IP-Gateway

IP1200

Administrator Handbuch

innovaphone

Pure IP-Telephony

IP-Gateway

IP1200

Handbuch
Version 6.0

Release 6.0, 3. Auflage, April 2007

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

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 zuückgesendet werden. Die Kosten für die Rücksendung übernimmt dabei die innovaphone-AG.

Inhaltsverzeichnis

1 Einführung

Das vorliegende Handbuch beschreibt das innovaphone-IP-DECT-Gerät IP1200. Das IP1200 Gateway realisiert eine Erweiterung für die innovaphone-PBX um DECT-kompatible Endgeräte. Es ist ein kombiniertes System mit dem Gateway und der DECT-Basisstation in einem Gehäuse.

Die IP1200 ist ein IP-DECT Gateway zur Erweiterung der innovaphone-PBX um DECT-kompatible Teilnehmer. Mit ihr lassen sich sehr komplexe DECT-Systeme aufbauen. Durch die Multicell-Fähigkeit der Basisstation IP1200 können mehrere Geräte installiert werden, zwischen denen Roaming und automatisches Handover funktionieren. Für die Anzahl der Basisstationen in einem DECT-System gibt es die theoretische Grenze von 256 Stück. Eine Basisstation unterstützt dabei im Singlecell-Betrieb bis zu 12 Kanäle und im Multicell-Betrieb bis zu 11 Kanäle parallel. Die Erweiterung mit einem Repeater erhöht die Reichweite des Empfangs und erreicht damit eine bessere Ausleuchtung, erhöht aber nicht die Anzahl der Kanäle. In einem gesamten DECT-System können maximal 256 Repeater eingesetzt werden.

1.1 Standards

Das System ist zur IP-Seite vollkommen H.323 kompatibel. Es unterstützt Echo Cancellation und mehrere Codecs zur Sprachkomprimierung. Auf der DECT-Seite besteht GAP-Kompatibilität. Besonders geeignet sind jedoch die Handsets IP50, IP52 und IP54 von innovaphone. Im Singlecell-Betrieb können maximal 35 Handsets und im Multicell-Betrieb maximal 1500 Handsets angebunden werden.

Für die professionelle Installation eines IP1200 DECT-Systems stellt innovaphone in Zukunft allen Technikern ein Kit bereit, das eine optimale Ausleuchtung schon zu Projektbeginn und noch vor der Installation gewährleistet soll.

1.2 Leistungsmerkmale

- GAP kompatibles VoIP-Gateway
- Basistation (1,8 GHz) mit bis zu 12 Kanälen
- Mehrfachinstallation, Multicell im Master-Slave-Betrieb
- Reichweitenerhöhung durch bis zu 3 Repeater in Reihe
- Roaming und "Seamless Handover" zwischen allen Zellen und Repeatern
- zwei Ethernet Schnittstellen
- unterstützt die Protokolle H.323 und SIP gleichzeitig

- Steckernetzteil, 110-240V, 45mA, oder "Power over Ethernet"

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**lectronical-**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*'-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.

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 Kaptiel: „*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:

Version	• Die Software-Version (6.00) <Gateway>[firmware]. • Die Bootcode-Version <Bootcode>[firmware]. • Die Hardware-Version <HW>[nr]. • Die Speichergröße <Flash/Ram>.
Serialno	Die Seriennummer bzw. die MAC-Adresse (**M**edia-**A**ccess-**C**ontrol) des Gerätes (6-stellige Hexadezimalzahl).
Coder	Die Anzahl und Art der Sprachkanäle.
HDLC	Die Anzahl der HDLC- Kanäle (**H**igh-level-**D**ata-**L**ink-**C**hannels).
Sync	Die für die Synchronisation verwendete physikalische Schnittstelle (TEL, PPP, BRI, PRI).
SNTP-Server	Die IP-Adresse des verwendeten SNTP-Servers (**S**imple-**N**etwork-**T**ime-**P**rotocol), sofern konfiguriert.
Time	Die lokale Zeit des Gerätes, gemäß den Angaben des NTP-Servers (**N**etwork-**T**ime-**P**rotocol) und der Zeitzone.
Uptime	Die Betriebsdauer seit dem letzten Kalt- oder Warmstart.

Im Abschnitt **DECT** erhalten Sie Informationen über das DECT-System:

Firmware	Die Firmwareversion des DECT-System.
System-ARI	Die Systemkennung des DECT-System.
Frequency	Die verwendete Frequenz des DECT Subsystem (EUR = 1.8 GHz; USA = 2.4 GHz).

4.1.1.2 Configuration/General/Admin

Der Administrator-Zugang wird hier konfiguriert.

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

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_0-ISDN Kanals.
- **PRI-LIC** - Ermöglicht die Freischaltung eines S_2M-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:

Type	Der installierte Lizenztyp (PBX, Relay oder DECT bei IP-DECT-Subsystem).
Name	Eine genaue Bezeichnung der Linzenz mit Angabe der Anzahl an Registrierungen gefolgt von der MAC-Adresse.
Action	Mit einem Klick auf den Button **download** können die angezeigten Lizenzen aus dem Gerät geladen und als Textdatei gesichert werden. Mit einem Klick auf den Button **delete** kann die angezeigte Lizenz aus dem Gerät gelöscht werden. Die Schaltflächen **download all** und **delete all** haben die gleiche Funktionalität wie die Schaltflächen **download** und **delete**, 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 (**U**niform-**R**esource-**L**ocator) 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 duch 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 gerätespezifischen 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.

Detailiertere 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**-** (**N**etwork-**T**ime-**P**rotocol) Server in der Lage, seine interne Uhr mit einer externen Zeitquelle zu synchronisieren. Diese wird benötigt, da ohne Angabe eines Zeitservers nach jedem Reset die interne Uhrzeit auf den 01.01.1970 0:00 Uhr zurückgesetzt wird.

Server	Die IP-Adresse des Zeitservers.
Interval [min]	Die Zeit in Minuten, mit welchem Intervall sich das Gerät mit dem Zeitserver synchronisieren soll.
Timezone	Eine Auswahlmöglichkeit der Zeitzone, in der sich das Gerät befindet.
String	Es können zusätzliche Zeitzonen gemäß IEEE- (**I**nstitute-of-**E**lectrical-and-**E**lectronics-**E**ngineers) POSIX- (**P**ortable-**O**perating-**S**ystem-**I**nterface-for-Uni**X**) Standard hinzugefügt werden.
Last sync	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.

Disable HTTP basic authentification	Die Anmeldedaten werden standardmäßig im Klartext und somit protokollier- und abhörbar übermittelt. Um diese Schwachstelle zu vermeiden empfielt es sich, die Standard-Authentifizierung (mit Benutzername und Passwort) zu deaktivieren und statt dessen die Digest-Hash-Authentifizierung zu verwenden.
Password protect all HTTP pages	Bis auf die Startseite *Configuration/General/Info* erfordern alle Bereiche der Benutzeroberfläche die Eingabe der Administrator-Nutzerkennung. Durch Aktivierung dieses Kontrollkästchens werden alle Seiten des Gerätes passwortpflichtig.

Port	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 Netzbereich (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 passwortgeschüzten 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 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`).
Auch hier können in der URL die Platzhalter #h und #m verwendet werden:

- #h - wird duch 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 gerätespezifischen 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-deamon` bezeichnet). Dieser ist dann für die weitere Auswertung oder Abspeicherung zuständig.

- In das Eingabefeld **Address** wird die IP-Addresse des `syslogd`-Servers eingetragen.
- Im Eingabefeld **Class** wird die gewünschte Meldungsklasse 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 Webservers eingetragen, der die Weiterverarbeitung der übermittelten Daten übernimmt.
- In das Eingabefeld **Path** wird die relative URL des Formularprogramms auf dem Webserver eingegeben.

  Das Gerät wird zum Webserver einen HTTP-GET-Request auf die eingetragene URL, gefolgt vom url-encodeten Syslog-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.

4.1.1.9 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). Detailierte 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 eingetragen werden.
Device Name	Zur detaillierteren Information kann hier dem SNMP-Agenten ein Geräte Name angegeben werden.
Contact	Sowie auch eine Kontaktperson (**Contact**).
Location	Genauso einen Standort (**Location**).
Authentication Trap	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.
Trap Destinations	Soll das Gerät die in der herstellerspezifischen innovaphone-MIB definierten Traps auslösen, so müssen zusätzlich noch Ziele für Trap-Meldungen definiert werden.
Allowed Networks	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.

Enable Telnet	Ein markiertes Kontrollkästchen aktiviert den Zugriff auf das Gerät mittels telnet. Mit Befehlen wie z.B: *reset, config change UP1 /url <http url> /poll <secs>* 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.

ToS Priority	Konfiguration des ToS**-**Feldes (**T**ype-**o**f-**S**ervice) bei Sprachpaketen. Standardmäßig wird der Wert `0x10` 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: „*Problembehebung*" 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 **N**etwork-**A**ddress-**T**ranslation (**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 Netzt darstellen. Diese Funktion ermöglicht H.323-Gespräche zwischen privaten und öffentlichen Netzen.

Enable H.323-NAT	Aktiviert NATfür H.323 VoIP-Gespräche.
Require authentication	Ein markiertes Kontrollkästchen setzt die H.323-Authentifizierung vorraus. Diese Option gilt als eine Sicherungsmaßname vor fremden Zugriffen auf das eigene private Netz. H323-Nachrichten ohne Authentifizierung werden nicht in das private Netz geleitet.
H.225/RAS destination	IP-Adresse des Servers im privaten Netzt, an den eingehende H.225/RAS-Nachrichten geleitet werden.
H.225/ Signalling destination	IP-Adresse des Servers im privaten Netzt, 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 PPP*n***:

Enable	Aktiviert / Deaktiviert die Schnittstelle. Die PPP-Schnittstelle wird in der Übersichtsseite PPP-State nur dann angezeigt, wenn sie aktiviert (Enable) ist.

Connection Port	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.
Descriptiv Name	Hier kann ein beschreibender Name für die Schnittstelle eingegeben werden. Dieser Name dient der Übersicht im Untermenü PPP-State (siehe Kapitel: „*Configuration/IP/PPP-State*“).
Bandwidth	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 Upsteam 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.
Maximum transfer unit (Bytes)	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: • X.25 - 576 • PPoE (z.B: DSL) - 1492 • ISDN, Ethernet - 1500 • ATM - 4500
IP Address for Remote Party	Weist der Gegenseite eine lokale IP-Adresse zu, um sie in das lokale Netz einzubinden.
Auto dial after boot	Bewirkt, dass die entsprechende PPP-Verbindung des Gerätes sofort nach dem Starten aufgebaut und offen gehalten wird.
Allow inbound connections	Als PPP-Server konfiguriert erlaubt ein markiertes Kontrollkästchen PPP-Wahlverbindungen, die auf dem Gerät eingehen (inbound).

No DNS on this interface	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.
Exclude interface from NAT	Mit dieser Option kann ein bestimmtes Interface von der NAT (**N**etwork-**A**ddress-**T**ranslation) ausgeschlossen werden, sollte NAT aktiviert sein (siehe Kapitel: *„Configuration/IP/NAT"*).
No IP Header compression	Die VoIP-Geräte unterstützen die Kompression von Sprachdaten auf der PPP-Strecke nach dem Verfahren **RTP Header Compression** (RFC 2508, 2509). Dadurch wird die benötigte Bandbreite für VoIP-Gespräche drastisch reduziert. Um dies zu unterdrücken, muss das Kontrollkästchen **No IP Header compression** aktiviert werden.
Adapt to Cisco PPP peers	Wird auf der Gegenseite ein Cisco-Router eingesetzt und es kommt bei der Übertragung von Sprachdaten zu Problemen, dann könnte die Option **Adapt to Cisco PPP peers** 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 Authentifizierung 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-**P**oint-**T**unneling-**P**rotokoll) 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 Password. Zusätzlich können die übertragenen Sprachdaten mit der MPPE (**M**icrosoft-**P**oint-to-**P**oint-**E**ncryption) verschlüsselt werden. Vorraussetzung 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.
Route to Interface	Hier können Verbindungsaufbau-Anfragen direkt an ein bestimmtes Interface weitergeleitet werden. Zum Beispiel: ETH0-1, PPP0-31.
Enable MPPE Encryption	Aktiviert das Microsoft Point-To-Point-Encryption-Protocol. MPPE (RFC 3078) benutzt den RSA-RC4-Algorithmus.
Stateless Operation	Dabei wird der Schlüssel nach jedem übertragenem Paket geändert.

40-Bit Encryption	Aktiviert die Verschlüsselung mit einem 40Bit-Session-Key.
128-Bit Encryption	Aktiviert die Verschlüsselung mit einem 128Bit-Session-Key verwendet.

Abschnitt **ISDN**:

Link Configuration	Hier kann die ISDN-Schnittstellenkonfiguration vorgenommen werden. Die PPP-Schnittstelle kann hier sowohl für eingehende als auch für ausgehende Rufe konfiguriert werden.
Link type	Es können vier verschiedenen Link-Typen gewählt werden. **Singlelink (64k)** - Eine Verbindung über einen B-Kanal. **Multilink (128k)** - Eine Verbindung über zwei gebündelte B-Kanäle. Stellt die doppelte Übertragungsgeschwindigkeit zur Verfügung. **Permanent B1** - Verwendet ausschließlich den B1-Kanal. **Permanent B2** - Verwendet ausschließlich den B2-Kanal.
Local Subscriber Number	Die **Local Subscriber Number** ist bei eingehenden Wahlverbindungen die Rufnummer (MSN), unter der eingehende Rufe akzeptiert werden sollen. Die **Local Subscriber Number** ist bei ausgehenden Wahlverbindungen die für den Ruf zu verwendende ausgehende Rufnummer (MSN).
2nd Local Subscriber Number	Wird **Multilink** 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.
Outbound Connections	Hier kann die ISDN-Schnittstelle für ausgehende PPP-Wahlverbindungen konfiguriert werden.
Called Party Number	Die für den ausgehenden Ruf zu verwendende Rufnummer (MSN).
2nd Called Party Number	Die für den ausgehenden Ruf zu verwendende Rufnummer (MSN) auf dem zweiten B-Kanal.

Inbound Connections	Hier kann die ISDN-Schnittstelle für eingehende PPP-Wahlverbindungen konfiguriert werden.
Calling Party Number	Mit Angabe der **Calling Party Number** 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.

Network Address	Die Netzwerk-Adresse der neu hinzuzufügenden Route.
Network Mask	Die Netzwerk-Maske der neu hinzuzufügenden Route.
Gateway	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 manuall die Verbindung zu schließen und wieder aufzubauen.

Interface	ID der PPP-Interfaces.
Address	Die lokale IP-Adresse des PPP-Interfaces.
Type	Der Typ des Interfaces. PPTP, PPPoE oder, falls es sich um PPP über einen ISDN-Kanal handelt, eine der ISDN-Schnittstellen.
State	Zeigt den aktuellen Zustand des Interfaces an. Mögliche Zustände: *Connecting, Up* oder *Down*.
Since	Hier wird die Zeit angegeben, seit wann die Verbindung besteht.

Action	• ***connect*** stellt eine Verbindung zum gewählten Interface her. • ***clear*** löscht die aktuelle Verbindung zum gewählten Interface. • ***info*** zeigt relevanten Verbindungsdaten des gewählten Interfaces an.
Name	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:

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

4.1.3 Configuration/ETH0-1

Hier können die Ethernet-Schnittstellen des Gerätes konfiguriert werden.

Der Aufbau beider Menüs ist identisch. Die Besonderheiten und Unterschiede der beiden Ehternet-Schnittstellen (**ETH0 & ETH1**) werden an entsprechender Stelle innerhalb dieses Kapitels im Text erklärt. Für beide Ethernet-Schnittstellen werden *CAT5-STP*-Kabel empfohlen.

4.1.3.1 Configuration/ETH0-1/Link

Die Übertragungsart der Ethernet-Schnittstelle wird hier festgelegt.

Standardmäßig ist die Übertragungsart **auto** selektiert:

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

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

4.1.3.2 Configuration/ETH0-1/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:

Disabled	Die IP-Adresse und andere Parameter werden manuell konfiguriert.
Server	Die IP-Parameter werden im *DHCP-Server-Modus* manuell konfiguriert (Standard-IP-Adresse `192.168.0.1`). Der DHCP-Server ist an und sollte wie im Kapitel: *„Configuration/ETH0-1/DHCP-Server"* entsprechend konfiguriert werden.
Client	Im *DHCP-Client-Modus* erhält das Gerät seine IP-Konfiguration von einem DHCP-Server, an dessen Netzwerk das Gerät angeschlossen ist.
Automatic	Nach dem erstmaligen Einschalten des Gerätes (Power-Up) arbeitet **ETH0** als DHCP-Client. Nach einem Neustart durch kurzes Drücken der Reset-Taste, wird der **ETH0**-Schnittstelle die konfigurierte IP-Adresse vergeben. Wurde nicht explizit eine IP-Adresse konfiguriert (siehe Kapitel: *„Configuration/ETH0-1/IP"*), dann ist standardmäßig die IP-Adresse `192.168.0.1` 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/ETH0-1/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 Ehternet-Segment, die über keine korrekte Routingeinstellung 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 Netzwerkrouten definiert werden, sollten ausser dem lokalen Netz noch andere Netzbereiche benötigt

werden.

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

4.1.3.4 Configuration/ETH0-1/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.

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

4.1.3.5 Configuration/ETH0-1/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 ausschlieslich in das angegebene VLAN übermittelt werden.

ID	Die ID des VLANs. Ist das Eingabefeld **ID** leer, wird der Wert 0 angenommen. Die VLAN-ID mit dem Wert 0 schaltet die QoS (**Q**uality-**o**f-**S**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/ETH0-1/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`).

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

Enblock Dialing Timeout [s] *	Schaltet Blockwahl für VoIP-Telefone ein.
Faststart [0|1] *	Mit der Option **Faststart[0|1]** kann man die H.323-Faststart Prozedur an/aus schalten.
Tunneling [0|1] *	Mit der Option **Tunneling[0|1]** kann man die H.245-Tunneling Prozedur an/aus schalten.
Language *	Alle VoIP-Telefone, die per DHCP ihre IP-Adresse erhalten, bekommen die hier festgelegte Sprache als Standard-Sprache eingerichtet.
Dialing Location *	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"*.
AM/PM Clock [0|1]	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.
LDAP Directory	Um allen VoIP-Geräten die per DHCP eingebunden werden, eine funktionierende LDAP-Konfiguration zu zuweisen, kann im Feld **LDAP Directory** 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 PHONEDIR0 ldap-config"*. Nach Absetzen dieses Befehls wird im Browser eine Konfigurationszeichenkette ausgegeben, welche man kopiert und in das Feld **LDAP Directory** des DHCP-Servers einfügt. Damit erhalten alle weiteren Geräte eine korrekte LDAP-Konfiguration.
Update Interval [min]	Alle per DHCP eingebundene Geräte erhalten den hier angegebenen Interval in das Feld **Interval [min]** 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 (**Q**uality**-o**f**-S**ervice) 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/ETH0-1/DHCP-Leases

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

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

Unter dem Abschnitt **Cleanup** können vergebene DHCP-Leases wieder glöscht 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.

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

4.1.3.8 Configuration/ETH0-1/Statistics

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

tx-good	Die Anzahl erfolgreich versendeter Pakete.
tx-unicast	Die Anzahl erfolgreich versendeter Unicast-Pakete.
tx-broadcast	Die Anzahl erfolgreich versendeter Broadcast-Pakete.
tx-multicast	Die Anzahl erfolgreich versendeter Multicast-Pakete.
tx-lostcarrier	Die Anzahl verlorener Trägersignale. Deutet auf ein defektes Medium (z.B.: Kabel) hin.
tx-deferred	Die Anzahl zurückgestellter Pakete.
tx-collision	Die Anzahl von kollidierenden Paketen (max. 16).
tx-excesscol	Die Anzahl der kollidierenden Pakete (wenn tx-collision > 16).
tx-latecol	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 *late collision* ausgegeben.

rx-good	Die Anzahl der erfolgreich empfangenen Pakete.
rx-unicast	Die Anzahl erfolgreich empfangener Unicast-Pakete.
rx-broadcast	Die Anzahl der erfolgreich empfangener Broadcast-Pakete.

rx-multi-cast	Die Anzahl der erfolgreich empfangener Multicast-Pakete.
rx-crc-err	Die Anzahl der empfangenen CRC-Prüfsummenfehler.
rx-align-err	Die Anzahl der Alignment Error (falscher Treiber, Kabel defekt) beim Empfang von Datenpaketen.
rx-too-short	Die Anzahl der zu kleinen Datenpakete, während der Übermittlung.
rx-too-long	Die Anzahl der zu großen Datenpakete, während der Übermittlung.
rx-collision	Die Anzahl der kollidierenden Pakete (max. 16).
rx-overrun-err	Die Anzahl der Buffer-Overrun-Error beim Empfang von Datenpaketen.
rx-queue-overrun	Die Anzahl der Queue-Overrun-Error beim Empfang von Datenpaketen.
rx-no-buffer	Die Anzahl der No-Buffer beim Empfang von Datenpaketen.

rx-tx-64	Die Gesamtanzahl gesendeter und empfangener Pakete mit 64 Bytes.
rx-tx-64-127	Die Gesamtanzahl gesendeter und empfangener Pakete zwischen 64 und 127 Bytes.
rx-tx-128-255	Die Gesamtanzahl gesendeter und empfangener Pakete zwischen 128 und 255 Bytes.
rx-tx-256-511	Die Gesamtanzahl gesendeter und empfangener Pakete zwischen 256 und 511 Bytes.
rx-tx-512-1023	Die Gesamtanzahl gesendeter und empfangener Pakete zwischen 512 und 1023 Bytes.
rx-tx-1024	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.

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

4.1.4.2 Configuration/LDAP/Server-Status

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

connections	Gesamtanzahl aller Verbindungen zum LDAP-Server.
write-connections	Anzahl der Verbindungen mit Schreibberechtigung.
rx-search	Anzahl der empfangenen Suchanfragen.
rx-modify	Anzahl der empfangenen Änderungsanforderungen.
rx-add	Anzahl der empfangenen Hinzufügeanforderungen.
rx-del	Anzahl der empfangenen Löschanforderungen.
rx-abandon	Anzahl der empfangenen Abbruchanforderungen.
tx-notify	Anzahl der gesendeten Benachrichtigungen.
tx-error	Anzahl der gesendeten Fehlerbenachrichtigungen.
tx-error-49	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.

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

4.1.5 Configuration/DECT

DECT-spezifische Einstellungen der IP1200 werden in diesem Kapitel vorgenommen.

4.1.5.1 Configuration/DECT/System

Die allgemeine Konfiguration des DECT-Systems sowie die Vergabe des DECT-System-Namen und Passwort wird in diesem Untermenü vorgenommen.

Name	Der Name des DECT-Systems. Dieser Name bestimmt den Namen des LDAP-Objektes, in dem die System-Parameter abgelegt werden. Bei einer Replikation von einer innovaphone-PBX muss ein entsprechendes Objekt in der PBX angelegt sein.
Pwd	Das Passwort für die Verschlüsselung aller Passwörter in der LDAP-Datenbank. Werden die Benutzerdaten von einer innovaphone-PBX repliziert, dann muss das PBX-Passwort konfiguriert werden.
Sys-Mask	Ohne Konfiguration einer Sys-Mask, wird immer das sogenannte *connection handover* verwendet. Mit Konfiguration einer Sys-Mask, kann das schnellere *bearer handover* zwischen der DECT-Base-Station und dem zugehörigen DECT-Repeater verwendet werden.
AC	Der Access-Code, der beim Einbuchen des DECT-Handsets angegeben werden muss. Diese Angabe ist nur erforderlich, wenn in der Auswahlbox *Subscriptions* der Wert *With user AC only* selektiert ist.

Subscriptions	Die Art der Handset-Registrierungen (Subscriptions). • **With User AC only**: Subscriptions erlaubt, die in der Benutzereingabemaske mit Angabe einer IPEI-Nummer und mit Angabe eines **A**uthentifizierungs **C**ode (**AC**) konfiguriert worden sind. Die Angabe des AC ist optional und kann somit leer sein. • **Allow Anonymous**: Anonymous subscriptions sind erlaubt. Die Handset-Einbuchung erfolgt immer mit dem System **AC**. Das Eingabefeld **AC** kann auch hier leer sein. • **Disable**: Subscriptions sind nicht möglich.
Tones	Hier können verschiedene Ton-Schemen verwendet werden.
Enbloc Dialing	Ein markiertes Kontrollkästchen aktiviert die Blockwahl. Dies ist nur erforderlich, falls der Gatekeeper oder SIP-Provider keine Einzelzifferwahl unterstützt.
Local R-Key/Display Handling	Die Leistungsmerkmale der R-Taste werden in DECT-Systemen auf entsprechender VoIP-Protokolle umgesetzt und sollten in der innovaphone-PBX immer aktiviert sein.
DTMF through RTP Channel	Ein markiertes Kontrollkästchen sendet DTMF-Daten nicht über die Signalisierungsverbindung (TCP) sondern über den RTP-Medien-Kanal.
No Transfer on Hangup	An einem Telefon wird ein Gespräch geführt. Ein zweiter Ruf geht auf diesem Telefon ein (Anklopfend), das erste Gespräch wird gehalten, das zweite Gespräch angenommen. Wurde das zweite Gespräch durch auflegen des Hörers beendet, so wird der gehaltene erste Ruf auf diesem Telefon gesondert signalisiert. Wurde dieses Kontrollkästchen markiert, so wird ein gehaltenes Gespräch beendet.
Coder	Der Coder ist die Art der Komprimierung der Sprachdaten. Dieser Coder wird für alle externen Gespräche verwendet. Unterstützt das entfernte VoIP-Gerät die eingestellte Kodierung nicht, wird eine gemeinsam unterstützte Kodierung ausgehandelt.
Frame	Die Framegröße der Sprachdaten in *ms*.

Exclusive	Ein markiertes Kontrollkästchen aktiviert den gewählten Coder als Exclusive. Damit wird die Verwendung der eingestellten Kodierung (Coder) erzwungen. Dies kann zu einem scheiternden Ruf führen, sollten dieses und das entfernte VoIP-Gerät keinen gemeinsamen Coder unterstützen.
SC	Ein markiertes Kontrollkästchen aktiviert die **S**ilence **C**ompression (**SC**). D.h.: bei Gesprächspausen werden keine Sprachdaten übermittelt.

4.1.5.2 Configuration/DECT/Master

Es ist notwendig die Betriebsart des DECT-Systems zu konfigurieren. Genauso muss hier auch ein Gatekeeper angegeben werden, auf welchem die innovaphone-PBX-Komponente betrieben wird.

Mode	**Active**, schaltet die DECT-Master-Funktion ein. In jedem DECT-System muss ein DECT-Master vorhanden sein. **Standby**, schaltet die Standby-Funktion für den DECT-Master ein. **Off**, schaltet die DECT-Master-Funktion aus.
GK	Die IP-Adresse des primären Gatekeeper. Das Gerät auf welchem die innovaphone-PBX-Komponente betrieben wird.
Alt-GK	Die IP-Adresse des sekundären, alternativen Gatekeeper.
GK-ID	Die Gatekeeper-ID des zu verwendenden Gatekeeper.
Prot	Das Protokoll, dass zur Kommunikation verwendet werden soll. Es besteht die Auswahlmöglichkeit zwischen: • **H.323** (*RFC 1889*), welches das für innovaphone VoIP-Geräte empfohlene Protokoll ist, da es die meisten Leistungsmerkmale enthält. • **SIP** (*RFC 3261*).

4.1.5.3 Configuration/DECT/Features

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 verschieden Arten von Anrufumleitungen.

Aktivität	Code	Beschreibung
CFU **Activate** **Deactivate**	 *21*$# #21#	Aktiviert, deaktiviert die permanente Anrufweiterleitung. Das $-Zeichen steht für die Zielrufnummer.
CFB **Activate** **Deactivate**	 *67*$# #67#	Aktiviert, deaktiviert die Anrufweiterleitung wenn besetzt. Das $-Zeichen steht für die Zielrufnummer.
CFNR **Activate** **Deactivate**	 *61*$# #61#	Aktiviert, deaktiviert die Anrufweiterleitung bei fehlender Antwort. Das $-Zeichen steht für die Zielrufnummer.

Sperren

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

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

PIN

Die PIN dient dazu, den Zugang für unberechtigte Nutzer zu verhindern. Mit die-

ser Funktion kann der Schutz aktiviert und eine PIN festgelegt werden.

Aktivität	Code	Beschreibung
Set PIN	*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
Do not Disturb		Aktiviert, deaktiviert die Stummschaltfunktion sowohl für eingehende **externe** und **interne** Rufe.
On	*42#	
Off	#42#	
Do not Disturb Int.		Aktiviert, deaktiviert die Stummschaltfunktion für eingehende **interne** Rufe.
On	*421#	
Off	#421#	
Do not Disturb Ext.		Aktiviert, deaktiviert die Stummschaltfunktion für eingehende **externe** Rufe.
On	*422#	
Off	#422#	

Anklopffunktionen

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

Lokale Einstellungen löschen

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

Pickup

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

Aktivität	Code	Beschreibung
Pickup Group	*0#	*Pickup Group* holt ungezielt einen Ruf einer Pickup-Gruppe heran.
Directed	*0*$#	Mit *Directed* 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 die Amtsleitung oder die Warteschleife sein.

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

Aktivität	Code	Beschreibung

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

Join Group

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

Rückruf

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

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

4.1.5.4 Configuration/DECT/Radio

In diesem Menü kann das DECT-System als DECT-Radio konfiguriert werden, Vorrausgesetzt ein DECT-Master wurde bereits konfiguriert.

Disable	Ein markiertes Kontrollkästchen, deaktiviert das DECT-Radio (Funkzelle).
Master	Die IP-Adresse des DECT-Masters. Wurde das Gerät selbst als DECT-Master definiert, dann muss hier keine IP-Adresse eingetragen werden. Die lokale IP-Adresse `127.0.0.1` wird automatisch eingetragen.
Alt-Master	Die IP-Adresse des Standby-Masters.

Radio-ID	Im **Singlecell**- Betrieb muss die Radio-ID 0 angegeben werden. Im **Multicell**- Betrieb muss jedes Radio eine eindeutige ID besitzen. Die ID muss im Bereich 0 - Sys-Mask (mit Sys-Mask Angabe) oder 0 - 254 (ohne Sys-Mask Angabe) liegen.
Sync-Source	Die Radio-Id, mit welcher sich das Radio synchronisieren soll.
Alt-Sync-Source	Die Radio-Id, mit welcher sich das Radio synchronisieren soll, sollte der Sync-Master nicht erreichbar sein. Dabei ist zu beachten, dass keine Schleifen angelegt werden dürfen. D.h. existiert ein Sync-Master mit der Radio-Id 1 und ein Alt-Sync-Master mit der Radio-Id 3, dann darf sich der Alt-Sync-Master auf gar keinen Fall mit einem beliebigen Radio synchronisieren, da sich das Radio beim Ausfall des Sync-Masters mit dem Alt-Sync-Master synchronisiert.

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.

Das Anmelden (Subscription) von DECT-Handsets ist auch ohne PBX-Komponente direkt an der IP1200 möglich. Jedes Handset wird über seine eindeutige IPEI-Nummer identifieziert. Eine Subscription am Telefon bewirkt, dass wie im LDAP, die Subscription im Telefon gespeichert wird. Es gibt zwei Möglichkeiten, ein Telefon anzumelden:

1. Eintrag der IPEI-Nummer im entsprechenden User-Objekt, anschließend kann die Subscription am Telefon durchgegeführt werden (Known subscription).
2. Die Subscription am Telefon wird zuerst durchgeführt (Unknown subscription), anschließend wird die Rufnummer des gewünschten freien User-Objektes gewählt. Die IPEI-Nummer wird in dieses User-Objekt automatisch eingetragen.

4.2.1 Administration/DECT

DECT-administrative Einstellungen der IP1200 werden hier vorgenommen.

4.2.1.1 Administration/DECT/Statistics

Hier befinden sich detaillierte Informationen über den DECT-Master und den DECT-Radios angezeigt. Der Abschnitt Master wird jedoch ausgeblendet, sollte das Untermenü Statistics von einem konfigurierten DECT-Radio aus betrachtet werden.

Abschnitt **Master:**

Calls in	Alle eingehenden Anrufe auf dem DECT-Master.
Calls in Delivered	Alle eingehenden Anrufe, die auf dem DECT-Master durchgestellt wurden.
Calls Out	Alle ausgehenden Anrufe auf dem DECT-Master.
Handover	Alle auf dem DECT-Master stattgefundenen Handover. Befindet sich ein Mobiltelefon im Sendebereich des DECT-Masters und wechselt in einen anderen Sendebereich (DECT-Radio), dann muss ein Handover zum nächsten Sendebereich stattfinden, sodass dem DECT-Master übermittelt wird, wie die Sprachdaten geroutet werden sollen.
Handover Failed	Alle fehlgeschlagenen Handover die im DECT-Master-Bereich stattfanden.
Abnormal Call Release	Alle sonstigen fehlgeschlagenen Anrufe. Ein solcher **Abnormal Call Release** kann z.B. ein leer gegangener Mobiltelefonakku sein.

Abschnitt **Radio:**

Calls in	Alle eingehenden Anrufe auf dem DECT-Radio.
Calls Out	Alle ausgehenden Anrufe auf dem DECT-Radio.
Handover	Alle stattgefundenen Handover, die auf den DECT-Radios veranlasst wurden. Befindet sich eine Mobiltelefon im Sendebereich eines DECT-Radios und verlässt diesen, dann muss ein Handover zum nächsten Sendebereich (Radio oder Master) stattfinden, so dass der DECT-Master weiß, wohin die Sprachdaten übermittelt werden sollen.
Handover Failed	Alle fehlgeschlagenen Handover, die auf den DECT-Radios veranlasst wurden.

Zuletzt wird noch die insgesamte Betriebsdauer des DECT-Subsystems angezeigt.

4.2.1.2 Administration/DECT/Users

Alle an der IP1200 konfigurierten Benutzer werden hier aufgelistet. Wurde eine LDAP-Replikation mit der innovaphone-PBX hergestellt, werden auch die in der PBX konfigurierten DECT-Benutzer hier angezeigt. Es besteht die Möglichkeit, einzelne, mehrere oder auch alle Benutzer anzeigen zu lassen. Um sich einen bestimmten Benutzer anzeigen zu lassen, muss dessen Name (**Long Name**) in das Eingabefeld eingetragen werden und anschließend auf *show* geklickt werden. Man kann auch mehrere Benutzer anzeigen lassen, in dem man nur den Anfangsbuchstaben eines Benutzers in das Eingabefeld einträgt und anschließend auf *show* klickt. Ein Klick auf *show* ohne Angabe einer Zeichenkette bzw. eines Buchstabens zeigt alle angelegten Benutzer an.

Die Anzeige der Benutzerdaten ist in folgende Spalten gegliedert:

Long Name	Angabe des in der PBX registrierten „Long Name".
No	Angabe der in der PBX registrierten Rufnummer.
Name	Angabe des in der PBX registrierten „Name".
Display	Angabe der zum Display übermittelten Anzeige.
IPEI	Angabe der 12-stelligen IPEI-Nummer.
AC	Es besteht die Möglichkeit, bei der Einrichtung eines Benutzers in der innovaphone-PBX einen Zugriffscode (**AC**) zu vergeben. Wurde dies getan, so wird dieser hier angezeigt. Siehe auch Kapitel: „*Configuration/DECT/System*".
Registration	Angabe des aktuellen Registrierungszustand. Mögliche Zustände: *subscribing*, *pending* oder *IP-Adresse* des VoIP-Gerätes, an welchem sich der Benutzer angemeldet hat.

Um einen neuen Benutzer hinzuzufügen, muss der Link *new* neben der tabellarischen Anzeige der bereits vorhandenen Benutzer angeklickt werden.

4.2.1.3 Administration/DECT/Unknown

Hier werden alle Subscriptions (Unknown subscription) angezeigt, die noch keinem (PBX-) Benutzer zugeordnet sind.

- Ein Klick auf **Delete** löscht die unbekannte Subscription aus der Liste.
- Unbekannte subscriptions können die Rufnummer eines freien Benutzers wählen, um sich an diesem Objekt zu registrieren.

4.2.1.4 Administration/DECT/Radios

Hier werden alle an- bzw. abgemeldeten DECT-Base-Stationen zeilenweise an-

gezeigt. Eine Zeile enthält folgende Informationen: *Name ID Address Sync Lost Busy Product Version Uptime*:

Name	<*Gerätetyp*> + <*NetBIOS Name*> z.B: *IP1200-a1-a2-a3* (*die letzten drei Stellen der MAC-Adresse des* DECT-Gerät).
ID	Die vergebene Radio-ID des DECT-Radio.
Address	Die IP-Adresse des DECT-Radio. Sollte ein konfiguriertes DECT-Radio nicht erreichbar sein, so wird anstelle der IP-Adresse der Link *del* angezeigt. Damit kann das DECT-Radio aus der Liste gelöscht werden.
Sync	Ist das betreffende DECT-Gerät der DECT-Master, so wird die Zeichenkette Master ausgegeben. Ist das betreffende DECT-Gerät ein DECT-Radio, so wird die Zahl der Radio-ID, von welchem sich das DECT-Radio synchronisiert hat, ausgegeben. Diese wird in der Farbe Grün ausgegeben, sollte das DECT-Gerät sich bereits erfolgreich synchronisiert haben. Bei Misserfolg wird diese Zahl in Rot ausgegeben.
Lost	Der erste Wert in der Spalte **Lost** bezieht sich auf den **Sync-Master** und gibt an, wie oft die Synchronisierung zum DECT-Master verloren ging. Der zweite Wert bezieht sich auf den **Alt-Sync-Master**, welcher angibt, wie oft die Synchronistation zum alternativen DECT-Master verloren und damit ganz verloren ging.
LDAP	Zeigt den Status des jeweiligen DECT-Gerätes an. Mögliche Zustände: *up*, *Down*, *Starting* und *Stopped*, *server* und *Replicator*.
Busy	Zeigt an, wie oft alle Kanäle eines DECT-Radios belegt waren. Damit ist ersichtlich, ob noch weitere DECT-Base-Stations benötigt werden.
Product	Zeigt den Namen des jeweiligen DECT-Gerätes an, sofern dieser im Kapitel: „*Configuration/General/Admin*“ im Eingabefeld **Device Name** konfiguriert wurde. Wurde kein Produkt Name (**Device Name**) konfiguriert, wird der Standard-Name des Gerätes verwendet (z.B.: innovaphone-IP1200)
Version	Zeigt die aktuelle Firmware-Version des jeweiligen DECT-Gerätes an.
Uptime	Zeigt die Dauer des Betriebs in Form von *Tage Stunden Minuten Sekunden* des jeweiligen DECT-Gerätes an.

4.2.1.5 Administration/DECT/Mastercalls

Die aktuell aktiven Rufe, die über den DECT-Master geführt werden, können beobachtet werden. Dabei ist zu bemerken, dass interne Gespräche zwischen innovaphone-PBX-Teilnehmern nicht angezeigt werden, sollte die optionale innovaphone-PBX-Komponente installiert sein.

A	*<Sender>*	Anrufender Teilnehmer
B	*<Empfänger>*	Angerufener Teilnehmer
State	`Calling`	Rufaufbau
	`Alerting`	Ruf wird signalisiert
	`Connected`	Ruf verbunden
	`Incomplete`	Ruf unvollständig
	`Disconnecting`	Ruf wird abgebaut
Radio	`IP1200-xx-xx-xx`	Angabe des verwendeten DECT-System.
Local Media	`xxx.xxx.xxx.xxx:xxxx`	Angabe der IP-Adresse und Port des verwendeten DECT-System.
Remote Media	`xxx.xxx.xxx.xxx:xxxx`	Angabe der IP-Adresse und Port des VoIP-Gerät, auf dem die innovaphone-PBX-Komponente aktiviert ist.

4.2.1.6 Administration/DECT/Radiocalls

Die aktuell aktiven Rufe, die über die DECT-Radios geführt werden, können beobachtet werden.

Werden keine Werte bzw. Angaben übermittelt, so wird der entsprechende Wert gestrichen angezeigt (-).

DECT	*<Sender>*	Anrufender Teilnehmer
Master	*<Empfänger>*	Angerufener Teilnehmer
Handover	`Calling`	Rufaufbau
	`Alerting`	Ruf wird signalisiert
	`Connected`	Ruf verbunden
	`Incomplete`	Ruf unvollständig
	`Disconnecting`	Ruf wird abgebaut

4.2.1.7 Administration/DECT/Handover

Die aktuell aktiven Rufe, die über mehrere DECT-Base-Stations gehen, können beobachtet werden.

Werden keine Werte bzw. Angaben übermittelt, so wird der entsprechende Wert gestrichen angezeigt (-).

4.2.1.8 Administration/DECT/Radio

In diesem Menü werden alle am DECT-Master angemeldeten DECT-Radios zeilenweise angezeigt.

Jede Zeile stellt ein DECT-Radio mit Angabe der RPN (**R**adion-**P**art-**N**umber) und der RSSI (**R**adio-**S**ignal-**S**trength-**I**ndication) dar:

RPN (Radio Part Number)	Die Radio Part Number ist die Radio-ID des DECT-Radios.
RSSI (Radio Signal Strenght Indication)	Die Radio Signal Strength Indication ist die Feldstärke des einzelnen DECT-Radios.

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 Aufspielens 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/inno-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/Radio

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

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

Dabei ist zu beachten, dass alle aktiven Rufe beendet werden, sobald die Radio-Firmware auf das Gerät geladen wird.

Während des Ladens der neuen Radio-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.

Die neue Radio-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 Gerätes sind im Kapitel: „Administration/Reset" enthalten.

4.2.3.4 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:

TCP	Alle TCP-Verbindungen.
PPP	Alle PPP-Verbindungen.
Relay-Calls	Alle Rufe, die über das Relay gehen - nur bei Geräten mit S_0 oder S_2m Schnittstelle sichtbar.
Relay-Routing	Alle Rufe, die über das Relay geroutet werden müssen - nur bei Geräten mit S_0 und S_2m Schnittstelle sichtbar.
DECT-Master	Alle DECT-Master-Verbindungen - Nur bei IP-DECT-Systemen sichtbar.

DECT-Radio	Alle DECT-Radio-Verbindungen - Nur bei IP-DECT-Systemen sichtbar.
H.323-Registrations	Alle H.323-Registrierungen.
SIP-Registrations	Alle SIP-Registrierungen.
Config-Changes	Alle Konfigurations Änderungen.
TEL1-n	Alle TEL1-n-Verbindungen - Nur bei Geräten mit TEL-Schnittstelle sichtbar.
PPP	Alle PPP-Verbindungen - Nur bei Geräten mit PPP-Schnittstelle sichtbar.
BRI1-n	Alle BRI1-nVerbindungen - Nur bei Geräten mit BRI-Schnittstelle sichtbar.
PRI1-n	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:**

System	Informationen zum DECT-System.

Master	Informationen zum DECT-Master.
Radio	Informationen zum DECT-Radio.

Abschnitt **Interfaces**:

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

Abschnitt **VOIP**::

H.323/ RAS	Informationen zu H.323-RAS.
H.323/ H.225	Informationen zu H.323/H.225.
H.323/ H.245	Informationen zu H.323/H.245.
H.323/ T.38	Informationen zu H.323/T.38
H.323/ T.30	Informationen zu H.323/T.30
SIP/Messages	Informationen zu SIP/Messages.
SIP/ Events	Informationen zu SIP/Events.
SIP/T.38	Informationen zu SIP/T.38.
DSP	Informationen zu DSP.
DSP control messages	Informationen zu DSP control messages.
DSP data messages	Informationen zu DSP data messages.

Abschnitt **IP**:

PPP	Informationen zum PPP-Protokoll.
PPTP	Informationen zum PPTP-Protokoll.
PPoE0-1	Informationen zum PPoE0/1-Protokoll.
DHCP0-1	Informationen zum DHCP0/1-Server.
HTTPCLIENT	Informationen zum HTTP-Client.
HTTPCLIENT verbose	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 Textform 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: „*Anzschlüsse und Bedienelemente*" in der Tabelle 1 „*Anzeigen und Anschlüsse der IP6000*" („Reset") enthalten.
Weitere, detailiertere Information können dem innovaphone knowledgebase Artikel „*How to Reset IPxxx , factory default, led behaviour, tftp mode,clear config,gwload*" (`http://www.innovaphone.com/inno-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

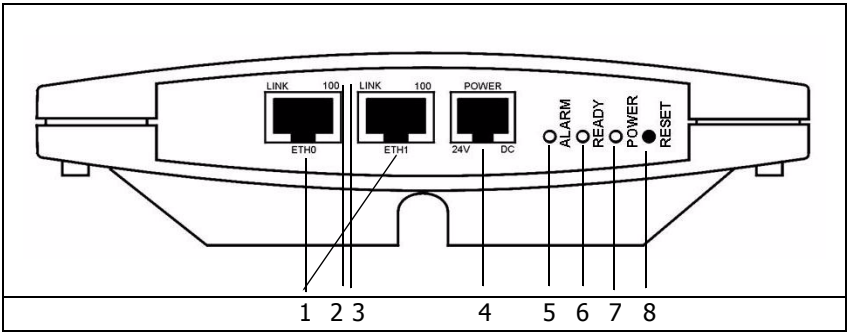


Abbildung 1 - Anzeigen und Anschlüsse der IP1200

Pos.	Symbol	Beschreibung und Funktion
1	**ETH0-1**	RJ45-Buchse zum Anschluss eines 100 MBit/s Ethernet (10/100Base-T auto sense).
2	**100**	LED zur Anzeige, dass das 100 MBit/s Netz für die **ETH0/1** Schnittstelle aktiv ist.
3	**LINK**	LED zur Anzeige, dass Daten auf der **ETH0/1** Schnittstelle gesendet oder empfangen werden.
4	**POWER**	Buchse zum Anschluss eines externen Steckernetzteils zur Stromversorgung.
5	**ALARM LED**	LED zur Anzeige, dass die IP1200 gerade einen Neustart tätigt oder aber auch ob ein Störungsfehler vorliegt.
6	**READY LED**	LED zur Anzeige, dass die IP1200 betriebsbereit ist.

7	**POWER LED**	LED zur Anzeige, dass die IP1200 über eine Stromversorgung verfügt.
8	**RESET**	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. **Kurzer Reset:** Ein kurzer Reset startet das Gerät neu. Alle aktiven Rufe gehen verloren. **Mittlerer Reset (TFTP-Reset):** 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. **Langer Reset (Factory-Reset):** 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. **Power-Cycle:** Bedeutet das Gerät kurz von der Stromzufuhr zu nehmen. Funktioniert sowohl technisch als auch optisch wie der kurze Reset.

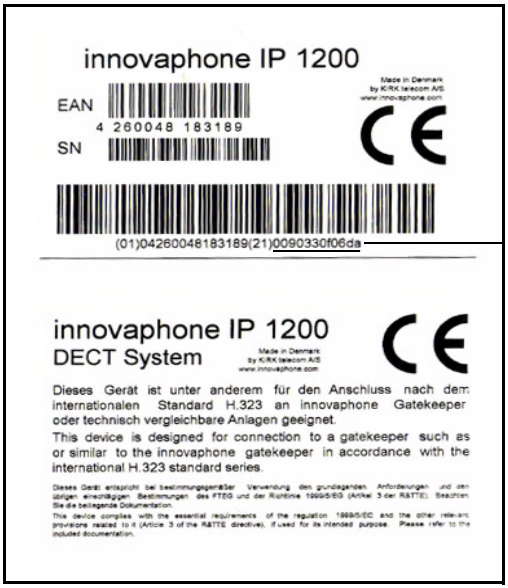
Tabelle 1 Anzeigen und Anschlüsse der IP1200

Hinweis

Informationen bezüglich der Software-Reset Funktion über den Webbrowser sind im Kapitel: „Administration/Reset" enthalten.
Weitere, detailiertere Information können dem innovaphone knowledgebase Artikel „*How to Reset IPxxx , factory default, led behaviour, tftp mode,clear config,gwload*" (`http://www.innovaphone.com/inno-kb/`) entnommen werden.

Das Seriennummernetikett

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



(**MAC-Adresse**)

Abbildung 2 - Das Seriennummernetikett der IP1200

Die MAC-Adresse ist gleichzeitig die Seriennummer Ihrer IP1200.

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 (0F06DA oder 0F-06-DA) die fortlaufende Seriennummer der IP1200 darstellen.

Anhang B: Problembehebung

Bestimmte Probleme treten unserer Erfahrung nach häufiger auf. Die nachstehende Tabelle 2 listet diese Probleme und gibt Hinweise zu deren Behebung.

Typische Probleme

Symptom	Erläuterung	Maßnahme
Das VoIP-Gerät reagiert nicht. **Ready**, **Link** und **100M**. LED leuchten ununterbrochen.	Das VoIP-Gerät wartet auf einen Firmware-Download.	• Führen Sie einen Kurzen Reset durch Betätigen der **Reset**-Taste durch.
Das VoIP-Gerät reagiert nicht. **Ready** LED leuchtet, **Link** LED blinkt unregelmäßig.	Die Ethernet-Verbindung funktioniert nicht.	• Überprüfen Sie die Ethernet-Verkabelung.
Das VoIP-Gerät reagiert nicht. **Ready** und **Link** LEDs leuchten, **100M**. LED blinkt bei Zugriffsversuch.	Das VoIP-Gerät hat eine falsche IP-Adresse konfiguriert.	• Stellen Sie die IP-Parameter korrekt ein.
Im Auslieferungszustand weist das VoIP-Gerät dem PC keine IP-Adresse zu.	Nach dem Einschalten ist der DHCP-Client aktiv.	• Betätigen Sie kurz die Reset-Taste. • Lassen Sie dem PC erneut eine IP-Adresse zuweisen.
Es können Rufe zu einem entfernten VoIP-Gerät aufgebaut werden, es ist jedoch keine Verständigung möglich.	Die erforderliche Bandbreite für die Übertragung der Gesprächsdaten ist nicht verfügbar.	• Konfigurieren Sie in der Konfiguration für das entfernte VoIP-Gerät eine effizientere Sprachkodierung.

Es können Rufe zu einem entfernten VoIP-Gerät aufgebaut werden, es kommt jedoch keine Sprachverbindung zustanden.	Der Medienkanal kann nicht aufgebaut werden, da die beiden VoIP-Geräte über keinen gemeinsamen Sprachkodierer verfügen.	• Stellen Sie sicher, dass das Kontrollkästchen *„exclusive„* deaktiviert ist.
Es können Rufe zu einem entfernten VoIP-Gerät aufgebaut werden, es kommt jedoch keine Sprachverbindung zustande.	Der Medienkanal kann nicht aufgebaut werden, da die beiden VoIP-Geräte über keinen gemeinsamen Sprachkodierer verfügen.	Nur der Medienkanal wird direkt zwischen den beiden VoIP-Geräten aufgebaut, alle Signalisierverbindungen laufen über den Gatekeeper. • Stellen Sie sicher, dass beide VoIP-Geräte über eine korrekte IP-Routingkonfiguration verfügen, insbesondere Subnetzmaske und Standardgateway.
Rufe zu einem entfernten Telefoniegateway werden von diesem immer abgelehnt.	Das Gerät unterstützt keine Einzelziffernachwahl .	• Fügen Sie im Rufnummernpräfix der zu diesem Gateway führenden Route eine Raute (#) ein, um Blockwahl zu erzwingen.
Das VoIP-Gerät verliert seine Konfiguration nach dem Trennen von der Stromversorgung.	Die Konfiguration wurde nicht in den nichtflüchtigen Speicher gesichert.	• Sichern Sie die Konfiguration nach erfolgreichen Änderungen in den nichtflüchtigen Speicher.
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.	• Schalten Sie in der Firewall den Zugriff des VoIP-Gerätes für den Dienst tcp/80 (http) frei.

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.	• Aktivieren Sie in Ihrer Firewall-Software das „*H.323 Firewalling*“ und ggf. auch „*H.323 NAT*“. Konsultieren Sie zu diesem Zweck die Dokumentation Ihrer Firewall. • Lesen Sie im Kapitel „*NAT und Firewalls*“ nach.

Tabelle 2 Fehlerbehebung

Port-Einstellungen bez. NAT und Firewalls

Ist ein Netzwerk durch eine Firewall zum Internet hin geschützt und soll eine Verbindungen 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 symetrisch 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 (**T**ype**-o**f**-S**ervice) priorisieren, kann diese Funktion verwendet werden. Das VoIP-Gerät setzt in allen IP-Paketen die es sendet das ToS**-**Priority-Feld auf den Wert `0x10`. 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: 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, Datasheets 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 D: 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 wiederrum 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" frägt regelmäßig eine bestimmte Webadresse nach geänderten Konfigurations Informationen ab. Wurden bestimmte Vorraussetzungen erfüllt, so wird UP1 das angeforderten Update durchzuführen.

System Vorraussetzungen

- 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 mehere 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 vergleichen. 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 kommagetrennte 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** Paramter gesetzt sein, werden keine weiteren Befehle innerhalb der angegebene 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 Prozzesse 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 auserhalb 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 herunterladen und auf das Gerät aufspielen. 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 **<build-serial>** mit der UPDATE/PROT Variable vergleichen. 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 **<build-serial>** mit der Built-Number der aktuellen Firmware verglichen. Nach einem erfolgreichen Herunterladen der Firmware wird die Variable UPDATE/PROT mit dem Inhalt von **<build-serial>** überschrieben. Man beachte, dass der Parameter **<build-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 /pro-
tect
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-

dard-Funktionen für das Gerät programmiert.

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

Anhang E: 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 Klammern):

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

Std ist der Bezeichner der Zeitzone (z.B. CET für **C**entral-**E**uropean-**T**ime 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 **C**entral-**E**uropean-**S**ummer-**T**ime oder MES für **M**iddle-**E**uropean-**S**ummer-**T**ime).

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

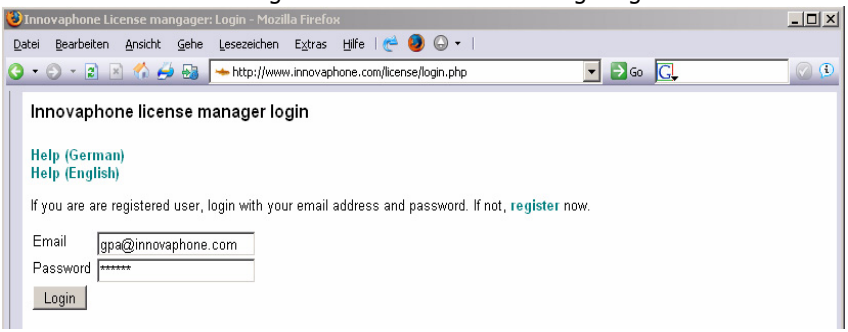
Weitere Informationen zum POSIX-Standard können unter der Webadresse http://standards.ieee.org/catalog/olis/posix.html abgerufen werden.

Anhang F: 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.

Login

Anschließend wird der folgende Anmeldebildschirm angezeigt.



Wurden bisher noch keine Lizenzen bei innovaphone herunter geladen, sollten zuerst einmal die Hilfe-Seiten durchsucht werden.

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

Download

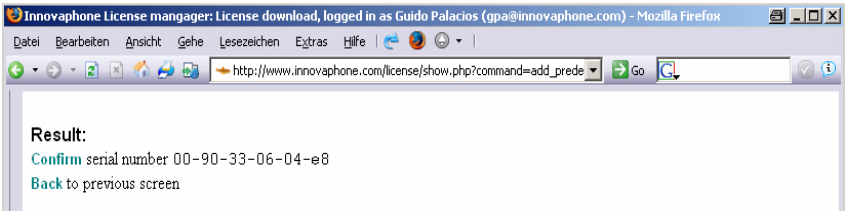
Im oberen Teil des Bildschirms wird angezeigt, ob man sich ordnungsgemäß eingeloggt hat. Hier erscheint "*Welcome you are logged in as Name { E-mail Addresse }*".

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

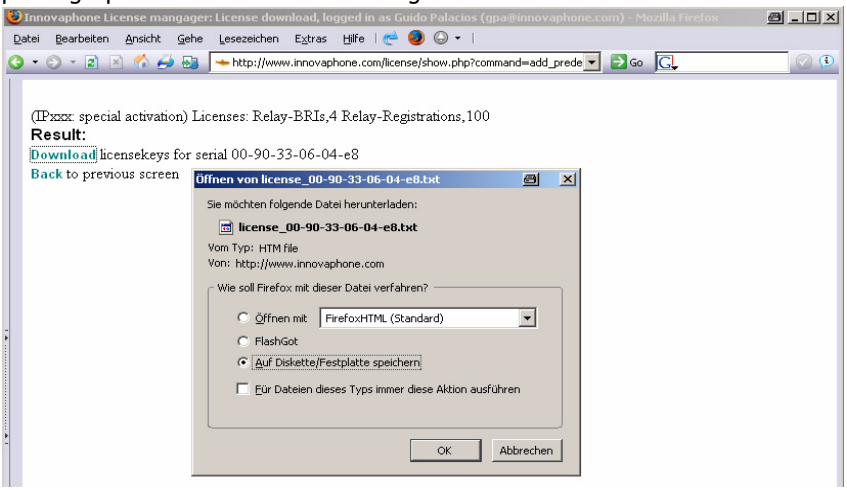
Als nächstes muss das Herunterladen des Licensekeys bestätigt werden.



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 G: DECT-Ausleuchtung

Einer der wichtigsten Vorraussetzungen für eine professionelle DECT-Aufstellung ist eine DECT-Radio-Vermessung vor Ort. Das ist letztendlich der einzige Weg, um festzustellen, wie viele Lokationen mit DECT-Basis-Stationen und Repeatern ausgestattet werden müssen. Die innovaphone-AG bietet hierfür ein mobiles DECT-Aufstellungs-Werkzeug, um diese Vermessung vorzunehmen, ohne zuvor eine DECT-Umgebung installiert zu haben. Dieses Werkzeug kann ausgeliehen oder gemietet werden, was ein sehr kostensparender Weg ist, eine professionelle DECT-Umgebung in Betrieb zu nehmen.

Weiter Informationen zur DECT-Ausleuchtung können folgenden Artikeln der innovaphone-Knowledgebase entnommen werden:

Rules for succesful IP1200 deployment - `http://www.innovaphone.com/inno-kb/article.aspx?id=10531`

Debugging tools for DECT deployment - `http://www.innovaphone.com/inno-kb/article.aspx?id=10536`

Understanding DECT handover with ip1200 - `http://www.innovaphone.com/inno-kb/article.aspx?id=10533`

In der innovaphone-Knowledgebase sind noch weitere DECT-Themen enthalten, welche mit dem Suchbegriff *DECT* abgerufen 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 µ-Law-Verfahren. Dieses Verfahren zeichnet sich durch eine Dynamikkennlinie aus, die im Niedrigpegelbereich 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-Schittstelle 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 × 64 kbit/s + 16 kbit/s = 144 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

(**C**all-**R**eference), 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 Luftschnittstelle 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 angehangen 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**e**lephone-**Num**ber-**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**lectronical-**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**dentity), 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 Fernsprechnetz hervorgegangen. Die digitale Übertragung ermöglicht eine gleichartige Behandlung von Text-, Grafik- und Sprachdaten. Ebenso wie im analogen Fernsprechnetz 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**ubsciber-**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-Namentabellen 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 Abtasttheorem nach Nyquist, in ein Digitalsignal umzuwandeln. Dazu wird das Analogsignal 8.000-mal pro Sekunde abgetastet und in eine 8-Bit-Wertigkeit gewandelt, sodass alle 125 µs 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 µ-Law-Verfahren und das A-Law-Verfahren

PING

Mit dem Programm ping (**P**acket-**I**nter**n**et-**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-Uni**X**) ist ein gemeinsam von der IEEE (**I**nstitute- of **E**lectrical- and **E**lectronical-**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 leitungsvermittelte 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-**o**ver-**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**rivate-**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**rimary-**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-**o**f-**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-**Sig**nalling-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 erhöt den Abdekkungsbereich 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**equest-**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-Steckserysteme 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 transpor-

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**eal-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 Gespäch 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 Gespächspartner 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 (**Tel**etype-**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**roticol) ist das **U**ser-**D**atagram-**P**rotocol ein minimales, verbindungsloses Netzprotokoll, 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 µ-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**rivate-**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 Fernsprechnetz (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

I

J

K

L

O

P

Q

R

S

T

U

V

W

Z

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