-Homepage aufzusetzen. Dies ermöglicht einen einfacheren und schnelleren Bearbeitungsprozess.



## Anhang E: Konfiguration des Update-Servers

Es besteht die Möglichkeit, die Firmware und Konfiguration einer großen Anzahl von innovaphone-Geräten in einer verteilten Umgebung automatisch zu aktualisieren.

Das geschieht, indem die Konfigurations- und Firmware-Informationen auf einen Standard-Webserver abgelegt werden, welche wiederum von den einzelnen Geräten abgerufen wird.

Die Geräte besitzen zwei Module, die zusammen arbeiten. Das erste Modul „UP0“ ist für den down- und upload von Konfigurationsinformationen sowie auch für den download von neuen Firmware-Dateien zuständig. UP0 wird mit den beschriebenen Kommandos weiter unten im Text gesteuert.

Das zweite Modul, bekannt als „UP1“ fragt regelmäßig eine bestimmte Webadresse nach geänderten Konfigurations Informationen ab. Wurden bestimmte Voraussetzungen erfüllt, so wird UP1 das angeforderten Update durchzuführen.

### System Voraussetzungen

- Ein oder mehrere von den Geräten erreichbarer Webserver.
- Getestet wurden MS-IIS und der Apache-Server. Es sollte aber auch mit allen anderen gängigen Webservern funktionieren.
- Um bestmögliche Ergebnisse zu erzielen, sollte der Webserver eine große Anzahl von gleichzeitigen HTTP-Sessions verwalten können. Der MS-Personal-Webserver ist zum Beispiel ein ungeeigneter Webserver, da er maximal 10 gleichzeitige HTTP-Sessions verwalten kann.

### Installation

Um Gerätekonfigurationen auf den Webserver übertragen zu können, muss dieser HTTP-PUT-Anfragen erlauben. Alle anderen Funktionen setzen lediglich eine HTTP-GET-Berechtigung voraus.

Da alle HTTP-Anfragen unauthentifiziert ausgeführt werden, muss der Webserver anonymes Lesen und eventuell auch anonymes Schreiben erlauben.

Um auf einen MS-IIS HTTP-PUT-Kommandos zu erlauben, muss in der Konfiguration des entsprechenden Virtuellen-Verzeichniss das Kontrollkästchen *read* und *write* aktiviert sein.

## Konfiguration

Detaillierte Information wie der URL-Parameter des Update-Servers auf den innovaphone-Geräten konfiguriert wird, können dem Kapitel „*Configuration/General/Update*“ entnommen werden.

Dabei ist zu beachten, dass der URL-Parameter genau auf den Speicherort der Datei mit den enthaltenen Wartungs-Kommandos zeigen muss. Genauso ist zu beachten, dass diese URL (sowie alle anderen URL's, die von innovaphone-Geräten verwendet werden) keine Hostnamen unterstützt. Demnach muss immer eine gültige IP-Adresse angegeben werden.

Sollte die URL mit einem '/' enden, dann wird ein Standard-Dateiname basierend auf der Produktbeschreibung verwendet. Wenn zum Beispiel die URL `http://1.2.3.4/configs/` ist, dann wird diese im Falle einer IP1200 um `http://1.2.3.4/configs/update-ip1200.htm` erweitert. Der Produktname ist im Kapitel „*Configuration/General/Info*“ in der ersten Zeile angegeben. Die Dateiendung ist dabei irrelevant. Es kann `.txt` oder auch `.htm` oder aber auch gar keine Dateiendung verwendet werden. Dabei ist zu beachten, dass bei Angaben von URLs, manche Webserver zwischen Groß- und Kleinschreibung unterscheiden.

## Wartungsdurchführung

Die Update-Datei wird sofort gelesen und auch sofort ausgeführt. Nach einem Neustart des Gerätes wird der Update-Server automatisch mit dem eingestellten Intervall periodisch abgefragt.

Wenn die Wartungsdatei erfolgreich empfangen wurde, wird diese sequentiell ausgeführt. Theoretisch können alle Kommandos, die in einer Telnet-Session an das Gerät abgesetzt werden können oder welche in einer Konfigurationsdatei auftreten, in der Wartungsdatei verwendet werden.

## Wartungskommandos

Es sind zusätzliche, spezielle Kommandos verfügbar, die extra für den Update-Server implementiert wurden.

Die Wartungsdatei wird jedes Mal (abhängig vom eingestellten Intervall) ausgeführt, sobald diese empfangen wurde.

## Check-Kommando

In den meisten Fällen jedoch soll die Wartungsdatei nicht jedes Mal ausgeführt

werden, sobald diese empfangen wird, sondern nur einmal. Angenommen, es soll eine sichere Konfiguration auf mehrere Geräte aufgespielt werden, dann sollte dies idealerweise von einem Gerät vorgenommen werden. Das kann mit dem Kommando `check` erreicht werden:

```
mod cmd UP1 check <final-command> <serial>
```

innovaphone-Geräte besitzen eine interne, initial leere Variable (oder wenn das Gerät mit den Standard-Einstellungen zurückgesetzt wurde) namens UPDATE/CHECK. Das `check` Kommando wird den Inhalt von `<serial>` mit der UPDATE/CHECK Variable verglichen. Stimmen beide überein, wird jeder weitere Prozess der Wartungsdatei abgebrochen.

Wenn Sie sich unterscheiden sollten, werden die restlichen Prozesse ausgeführt und nachdem der letzte Prozess ausgeführt wurde, wird die UPDATE/CHECK Variable mit dem Inhalt von `<serial>` überschrieben und der Inhalt von `<final-command>` wird ausgeführt. Die folgenden Kommandos sind brauchbare Inhalte für `<final-command>`

- `ireset`: Setzt das Gerät zurück, sobald dieses nicht aktiv verwendet wird.
- `reset`: Setzt das Gerät sofort zurück.
- `iresetn`: Setzt das Gerät zurück, sobald dieses nicht aktiv verwendet wird und ein Rücksetzen erforderlich ist.
- `resetn`: Setzt das Gerät sofort zurück, sollte ein Rücksetzen erforderlich sein.
- `ser`: Ist eine globale Variable und keine Funktion.

## Time-Kommando

Oft wird es gewünscht, solche Änderungen zu bestimmten Zeiten durchzuführen (z.B.: Nachts, da in dieser Zeit nicht gearbeitet wird). Dies kann mit dem `times` Kommando erreicht werden:

```
mod cmd UP1 time [/allow <hours>]
```

Das `time`-Kommando wird die aktuelle Zeit mit dem Inhalt von `<hours>` vergleichen. `<hours>` ist eine kommasetrennte Liste von Stundenangaben, in der eine Ausführung der Wartungsdatei möglich ist. Stimmt der Inhalt von `<hours>` mit der Eingrenzung nicht überein, so wird jeder weitere Prozess abgebrochen. Folgende Stunden wurden als gültige Zeiten erachtet, in der eine Ausführung der Wartungsdatei sinnvoll ist.

```
mod cmd UP1 time /allow 12,22,23,0,1,2,3,4
```

Mit diesem Befehl wird eine Ausführung der Wartungsdatei in den Stunden von

12:00 Uhr - 12:59 Uhr und von 22:00 Uhr - 04:59 Uhr gestattet. Sollte das Gerät nicht über eine Zeit verfügt, werden alle Prozesse abgebrochen.

```
mod cmd UP1 time [/allow <hours>] [/initial <minutes>]
```

Sollte der `/initial` Parameter gesetzt sein, werden keine weiteren Befehle innerhalb der angegebenen Minutenzahl `<minutes>` ausgeführt, nachdem das Gerät zurückgesetzt wurde. Dies wurde implementiert, um während der Installation der Geräte einen Firmware-Download und Flashen zu vermeiden.

```
mod cmd UP1 time /allow 12,22,23,0,1,2,3,4 /initial 6
```

Mit dieser Angabe werden alle Prozesse der Wartungsdatei innerhalb der ersten 6 Minuten und innerhalb der angegebenen gültigen Zeiten im `/allow` Parameter nach jedem Neustart des Gerätes unterdrückt. Wurde der Parameter `/initial` gesetzt, können neue Geräte (oder Geräte die mit den Standard-Einstellungen zurückgesetzt wurden) nach einem Neustart die Wartungsdatei innerhalb der angegebenen Minuten im Parameter `/initial` empfangen, auch wenn Sie außerhalb der gültigen Zeiten, wie im Parameter `/allow` angegeben liegen. Dies erlaubt neuen Geräten schnell, eine aktuelle Standard-Konfiguration zu erhalten.

## Prot-Kommando

Um ein Firmware-Update einzuleiten, kann folgender Befehl abgesetzt werden:

```
mod cmd UP0 prot <url> <final-command> <built-serial>
```

Dieser Befehl wird eine neue Firmware (wenn vorhanden) von angegebener URL heruntergeladen und auf das Gerät aufgespielt. Zuletzt wird das `<final-command>` ausgeführt.

innovaphone Geräte besitzen eine interne, initial leere Variable (oder wenn das Gerät mit den Standard-Einstellungen zurückgesetzt wurde) namens UPDATE/PROT. Das `prot`-Kommando wird den Inhalt von `<built-serial>` mit der UPDATE/PROT Variable verglichen. Stimmen beide überein, wird keine Firmware heruntergeladen und aufgespielt. Ist die Variable UPDATE/PROT nicht gesetzt (bei Neugeräten oder nach einem Neustart des Gerätes), wird der Inhalt von `<built-serial>` mit der Built-Number der aktuellen Firmware verglichen. Nach einem erfolgreichen Herunterladen der Firmware wird die Variable UPDATE/PROT mit dem Inhalt von `<built-serial>` überschrieben. Man beachte, dass der Parameter `<built-serial>` nicht mit der aktuell geladenen Firmware-Version verglichen wird. Es ist die Zuständigkeit des Administrators, dies einheitlich zu halten.

Wenn der Parameter `<url>` mit einem Slash (`/`) endet, wird ein Standard-Firmware-Dateiname der URL angehängt, abhängig von der Produktbezeichnung

(z.B: IP1200.bin für ein IP-DECT-System).

```
mod cmd UP0 prot http://192.168.0.10/firm/ip1200.bin ireset
04-5656
```

Der Befehl

```
mod cmd UP0 prot http://192.168.0.10/firm/ ireset 04-5656
```

ermittelt, ob die Firmware-Version 04-5656 bereits installiert wurde. Ist dies nicht der Fall, dann wird die aktuelle Firmware von der Adresse `192.168.0.10/firm/ip1200.bin` heruntergeladen, die interne Variable `UPDATE/PROT` mit 04-5656 überschrieben und zuletzt wird das Gerät zurückgesetzt, sobald dieses nicht mehr aktiv verwendet wird.

## Boot-Kommando

Ähnlich wie beim `prot`-Kommando, wird beim `boot`-Kommando der Bootcode aktualisiert.

```
mod cmd UP0 boot <url> <final-command> <built-serial>
```

Der Befehl

```
mod cmd UP0 boot http://192.168.0.10/firm/ ireset 205
```

ermittelt, ob die Bootcode-Version 205 bereits installiert wurde. Ist dies nicht der Fall, dann wird der aktuelle Bootcode von der Adresse `192.168.0.10/firm/bootip1200.bin` heruntergeladen, die interne Variable `UPDATE/BOOT` mit der Versionsnummer der heruntergeladenen Bootcode-Version (205) überschrieben und zuletzt wird das Gerät zurückgesetzt, sobald dieses nicht mehr aktiv verwendet wird.

## SCFG-Kommando

Wird die Schnittstelle **UP0** verwendet, dann kann die Gerätekonfiguration auf einem Webserver gespeichert werden.

```
mod cmd UP0 scfg <url>
```

Dieser Befehl wird das Gerät dazu veranlassen, seine aktuelle Konfiguration auf die `<url>` hochzuladen. Dies kann mit dem HTTP-PUT-Kommando erreicht werden. Die `url` muss schreibbar sein. In der `url` können folgende Konstanten verwendet werden:

Sequenz	Ersetzt	Beispiel
#d	Aktuelles Datum und Zeit	20051010-170130

Sequenz	Ersetzt	Beispiel
#m	MAC-Adresse des Gerätes	00-90-33-03-0d-f0
#h	Geräte Hardware Nummer	IP1200-03-0d-f0

## Beispiel

Es existiert ein Webserver unter der Adresse 192.168.0.10 mit einem Unterverzeichnis namens `configs`. In diesem Verzeichnis wiederum existieren weitere Unterverzeichnisse, in denen die aktuellen Firmware-Dateien für alle innovaphone-Geräte abgelegt sind.

Den DHCP-Server stellen Clients mit der Option #215 als `http://192.168.0.10/configs/` bereit. In diesem Verzeichnis existiert eine Datei `update-ip1200.htm` welche folgende Zeilen abarbeitet:

```
mod cmd UP1 times /allow 23,0,1,2,3,4 /initial 6
mod cmd UP0 scfg http://192.168.0.10/configs/saved/
#h.txt
mod cmd UP0 prot http://192.168.0.10/configs/04-5679 /
ser 04-5679
mod cmd UP1 check ser 20040330-01
config change PHONECFG0 /coder G729A,60, /lang eng /protect
config change PHONEAPP0 /f4-10 BellOff /f4-v0 %1BE /f5-10 BellOn /f5-v0 %1BF
config write
config activate
iresetn
```

Es gibt auch die Datei `update-ip3000.htm`, welche folgende zwei Zeilen liest:

```
mod cmd UP1 time /allow 23,0,1,2,3,4
mod cmd UP0 prot http://192.168.0.10/configs/04-5679 /
ser 04-5679
```

Dieses Beispiel demonstriert, wie die Konfiguration eines Gerätes auf einen Webserver abgespeichert wird, anschließend alle IP1200 Geräte dazu veranlasst werden, die Firmware-Version 04-5679 im Zeitraum von 23:00 Uhr - 04:59 Uhr aufzuspielen bzw. zu aktualisieren. Neue Geräte werden nach einem Neustart und nach Ablauf der angegebenen 6 Minuten aktualisiert. Die Geräte werden so konfiguriert, dass sie den G729-Codec mit einer Rahmengröße von 60ms verwenden, die Spracheinstellung englisch und die Konfiguration schreibgeschützt ist. Somit kann eine Änderung dieser Datei nur von einem Administrator mit entsprechender Berechtigung vorgenommen werden. Zusätzlich wurden zwei Stan-

Standard-Funktionen für das Gerät programmiert.

IP3000-Geräte werden im Zeitraum von 23:00 Uhr - 04:59 Uhr auf Firmware-Version 04-5679 aktualisiert.

## Anhang F: Konfiguration eines NTP-Servers/ -Clients

Sollte ein Netzwerk über keinen NTP-Server verfügen, dann kann ein öffentlicher Zeit-Server verwendet werden. So bietet beispielsweise die TU-Berlin unter der IP-Adresse 130.149.17.21 einen Zeitdienst an. Dieser Service ist freiwillig, womit kein Anspruch auf dessen Verfügbarkeit besteht.

Jeder Windows-Server kann als NTP-Server fungieren. Ebenso gibt es verschiedene NTP-Softwarepakete für Windows- und Unix/Linux-Plattformen.

Die innovaphone VoIP-Geräte arbeiten gleichzeitig auch als NTP-Server. Sollten mehrere Geräte verwendet werden, so kann ein Gerät sich mit einem, gegebenenfalls externen Zeitserver synchronisieren und alle anderen wiederum mit diesem einen.

Das taktvorgebende VoIP-Gerät arbeitet dann selbst als Zeitdienst und wird dann die korrekte Zeit an die anderen Geräte übermitteln. Es sollte vermieden werden, alle Geräte mit einem externen Zeitdienst zu synchronisieren, da dies zu unnötig hoher Last auf diesen Server führt.

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

### Timezone-Strings (TZ-String):

Zeitdienste liefern immer die koordinierte Weltzeit UTC (**U**niversal-**T**ime-**C**oordinated), dies entspricht der GMT (**G**reenwich-**M**ean-**T**ime), nicht jedoch die korrekte Zeitzone und auch nicht die Sommerzeit. Daher besteht die Möglichkeit, die Distanz der Zeitzone zur Weltzeit im Feld **String** anzugeben. In der Zeitzone GMT+1 (das ist die Mitteleuropäische Zeitzone) beträgt diese Distanz 60 Minuten. In der Sommerzeit kommen noch weitere 60 Minuten hinzu, sodass der Abstand insgesamt 120 Minuten beträgt. In diesem Fall muss jedoch bei Umstellung von Winter- auf Sommerzeit und umgekehrt die Distanz manuell entsprechend angepasst werden.

Wurde ein so genannter Timezone-String in das Feld **String** eingetragen, so kann das Gerät die Umstellung von Sommer- auf Winterzeit automatisch vornehmen. In dieses Feld werden der Name der Zeitzone, der Name der Sommerzeitzone, Ihre jeweilige Distanzen zur UTC und die Umschaltzeitpunkte kodiert.

Es gibt verschiedene Formate wie dieser String angegeben werden muss. Diese Formate werden durch den IEEE-POSIX-Standard definiert.

POSIX-Timezone-Strings haben folgende Form (optionale Teile in eckigen Klamm-



mern):

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

`std` ist der Bezeichner der Zeitzone (z.B. `CET` für **Central-European-Time** oder `MEZ` für **Mittel-Europäische-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. Falls die Distanz nicht ganze Stunden umfasst, kann die Anzahl von Minuten abgehängt werden, beispielsweise `-1:30`.

Wird keine Sommerzeit verwendet, dann 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 **Middle-European-Summer-Time**).

Der optionale zweite `offset` Parameter gibt die Distanz der Sommerzeit zur 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 `Mm.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`

Weitere Informationen zum POSIX-Standard können unter der Webadresse <http://standards.ieee.org/catalog/olis/posix.html> abgerufen werden.

## Anhang G: Anleitung zum Herunterladen von Lizenzen

Aufruf der Seite <http://www.innovaphone.com/index.php?id=29&L=1>. Es wird der Lizenzvertrag angezeigt, der mit *Ja* bestätigt werden muss.



The screenshot shows a Mozilla Firefox browser window displaying the website <http://www.innovaphone.com/index.php?id=29&L=1>. The page features the innovaphone logo with the tagline "PURE IP-TELEPHONY" and a search bar. A navigation menu on the left includes links for Home, Unternehmen, Lösungen, Produkte, Presse, Partner, Schulungen, Download, Lizenzmanager, and Login / Logout. The main content area is titled "Lizenzvertrag für die innovaphone PBX Software" and contains the following text:

Bitte lesen Sie die nachfolgenden Bestimmungen dieses Vertrages sorgfältig durch. Mit der Verwendung der innovaphone PBX Software erklären Sie sich einverstanden, durch die Bestimmungen dieses Lizenzvertrages gebunden zu sein. Wenn Sie die innovaphone PBX Lizenz nicht bei innovaphone direkt, sondern bei einem innovaphone Vertriebspartner gekauft haben, sind zwischen Ihnen und der innovaphone AG noch keine vertraglichen Beziehungen entstanden. Wenn Sie im Nachgang zum Lesen dieses Dokumentes mit JA bestätigen, erklären Sie sich einverstanden, durch die Bestimmungen dieses Lizenzvertrages gebunden zu sein. Sind Sie nicht mit dem Lizenzvertrag einverstanden, bestätigen Sie im Nachgang mit NEIN.

Dieser Lizenzvertrag enthält sämtliche Vereinbarungen im Verhältnis zwischen Ihnen (im folgenden auch Kunde genannt) und der innovaphone AG (im folgenden innovaphone) bezüglich der Nutzung der innovaphone PBX Software und ersetzt alle Vorschläge oder früheren mündlichen oder schriftlichen Vereinbarungen hinsichtlich des Vertragsgegenstandes.

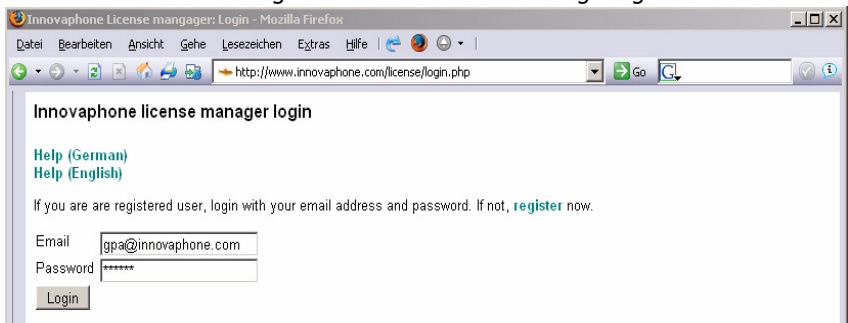
**§ 1 Vertragsgegenstand**

(1) Gegenstand dieses Vertrages ist die Übertragung des Nutzungsrechts an der innovaphone PBX Software, die Sie nach Durchlesen und Bestätigen dieses Lizenzvertrages aktivieren können. Die innovaphone PBX Software kann derzeit auf jedem beliebigen innovaphone Voice-over-IP Gateway aktiviert, bzw. installiert werden. innovaphone behält sich vor, die Software für weitere, später verfügbare innovaphone Hardware nicht verfügbar zu machen. In jedem Fall darf die innovaphone PBX Software nur auf innovaphone Hardware betrieben und genutzt

Additional elements on the page include an "innovaphone Knowledge Base" logo, an "Activate! innovaphone License Activator" button, a newsletter subscription form, and a "Werden Sie Reseller" logo.

## Login

Anschließend wird der folgende Anmeldebildschirm angezeigt.



The screenshot shows a Mozilla Firefox browser window displaying the "Innovaphone license manager login" page. The page title is "Innovaphone license manager: Login - Mozilla Firefox" and the URL is <http://www.innovaphone.com/license/login.php>. The page content includes:

**Innovaphone license manager login**

[Help \(German\)](#)  
[Help \(English\)](#)

If you are a registered user, login with your email address and password. If not, [register](#) now.

Email:

Password:

Wurden bisher noch keine Lizenzen bei innovaphone herunter geladen, sollten

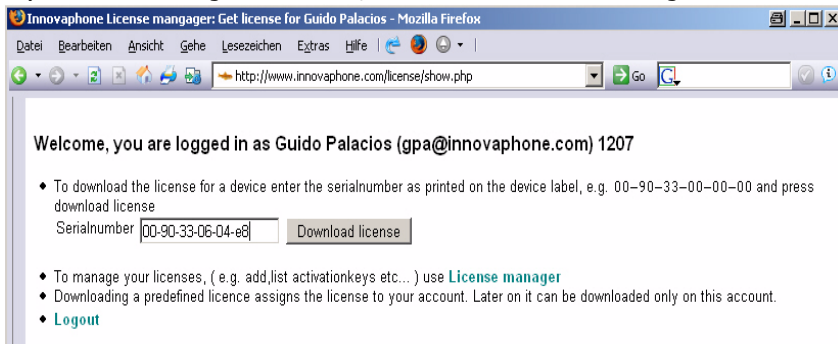
zuerst einmal die Hilfe-Seiten durchsucht werden.

Ansonsten muss eine gültige E-Mail-Adresse im Feld E-Mail und ein zugehöriges Passwort im Feld Passwort eingetragen werden.

## Download

Im oberen Teil des Bildschirms wird angezeigt, ob man sich ordnungsgemäß eingeloggt hat. Hier erscheint "Welcome you are logged in as Name { E-mail Adresse }".

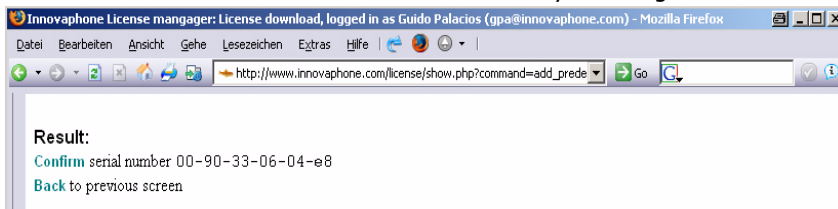
Darunter kann in dem leeren Feld *Serialnumber* die Seriennummer (MAC-Adresse) des Gerätes eingeben werden, für welches Lizenzen benötigt werden.



Ein Klick auf den Button *Download License* lädt die Lizenzen herunter.

## Ergebniss bestätigen

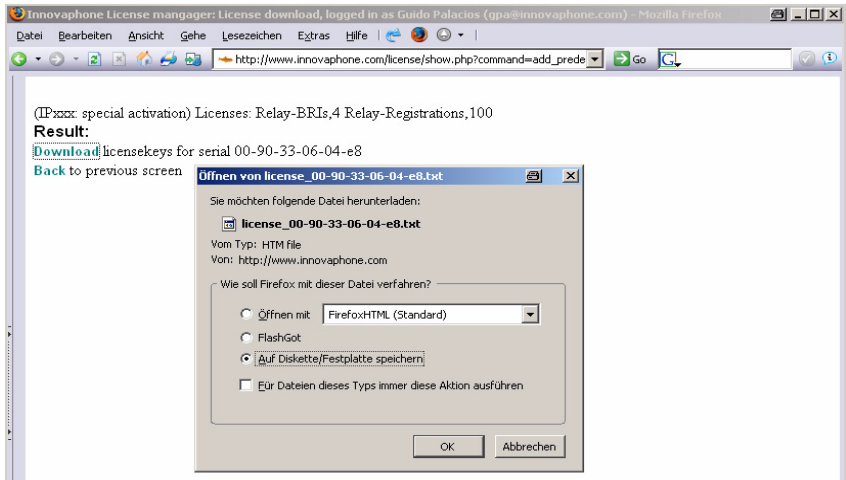
Als nächstes muss das Herunterladen des Licensekeys bestätigt werden.



Hierzu muss der Link *Confirm* betätigt werden, um die Seriennummer zu bestätigen und endgültig herunterzuladen.

## Ergebnis downloaden

Nach Bestätigung der Seriennummer ändert sich der Bestätigungslink in einen Downloadlink. Wird dieser angeklickt, öffnet sich ein „Öffnen mit - Speichern unter“- Dialog, in dem angegeben werden kann, ob die Datei auf der lokalen Festplatte gespeichert werden oder sofort geöffnet und betrachtet werden soll.



Die Lizenzen werden automatisch auch im Lizenzmanager verwaltet, sodass sie jederzeit wieder neu heruntergeladen werden können.

## Anhang H: Glossar

Der folgende Glossar bezieht sich auf alle innovaphone-Gateways und auch auf innovaphone-DECT-Gateways:

### A

#### A-Law

Das A-Law-Verfahren ist ein Verfahren für die Dynamikkompression von Audiosignalen, das in der ITU-Empfehlung G.711 beschrieben ist. Die Dynamikkompression dient der Verbesserung des Störspannungsabstands bei gleichen Übertragungsbedingungen. Das Verfahren verwendet eine logarithmische Dynamikkennlinie, die besonders bei niedrigen Eingangspegeln eine hohe Dynamik aufweist und bei hohen Eingangspegeln eine sehr geringe. Dadurch wird das Rauschen bei geringen Pegeln, also bei leisen Tönen reduziert. Das A-Law-Verfahren wird hauptsächlich in Europa verwendet, in den USA dagegen ein geringfügig in den Quantisierungsstufen abweichendes Verfahren, das  $\mu$ -Law-Verfahren. Dieses Verfahren zeichnet sich durch eine Dynamikkennlinie aus, die im Niederpegelbereich noch steiler ist als die des A-Law-Verfahrens.

#### Alt-Sync-Master

Eine alternative Synchronisierungsquelle.

#### ARI

Eine ARI (**A**ccess-**R**ights-**I**dentifier) ist ein eindeutiger Bezeichner für ein DECT-System.

#### ARP

Das ARP-Protokoll (**A**ddress-**R**esolution-**P**rotocol) ist ein typisches ES-IS-Protokoll (**E**nd-**S**ystem - **I**ntermediate-**S**ystem-**P**rotocol), das dazu dient die MAC-Adressen (**M**essage-**A**uthentication-**C**ode) in die zugehörigen IP-Adressen (**I**nternet-**P**rotocol) umzuwandeln, damit überhaupt eine Kommunikation auf der Vermittlungsschicht mittels des IP-Protokolls stattfinden kann. Das ARP-Protokoll legt zu diesem Zweck Mapping-Tabellen an, die die MAC-Adressen den Netzwerkadressen zuordnen.

#### Auto-MDX

Die Auto-MDX-Funktion ist die automatische Erkennung eines Uplink-Ports

an einer Ethernet-Schnittstelle. Mittels der Auto-MDX-Funktion werden keine Crossover-Kabel benötigt da die Ethernet-Schnittstelle die Sende- und Empfangsleitung automatisch wechseln kann.

## **B**

### **BRI**

Der Basisanschluss (BA), auch als BRI-Schnittstelle (**B**asic-**R**ate-**I**nterface) bezeichnet, ist der Standard-Anschluss an das ISDN (**I**ntegrated-**S**ervices-**D**igital-**N**etwork). Ein Basisanschluss bietet zwei Nutzkanäle (B-Kanäle, abgeleitet von bearer) mit je 64 kbit/s und einen Signalisierungskanal (D-Kanal, abgeleitet von data) mit 16 kbit/s. Die Nettobandbreite beträgt:  $2 \times 64 \text{ kbit/s} + 16 \text{ kbit/s} = 144 \text{ kbit/s}$ . Der Basisanschluss wird hauptsächlich von Privatkunden oder kleineren Betrieben genutzt, größere Unternehmen mit hohem Telefonaufkommen nutzen stattdessen den Primärmultiplexanschluss.

### **Broadcast**

Eine Broadcast-Übertragung entspricht einem Rundruf: gleichzeitige Übertragung von einem Punkt aus zu allen Teilnehmern. Um in einem lokalen Netz bestimmte Klassen von Empfängern oder alle angeschlossenen Stationen gleichzeitig anzusprechen, bestehen die Möglichkeiten des Multicast oder des Broadcast. In Lokalen Netzen ist ein Broadcast eine Nachricht, die an allen Geräten in allen Netzen verschickt wird. Sie wird von jedem Router an alle angeschlossenen Netzwerke weitergeleitet. Sollen alle Endgeräte eines bestimmten Netzes angesprochen werden, spricht man von Multicast oder Netzwerk-Broadcast.

## **C**

### **CCFP**

CCFP (**C**entral-**C**ontroller-**F**ixed-**P**art) ist eine Einheit, welche alle Basis-Stationen kontrolliert. Zuvor (mit der ip1500) wurden die DECT-Basis-Stationen über eine proprietäre Schnittstelle mit dem CCFP über ein 2-adriges Kabel verbunden.

Mit der IP1200 werden die DECT-Basis-Stationen über IP mit der CCFP Schnittstelle verbunden. Jede IP1200 verfügt über eine DECT-Basis-Station und eine Steuereinheit. In einer *multicell* Installation wird nur eine Steuer-

einheit von einer IP1200 verwendet (auch bekannt als IP-Master). Alle anderen DECT-Radios werden von diesem einen gesteuert. Das DECT-Radio in dieser Master IP1200 kann verwendet werden (gewöhnlich wird diese wie ein normales DECT-Radio verwendet, nur wenn das IP-DECT-System mehr als 64 Basis-Stationen verwendet, sollte das DECT-Radio in dem IP-Master nicht verwendet werden).

## **CDR**

Mit CDRs (**C**all-**D**etail-**R**ecords) bezeichnet man die Aufzeichnung aller Verbindungen in einer Datenbank, die für nachträgliche Aktivitäten, wie die Berechnung von Verbindungsgebühren oder für die Netzwerkanalyse, zur Verfügung stehen. CDR-Files werden in Festnetzen, in IP-Netzen bei der IP-Telefonie und auch in Mobilfunknetzen benutzt. In gewählten virtuellen Verbindungen beinhalten CDRs die Rufnummer, den Namen des Knotenrechners, das Datum und die Uhrzeit, die Verbindungsdauer und die Fehlermeldungen.

## **CFB**

Mit dem ISDN-Leistungsmerkmal CFB (**C**all-**F**orwarding-**B**usy) wird ein eingehender Anruf an eine bestimmte Nebenstelle weitergeleitet, sollte der Anschluss zu diesem Zeitpunkt besetzt sein.

## **CFNR**

Mit dem ISDN-Leistungsmerkmal CFNR (**C**all-**F**orwarding-**N**o-**R**esponse) wird ein eingehender Anruf an eine bestimmte Nebenstelle weitergeleitet, sollte nach einer konfigurierten Zeit der Anruf nicht entgegengenommen werden.

## **CFU**

Mit dem ISDN-Leistungsmerkmal CFU (**C**all-**F**orwarding-**U**nconditional) wird ein eingehender Anruf sofort an eine bestimmte Nebenstelle weitergeleitet.

## **CHI**

Ein Informationselement in GSM-Netzen, das den an der Benutzer-Netz-Schnittstelle zu verwendenden Kanal angibt.

## **CR**

Da bei ISDN eine Endeinrichtung mehrere Verbindungen gleichzeitig steuern kann, werden die einzelnen Verbindungen durch die Verbindungskennung eindeutig unterscheidbar. Jede Verbindung benutzt daher einen eigenen CR

(**Call-Reference**), der bei abgehenden Verbindungen von der Endeinrichtung vergeben wird, bei ankommenden vom Netz.

## **CTI**

CTI (**C**omputer-**T**elefonie-**I**ntegration) ist ein Mehrwertdienst zur Effizienzerhöhung bei Sprachübertragungen. Mit diesem Dienst können einfachste Anwendungen, wie die computerunterstützte Rufnummernwahl, bis hin zu kompletten Call-Centern als Dienstleistungen angeboten werden. Bei CTI handelt sich um die Unterstützung des Telefondienstes durch die Computertechnik. Dazu gehören neben der Unterstützung von Dienstleistungsmerkmalen mit ihren diversen Vermittlungsfunktionen auch das Management der TK-Anlage und der Benutzerkonten.

## **D**

## **DECT**

DECT (**D**igital-**E**uropean bzw. **E**nhanced-**C**ordless-**T**elecommunications) ist ein europäischer Standard für schnurlose Telefonie. DECT definiert die Luft-schnittstelle zwischen dem mobilen Handgerät und der Basisstation, wobei sowohl Sprachübertragung als auch Datenübertragung mit flexiblen Übertragungsgeschwindigkeiten unterstützt werden.

## **DECT-Base-Station**

Eine DECT-Base-Station kann einen Sprachkanal zwischen einem IP-DECT-Telefon und der innovaphone-PBX aufbauen.

## **DECT-Controller**

Kurzschrift für CCFP (**C**entral-**C**ontroller-**F**ixed-**P**art).

## **DECT-System**

Eine Sammlung von DECT-Radios mit einem Steuergerät. Alle DECT-Radios in diesem System teilen sich einen gewöhnlichen Identifikator (die sogenannte ARI). Ein Handover zwischen DECT-Radios ist nur in einheitlichen IP-DECT-Systemen möglich.

## **DHCP**

Das DHCP-Protocol (**D**ynamic-**H**ost-**C**onfiguration-**P**rotocol) ermöglicht mit Hilfe eines entsprechenden Servers die dynamische Zuweisung einer IP-Adresse und weiterer Konfigurationsparameter an Computer in einem Netz-



werk (z. B. Internet oder LAN).

## **DMS100**

Das veraltete DMS-100-Protokoll (**D**igital-**M**ultiplex-**S**ystem) der Northern Telecom (USA) ist der Vorläufer des NI-1-Protokolls.

## **DNS**

Das DNS-Protokoll (**D**omain-**N**ame-**S**ystem) ist ein Protokoll für die Umwandlung der IP-Adressen in Domain-Adressen. Es gehört zu der Gruppe der Namensdienste, bei denen die langen, komplizierten, in DDN (**D**otted-**D**ecimal-**N**otation) dargestellten IP-Adressen durch einfache Domain-Namen ersetzt werden. Die Umwandlung der IP-Adressen in eine Domain-Adresse kann sowohl über Host-Tabellen erfolgen als auch über das weltweit verteilte DNS, in der die Name-Server hierarchisch aufgebaut sind.

## **DTMF**

DTMF (**D**ual-**T**one-**M**ultiple-**F**requency, zu dt. Doppeltonmehrfrequenz) bzw. MFV ist das Mehrfrequenzwahlverfahren, auch Tonwahlverfahren genannt, welches die bei der analogen Telefontechnik gebräuchliche Wähltechnik ist und welches das heute überwiegend in der Telefonvermittlungstechnik zur Übermittlung der Rufnummer an das Telefonnetz oder einer Nebenstellenanlage genutzte Verfahren ist.

## **DSL**

Über DSL (**D**igital-**S**ubscriber-**L**ine) können Haushalte und Firmen Daten mit hoher Übertragungsrate senden (1000 bis 16.000 kbit/s) und empfangen. Dies ist eine wesentliche Verbesserung gegenüber Modem- oder ISDN-Verbindungen mit nur bis zu 64 kbit/s. An der verlegten Telefonleitung muss nichts geändert werden, denn DSL nutzt die bereits verlegten zwei bis vier Kupferadern des Telefonnetzes auf einer anderen, höheren Frequenz.

## **E**

### **E.164**

Die E.164-Nummerierung ist der am meisten benutzte Adressierungs-Standard in öffentlichen Kommunikationsnetzen. Dieses Rufnummernschema bildet das Regelwerk für die internationalen Rufnummern.

Die Rufnummern in E.164 umfassen maximal 15 Dezimalstellen, die von öffentlichen Netzen ausgewertet werden können. Darüber hinaus können

teilnehmerspezifische Rufnummern und Dienste mit weiteren 40 Dezimalstellen angehängen werden. Diese werden aber nur von Nebenstellenanlagen und Endsystemen erfasst.

## **E-DSS1**

Das DSS1-Protokoll (**D**igital-**S**ubscriber-**S**ignalling-System Nr. **1**) wird zeitweise auch mit E-DSS1-Protokoll bezeichnet, wobei das "E" für Euro-ISDN steht.

## **ENUM**

ENUM (**T**elephone-**N**umber-**M**apping) ist eine Technik zur Vereinheitlichung der verschiedenen Kommunikations- und Telefonadressen. Für die privaten und geschäftlichen Telefon-, Telefax- und Handy-Nummern, für Webseiten, Kurznachrichtendienste, Instant Messaging und E-Mails. Das ENUM-Protokoll verknüpft die Ressourcen aus den Telekommunikationsnetzen und dem Internet miteinander und definiert wie eine Telefonnummer auf einer Domain-Adresse abgebildet wird. Die Telefonnummern werden in das DNS (**D**omain-**N**ame-**S**ystem) eingebunden. Damit die Telefonnummern den internationalen Rufnummernplan entsprechen, gibt es den ITU-Standard E.164.

## **F**

### **FTY**

FTY bzw. FIE (**F**acility-**I**nformation-**E**lement) ist das wichtigste Informationselement im ISDN für die Rufsignalisierung, Registrierung und alles bezüglich den Supplementary Services.

### **5ESS**

5ESS (**5**. Version des AT&T's **E**lectronic-**S**witching-**S**ystem). Wie auch an den ISDN-Anschlüssen, die das nationale amerikanische D-Kanal-Protokoll NI1 einsetzen, sind hier lediglich Datenübertragungen mit einer Geschwindigkeit von 56 kBit/s gegenüber 64 kBit/s bei DSS1 und 1TR6 möglich. Die verbleibenden 8 kBit/s werden zur Übermittlung der Steuerdaten verwendet, da beide Protokolle keinen separaten D-Kanal vorsehen. Zudem verfügen viele dieser Anschlüsse nur über einen B-Kanal.

### **FTP**

Das FTP-Protokoll (**F**ile-**T**ransfer-**P**rotokoll) dient dem Dateitransfer zwischen

verschiedenen Systemen und der einfachen Dateihandhabung. FTP basiert auf dem Transportprotokoll TCP (**T**ransmission-**C**ontrol-**P**rotocol) und kennt sowohl die Übertragung zeichencodierter Information als auch von Binärdaten. In beiden Fällen muss der Benutzer eine Möglichkeit besitzen zu spezifizieren, in welcher Form die Daten auf dem jeweiligen Zielsystem abzulegen sind. Die Dateiübertragung wird vom lokalen System aus gesteuert, die Zugangsberechtigung für das Zielsystem wird für den Verbindungsaufbau mittels User-Identifikation und Passwort überprüft.

## **G**

### **GAP**

GAP (**G**eneric-**A**ccess-**P**rofile) ist ein Übertragungsprotokoll für schnurlose Telefone und erlaubt die Kommunikation von DECT-Geräten unterschiedlicher Hersteller. So können schnurlose Telefone verschiedener Hersteller parallel an einer DECT-Basisstation genutzt werden, da sie alle das gleiche Übertragungsprotokoll verwenden und so eine herstellerübergreifende Kommunikation der Geräte ermöglicht wird.

### **GMT**

GMT (**G**reenwich-**M**ean-**T**ime), ist die mittlere Sonnenzeit am Nullmeridian. Die GMT war von 1884–1928 Weltzeit und ist in dieser Funktion heute von der Koordinierten Weltzeit UTC (**U**niversal-**T**ime-**C**oordinated) ersetzt.

## **H**

### **Handover**

Der Prozess der stattfindet, wenn ein DECT-Handset während eines Gespräches von einem DECT-Radio zu einem anderen wechselt.

### **Handset**

Ein DECT-Handset ist ein schnurloses Telefon.

### **HLC**

HLC (**H**igh-**L**ayer-**C**ompatibility) ist ein Informationselement im ISDN mit dem die Protokolle und Parameter angezeigt werden, die in den Schichten 4 bis 7 der Nutzkanäle verwendet werden.

## H.225

H.225 ist ein von der ITU-T (**I**nternational-**T**elecommunication-**U**nion-**T**elecommunications) standardisiertes Signalisierungsprotokoll, das in H.323-Netzwerken eingesetzt wird und die Daten-, Sprach- und Video-Übertragung unterstützt. Das Protokoll dient dem Verbindungsaufbau und -abbau sowie der Verbindungskontrolle. Innerhalb des Protokolls erfolgt die Signalisierung auf Basis von Q.931.

H.225 verwendet für die Echtzeitübertragung der multimedialen Daten das RTP-Protokoll.

## H.323

H.323 ist ein internationaler ITU-Standard (**I**nternational-**T**elecommunication-**U**nion) für die Sprach-, Daten- und Videokommunikation über paketorientierte Netze, der die spezifischen Fähigkeiten von Endgeräten im IP-Umfeld festlegt. H.323, das funktional vergleichbar ist mit dem SIP-Protokoll, wurde für die Übertragung von Multimedia-Applikationen entwickelt und bildet die Grundlage für VoIP. Über diesen Standard wird die Echtzeitkommunikation in LANs definiert.

Der H.323-Standard besteht aus einer ganzen Reihe von Protokollen für die Signalisierung, zum Austausch von Endgerätefunktionalitäten, zur Verbindungskontrolle, zum Austausch von Statusinformationen und zur Datenflusskontrolle. Der Standard ist mehrfach überarbeitet worden und definiert in der dritten Version die Übertragung von Leistungsmerkmalen. Der Standard ist abgeleitet aus dem H.320 Multimedia-Standard für ISDN.

## H.245

Das von der ITU (**I**nternational-**T**elecommunication-**U**nion) standardisierte H.245-Protokoll handelt in H.323-Netzwerken Endgerätefunktionen, die Steuerung von logischen Verbindungen für die Übertragung der Audiodaten, die Flusskontrolle und die Übertragung weiterer Steuerungsnachrichten aus. Bei den Endgerätefunktionen übernimmt H.245 die Einstellung des Sprachcodierverfahrens, das identisch sein muss mit dem Kompressionsverfahren.

## *I*

## IEEE

IEEE (**I**nstitute- of **E**lectrical- and **E**lectrical-**E**ngineers) ist ein Verband amerikanischer Ingenieure, der sich auch Normungsaufgaben widmet und

z.B. in der Arbeitsgruppe 802 die Standardisierung von lokalen Netzen vorantreibt.

## **IP**

Die Aufgabe des IP (**I**nternet-**P**rotokolls) besteht darin, Datenpakete von einem Sender über mehrere Netze hinweg zu einem Empfänger zu transportieren. Die Übertragung ist paketorientiert, verbindungslos und nicht garantiert. Die IP-Datagramme werden auch bei identischen Sendern und Empfängern vom IP als voneinander unabhängige Datenpakete transportiert. IP garantiert weder die Einhaltung einer bestimmten Reihenfolge noch eine Ablieferung beim Empfänger, d.h. Datagramme können z.B. wegen Netzüberlastung verloren gehen.

## **IPEI**

DECT-Telefone (Handsets) besitzen solch eine IPEI-Nummer (**I**nternational-**P**ersonal-**E**quipment-**I**dentify), welche auch als Seriennummer angesehen werden kann und zur Identifikation in DECT-System dient.

## **IP-Master**

Die IP1200, die alle anderen DECT-Basis-Stationen in einem IP-DECT-System kontrolliert, wird oft als IP-Master bezeichnet. Es ist möglich, dass dieser dieselbe DECT-Basis-Station ist wie der Sync-Master.

## **ISDN**

ISDN (**I**ntegrated-**S**ervices-**D**igital-**N**etwork) wurde als Kommunikationsnetz für Sprachübertragungen konzipiert, was sich an der Übertragungsgeschwindigkeit von 64 kbit/s erkennen lässt und ist aus dem analogen Fernsprechnet hervorgegangen. Die digitale Übertragung ermöglicht eine gleichartige Behandlung von Text-, Grafik- und Sprachdaten. Ebenso wie im analogen Fernsprechnet nutzt ISDN die Leitungsvermittlung, wobei nach Bedarf eine transparente physikalische End-zu-Ende-Verbindung aufgebaut wird. Zwischen den kommunizierenden Endteilnehmern entsteht quasi eine physikalische Leitung, die in den einzelnen ISDN-Vermittlungsstellen durchgeschaltet wird.

## **ITU**

Die ITU (**I**nternational-**T**elecommunication-**U**nion) ist eine weltweit tätige Organisation, in der Regierungen und der private Telekommunikationssektor den Aufbau und Betrieb von Telekommunikationsnetzen und -diensten koordinieren.

## *J*

### **Jitter**

Mit Jitter bezeichnet man in der Datenübertragung die Phasenschwankungen und damit zeitliche Änderungen von Signalfrequenzen. Es handelt sich um Schwankungen von fixierten Zeitpunkten z.B. der Zeitpunkt des Übergangs eines Digitalsignals von einer Signalamplitude auf eine andere. Jitter tritt speziell bei hohen Frequenzen auf und kann zu Datenverlusten führen. Verursacht wird Jitter durch Rauschen und Übersprechen, durch Einstreuungen, Flankenverzerrungen und minimale Pegelschwankungen.

## *K*

## *L*

### **LAN**

Ein LAN (**L**ocal-**A**rea-**N**etwork) hat eine Ausdehnung von üblicherweise höchstens 10 km, obwohl es auch Netze gibt, die noch deutlich größere Entfernungen überwinden können. Es ist in den meisten Fällen als Diffusionsnetz ausgeführt und erreicht Übertragungsraten bis 10 Gbit/s (10-Gigabit-Ethernet). LANs können drahtgebunden arbeiten wie die standardisierten lokalen Netze Ethernet, Token-Ring und FDDI und auch drahtlos wie die WLANs nach 802.11.

### **LDAP**

Das LDAP-Protokoll (**L**ightweight-**D**irectory-**A**ccess-**P**rotocol) ist ein TCP/IP (**T**ransmission-**C**ontrol-**P**rotocol/**I**nternet-**P**rotocol)-basiertes Directory-Zugangsprotokoll, das sich im Internet und in Intranets als Standardlösung für den Zugriff auf Netzwerk-Verzeichnisdienste für Datenbanken, E-Mails, Speicherbereiche und andere Ressourcen etabliert hat. LDAP bietet einen einheitlichen Standard für Verzeichnisdienste/ DS (**D**irectory **S**ervice).

## *M*

### **MAC**

Die MAC-Adresse (**M**edia-**A**ccess-**C**ontrol) ist die Hardware-Adresse jedes einzelnen Netzwerkadapters, die zur eindeutigen Identifikation des Geräts

im Netzwerk dient. Die MAC-Adresse wird der Sicherungsschicht, Schicht 2 des OSI-Modells, zugeordnet. Um die Sicherungsschicht mit der Vermittlungsschicht zu verbinden, wird zum Beispiel bei Ethernet das ARP-Protokoll (**A**ddress-**R**esolution-**P**rotocol) verwendet.

## **MIB**

Eine MIB (**M**anagement-**I**nformation-**B**ase) ist eine Art Tabelle in der definiert ist, welche Informationen abgerufen werden können. Die MIB eines Agenten (Host, Router, Access-Point...) wird durch den Hersteller festgelegt. Aufgabe dieser MIB ist es, die übertragenen Informationen und Daten in dem Agenten abzulegen und zu speichern. Durch den Einsatz von MIBs können über SNMP (**S**imple-**N**etwork-**M**anagement-**P**rotocol) die Agenten überwacht und administriert werden.

## **MOH**

Mit MoH (**M**usic-**o**n-**H**old) wird in allen gängigen TK-Anlagen eine Wartemusik eingespielt, während ein Gespräch gehalten wird.

## **MPPE**

Das MPPE-Protokoll (**M**icrosoft-**P**oint-to-**P**oint-**E**ncryption) dient der Verschlüsselung von PPTP-Datenpakete. Dazu bietet das MPPE-Protokoll als internationale Version eine Schlüssellänge von 40 Bit und als US-Version eine Schlüssellänge von 128 Bit, bei dem die Datencodierung mit RSA 4 Stream Cipher (RC4) verwendet wird. Bei dem 128-Bit-Schlüssel wird zur Erhöhung der Sicherheit für jede neue Session ein 64 Bit großer Teil des Schlüssels geändert.

## **MSN**

Eine MSN (**M**ultiple-**S**ubscriber-**N**umber) ist ein Leistungsmerkmal von Euro-ISDN. Es handelt sich dabei um eine Mehrfachrufnummer für einen Mehrgeräte-Anschluss. Im ISDN können bis zu zehn beliebige, freie Rufnummern aus dem Rufnummernvolumen des jeweiligen Anschlussbereiches für den Mehrgeräte-Anschluss vergeben werden. Jedem Endgerät kann somit eine individuelle Rufnummer zugeordnet werden. Einem ISDN-Endgerät oder einer TK-Anlage können auch mehrere Rufnummern zugeordnet werden. Andererseits können mehrere Endgeräte am passiven Bus über eine Mehrfachrufnummer angeschlossen werden.

## **MTU**

Eine MTU (**M**aximum-**T**ransmission-**U**nit) ist die größtmögliche Dateneinheit

bzw. Frame-Länge, die über ein vorhandenes physikalisches Übertragungsmedium bzw. über einen LAN- oder WAN-Pfad gesendet werden kann. Wenn größere Frame-Längen auftreten, werden sie entweder entsprechend den verwendeten Protokollregeln fragmentiert, oder das Frame wird verworfen. WANS haben in aller Regel geringere MTU-Größen als LANs.

## Multicast

Unter Multicast versteht man eine Übertragungsart von einem Punkt zu einer Gruppe. Man spricht bei Multicast auch von Mehrpunktverbindung. Der Vorteil von Multicast liegt darin, dass gleichzeitig Nachrichten über eine Adresse an mehrere Teilnehmer oder geschlossene Benutzergruppen übertragen werden. Neben der Multicast-Verbindung gibt es die Punkt-zu-Punkt-Verbindung und die Broadcast-Übertragung.

## N

### NAT

NAT (**N**etwork-**A**ddress-**T**ranslation) ist in Computernetzen ein Verfahren, um eine IP-Adresse (**I**nternet-**P**rotocol) in einem Datenpaket durch eine andere zu ersetzen. Häufig wird dies benutzt, um private IP-Adressen auf öffentliche IP-Adressen abzubilden. Werden auch die Port-Nummern umgeschrieben, spricht man dabei von Maskieren oder PAT (**P**ort-**A**ddress-**T**ranslation).

Üblicherweise wird NAT an einem Übergang zwischen zwei Netzen durchgeführt. Der NAT-Dienst kann auf einem Router, einer Firewall oder einem anderen spezialisierten Gerät laufen. So kann zum Beispiel ein NAT-Gerät mit zwei Netzwerkadaptern das lokale private Netz mit dem Internet verbinden. Man unterscheidet zwischen Source-NAT, bei dem die Quell-IP-Adresse ersetzt wird, und Destination-NAT, bei dem die Ziel-IP-Adresse ersetzt wird.

### NBTSTAT

Zeigt NetBIOS über TCP/IP-Protokollstatistiken (NetBT), NetBIOS-Namens-Tabellen sowohl für lokale Computer als auch für Remotecomputer und den NetBIOS-Namenzwischenspeicher an. Nbtstat ermöglicht das Aktualisieren des NetBIOS-Namenzwischenspeichers und der im WINS (**W**indows-**I**nternet-**N**ame-**S**ervice) registrierten Namen.

### NI

NI1 ist das in den USA eingesetzte nationale ISDN-Protokoll für den D-Kanal.



Einige Telekommunikationsunternehmen setzen allerdings noch auf das ältere Protokoll 5ESS. Gegenüber dem europäischen DSS1 unterscheiden sich NI1 und 5ESS vor allem in der Übertragungsgeschwindigkeit. Bei beiden sind lediglich Datenübertragungen mit einer Geschwindigkeit von 56 kBit/s möglich. Die verbleibenden 8 kBit/s werden zur Übermittlung der Steuerdaten verwendet, da beide Protokolle keinen separaten D-Kanal vorsehen. Zudem verfügen viele dieser Anschlüsse nur über einen B-Kanal.

## **NMBLOOKUP**

Durch nmblookup können NetBIOS Namen unter Linux mittels NetBIOS über TCP/IP abgefragt werden.

## **NTP**

Das NTP-Protokoll (**N**etwork-**T**ime-**P**rotocol) ist ein Standard zur Synchronisierung von Uhren in Computersystemen über paketbasierte Kommunikationsnetze. NTP verwendet das verbindungslose Netzwerkprotokoll UDP (**U**ser-**D**atagram-**P**rotocol). Es wurde speziell dafür entwickelt, eine zuverlässige Zeitgabe über Netzwerke mit variabler Paketlaufzeit zu ermöglichen.

## **O**

## **OSI**

Das OSI-Referenzmodell (**O**pen-**S**ystems-**I**nterconnection) ist ein Schichtenmodell für die Kommunikation offener, informationsverarbeitender Systeme. Es handelt sich um vereinheitlichte Verfahren und Regeln für den Austausch von Daten. Es wird seit 1979 entwickelt und ist von der ISO standardisiert worden. Das OSI-Modell dient als die Grundlage für eine Reihe von herstellerunabhängigen Netzprotokollen, die in der öffentlichen Kommunikationstechnik im Transportnetz fast ausschließlich eingesetzt werden.

## **P**

## **PL**

PL (**P**acket-**L**oss) bzw. Paketverlust tritt bei der paketbasierten Datenübertragung in Netzwerken auf. Paketverlust kann in verschiedenen Schichten des OSI-Modells auftreten.

## PCM

PCM (**P**uls-**C**ode-**M**odulation) ist ein ITU-Standard für die Digitalisierung von Sprache, beschrieben in G.711. Bei dieser Modulationsart werden analoge Signale durch Quantisierung in zeit- und wertdiskrete Binärsignale umgewandelt.

In der Sprachübertragung wird die PCM-Technik benutzt, um ein analoges Sprachsignal, basierend auf dem Abasttheorem nach Nyquist, in ein Digital-signal umzuwandeln. Dazu wird das Analogsignal 8.000-mal pro Sekunde abgetastet und in eine 8-Bit-Wertigkeit gewandelt, sodass alle 125  $\mu$ s ein Abtastwert entsteht. Die resultierende Übertragungsgeschwindigkeit beträgt 64 kbit/s, die übertragbare Sprachfrequenz 4 kHz.

Zur Dynamisierung der Sprache hat die ITU in G.711 zwei Verfahren zur Dynamikkompression definiert: das  $\mu$ -Law-Verfahren und das A-Law-Verfahren

## PING

Mit dem Programm ping (**P**acket-**I**nternet-**G**rouper) kann überprüft werden, ob ein bestimmter Host in einem IP-Netzwerk erreichbar ist und welche Antwortzeit er besitzt.

## POE

PoE (**P**ower-**o**ver-**E**thernet) bezeichnet eine Technologie, mit der netzwerkfähige Geräte über das 8-adrige Ethernet-Kabel mit Strom versorgt werden können.

## POSIX

POSIX (**P**ortable-**O**perating-**S**ystem-**I**nterface-for-**U**ni**X**) ist ein gemeinsam von der IEEE (**I**nstitute- of **E**lectrical- and **E**lectrical-**E**ngineers) und der Open Group für Unix entwickeltes standardisiertes Applikationsebeneninterface, das die Schnittstelle zwischen Applikation und dem Betriebssystem darstellt.

## PP

PP (**P**ortable-**P**art) und wird als Synonym für ein schnurloses Telefon (Handset) verwendet.

## PPP

Das PPP-Protokoll (**P**oint-to-**P**oint-**P**rotocol) ist als Protokoll für die Einwahl ins Internet über leitungvermittelte Netze konzipiert. Das PPP-Protokoll

ermöglicht die Übermittlung von Daten über synchrone und asynchrone Wähl- und Standleitungen. Es ist dadurch in der Lage unabhängig vom jeweiligen physikalischen Interface zu arbeiten. Die einzige Voraussetzung, die beim Einsatz des PPP-Protokolls gefordert wird, besteht in einer vollkommen transparenten, voll duplexfähigen Datenleitung.

## PPPOE

PPPoE (**P**oint-to-**P**oint-**P**rotocol-over-**E**thernet) ist die Verwendung des Netzwerkprotokolls PPP (**P**oint-to-**P**oint-**P**rotocol) über eine Ethernet-Verbindung.

## PPTP

Das PPTP (**P**oint-to-**P**oint-**T**unneling-**P**rotocol) ist ein von einem Herstellerkonsortium (Ascend Communications, Microsoft Corporation, 3Com u. a.) entwickeltes Protokoll zum Aufbau eines VPN (**V**irtual-**P**riate-**N**etwork). Es ermöglicht das Tunneling des PPP (**P**oint-to-**P**oint-**P**rotocol) durch ein IP-Netzwerk, wobei die einzelnen PPP-Pakete wiederum in GRE-Pakete (**G**eneric-**R**outing-**E**ncapsulation) verpackt werden. Zur Sicherung der Datenübertragung verfügt PPTP über einen 40- oder 128-bit großen RC4-Algorithmus (**R**ivest-**C**ipher).

## PRI

PRI (**P**rietary-**R**ate-**I**nterface) dient dem Anschluss von mittleren bis großen Nebenstellenanlagen und bietet gegenüber dem Basisanschluss wesentlich höhere Übertragungsgeschwindigkeiten. Er gestattet die Anschaltung von Teilnehmereinrichtungen an die ISDN-Ortsvermittlungsstelle, wobei über die S2M-Schnittstelle dem Endanwender eine maximale Informationskapazität von 30 Basis-Kanälen mit jeweils 64 kbit/s und zusätzlich einem D-Kanal mit einer Kapazität von 64 kbit/s zur Verfügung stehen.

## Q

## QoS

Unter Dienstgüte QoS (**Q**uality-of-**S**ervice) versteht man alle Verfahren, die den Datenfluss in LANs (**L**ocal-**A**rea-**N**etworks) und WANs (**W**ide-**A**rea-**N**etworks) so beeinflussen, dass der Dienst mit einer festgelegten Qualität beim Empfänger ankommt.

## QSIG

QSIG (**Q**-Interface-**S**ignalling-Protocol) basiert auf dem D-Kanal-Protokoll nach dem ITU-T-Standard (**I**nternational-**T**elecommunication-**U**nion-**T**elecommunications) der Q.93x-Serie für Basic Call und der Q.95x-Serie für die Supplementary Services. Damit ist sichergestellt, dass QSIG und ISDN kompatibel in ihren Leistungsmerkmalen sind und ISDN-Applikationen bzw. -Zusatzdienste der öffentlichen ISDN-Netze auch in einem privaten Netz genutzt werden können.

## Q-Value

Ein Indikator für die Übertragungsqualität in einem aufgebauten DECT-Anruf. Auch bezeichnet als Q52-Wert.

## Q.931

Q.931 ist das von der ITU (**I**nternational-**T**elecommunication-**U**nion) standardisierte Protokoll für die Signalisierung im D-Kanal von Euro-ISDN, das dem Verbindungsaufbau, -abbau sowie der Verbindungskontrolle dient.

## *R*

## Radio

Ein DECT-Radio ist entweder eine DECT-Basis-Station oder ein Repeater.

## RC4

Bei dem Verschlüsselungs-Algorithmus RC4 (**R**ivest-**C**ipher) handelt es sich um ein symmetrisches Verschlüsselungsverfahren, bei dem der Schlüssel von einem Zufallszahlengenerator erzeugt wird. RC4 arbeitet mit einem geheimen Schlüssel, der dem Sender und dem Empfänger bekannt ist. Die variable Schlüssellänge kann bis zu 2.048 Bit lang sein. Jedes Zeichen wird einzeln verschlüsselt. RC4 gilt als sehr sicher, obwohl es relativ einfach ist.

## Repeater

Ein DECT-Radio, welches keine direkte Verbindung zum CCFP hat. Dieses benötigt (entweder direkt oder indirekt) Zugriff zu einer DECT-Basis-Station, welche einen Kanal zur PBX bereitstellt. Ein Repeater erhöht den Abdeckungsbereich des IP-DECT-Systems, aber nicht die mögliche Anzahl, gleichzeitig geführter Rufe.

Ein Repeater benötigt eine Synchronisierungsquelle (wie jedes andere

DECT-Radio auch). Das DECT-Radio, welches als Synchronisierungskette dient, wird ebenfalls benutzt, um Zugriff zum Sprachkanal der PBX zu erhalten. Das bedeutet, dass Rufe, die über einen Repeater verlaufen, immer über die Repeater-Sync-Source abgewickelt werden.

## Repeater-Chain

Sollte ein Repeater einen anderen Repeater als Synchronisierungsquelle angegeben haben, dann spricht man von einer Repeaterkette. Keines der DECT-Radios in einer Repeaterkette kann als Synchronisierungsquelle für ein IP1200-DECT-Radio angegeben werden. Für Repeaterketten gelten spezielle Regeln.

## RFC

Spezifikationen, Vorschläge, Ideen und Richtlinien, das Internet betreffend, werden in Form von so genannten RFCs (**R**equ**e**s**t**-**F**or-**C**omments) veröffentlicht.

## RFP

RFP (**R**adio-**F**ixed-**P**art) wird als Synonym für DECT-Basis-Stationen verwendet.

## RJ

RJ-Steckverbinder haben sich weltweit für UTP-Kabel (**U**nshielded-**T**wisted-**P**air) durchgesetzt, insbesondere in der Arbeitsplatzverkabelung und in der Rangierung. Dank verbesserter HF-Übertragungseigenschaften (**H**igh-**F**requency) werden RJ-Steckersysteme sowohl in der Telekommunikation als auch im Netzwerkbereich bis hin zu ATM (**A**synchronous-**T**ransfer-**M**ode) und Gigabit-Ethernet (RJ-45) eingesetzt. Die bekanntesten RJ-Stecker sind RJ-10, RJ-11, RJ-12 und RJ-45, die sich in der Kontaktzahl unterscheiden.

## Roaming

Die Fähigkeit eines DECT-Telefons, in mehr als einem IP-DECT-System (in verschiedenen Lokationen) zu operieren. Dazu muss das DECT-Telefon in allen IP-DECT-Systemen angemeldet sein.

## RT

Unter RT (**R**ound-**T**rip) versteht man die Reaktionszeit eines kompletten Netzwerks. Es ist die Zeitspanne, die erforderlich ist, um ein Signal von einer Quelle über das Netzwerk zum Empfänger zu senden und die Antwort des Empfängers wiederum über das Netzwerk zurück zum Sender zu transportieren.

tieren. Die Round-Trip-Zeit wird in einigen Routing-Algorithmen zur Bestimmung der optimalen Route berücksichtigt.

## **RSA**

RSA (**R**ivest-**S**hamir-**A**dleman) ist ein asymmetrisches Verfahren oder Algorithmus zur Verschlüsselung diskreter Daten, der verschiedene Schlüssel zum Ver- und Entschlüsseln verwendet, wobei der Schlüssel zum Entschlüsseln nicht oder nur mit hohem Aufwand aus dem Schlüssel zum Verschlüsseln berechenbar ist. Der Schlüssel zur Verschlüsselung kann daher veröffentlicht werden. Solche Verfahren werden als asymmetrische oder Public-Key-Verfahren bezeichnet. Es ist nach seinen Erfindern Ronald L. Rivest, Adi Shamir und Leonard Adleman benannt.

## **RTP**

Das RTP-Protokoll (**R**ead-Time-**T**ransport-**P**rotocol) ist ein Protokoll zur kontinuierlichen Übertragung von audiovisuellen Daten (Streams) über IP-basierte Netzwerke. Es dient dazu, Multimedia-Datenströme (Audio, Video, Text, etc.) über Netzwerke zu transportieren, d.h. die Daten zu kodieren, zu paketieren und zu versenden. RTP ist ein Paket-basiertes Protokoll und wird normalerweise über UDP betrieben. Das RTP dient der Aushandlung und Einhaltung von QoS-Parametern (**Q**uality-**O**f-**S**ervice). Es findet Anwendung in vielen Bereichen, u.a. wird es bei den IP-Telefonie-Technologien H.323 und SIP (**S**ession-**I**nitiation-**P**rotocol) dazu verwendet die Audio-/Videoströme des Gespräches zu übertragen.

## **S**

## **SC**

Die meiste Zeit während eines Telefonats besteht aus Pausen. Es wäre unnötig, in diesen Zeitabschnitten mit der vollen Datenrate zu arbeiten. Daher enthalten Codecs wie der G.723.1 oder der G.729 eine SC (**S**ilence-**C**ompression). Sie besteht im Wesentlichen aus den drei Komponenten: VAD, DTX und CNF.

Die Aufgabe von VAD (**V**oice-**A**ctivity-**D**etector) ist es, festzustellen, wann ein Gesprächsteilnehmer spricht und wann er still ist. Hierzu muss der Algorithmus schnell reagieren, um zu verhindern, dass nach einer solchen Ruhe die erste Silbe verloren geht. Für die sichere Unterscheidung zwischen Gespräch und Stille benötigt der Codec einen Zwischenspeicher, der einen zusätzlichen Delay verursacht.

DTX (**D**iscontinuous-**T**ransmission) ermöglicht es einem Codec theoretisch, wenn VAD Stille erkannt hat, die Verbindung zu unterbrechen. Da eine solche Unterbrechung aber absolute Stille beim Gesprächspartner bedeuten würde, wird die Verbindung nicht wirklich komplett unterbrochen, sondern es wird ein kleiner Satz an Daten übertragen, der die Erzeugung von Hintergrundgeräuschen beim Empfänger ermöglicht.

CFG (**C**omfort-**N**oise-**G**enerator) setzt genau an dieser Stelle an. Er ist in der Lage, selbstständig Hintergrundgeräusche zu erzeugen. Dazu benutzt er die bei der vorherigen Gesprächsphase vorhandenen Hintergrundgeräusche.

## SNTP

Das SNTP-Protocol (**S**imple-**N**etwork-**T**ime-**P**rotocol) wird für die Übertragung einer offiziellen Zeit in Netzwerken und im Internet verwendet. Die erweiterte Variante heißt NTP (**N**etwork-**T**ime-**P**rotocol).

## SNMP

Das **S**imple-**N**etwork-**M**anagement-**P**rotokoll erlaubt ein zentrales Netzwerkmanagement für viele Netzwerkkomponenten. Die primären Ziele von SNMP sind die Verringerung der Komplexität der Management-Funktionen, die Erweiterbarkeit des Protokolls und die Unabhängigkeit von irgendwelchen Netzwerkkomponenten.

## Synchronisation

Damit DECT-Radios kommunizieren können, müssen diese miteinander synchronisiert sein. In einem IP1500-System erhielt man die Synchronisierung über die 2-adrige Schnittstelle des CCFP. In einem IP1200-System erhält man die Synchronisierung jedoch über die Luft. Deshalb muss eine als DECT-Radio konfigurierte IP1200 innerhalb der Abdeckung eines anderen DECT-Radios angelegt werden, von welchem die Synchronisierung bezogen werden kann.

In einem IP1500-System müssen nur die Repeater innerhalb der Abdeckung eines DECT-Radios angelegt werden. Dies gilt natürlich auch in einem IP1200-System.

## Synchronisation-Chain

In einem geschlossenen System muss jedes IP1200-DECT-Radio mit allen anderen IP1200-DECT-Radios synchronisiert werden. Das setzt voraus, dass jedes DECT-Radio (ausser eines) ein anderes als Synchronisierungsquelle konfiguriert hat.

Das eine DECT-Radio, welches keine Synchronisierung von einem anderen DECT-Radio erhält, nennt man „Sync-Master“. Dieser muss eine IP1200 und darf kein Repeater sein. Alle anderen DECT-Radios erhalten ihre Synchronisierung von diesem DECT-Radio, entweder direkt oder indirekt.

Das Eingabefeld, welches für die Angabe der Synchronisierungsquelle benutzt wird, ist eigentlich fehlbezeichnet als „Sync-Master“. Fakt ist, dass hier nicht die Radio-ID des Sync-Masters angegeben wird, sondern die Radio-ID des Radios, von welchem die Synchronisierung erhalten werden soll. Man könnte auch sagen das nächste DECT-Radio in der Synchronisierungskette.

Für Redundanz kann ein „Alt-Sync-Master“ konfiguriert werden. Dieser wird als Synchronisierungsquelle verwendet, sollte das als „Sync-Master“ konfigurierte DECT-Radio nicht verfügbar sein.

Es sollte offensichtlich sein, dass in der Synchronisierungskette keine Kreise vorhanden sein dürfen.

Ein Repeater benötigt ebenfalls eine Synchronisierungsquelle. Dieser darf aber nicht mit einer alternativen Synchronisierungsquelle konfiguriert werden, da diese nur im Falle eines Ausfalls des Sync-Masters als Synchronisierungsquelle dient. Deshalb sollte man auch keinen Repeater als Synchronisierungsquelle für ein IP1200-DECT-Radio verwenden.

Genauso sollte man in einer Repeaterkette auch keinen Repeater als Synchronisierungsquelle verwenden.

## **Sync-Master**

Das DECT-Radio in einer IP1200-Installation, welches seine Synchronisation von keiner anderen Quelle bezieht.

Wird auch in der IP1200-DECT-Radio-Konfiguration verwendet, um die Sync-Source des DECT-Radios zu konfigurieren.

## **Sync-Source**

Ein DECT-Radio, welches anderen DECT-Radios als Synchronisierungsquelle dient.

## **T**

## **TCP**

Das TCP-Protocol (**T**ransmission-**C**ontrol-**P**rotocol) ist ein verbindungsorien-



tiertes Transportprotokoll für den Einsatz in paketvermittelten Netzen. Das Protokoll baut auf dem IP-Protokoll auf, unterstützt die Funktionen der Transportschicht und stellt vor der Datenübertragung eine gesicherte Verbindung zwischen den Instanzen her.

## Telnet

Telnet (**Teletype-Net**work) ist der Name eines im Internet weit verbreiteten Netzwerkprotokolls. Der Sinn des Telnet-Protokolls besteht darin, eine ziemlich allgemeine, bidirektionale, 8-bit-pro-Byte-orientierte Kommunikationsmöglichkeit zu bieten. Es wird üblicherweise dazu verwendet, Benutzern den Zugang zu Internetrechnern über die Kommandozeile zu bieten. Das Telnetprogramm stellt dabei die benötigten Clientfunktionen des Protokolls zur Verfügung. Aufgrund der fehlenden Verschlüsselung wird dieses jedoch kaum noch eingesetzt.

## TFTP

Das TFTP-Protocol (**T**rivial-**F**ile-**T**ransfer-**P**rotocol) ist ein sehr einfaches Dateiübertragungsprotokoll. TFTP unterstützt lediglich das Lesen oder Schreiben von Dateien. Nicht vorhanden sind viele Funktionen des mächtigeren FTP (**F**ile-**T**ransfer-**P**rotocol) wie etwa Rechtevergabe mittels chmod, Anzeigen der vorhandenen Dateien oder Benutzerauthentifizierung. Im Gegensatz zu FTP, das ein verbindungsorientiertes Transportprotokoll erfordert, wird TFTP normalerweise über ein verbindungsloses Protokoll wie UDP betrieben.

## TOS

Das ToS-Feld (**T**ype **O**f-**S**ervice-Feld) ist ein Datenfeld im IP-Header in dem die Dienste des Datagramms definiert sind. Mit den ToS-Informationen können Rechner netzwerkrelevante Dienstarten angeben. Dabei können verschiedene Parameter wie die Bandbreite, die Übertragungsgeschwindigkeit oder die Zuverlässigkeit der Übertragung definiert werden. Darüber hinaus können die vorrangige Behandlung von Datagrammen, die Durchsatzart sowie die Belegung von Ressourcen in den Routern festgelegt werden.

## Trace

Ein Trace (zu dt. Ablaufverfolgung) ist eine Anweisungssequenz, der mit einem beliebigen Startpunkt beginnt und in dem die Programmverzweigungen und deren Wegwahl definiert sind. Ein solcher Trace ermöglicht die schrittweise Verfolgung des Programmablaufs. Die Ablaufverfolgung dient vor allem der Fehlersuche und -behebung (Debugging).

## U

### UDP

Im Gegensatz zum verbindungsorientierten TCP (**T**ransmission-**C**ontrol-**P**rotocol) ist das **U**ser-**D**atagram-**P**rotocol ein minimales, verbindungsloses Netzwerkprotokoll, das zur Transportschicht der Internetprotokollfamilie gehört.

Aufgabe von UDP ist es, Daten, die über das Internet übertragen werden, der richtigen Anwendung zukommen zu lassen. Mit UDP wurde ein Protokoll benötigt, das nur für die Adressierung zuständig war, ohne die Datenübertragung zu sichern, da dies zu Verzögerungen bei der Sprachübertragung führen würde.

### URL

Als **U**niform-**R**esource-**L**ocator bezeichnet man eine Unterart von **U**niform-**R**esource-**I**dentifiern (URI). URLs identifizieren eine Ressource über ihren primären Zugriffsmechanismus (häufig http oder ftp) und den Ort der Ressource in Computernetzwerken. Der Name des URI-Schemas ist daher in der Regel vom hierfür verwendeten Netzwerkprotokoll abgeleitet. Beispiele hierfür sind HTTP oder FTP.

### UTC

UTC (**U**niversal-**T**ime-**C**oordinated) ist die aktuelle (koordinierte) Weltzeit, und hat in der Funktion die mittlere GMT-Zeit (**G**reenwich-**M**ean-**T**ime) abgelöst. Sie ist eine Kombination aus der internationalen Atomzeit TAI (**T**empus-**A**tomique-**I**nternational) und der Universalzeit UT (**U**niversal-**T**ime). Die Zeitzonen werden als positive oder negative Abweichung von UTC angegeben (z. B. UTC+2 entspricht der MESZ). Die UTC kombiniert die physikalische Atomzeit (TA) mit der astronomischen Zeit (UT) und wird auch Bürgerliche Zeit genannt.

### μ-Law

Das μ-Law-Verfahren ist ein Digitalisierungsverfahren für analoge Audiosignale, das in der Empfehlung G.711 der ITU (**I**nternational-**T**elecommunication-**U**nion) standardisiert ist. In ähnlicher Weise wie das A-law-Verfahren arbeitet das μ-law-Verfahren mit einer logarithmischen Quantisierungskennlinie, um ein besseres Signal-Rausch-Verhältnis zu erzielen. Ebenso wie bei diesem Verfahren werden jeweils 8-Bit-Werte erzeugt. Jedoch ist die Quantisierungskennlinie bei niedrigen Pegeln steiler. Außerdem ist die Codierung darauf ausgelegt, keine kontinuierlichen 0-Folgen zu erzeugen, sondern

ständig wechselnde Bitzustände. Damit wird ein bestimmtes Verfahren zur Taktrückgewinnung beim Empfänger des digitalen Signals erleichtert. Das  $\mu$ -Law-Verfahren wird von der PCM-Technik in Nordamerika und Japan verwendet.

## V

### VLAN

VLANs (**V**irtual-**L**ocal-**A**rea-**N**etwork) sind ein technologisches Konzept zur Implementierung logischer Workgroups innerhalb eines Netzes. Die Realisierung eines solchen Netzes erfolgt mittels LAN-Switching oder mittels virtuellem Routing auf der Sicherungsschicht oder auf der Vermittlungsschicht. Virtuelle Netze werden durch eine Menge von Switching Hubs aufgebaut, die ihrerseits durch einen Backbone miteinander verbunden sind.

### VPN

Der Begriff VPN (**V**irtual-**P**ivate-**N**etwork) wird in mehreren Bedeutungen verwendet. Ganz allgemein spricht man von einem VPN, wenn innerhalb eines öffentlichen Wählnetzes kundenspezifische logische Teilnetze gebildet werden. Das können Netze der Sprachkommunikation sein oder X.25, Frame Relay oder ISDN. Die heute gebräuchliche Interpretation für VPNs sind die IP-VPNs, bei denen die Teilnehmer über IP-Tunnel verbunden sind.

## W

### WAN

WANs (**W**ide-**A**rea-**N**etwork) bzw. Weitverkehrsnetze sind für die Sprach- oder Datenübertragung über weite Strecken konzipiert. Diese Netze sind in allen Industrieländern flächendeckend aufgebaut und können uneingeschränkt für die geschäftliche und private Kommunikation genutzt werden. Die Konzeption solcher Netze wird im Wesentlichen durch das Dienstangebot geprägt. So eignet sich das klassische analoge Fernsprechnet (POTS) ebenso wie ISDN für die Telefonie. Dagegen wurden die öffentlichen Datenpaketnetze für Datenübertragungsdienste konzipiert. In diesem Zusammenhang sind auch ATM, Frame Relay oder Fast Packet Switching zu nennen.

### WINS

WINS (**W**indows-**I**nternet-**N**aming-**S**ervice) ist ein Verfahren, um Computer-

namen in Windows-Netzwerken in IP-Adressen umzuwandeln. Dabei berücksichtigt das WINS-Verfahren, dass niemals zwei Computer mit den gleichen Namen oder der gleichen IP-Adresse im Netzwerk angemeldet sind.

Bei WINS, das das UDP-Protokoll zur Übertragung benutzt, meldet sich der gestartete Client mit seinem NetBIOS-Namen und der IP-Adresse beim WINS-Server an. Dieser überprüft die Adressen, ob sie nicht anderweitig besetzt ist, und trägt sie in die Adress-Datenbank des WINS-Servers. Bei der Abmeldung eines Clients wird die Adresse wieder aufgelöst und kann anderweitig vergeben werden.

## **WRFP**

WRFP (**W**ireless-**R**adio-**F**ixed-**P**art) wird als Synonym für Repeater verwendet.

# Stichwortverzeichnis

## Symbols

+ 57

+32db 43

μ-Law 122

## Numerics

0x10 22, 34, 82, 83

100-240V 4

100-MBit-Full-Duplex 31

100-MBit-Half-Duplex 31

100m-fdx 31

100m-hdx 31

10-MBit-Full-Duplex 31

10-MBit-Half-Duplex 31

10m-fdx 31

10m-hdx 31

128-Bit-Encryption 28

2nd Called-Party-Number 29

2nd Local-Subscriber-Number 28

-32db 43

40-Bit-Encryption 28

50Hz 4

5ESS 106

802.1p 37

802.1q 37

802.3af 4, 10

## A

a/b-LIC 15

AB 49

Abbreviated 57

ABs 49

Account 54

Acknowledged 38

Action 16

Active-Calls 24

Adapt to Cisco PPP peers 26

Add 42

Add # 65

Add UII 64

Address 67

Address-Ranges 34

Administrator-Name 15

Administrator-Nutzerkennung 18

Administrator-Passwort 15

Administrator-Zugang 10, 15

A-Law 101

Alerting 68

Alias List 60

Allgemeine-Informationen 14

Allow inbound connections 26

Allowed-Networks 22

Alt-Sync-Master 101

AM/PM-Clock 36

Anklopfsignal 43

Anleitung zum Herunterladen von Li-  
zenzen 98

Ansagen 19

Anzeigen und Anschlüsse 76

Apache-Server 89

Area-Code 50

ARI 101

ARP 101

Aufstellung und Anschluss 4

Auslieferungszustand 11, 32

Authentication 26

Authentication-Trap 22

Authorization 59

Auto 31  
Auto dial after boot 26  
Automatic 31  
Automatic CGPN Mapping 64, 65  
Automatic CGPN-Mapping 44  
Auto-MDX 10, 101  
Autonegation 31

## **B**

Bandbreite (Bandwidth) 25  
Basic-LIC 15  
Bearer-Capability Audio 43  
Bearer-Capability Speech 43  
Benutzerdatenbank 41  
Benutzeroberfläche 12  
Betriebsdauer 14  
Betriebsmodi 31  
Betriebstemperatur 4  
Betriebszustand 21, 70  
Billing CDR's only 45  
Blockwahl 36, 65  
Bootcode 88, 93  
Bootcode-Firmware 70  
Bootcode-Version 14, 70, 93  
Boot-File 70  
Boot-Kommando 93  
BRI 48, 102  
BRI1-4 50, 55  
BRI1-x 71  
BRI-LIC 15  
Broadcast 102  
Built-Number 92

## **C**

Call busy 43  
Call Completion 48

Call-Counter max 65  
Call-Detail-Records 45, 66  
Called-Party-Number 29  
Calling 68  
Calling-Party-Number 29  
Call-Logging 44  
Calls 68  
Call-Waiting On 47  
Cancel 48  
Cause (DISC) 64  
CCFP 102  
CDPN-In 49, 57, 58  
CDPN-Out 49, 57, 58  
CDR 45, 66, 67, 103  
CDR0 66  
CDR1 66  
CDR-Server 66  
CDR-Typ 66  
CEST 97  
CET 97  
CFB 103  
CFB Activate 45  
CFNR 103  
CFNR Activate 46  
CFU 103  
CFU Activate 45  
CGPN 62  
CGPN-In 49, 57, 58  
CGPN-Map 62  
CGPN-Maps 62  
CGPN-Out 49, 57, 58  
Channels 49  
Check-Kommando 90  
CHI 103

- Class 20, 67
- Cleanup 37
- Clear All Leases 37
- Clear Dynamic Leases 37
- Clear Local Settings 47
- Clear Reserved Leases 37
- Client 31
- Coder 14, 35, 51, 68
- Coder-Preferences 51
- Codes 45
- Command File URL 17
- Community-Name 21
- Config Changes 71
- Config Show 73
- Configuration 14
- Connected 68
- Connection-Port 25
- Connections 40
- Contact 21
- CR 103
- Create Metering Pulses 43
- Crossover-Kabel 10
- CTI 104
- D**
- Datasheet 88
- db 43
- Deactivate 45, 46
- DECT 104
- DECT-Base-Station 104
- DECT-Controller 104
- DECT-Master 41, 71
- DECT-Radio 41, 71
- DECT-System 104
- Default Forward Destination 24
- Default-Gateway 32, 34
- Default-Router 30
- Del 42
- Delay 51
- Description 63
- Descriptiv-Name 25
- Destination-Network 30
- Device-Name 15, 21
- Dezibel 43
- DHCP 104
- DHCP-Automatic-Modus 10, 11, 32
- DHCP-Client 31
- DHCP-Client-Modus 31
- DHCP-Disabled-Modus 32
- DHCP-Funktion 31
- DHCP-Lease 34, 37, 38
- DHCP-Server 10, 11, 31, 34, 37
- DHCP-Server-Modus 31
- Diagnostics 70
- Dialing-Location 36
- Dial-Tones 35
- Digest-Hash-Authentifizierung 18
- Direct-Dial 53, 54
- Directed 47
- Disable 42, 50, 55, 58
- Disable Echo-Canceler 65
- Disable HTTP basic authentication 18
- DISC 64
- Disconnecting 68
- Disconnection-Cause 64
- Display-Name (secondary) 54
- DMS100 105
- DNS 105

- DNS-Server 32, 35
- DNS-Server-1 35
- DNS-Server-2 35
- Do not Disturb Ext. On 47
- Do not Disturb Int. On 47
- Do not Disturb On 46
- Down 30, 31, 41, 49
- Download 68
- DSL 105
- DSL-Provider 27
- DSP 49
- DSP-LIC 15
- Dst 97
- Dynamic 38
- Dynamic-Group 53, 54
- E**
- E.164 60, 105
- E.164-Rufnummer 60
- Echokompensation 65
- E-DSS1 106
- Einführung 9
- Eingabebereich 12
- Enable 25, 41, 45
- Enable H.323-NAT 24
- Enable MPPE-Encryption 28
- Enable NAT 24
- Enable PCM 52
- Enable T.38 52
- Enable Telnet 22
- Enblock-Dialing-Timeout 36
- Entsorgung 4
- ENUM 59, 106
- ETH0 11, 30, 76
- ETH0-100M LED 76

- ETH0-Link LED 76
- ETH1 11, 30
- Ethernet-Schnittstelle 30, 31, 33
- Ethernet-Schnittstellen 10
- ETHn 33
- Exclude Address 33
- Exclude from Auto-CGPN 44, 64
- Exclude interface from NAT 26
- Exclude Mask 33
- Exclusive 51, 52
- Expires 38
- F**
- Facility 61
- Faststart 36
- FAX-Gerät 43
- Fax-Gerät 52
- Fax-Over-IP-Protokoll 52
- Feature-Codes 45, 53
- Fehlerbehebung 80
- Final-Map 64
- Final-Route 64
- Firewall 81
- Firmware 69, 70
- Firmware-Download 92
- Firmware-Update 88, 92
- Firmware-Upload 88
- Firmware-Version 69, 88, 92
- First Address 34
- First UDP-NAT port / numbers of port 23
- First UDP-RTP port / numbers of port 23
- Flash-Signal 43
- Force-Enblock 65



Frame 51  
Frame Speichern unter 74  
From 62  
FTP 106  
FTY 61, 106  
Full-Replication 41  
Funktionsstörung 4

## **G**

G711A 51  
G711u 51  
G723-53 51  
G726-32 51  
G729A 51  
GAP 107  
Gatekeeper 35  
Gatekeeper/Registrar 59  
Gatekeeper6 48  
Gatekeeper-Address (primary) 52, 59  
Gatekeeper-Address (secondary) 52, 59  
Gatekeeper-Discovery 59  
Gatekeeper-ID 35, 44, 53, 59  
Gatekeeper-Identifizier 35, 59  
Gatekeeper-IP-Adresse 35, 52, 59  
Gatekeeper-Lizenz 44, 48  
Gateway 29, 30, 33, 44, 48  
Gateway without Registration 59  
Gateway-Einstellung 44  
Gateway-Konfiguration 44  
Gateway-Lizenz 48  
Gebührenimpuls 43  
General 14  
Gerätekonfiguration 93

Gerätename 15  
Geschützte Bereiche 13  
GMT 96, 107  
Group-Join 48  
GW1-12 62  
GWLoad 75

## **H**

H 108  
H.225 108  
H.225-RAS-Destination 24  
H.225-Signalling-Destination 24  
H.245 108  
H.245-Tunneling 36, 61  
H.323 60, 108  
H.323-Authentifizierung 24  
H.323-Faststart 36  
H.323-Firewalling 81  
H.323-Interop-Tweaks 60  
H.323-Name 60  
H.323-NAT 24, 82  
H.323-Registrierung 52, 71  
H.3245-Faststart 60  
Handover 107  
Handset 107  
Hardware-Version 14  
HDLC 14  
Hexadezimalzahl 14  
High-Layer-Compatibility 61  
HLC 61, 107  
Hostname 38  
Hotfix 88  
HTTP 19, 21, 56, 67  
HTTP-GET 21, 67, 89  
HTTP-Port 18

HTTP-PUT 89, 93

HTTP-Session 89

## **I**

ID 33

ID @ 54

Idle-Reset 75

IEEE 4, 10, 108

IEEE-POSIX-Standard 18, 35, 96

Immediate reset 70

Inbetriebnahme 10

Inbound-Connections 29

Inbound-Password 27

Inbound-User 27

Include Interface in NAT 33

Info 14

innovaphone-AG 4

innovaphone-GWLoad 75

innovaphone-Händler 21, 69, 70

innovaphone-Homepage 21, 88

innovaphone-Knowledgebase 75

innovaphone-Neuigkeiten 88

innovaphone-PBX 41

Insert Route below 62

Interface 30, 49, 58, 68

Interface-Maps 50

Interleaving 83

International 57

International-Prefix 50, 51

Interworking (QSIG) 65

IP 109

IP-Address 32, 34, 37

IP-Address for Remote Party 25

IP-Adressbereich 22

IPEI 109

IP-Einstellungen 22

IP-Konfiguration 31

IP-Master 109

IP-Parameter 31

IP-Protokoll 22

IP-Routes 29

IP-Routing 35

IPxxx 13

ISDN 28, 30, 57, 109

ISDN-Fehlercode 64

ISDN-Schnittstelle 44, 61

ITU 109

## **J**

Jitter 68, 110

## **K**

Kaltstart 14

Kollision 38

Konfiguration des Update-Servers  
89

Konfiguration des VoIP-Gerät 68

Konfiguration eines NTP-Client 96

Konfiguration eines NTP-Server 96

Konfigurationsdatei 68, 69

Koordinierte-Weltzeit 96

## **L**

Lagertemperatur 4

LAN 110

Language 36

Last Address 34

Last sync 18

LDAP 110

LDAP-Benutzer 41

LDAP-Benutzer-Name 40

LDAP-Benutzer-Passwort 40

LDAP-Clients 40  
LDAP-Datenbank 40  
LDAP-Directory 36  
LDAP-Konfiguration 36  
LDAP-Replikator 39  
LDAP-Server 39, 40, 41  
Least-Cost-Routing 56  
Leave 48  
Leistungsmerkmale 45, 53  
Licenses 48  
Link-Configuration 28  
Link-Type 28  
Lizenzen 15  
Lizenztyp 16  
Local 30, 42  
Local-Subscriber-Number 28  
Location 22  
Lock Phone 46  
Locked-White-List 53, 55  
Logging 20, 71  
Log-Meldung 21, 67, 71  
Log-Type 20  
Lokale Zeit 14  
Lokation 41  
Loss 68  
**M**  
MAC-Address 14, 37, 78, 110  
Manual 88  
Map-Eintrag 62, 63, 65  
Mask 59  
Master-PBX 41  
Maximum-Transfer-Unit 25  
Media-Access-Control 14  
Media-Relay 23

Meldungsklasse 20, 67  
MES 97  
MEZ 97  
MIB 21, 111  
Check Interval 34  
Interval 17, 18  
Lease Time 34  
Mode 59  
Model 51  
Modify 42  
MoH 19, 111  
MPPE 27, 111  
MS-IIS 89  
MSN 111  
MSN1-3 / Ext. 51  
MTU 111  
MTU-Size 83  
Multicast 32, 112  
Multicast-Address 59  
**N**  
Name 16, 49, 53, 55, 58, 60  
Name-In 66  
Name-Out 64  
NAT 24, 26, 33, 81, 112  
National 57  
National-Prefix 50, 51  
NAT-Modus 82  
Navigationsbereich 12  
Nbtstat 10, 112  
Network-Address 29  
Network-Address-Translation 33  
Network-Destination 33  
Network-Mask 29, 30, 32, 33, 34  
Network-Specific 57

- Network-Time-Protocol 14
- Netzwerkrouen 32
- Neustart 31
- Newsletter 88
- NI 112
- Nmblookup 11, 113
- No Call Transfer on Hook-On 43
- No Call Waiting 43
- No DNS on this interface 26
- No Faststart 60
- No H.245 Tunneling 61
- No IP Header compression 26
- No Reply from 74
- Notify 41, 42
- NTP 113
- NTP-Server 14, 17, 96
- NTP-Softwarepakete 96
- Number 53, 60, 68
- Number-In 63, 66
- Number-Out 63, 66
- O**
- Off 20, 46, 47, 66
- Offer Parameters 34
- Offset 97
- OSI 113
- Outbound-Connections 29
- Outbound-Password 27
- Outbound-User 27
- Overhead 51
- P**
- Park 48
- Park To 48
- Passive 43
- passiver Modus 43
- Password 15, 19, 40
- Password / Retype 53, 54, 60
- Password protect all HTTP pages 18
- Path 67
- PBX-LIC 16
- PBX-Zugriffsnummern 36
- PCM 114
- Pending 42
- Pickup-Group 47
- Ping 74, 114
- PL 113
- PoE 4, 10, 114
- Point-to-Point 50
- Poll-Richtung 41
- Popup-Seite 49, 57, 58, 62, 68
- Port 18, 67
- Port Specific Forwardings 24
- POSIX 114
- POSIX-Timezone-Strings 96
- Power-over-Ethernet 4, 10
- PP 114
- PPP 25, 50, 55, 71, 114
- PPP Interface PPPn 25
- PPPO-31 30
- PPPoE 27, 115
- PPP-Schnittstelle 32
- PPP-Verbindung 26
- PPTP 27, 115
- PRI 48, 115
- PRI1-4 50, 55
- PRI1-x 71
- PRI-LIC 15
- Primary Gatekeeper 35
- Priorisierung 34, 37, 82

Priority 34  
Private 57  
Private Networks 23  
Produkt 90  
Prot-Kommando 92  
Protocol 68  
Protocol-Firmware 70  
Protokoll 58  
Proxy-ARP 32  
Public 21  
Pulse 42  
Pulswahl 42  
Push-Richtung 42  
**Q**  
Q.931 116  
QoS 37, 115  
QSIG 116  
Quality-of-Service 37  
Quellschnittstelle 62, 63  
Q-Value 116  
**R**  
Radio 116  
RC4 116  
Read 89  
Ready LED 77  
Ready-LED 10  
Referenzkonfigurationen 74  
Register as Endpoint 59  
Register as Gateway 59  
Registered-Clients 24  
Registration 49, 50, 51, 55, 58  
Registrierung 49  
Registrierungsarten 59  
Relay-Calls 71

Relay-Routing 71  
Remote 41  
Repeater 116  
Repeater-Chain 117  
Replicator-Status 41  
Replikationsverbindungen 40  
Reply from 74  
Require authentication 24  
Reserve IP Adress 37  
Reserved 38  
Reset 70, 75, 77  
Reset required 13  
Reset when idle 70  
Reset-Taste 31  
Reverse 42  
RFC 117  
RFP 117  
RJ 117  
RJ45 10  
Roaming 117  
Round-Trip 68  
Route 30, 61  
Route to Interface 28  
Route-Logging 44  
Routendefinition 64  
Routeneinstellung 62  
Routing-Tabelle 62  
RSA 118  
RT 117  
R-Taste 43  
RTP 118  
Rufbehandlung 61  
Rufrichtung 61  
Rufvermittlung 62

Rx 38  
Rx-abandon 40  
Rx-add 40  
Rx-align-err 39  
Rx-broadcast 38  
Rx-collision 39  
Rx-crc-err 39  
Rx-del 40  
Rx-good 38  
Rx-modify 40  
Rx-multicast 39  
Rx-no-buffer 39  
Rx-overflow-err 39  
Rx-queue-overflow 39  
Rx-search 40  
Rx-too-long 39  
Rx-too-short 39  
Rx-tx-1024 39  
Rx-tx-128-255 39  
Rx-tx-256-511 39  
Rx-tx-512-1023 39  
Rx-tx-64 39  
Rx-tx-64-127 39  
Rx-unicast 38

**S**  
SC 52, 118  
SCFG-Kommando 93  
Secondary Gatekeeper 35  
Selektive Amtsberechtigung 65  
Seriennummer 14  
Seriennummernetikett 78  
Server 18, 31, 41  
Server-Address 27  
Server-Address (primary) 54  
Server-Address (secondary) 54  
Server-Status 40  
Service-Packs 88  
Set PIN 46  
Signalisierungskanal 64  
Silence Compression 52  
Simple-Network-Time-Protocol 14  
SIP1-4 55  
SIP-Provider 54  
SIP-Registration 54  
SIP-Registrations 71  
SIP-Schnittstellen 55  
Slave 41  
SNMP 21, 119  
SNMP-Agenten 21  
SNTP 14, 119  
SNTP-Server 14  
Software-Version 14  
Sommerzeit 96  
Sommerzeitzone 97  
Speech Bearer Capability 43  
Speichergröße 14  
Speichern der Einstellungen 13  
Sprache 36  
Sprachkanäle 14  
Standard-Authentifizierung 18  
Standard-Benutzer-Kennwort 13  
Standard-Benutzer-Name 13  
Standard-Community-Name 21  
Standard-Dateiname 90  
Standard-Einstellungen 91, 92  
Standard-Firmware-Dateiname 92  
Standard-Konfiguration 92  
Standard-MIB-II 21

- Standard-Router 32
- Standby-PBX 41
- Starting 41
- State 30, 49, 68
- Stateless-Operation 28
- Static IP-Routes 32, 35
- Statistics 38
- Status 24, 31
- Std 97
- StdOffset 97
- Stop 41
- String 18
- Stromversorgung 4, 10
- STUN-Server 54
- Subaddress 61
- Subscriber 57
- Subscriber-Number 50
- Supplementary-Services 45, 53, 54
- Suppress FTY 61
- Suppress HLC 61
- Suppress Subaddress 61
- Sync 14
- Synchronisation 18, 96, 119
- Synchronisation-Chain 119
- Sync-Master 120
- Sync-Source 120
- Syslog 20, 67, 71
- Syslogd 20, 67
- Syslog-Deamon 20, 67
- Syslogd-Server 67
- Syslog-Einträge 20
- Syslog-Empfänger 20, 67
- Syslog-Information 44
- Syslog-Server 20, 35, 67

## T

- T.38 52
- Tarifimpuls 43
- TCP 20, 67, 71, 120
- TCP-Verbindung 20, 67
- TEL1 61
- TEL1-2 76
- TEL1-2 LED 76
- TEL1-4 50, 55
- TEL1-x 71
- TEL2 61
- Telnet 121
- Telnet-Protokoll 22
- Telnet-Session 90
- TEL-Schnittstelle 42
- TEST 56
- TFTP 121
- TFTP-Mode 75
- TFTP-Reset 75
- TFTP-Server 35
- Time 14
- Time-Kommando 91
- Time-Server 35
- Timezone 18
- Timezone-String 35, 96
- To 62
- TONE 56
- Tones 50, 56
- ToS 22, 34, 82, 121
- ToS-Priority 22, 34, 82, 83
- Trace 121
- Trace (buffer) 72
- Trace (continuous) 72
- Trace-Informationen 72

Trace-Varianten 72  
Trap 22  
Trap-Destinations 22  
Trap-Meldungen 22  
Trunk-Point-to-Multipoint 50  
Tunneling 36  
Twisted-Pair-Kabel 10  
Tx 38  
Tx-broadcast 38  
Tx-collision 38  
Tx-deferred 38  
Tx-error 40  
Tx-error-49 40  
Tx-error-50 41  
Tx-excesscol 38  
Tx-good 38  
Tx-latecol 38  
Tx-lostcarrier 38  
Tx-multicast 38  
Tx-notify 40  
Tx-unicast 38  
Type 16, 38  
Type-of-Service 22, 34, 82  
TZ-String 96

## **U**

Übertragungsart 31  
Übertragungsgeschwindigkeit 31  
UDP 122  
UDP-NAT 23  
UDP-RTP 23  
Universal-Time-Coordinated 96  
Unknown 56, 57  
Unlock 46  
Unpark 48

Unpark From 48  
Up 30, 31, 41, 49  
Update 68  
Update-Datei 90  
Update-Interval 36  
Update-Script 17  
Update-Server 17, 36, 37, 89, 90  
Update-Server URL 37  
Upload 69, 70  
Uptime 14  
URI 54  
URL 17, 19, 37, 67, 90, 92, 122  
URL-Parameter 90  
User 19  
User & Password 41  
User-Name 15  
Username 40  
UTC 96, 122

## **V**

Verify CGPN 65  
Version 14  
Versionsbezeichnung 88  
Virtual-Local-Area-Network 33  
Virtuelle-Schnittstellen 56  
VLAN 33, 123  
VLAN-ID 33, 37  
VLAN-Priority 37  
Voicemail 19  
Voicemail-LIC 16  
VoIP-Gatekeeper 35  
VoIP-Schnittstelle 62  
Volume 43  
VPN 27, 123



## **W**

Wahlton 35  
Wahlziffern 65  
WAN 123  
WAN-Strecken 82  
WAN-Verbindung 32  
Warmstart 14  
Wartungsdatei 90, 91, 92  
Wartungsdurchführung 90  
Wartungskommandos 90  
Waste-Electrical-and-Electronic-Equipment 4  
Webserver 21, 67, 89  
WEEE-Richtlinien 4  
Weltzeit 96  
Wiedergabe 43  
Windows-Server 96  
WINS 123  
WINS-Server 35  
Winterzeit 96  
WRFP 124  
Write 89  
Write-Access 40  
Write-Connections 40

## **X**

XPARENT 51

## **Z**

Zeitdienst 96  
Zeitformat 36  
Zeit-Server 18, 35, 96  
Zeitzone 14, 18, 35  
Zielhost 74  
Zielschnittstelle 62, 64



*innovaphone® AG  
Böblinger Straße 76  
D-71065 Sindelfingen*

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

*www.innovaphone.com  
info@innovaphone.com*