

Installation, Verwaltung und Wartung

DECToverSIP

Release 1.8

Dokument-ID: depl-0900

Version: 1.8

Aastra Zeughofstr. 1
10997 Berlin, Deutschland

©Februar –2010 - Alle Rechte
vorbehalten

Kein Teil dieses Dokuments darf auf irgend eine Art und Weise elektronisch oder mechanisch und zu keinem wie auch immer gearteten Zweck ohne ausdrückliche schriftliche Genehmigung durch Aastra reproduziert oder gesendet werden. Dies schliesst unter anderem das Fotokopieren und Aufzeichnen sowie alle Informationsspeicherungs- und Abrufsysteme ein.

Inhaltsverzeichnis

1	ÜBERBLICK	4
1.1	ZWECK	4
1.2	KONFORMITÄTSERKLÄRUNG	4
1.3	ABKÜRZUNGEN UND DEFINITIONEN	4
1.3.1	ABKÜRZUNGEN	4
1.3.2	DEFINITIONEN	4
1.4	REFERENZEN	7
2	EINLEITUNG	8
2.1	DIE DECTOVERIP USING SIP LÖSUNG	8
2.2	ACCESS POINTS (BASISSTATIONEN, RFPs)	9
2.3	OPENMOBILITY MANAGER	12
2.4	IP-SIGNALISIERUNG UND MEDIA-STREAM	12
2.5	RFP-SYNCHRONISATION	15
2.6	KANALKAPAZITÄT EINES RFP	17
2.7	ENDGERÄTE (PPS)	17
2.8	SYSTEMKAPAZITÄTEN	18
3	INSTALLATION UND KONFIGURATION	19
3.1	START VON OPENMOBILITY	19
3.1.1	START DER RFPs'	19
3.1.1.1	Booten, Überblick	19
3.1.2	START DES OPENMOBILITY MANAGER	20
3.1.3	BOOTER	20
3.1.3.1	DHCP-Client	20
3.1.3.1.1	DHCP-Anforderung	20
3.1.3.1.2	DHCP-Angebot	22
3.1.3.1.3	Wiederholungsversuche	22
3.1.3.2	TFTP-Client	22
3.1.4	ANWENDUNG	22
3.1.4.1	Booter-Update	24
3.1.4.2	Auswahl des richtigen DHCP-Servers	24
3.1.5	LED-STATUS DES RFP	25
3.1.6	ZUSTANDSDIAGRAMM DER EINZELNEN STARTPHASEN	27
3.2	STATISCHE LOKALE KONFIGURATION EINES RFP	28
3.3	OPENMOBILITY MANAGER KONFIGURIEREN	33
3.3.1	ANMELDEPROZEDUR FÜR DEN DIENST	33
3.3.2	SYSTEM	35
3.3.2.1	Systemeinstellungen	35
3.3.2.1.1	Neustart des OMM	37
3.3.2.1.2	Verschlüsselung	38
3.3.2.1.3	Regulierungsdomäne	38
3.3.2.2	SIP	38
3.3.2.3	Benutzerverwaltung	41
3.3.2.4	Zeitzone	42
3.3.2.5	Datenbank-Management	43
3.3.2.5.1	Manueller Datenbankimport	45
3.3.2.5.2	Manueller Datenbankexport	45
3.3.2.5.3	Automatischer Datenbankimport	46
3.3.2.5.4	Automatischer Datenbankexport	48
3.3.3	KONFIGURIEREN DER BASISSTATION	48
3.3.3.1	Erzeugung und Änderung von RFPs	49
3.3.3.1.1	Schaltfläche "Neu", "Ändern" und "Löschen"	49
3.3.3.1.2	Import durch Konfigurationsdateien	50
3.3.3.1.3	Erfassung von RFPs	51
3.3.3.2	RFP-Betriebszustände	52
3.3.3.3	Hardwaretyp des RFP	52
3.3.3.4	OMM-/RFP-Software-Versionsprüfung	53
3.3.4	ENDGERÄTE KONFIGURIEREN	53
3.3.4.1	Erzeugung und Änderung von PPs	54
3.3.4.1.1	Schaltfläche "Neu", "Ändern" und "Löschen"	54
3.3.4.1.2	Import durch Konfigurationsdateien	55
3.3.4.2	Anmeldung	57
3.3.4.2.1	Anmeldung mit konfigurierter IPEI	58
3.3.4.2.2	Wildcard-Anmeldung	58

3.3.4.3	Suche innerhalb der PP-Liste	58
3.3.5	WLAN-KONFIGURATION (NUR RFP L42-WLAN)	59
3.3.5.1	Optimierung des WLAN	62
3.3.5.2	Sicherstellung des WLAN mit Radius	62
3.3.5.3	Anforderungen für das WLAN	66
3.3.6	SYSTEMFUNKTIONEN	66
3.3.6.1	Zentrale Konfiguration des LDAP-Zugangs	66
3.3.6.2	Stellenbehandlung	68
3.3.6.3	Service-Codes	68
4	SICHERHEIT	70
4.1	DAS SICHERHEITSKONZEPT	70
4.2	KONTOTYPEN	70
4.3	ÄNDERUNG VON KONTODATEN	71
4.4	POTENZIELLE FALLGRUBEN	72
5	OMM-RESILIENCY	73
5.1	WIE OMM RESILIENCY (FEHLERTOLERANZ) ARBEITET	73
5.2	EINLEITUNG	73
5.3	KONFIGURIERUNG DER OMM-FEHLERTOLERANZ (RESILIENCY)	73
5.4	ABSTURZSITUATIONEN	74
5.5	ABSTURZ-FEHLSCHLAGSITUATIONEN	74
5.6	SPEZIFISCHE FEHLERTOLERANTE ZUSTÄNDE	75
5.6.1	WIE EIN FEHLERTOLERANTER OMM AKTIV WIRD	75
5.6.2	BEHANDLUNG, WENN BEIDE OMMS NICHT SYNCHRONISIERT SIND	75
5.6.2.1	Zwei DECT-Funkschnittstellen	76
6	DOWNLOAD NEUER FIRMWARE IN DIE ENDGERÄTE	77
6.1	SO FUNKTIONIERT DER DOWNLOAD NEUER FIRMWARE IN DIE ENDGERÄTE	77
6.2	DOWNLOAD NEUER FIRMWARE KONFIGURIEREN	78
7	WARTUNG	82
7.1	MESSAUSRÜSTUNG FÜR DIE STANDORTAUFNAHME	82
7.2	FIRMWARE-VERSION DES AASTRA DECT 142 / AASTRA 142D HANDSET PRÜFEN	82
7.3	DIAGNOSEFUNKTIONEN	82
7.3.1	STANDORTAUFNAHME-BETRIEBSART DES AASTRA DECT 142 / AASTRA 142D82	
7.3.2	ANRUFTEST-BETRIEBSART DES AASTRA DECT 142 / AASTRA 142D	83
7.3.3	ANNAHMETEST-BETRIEBSART DES AASTRA DECT 142 / AASTRA 142D	83
7.3.4	SYSLOG	84
7.3.5	SSH-BENUTZEROBERFLÄCHE	84
7.3.5.1	Anmelden	85
7.3.5.2	Befehlsübersicht	85
7.3.5.3	RFP-Konsolenbefehle	86
7.3.5.4	OMM-Konsolenbefehle	86
7.3.6	ERFASSUNG VON CORE-DATEIEN	87
7.3.7	DECT-MONITOR	88
8	ANHANG	93
8.1	FERNMELDERECHTLICHE INFORMATIONEN ZU AASTRA DECT 142 US	93
8.2	FERNMELDERECHTLICHE INFORMATIONEN ZU RFP 32 BZW. RFP 34 (NA)	94
8.3	REGELN FÜR DATEIEN VOR DER KONFIGURATION	97
8.3.1	PP KONFIGURATIONSDATEI (OMM-DATENBANK)	98
8.3.1.1	Unterstützte Anweisungen	98
8.3.1.2	Datenbereichsfelder	98
8.3.1.3	Beispiel	98
8.3.2	PP KONFIGURATIONSDATEI/ ZENTRAL (OMM-DATENBANK)	100
8.3.2.1	Unterstützte Anweisungen	100
8.3.2.2	Datenbereichsfelder	100
8.3.2.3	Beispiel	100
8.3.3	RFP-KONFIGURATIONSDATEI/LOKAL (OM CONFIGURATOR)	102
8.3.3.1	Unterstützte Anweisungen	102
8.3.3.2	Datenbereichsfelder	103
8.3.3.3	Beispiel	103
8.4	PROTOKOLLE UND PORTS	106

1 Überblick

1.1 Zweck

Dieses Dokument beschreibt die Installation, Konfiguration und Wartung der Lösung DECToverIP using SIP .

1.2 Konformitätserklärung

Das CE-Zeichen auf dem Produkt bestätigt die Einhaltung der zum Zeitpunkt der entsprechenden Konformitätserklärung geltenden technischen Richtlinien für die Benutzersicherheit und elektromagnetische Kompatibilität gemäss Europäischer Richtlinie 99/5/EC. Die Konformitätserklärung kann auf der Aastra-Homepage eingesehen werden.

1.3 Abkürzungen und Definitionen

1.3.1 Abkürzungen

AC	Authentication Code (Authentifizierungscode)
ADPCM	Adaptive Differential Pulse Code Modulation (adaptive Pulscodemodulation)
DECT	Digital Enhanced Cordless Telecommunication
DHCP	Dynamic Host Configuration Protocol
DSP	Digital Signal Processor (digitaler Signalprozessor)
FCC	Federal Communications Commission (US-Fernmeldebehörde)
GAP	Generic Access Profile
IPEI	International Portable Equipment Identity (DECT-Endgeräteidentifikation)
HTTP	Hyper Text Transfer Protocol
OMM	OpenMobility Manager
PARK	Portable Access Rights Key (Schlüssel der portablen Zugangsrechte)
PP	Portable Part (DECT-Endgerät)
SNMP	Simple Network Management Protocol (Protokoll zur Überwachung und Steuerung von Netzwerkgeräten)
TFTP	Trivial File Transfer Protocol (einfaches Dateiübertragungsprotokoll)
RFP	Radio Fixed Part (Basisstation, Access Point)
RTCP	Real Time Control Protocol (RTP-Steuerprotokoll)
RTP	Real Time Protocol (Internetprotokoll für den Transport von Echtzeitdaten)

1.3.2 Definitionen

Aastra DECT 142 Handset / Aastra Phone 142
Aastra DECT 142 Handset / Aastra Phone 142
 Im Zusammenhang mit der Lösung DECToverIP using SIP sind die Begriffe Aastra DECT 142 Handset, Aastra Phone 142 und Endgerät (PP) gegeneinander austauschbar.

Aufgrund der Unterschiede zwischen den gesetzlichen Bestimmungen in Nordamerika und den anderen Teilen der Welt gibt es zwei PP-Varianten, die unterschiedliche Frequenzbänder und Feldstärken nutzen.

- Aastra DECT 142
für den Einsatz in Nordamerika
- Aastra 142d
für den Einsatz in allen anderen Ländern

Access Point

Access Point

Im Zusammenhang mit der Lösung DECToverIP using SIP sind die Begriffe „Access Point“ und Basisstation (RFP) gegeneinander austauschbar.

Asterisk

Asterisk

Asterisk ist eine vollständige Open-Source-PBX-Software. Sie läuft unter Linux, BSD und MacOSX und besitzt einen grossen Funktionsumfang. Asterisk unterstützt IP-Sprachübertragungen (Voice over IP) in vielen verschiedenen Protokollen und arbeitet mit fast jeder der Norm entsprechenden Telefonanlage zusammen.

DECT

Digital Enhanced Cordless Telecommunication

- Die Norm (ETS 300 175) spezifiziert im wesentlichen die Funkschnittstelle. Über diese Schnittstelle können sowohl Sprache als auch Daten übertragen werden.
- In Europa sind folgende wichtige technische Daten vorgegeben:
 - Frequenzbereich: ca. 1'880 bis 1'900 MHz (Bandbreite ca. 20 MHz)
 - 10 Trägerfrequenzen (1'728 kHz Abstand) mit je 12 Zeitschlitzten
 - Verdopplung der Anzahl der Zeitschlitzte (auf 24) mit TDMA-Prozess
 - Netto-Datenrate pro Kanal 32 kb/s (für Sprachübertragungen mit ADPCM)
 - Sprachcodierung mit ADPCM-Methode

In Nordamerika sind folgende wichtige technische Daten vorgegeben:

- Frequenzbereich: ca. 1'920 bis 1'930 MHz (Bandbreite ca. 10 MHz)
- 5 Trägerfrequenzen (1'728 kHz Abstand) mit je 12 Zeitschlitzten
- Verdopplung der Anzahl der Zeitschlitzte (auf 24)

mit TDMA-Prozess

- Netto-Datenrate pro Kanal 32 kb/s (für Sprachübertragungen mit ADPCM)
- Sprachcodierung mit ADPCM-Methode

GAP

Generic Access Profile

- GAP ist die Abkürzung für „Generic Access Profile“, das Übertragungsprofil für DECT-Telefone.
- Der GAP-Standard (ETS 300 444) basiert auf der gleichen Technologie wie DECT, beschränkt sich aber auf die wichtigsten Grundmerkmale. Dieser Standard wurde geschaffen, um die Verwendung von Telefonen verschiedener Hersteller an jedem DECT-System zu gestatten. Er stellt daher den kleinsten gemeinsamen Nenner aller herstellerspezifischen Varianten des DECT-Standards dar.
- Eine wichtige Einschränkung des GAP-Standards ist, dass kein externes Handover möglich ist. Aus diesem Grund wird mit Verbindungs-Handover gearbeitet, das von GAP-Endgeräten unterstützt wird.
- GAP-fähige Telefone werden ähnlich wie analoge Endgeräte bedient. So lassen sich zum Beispiel Leistungsmerkmale über “*” und “#” aufrufen.

Handover

Handover

Ein Handover ähnelt dem Roaming, findet aber während eines laufenden Anrufs statt. Das Handover läuft in der Regel „im Hintergrund“ ab, ohne dass der Anruf unterbrochen wird (nahtloses Handover).

IPEI

International Portable Equipment Identity (DECT-Endgeräteidentifikation)

- 13-stelliger Identifikationscode für PPs
- Beispiel: 00019 0592015 3 (Die letzte Stelle ist eine Prüfsumme).
- Der Code wird in Dezimalform angegeben.
- Er ist weltweit eindeutig.

PARK

Portable Access Rights Key (Schlüssel der portablen Zugangsrechte)

Zugriffscode für das Endgerät. Dieser Code legt fest, ob ein PP auf ein bestimmtes DECT-System zugreifen kann. Er wird für die Auswahl eines bestimmten Systems von einem Endgerät aus zum Zeitpunkt der Anmeldung verwendet. Er ist auf der OpenMobility-CD angegeben und für jede SIP-DECT-Installation eindeutig.

Roaming

Roaming

Wenn er bewegt wird, führt das PP ständig Messungen durch, um festzustellen, welches RFP am besten empfangen wird. Das am besten empfangbare RFP wird als aktives RFP festgelegt. Um zu verhindern, dass das PP schnell zwischen zwei RFPs mit ähnlicher Signalstärke hin und her schaltet, gelten bestimmte Schwellenwerte.

1.4 Referenzen

- /1/ RFC 1350, The TFTP Protocol, Ausgabe 2, Juli 1992
- /2/ RFC 1889, RTP: A Transport Protocol for Real-Time Applications, Januar 1996
- /3/ RFC 2030, Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI, Oktober 1996
- /4/ RFC 2131, Dynamic Host Configuration Protocol, März 1997
- /5/ RFC 2327, SDP: Session Description Protocol, April 1998
- /6/ RFC 2474, Definition of the Differentiated Service Field (DS Field) in the IPv4 and IPv6 Headers, Dezember 1998
- /7/ RFC 2617, HTTP Authentication: Basic and Digest Access Authentication, Juni 1999
- /8/ RFC 3164, The BSD Sys Log Protocol, August 2001
- /9/ RFC 2833, RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals, Mai 2000
- /10/ RFC 3261, Session Initiation Protocol (SIP), Juni 2002
- /11/ RFC 3264, An Offer/Answer Model with Session Description Protocol (SDP), Juni 2002
- /12/ RFC 3420, Internet Media Type message/sipfrag, November 2002
- /13/ RFC 3515, The Session Initiation Protocol (SIP) Refer method, April 2003
- /14/ RFC 3665, The Session Initiation Protocol (SIP) Basic Call Flow Examples, Dezember 2003
- /15/ RFC 3842, A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP), August 2004
- /16/ RFC 3891, The Session Initiation Protocol (SIP) "Replaces" Header, September 2004
- /17/ RFC 3892, The Session Initiation Protocol (SIP) Referred-By Mechanism, September 2004

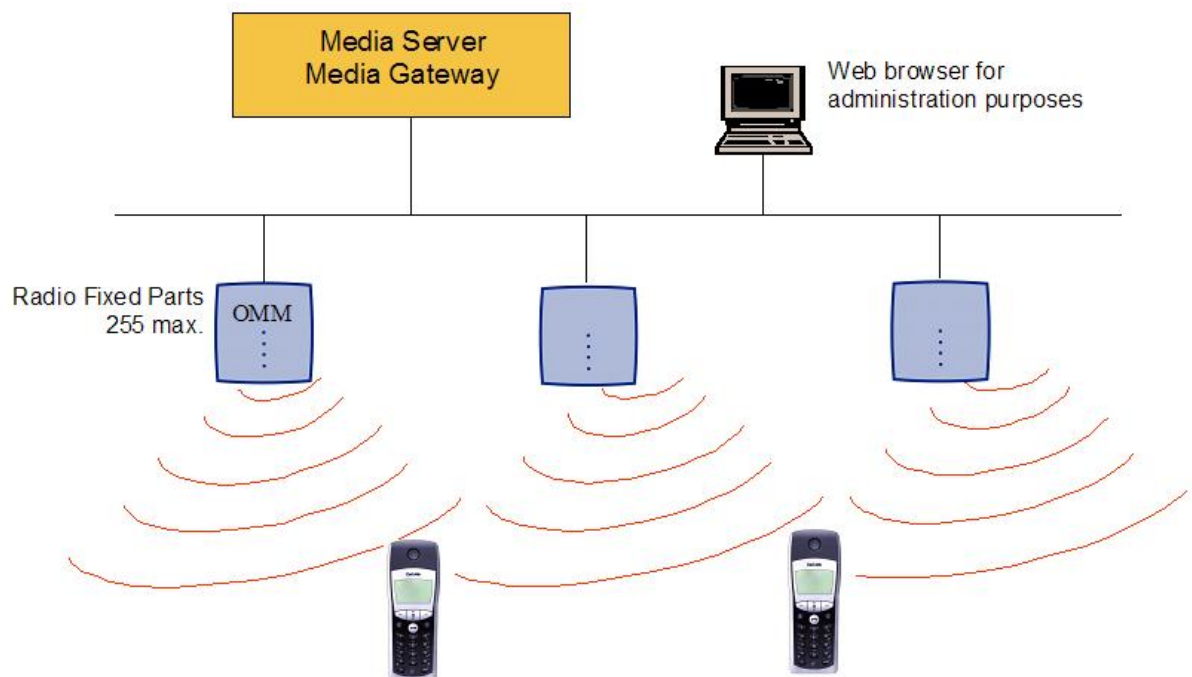
2 Einleitung

2.1 Die DECToverIP using SIP Lösung

Die Lösung DECToverIP using SIP besteht aus folgenden Komponenten:

- Aastra SIP-DECT Access Points (auch Radio Fixed Parts (RFPs, Basisstationen) genannt), die in einem IP-Netzwerk verteilt sind und DECT-Funk- und IP-Schnittstellen bereitstellen.
- SIP Call Manager/IP PBX/Media Server Plattform (z.B. Asterisk)
- Aastra DECT 142 Handsets / Aastra 142d (auch Endgeräte (PP) genannt)
- OpenMobility Manager (OMM): Management-Schnittstelle für die Lösung DECToverIP using SIP, läuft auf einer der Basisstationen.

Die folgende Abbildung ist ein grafischer Überblick über die Architektur einer drahtlosen DECT-IP-Lösung:



IP PBX / Media Server / Media Gateway, OMM und RFPs kommunizieren über die IP-Infrastruktur. Die RFPs und Endgeräte kommunizieren über eine Funkverbindung. Sie benutzen das DECT-GAP-Protokoll oder DECT GAP mit herstellerspezifischen Verbesserungen.

2.2 Access Points (Basisstationen, RFPs)

Aastra DeTeWe bietet 3 Arten von Access Points:

- RFP L32
DECT Access Point als Modell für den Betrieb in Innenräumen
- RFP L34
DECT Access Point als Modell für den Betrieb im Freien
- RFP L42 WLAN
DECT + WLAN Access Point als Modell für den Betrieb in Innenräumen

Im Allgemeinen besitzen RFP32 und RFP 34 die gleichen Hardware- und Software-Funktionen. Denken Sie jedoch an die unterschiedlichen gesetzlichen Bestimmungen in Nordamerika und anderen Teilen der Welt. Diese Unterschiede erzwingen verschiedene Varianten von RFP 32/34 mit unterschiedlichen Frequenzbändern und Feldstärken:

- RFP 32 NA oder RFP 34 NA (NA)
 - Frequenzband 1'920 bis 1'930 MHz
 - 5 Trägerfrequenzen
 - Sendeleistung 20 dBm
- RFP L32 IP oder RFP L34 IP (EMEA)
 - Frequenzband 1'880 bis 1'900 MHz
 - 10 Trägerfrequenzen
 - Sendeleistung 24 dBm

RFP L42 WLAN ist nur für die EMEA-Region erhältlich.

Ein RFP innerhalb jeder SIP-DECT-Installation muss für den Betrieb als OpenMobility Manager (OMM) ausgewiesen werden. Das RFP, die als OMM fungiert, muss ausserdem auch als normales RFP arbeiten, wenn es Bestandteil eines DECT-Clusters ist.

Ausschliesslicher Betrieb als RFP:

In dieser Betriebsart konvertiert das RFP das IP-Protokoll in das DECT-Protokoll und überträgt den Verkehr dann über einen DECT-Zeitschlitz zu und von den Endgeräten. Die Funkstrecke eines RFP kann zwölf Zeitschlitz nutzen. Acht davon können DSP-Ressourcen für Medien-Streams besitzen. Zwei weitere werden für Steuersignale zwischen RFPs und PPs genutzt, die beiden verbleibenden sind für Hand-in-Zwecke reserviert.

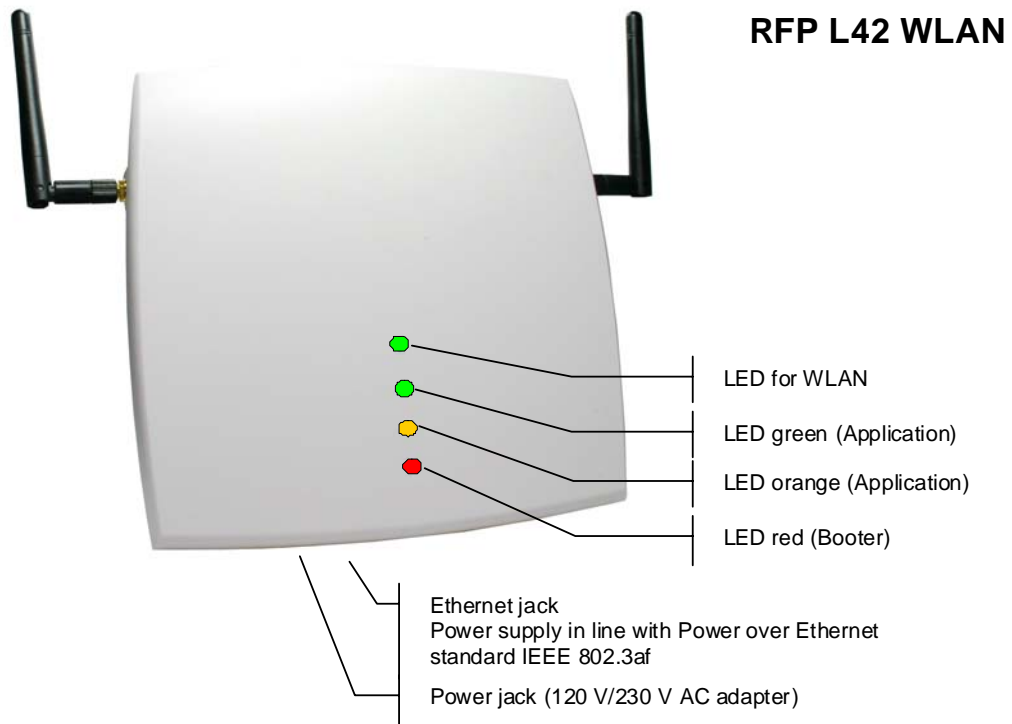
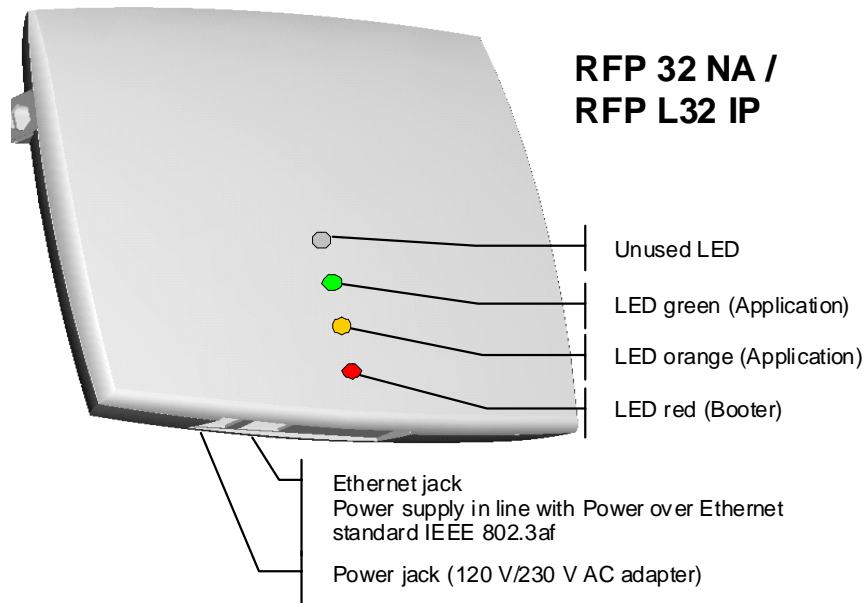
Die RFPs lassen sich zu Gruppen, so genannten Clustern, zusammenfassen. Die RFPs innerhalb eines Clusters sind synchronisiert, so dass beim Übertritt eines Benutzers vom Abdeckungsbereich eines RFP in einen anderen ein nahtloses Handover möglich ist. Für die Synchronisation müssen die einzelnen RFPs nicht direkt mit allen anderen RFPs im System kommunizieren. Jedes RFP muss lediglich mit dem nächsten RFP in der Kette kommunizieren können. Besser ist es jedoch, wenn jedes RFP mehrere andere RFPs sehen kann, da die Synchronisation so auch dann noch gewährleistet ist, wenn eines der RFPs ausfällt.

Die beiden für Steuersignale vorgesehenen Kanäle werden auch für Trägersignale verwendet, die dem Endgerät sagen, wann das Handover erfolgen soll. Wenn sich der Benutzer auf dem Standort bewegt und das Funksignal eines anderen RFP stärker wird als das der aktuellen RFPs, leitet das Endgerät das Handover zu dem RFP mit dem stärkeren Signal ein.

Betrieb als OpenMobility Manager

In dieser Betriebsart fungiert das RFP als normales RFP. Zusätzlich ist es für die SIP-Signale zwischen dem IP-DECT-System und dem Telefonie- oder Media-Server zuständig. Ausserdem übernimmt es die Verwaltung der IP-DECT-Lösung. Sie definieren ein RFP als OMM, indem Sie dem RFP eine IP-Adresse innerhalb des DHCP-Bereichs zuweisen (siehe 3) oder indem Sie die Parameter über den OM Configurator (siehe 3.2) festlegen. Nachdem Sie ein RFP als OMM definiert haben, führt dieses die zusätzlichen integrierten Funktionen aus (z.B. den für die Management-Schnittstelle zuständigen Web-Dienst). Alle RFPs laden die gleiche Firmware von einem TFTP-Server herunter. Die OMM-Dienste sind jedoch nur auf einem einzigen RFP aktiviert.

Hinweis: Der DECT-Teil eines RFP kann deaktiviert werden. Bei deaktivierter DECT-Schnittstelle stehen alle frei werdenden Ressourcen (CPU und Speicher) für den OMM zur Verfügung.



2.3 OpenMobility Manager

Der OpenMobility Manager (OMM) erfüllt folgende Aufgaben:

- Signalisierungs-Gateway (SIP <-> DECT)
- Media-Stream-Management
- Verwalten der Funkstrecken-Synchronisationsfunktionen zwischen RFPs.
- Vereinfachen von Änderungen an der Systemkonfiguration
- Bietet zusätzliche Dienste, z.B.
 - Unternehmens-Telefonbuch (LDAP-basiert)

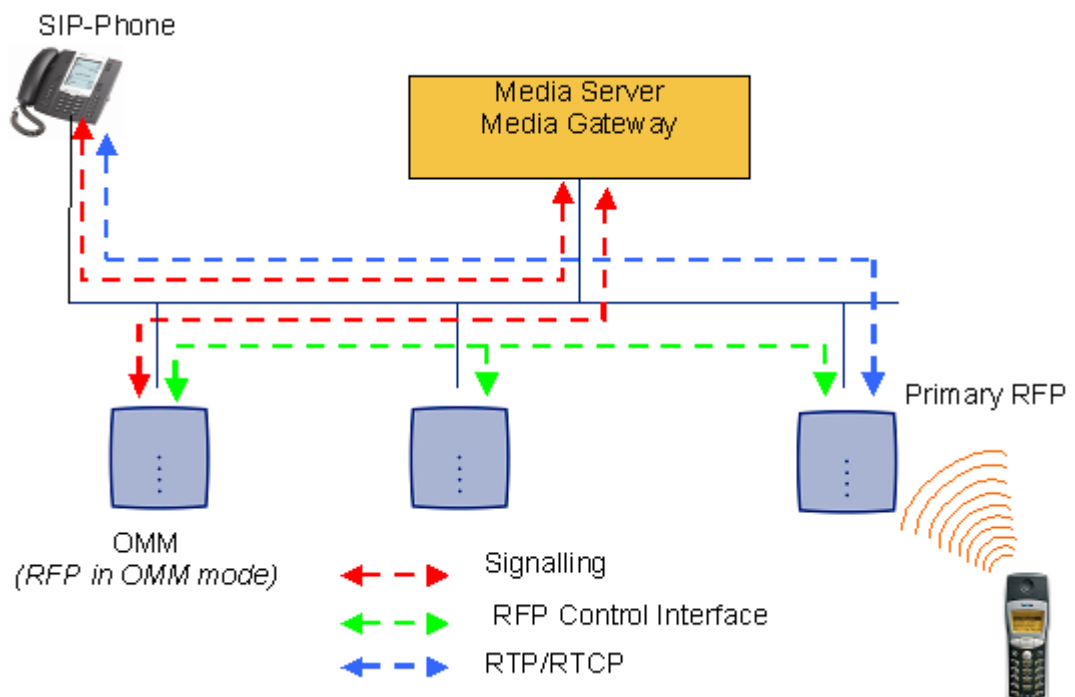
Der OpenMobility Manager (OMM) läuft auf einem der RFPs.

2.4 IP-Signalisierung und Media-Stream

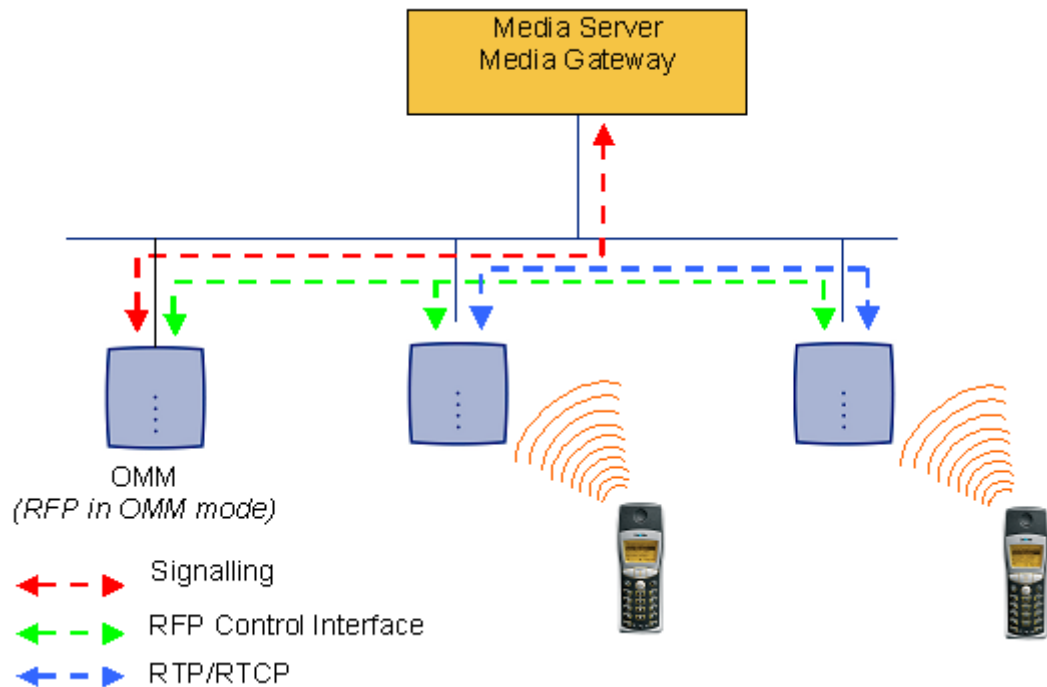
Um eine Verbindung zwischen einem IP-Telefon und einem PP (Aastra DECT 142 Handset / Aastra 142d) herzustellen, müssen folgende IP-Streams aufgebaut werden:

- ein Signalisierungskanal zum und vom SIP-Telefon
- ein Signalisierungskanal zum und vom OMM
- eine Steuerungsschnittstelle zwischen OMM und dem RFP, das eine Verbindung zum PP besitzt (das so genannte primäre RFP)
- Eine Verbindung mit Echtzeitprotokoll (RTP) und Echtzeit-Steuerprotokoll (RTCP) zwischen SIP-Telefon und dem primären RFP.

Die folgende Abbildung verdeutlicht dieses Szenario.

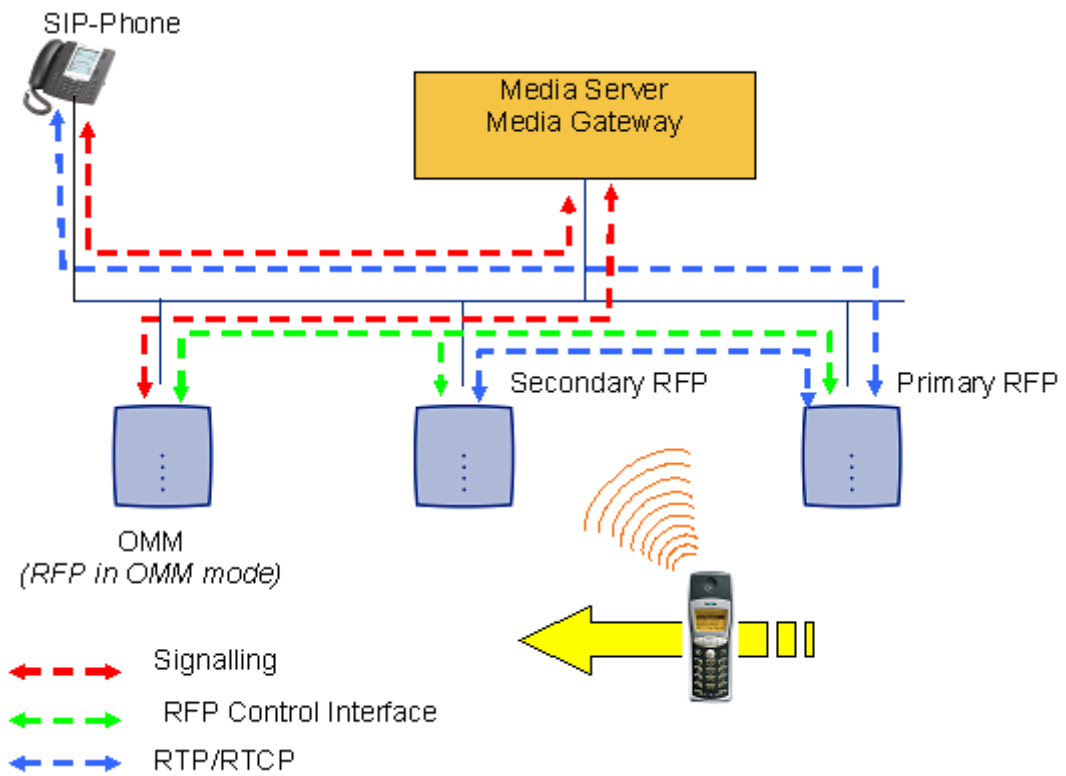


Um einen Anruf zwischen zwei PP's zu führen, müssen die gleichen IP-Streams wie im vorhergehenden Szenario aufgebaut werden. Lediglich das IP-Telefon entfällt. Die folgende Abbildung verdeutlicht dieses Szenario.

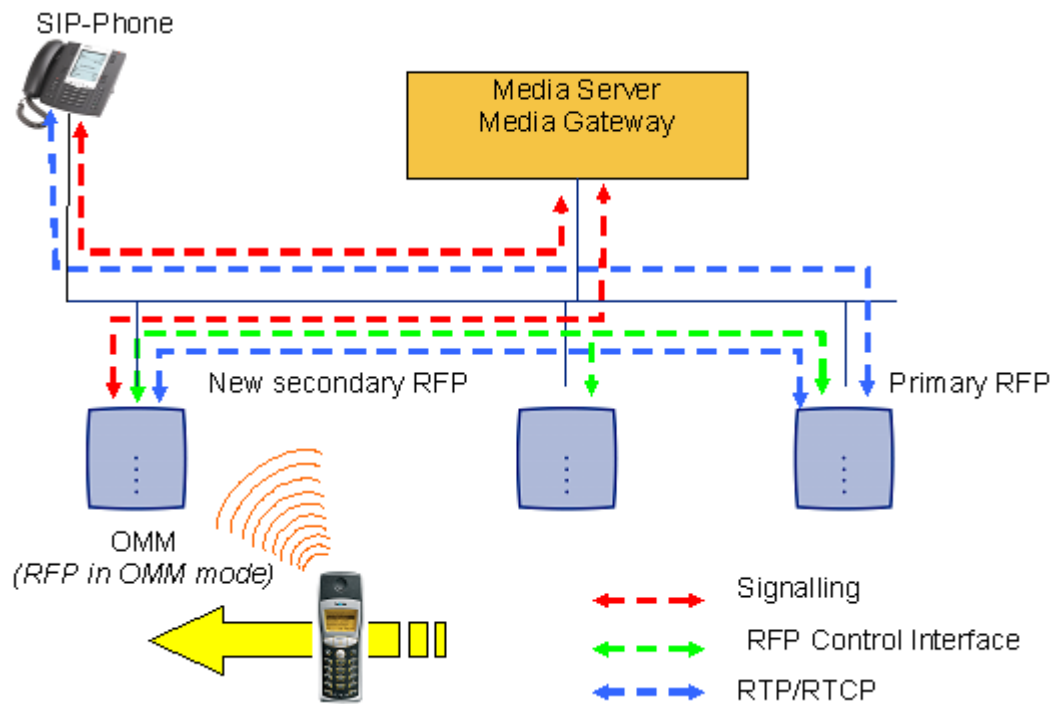


Ein Anruf von einem PP zu einem anderen, das das gleiche RFP nutzt, wird innerhalb des RFP geführt, solange kein Media-Gateway betroffen ist. Der Anruf wird also nicht über das Netzwerk (LAN) geführt. Zwar wirken sich die Sprachpakete nicht auf den Verkehr im LAN aus, wohl aber die Signalkpakete.

Wenn sich der Benutzer bewegt und das PP erkennt, dass ein anderes RFP eine höhere Signalstärke besitzt, leitet es den Handover-Vorgang ein. Der Medien-Stream vom IP-Telefon kann nicht zum sekundären RFP geleitet werden. Das primäre RFP leitet die Sprachverbindung daher über das LAN zum sekundären RFP, wie in der folgenden Abbildung gezeigt.



Wenn sich der Benutzer der in den Abdeckungsbereich des nächsten RFP bewegt, erkennt das PP, dass dieses RFP eine höhere Signalstärke besitzt. Auch hier kann der Media-Stream vom SIP-Telefon nicht zum sekundären RFP umgeschaltet werden. Das primäre RFP leitet die Sprachverbindung daher über das LAN zum sekundären RFP.

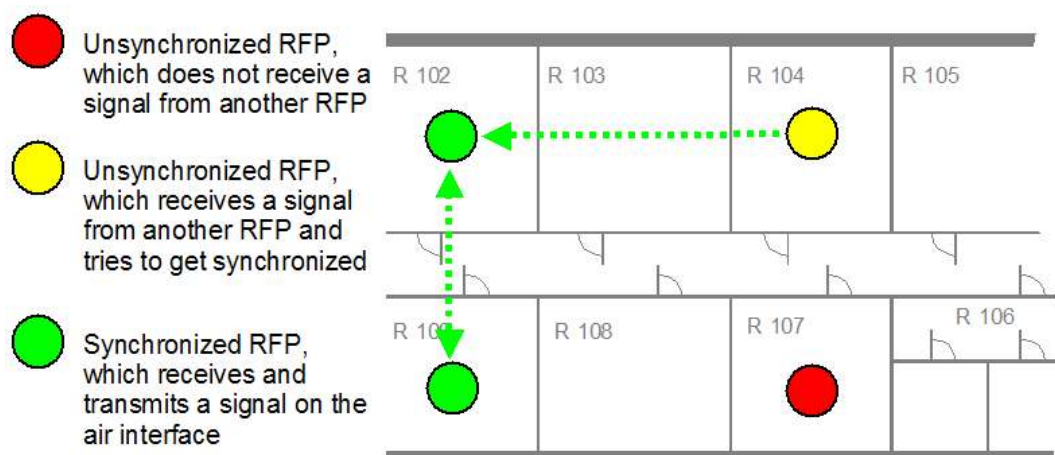


2.5 RFP-Synchronisation

Um ein nahtloses Handover zu gewährleisten, wenn sich ein Anrufer aus dem Abdeckungsbereich eines RFP in den Abdeckungsbereich eines anderen RFP bewegt, müssen die einzelnen RFPs exakt miteinander synchronisiert sein.

Diese Synchronisation der RFPs erfolgt über die Funkschnittstelle. Das erste RFP, das den Startvorgang beendet, sendet über Funk ein Signal an die anderen RFPs, mit dem sich diese synchronisieren können. Hat ein RFP die Synchronisierung abgeschlossen, sendet es ebenfalls ein Funksignal, das dann vom nächsten RFP zur Synchronisierung verwendet wird. Nur RFPs, die ein Synchronisationssignal empfangen können, werden synchronisiert.

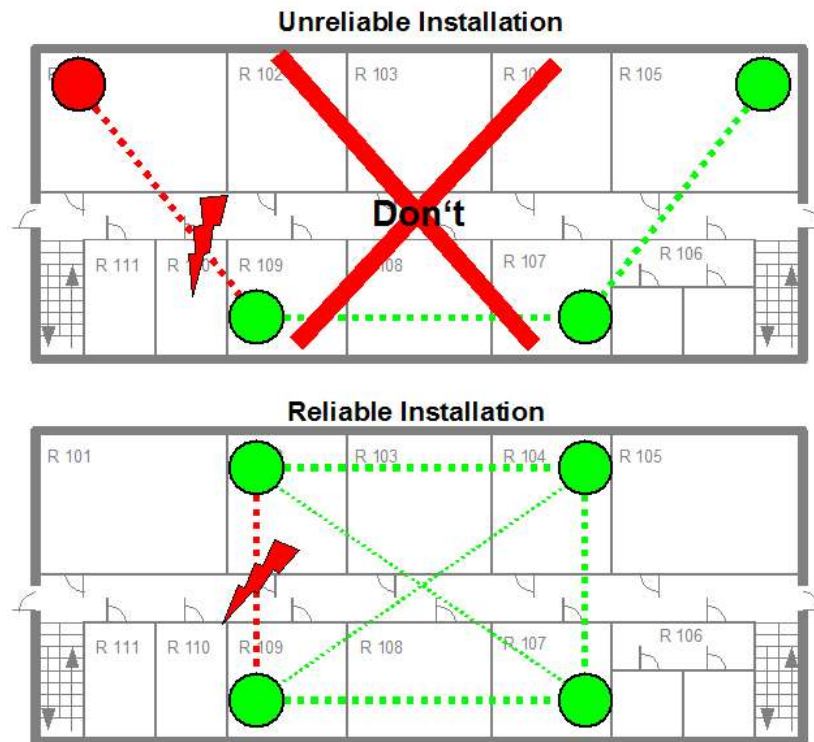
Damit sich ein RFP mit einem anderen RFP synchronisieren kann, darf die Signalstärke nicht unter -70 dBm absinken. Beachten Sie diese Anforderung bei der Standortaufnahme.



Solange ein RFP nicht synchronisiert ist, können keine Anrufe über dieses RFP geführt werden.

Wenn ein RFP die Synchronisation verliert, nimmt es keine neuen Anrufe entgegen („Besetzt-Bit“). Nach einer Verzögerung von maximal drei Minuten werden die über dieses RFP geführten, aktiven Anrufe beendet. Dann versucht das RFP erneut, sich zu synchronisieren.

IP-DECT-Installationen sind zuverlässiger, wenn jedes RFP die Signale mehrerer anderer RFPs empfangen kann, da dann mehrere Signale für die Synchronisation verwendet werden können.



Die Funk-Synchronisationslösung ist sehr zuverlässig, da alle vorhandenen redundanten Pfade für die Synchronisation verwendet werden können. Hardware-Toleranzen spielen daher nur eine sehr kleine Rolle. Kein RFP nimmt eine Schlüsselstellung ein.

Nur ungünstige Einrichtungen ohne redundante Synchronisationspfade können zu Problemen führen.

Manchmal müssen RFPs nicht synchronisiert werden, z.B. wenn sie sich in verschiedenen Gebäuden befinden. Diese RFPs können in unterschiedlichen Clustern zusammengefasst werden. RFPs in unterschiedlichen Clustern werden nicht miteinander synchronisiert. Die unterschiedlichen Cluster starten gleichzeitig und voneinander unabhängig.

2.6 Kanalkapazität eines RFP

RFPs besitzen zwölf freie Zeitschlitz:

- Acht Zeitschlitz besitzen DSP-Ressourcen für Media-Streams.
- Die vier verbleibenden Zeitschlitz werden z.B. für Steuersignale zwischen RFPs und PPs sowie für Hand-in-Zwecke verwendet.

Wenn alle acht Media-Stream-Kanäle in Verwendung sind, liefert das RFP ein „Besetzt-Bit“. Die PPs suchen in diesem Fall ein anderes RFP mit ausreichender Signalstärke. Falls ein solches gefunden wird, führt das entsprechende PP ein Handover zu diesem RFP durch. Nach Abschluss des Handover löscht das RFP sein „Besetzt-Bit“.

Bei jedem Eintritt in den Besetztzustand wird ein Eintrag in die Systemprotokolle vorgenommen. Wenn in einem bestimmten Bereich vermehrt Besetzt-Einträge auftreten, sollte dort ein zusätzliches RFP installiert werden, um die für Anrufe zur Verfügung stehende Zahl der Media-Streams zu verdoppeln.

2.7 Endgeräte (PPs)

Der Begriff „Endgerät“ (PP) ist DECT-Standardterminologie und in Zusammenhang mit der DECToverIP using SIP Lösung mit Mobilteil austauschbar.

Aastra bietet die folgenden Endgeräte:

- 142d
- 610d
- 620d
- 630d



Denken Sie an die unterschiedlichen gesetzlichen Bestimmungen in Nordamerika und anderen Teilen der Welt. Diese Unterschiede erzwingen verschiedene Varianten des 142d mit unterschiedlichen Frequenzbändern und Feldstärken:

- Aastra DECT 142 (NA)
 - Frequenzband 1'920 bis 1'930 MHz
 - 60 Duplex-Kanäle
 - 100 mW (maximale Ausgangsleistung pro aktivem Kanal)
 - 5 mW (durchschnittliche Ausgangsleistung pro aktivem Kanal)
- Aastra 142d (EMEA)
 - Frequenzband 1'880 bis 1'900 MHz
 - 120 Duplex-Kanäle
 - 250 mW (maximale Ausgangsleistung pro aktivem Kanal)
 - 10 mW (durchschnittliche Ausgangsleistung pro aktivem Kanal)

Die Modelle 610d / 620d / 630d entsprechen den in den USA und der Region EMEA geltenden gesetzlichen Bestimmungen.

Neben dem Aastra DECT 142 / Aastra 142d können mit der DECToverIP using SIP Lösung auch normale DECT-GAP-Telefone von Drittanbietern betrieben werden. Der Funktionsumfang kann jedoch abhängig von den Merkmalen des DECT-Telefons des Drittanbieters eingeschränkt sein.

2.8 Systemkapazitäten

Im System gibt es nur einen einzigen aktiven OpenMobility Manager (OMM). Der OMM besitzt folgende Kapazitäten:

- Steuerung von bis zu 256 RFPs (Access Points)
- Betrieb von bis zu 512 PPs (Endgeräten)

Der DECT-Teil eines RFP kann deaktiviert werden. Bei deaktivierter DECT-Schnittstelle stehen die frei werdenden Ressourcen (CPU und Speicher) für den OMM zur Verfügung.

3 Installation und Konfiguration

Um eine IP-DECT-Installation aufzubauen und zu betreiben, benötigt man eine Netzwerk-Infrastruktur mit mindestens den folgenden Komponenten:

- RFPs
- PPs
- IP PBX / Media-Server (z.B. Asterisk)
- TFTP-Server

Abhängig von der Betriebsart müssen folgende Dienste zur Verfügung stehen:

- DHCP
- SNTP
- DNS
- LDAP
- Syslog-Daemon

Hinweis: Im RFPs für den Betrieb im Freien (NA) dürfen nur mit den mit den Geräten mitgelieferten Antennen installiert werden. Es dürfen keine anderen Antennen und keine Kabel verwendet werden. In der EMEA-Region werden die RFPs für den Betrieb im Freien ohne Antennen ausgeliefert und Sie können die Einheiten mit einer der optionalen Antennen verwenden (separate Bestellnummer).

3.1 Start von OpenMobility

3.1.1 Start der RFPs'

Damit ein RFP gestartet werden kann, muss es im angebundenen Netzwerk mindestens einen TFTP-Server geben, damit die OMM-/RFP-Anwendungssoftware geladen werden kann.

Die wesentlichen Netzwerkeinstellungen können alternativ:

- zum Startzeitpunkt von einem DHCP-Server übermittelt werden
- mit dem Tool OM Configurator auf dem RFP konfiguriert werden. Die mit dem OM Configurator gemachten Einstellungen werden dauerhaft im integrierten Flash-Speicher jedes OMM/RFP gespeichert.

Das RFP erhält seine Boot-Imagedatei von einem TFTP-Server. Verwendete TFTP-Server müssen Teil 1.3, Referenz /1/ erfüllen. Verwendete DHCP-Server müssen Teil 1.3, Referenz erfüllen /4/.

TFTP- und DHCP-Server müssen sich nicht auf dem gleichen Host befinden.

3.1.1.1 Booten, Überblick

Das Booten erfolgt in zwei Schritten:

1. Start des Bootvorgangs
2. Start der Anwendung

Booter

Das RFP enthält in seinem Flash-Speicher eine kleine eigenständige Anwendung. Diese Software erledigt den so genannten Netzwerk-Bootprozess.

Beim Starten versucht jedes RFP mithilfe der Konfigurationseinstellungen im integrierten Flash-Speicher seine eigene IP-Adresse und andere Einstellungen der IP-Schnittstelle zu ermitteln. Stehen keine Einstellungen zur Verfügung oder sind diese Einstellungen deaktiviert, versucht das RFP, diese Einstellungen über DHCP zu erhalten.

Das RFP erhält seine Anwendungs-Imagedatei von vom TFTP-Server.

Anwendung

Nach dem Start des Anwendungs-Image prüft das RFP noch einmal die in seinem internen Flash-Speicher abgelegten lokalen Netzwerkeinstellungen. Sind keine Einstellungen vorhanden oder sind sie deaktiviert, startet es einen DHCP-Client, um die IP-Adresse des OMM und andere für den Start wichtige Einstellungen zu erhalten.

3.1.2 Start des OpenMobility Manager

Der Start des RFP, das für OMM-Betriebsart ausgewählt wurde, läuft genauso ab, wie der Start der RFPs in ausschliesslicher RFP-Betriebsart.

Die Entscheidung hängt von der OMM-IP-Adresse ab. Diese stammt:

- aus den lokalen Netzwerkeinstellungen, falls aktiv
- aus einer DHCP-Anfrage

Der OMM läuft auf dem RFP, dessen IP-Adresse der speziellen OMM-IP-Adresse entspricht.

3.1.3 Booter

3.1.3.1 DHCP-Client

Beim ersten Bootvorgang arbeitet der DHCP-Client mit folgenden Parametern:

- | | |
|-------------------------------------|----------------|
| • IP-Adresse | vorgeschrieben |
| • Netzmaske | vorgeschrieben |
| • Gateway | vorgeschrieben |
| • Name der Bootdatei | vorgeschrieben |
| • TFTP-Server | vorgeschrieben |
| • Public Option 224: „OpenMobility“ | vorgeschrieben |

3.1.3.1.1 DHCP-Anforderung

3.1.3.1.1.1 Vendor Class Identifier (Code 60)

Der DHCP-Client sendet den Vendor Class Identifier „**OpenMobility**“.

3.1.3.1.1.2 Parameter Request List (Code 55)

Der DHCP-Client des Booters fordert in der „Parameter Request List“ die folgenden Optionen an:

- **Subnet Mask Option (Code 1)**
- **Router Option (Code 3)**
- **Public Option 224 (Code 224)**
- **Public Option 225 (Code 225)**
- **Public Option 226 (Code 226)**

3.1.3.1.2 DHCP-Angebot

Der DHCP-Client wählt den DHCP-Server nach folgenden Regeln aus:

- Der Wert der **Public Option (Code 224)** ist die Zeichenkette **“OpenMobility”**.

oder

- Eine Unter-Zeichenkette im Feld **„file“** der DHCP-Nachricht lautet **„ip_rfp.cnt“**.

Trifft keine der oben genannten Bedingungen zu, wird das DHCP-Angebot ignoriert.

Vom DHCP-Angebot verwendete Informationen:

- Die zu verwendende IP-Adresse wird aus dem Feld **yiaddr** der DHCP-Nachricht entnommen.
- Die IP-Subnetzmaske wird aus **Subnet Mask Option (Code 1)** entnommen.
- Der Standard-Gateway wird aus **Router Option (Code 3)** entnommen.
- Die IP-Adresse des TFTP-Servers wird aus dem Feld **siaddr** der DHCP-Nachricht entnommen.
- Der Name der Boot-Imagedatei wird aus dem Feld **file** der DHCP-Nachricht entnommen. Ist dieses Feld leer, wird standardmässig der Dateiname **„iprfp.bin“** verwendet.

3.1.3.1.3 Wiederholungsversuche

Erhält der DHCP-Client kein passendes DHCP-Angebot, wird nach einer Sekunde eine erneute DHCP-Anforderung gesendet. Nach drei DHCP-Anforderungen wartet der DHCP-Client 60 Sekunden lang ab.

Während dieser Zeit akzeptiert der Booter eine lokale Konfiguration über den OpenMobility Configurator (OMC).

Dieser Zyklus wiederholt sich alle drei Minuten, bis entweder ALLE erforderlichen DHCP-Optionen zur Verfügung stehen oder das System manuell mit dem Tool OM Configurator konfiguriert wurde.

3.1.3.2 TFTP-Client

Der TFTP-Client lädt die Anwendungs-Imagedatei vom TFTP-Server herunter. Sowohl TFTP-Server als auch der Name der Anwendungs-Imagedatei werden über den DHCP-Client bereitgestellt. Das Anwendungsimage ist durch eine Prüfsumme geschützt.

3.1.4 Anwendung

Nach dem erfolgreichen Download und Start der Anwendung bezieht das RFP vom DHCP die IP-Adresse des OMM.

Der DHCP-Client kann Broadcast- und Unicast-DHCP-Antworten empfangen. Das Flag-Feld hat daher den Wert **0x0000**.

Die DHCP-Anforderung enthält das wohlbekannte magische Cookie (0x63825363) und die End-Option (0xFF).

Die folgenden Parameter werden in diesem Schritt unterstützt:

Option / Feld	Bedeutung	vorgeschrieben
yiaddr	IP-Adresse des IP-RFP	ja
siaddr	Parameter „Boot Server Host Name“, dessen Wert der IP-Adresse des TFTP-Servers entspricht	ja
file	Parameter „Bootfile Name“, dessen Wert dem Pfad (optional) und dem Namen der Anwendungs-Imagedatei entspricht. Beispiel: „omm_ffsip.tftp“.	ja
Code 1	Subnetzmaske	ja
Code 3	Standard-Gateway	ja
Code 6	Domain Name Server	nein
Code 15	Domänenname	nein
Code 42	IP-Adresse eines NTP-Servers	nein
Code 43	herstellerspezifische Optionen	ja
Public Option 224	Parameter „magic_str“, muss auf den Wert „OpenMobility“ gesetzt werden	ja

Die *herstellerspezifischen Optionen* sind:

herstellerspezifische Option	Bedeutung	Länge	vorgeschrieben
Option 10	ommip1: Für die Auswahl des IP-RFP, auf dem der OpenMobility Manager (OMM) laufen soll	4	ja
Option 14	syslogip: IP-Adresse eines Syslog-Daemon	4	nein
Option 15	syslogport: Port eines Syslog-Daemon	2	nein
Option 17	Country: für die Auswahl des Landes, in dem sich der OMM befindet. Dies ermöglicht landesspezifische Töne (Besetztton, Freizeichen usw.).	2	nein
Option 18	ntpservername: Name eines NTP-Servers	x	nein
Option 19	ommip2: Für die Auswahl des sekundären IP-RFP, auf dem der fehlertolerante oder Standby-OpenMobility Manager (OMM) laufen soll Diese Option ist bei Verwendung der OMM-Fehlertoleranz-Merkmals erforderlich (siehe Kapitel 5).	4	nein
Option 24	rsturl: URL wiederherstellen URL für den automatischen OMM-Datenbankimport (siehe Kapitel 3.3.2.5)	x	nein

Ein Beispiel für den Mindestinhalt des Parameterwerts „Option 43“ wäre:
0a 04 C0 A8 00 01, wobei C0 A8 00 01 für die OMM-IP-Adresse 192.168.0.1 steht.

Die Option 43 enthält eine Folge von Hexadezimalcodes. Im Beispiel sind „Optionsnummer“ „Länge“ „Wert“:

0a = Option 10 (ommip1)

04 = folgender Wert ist vier Blöcke lang

C0 A8 00 01 = 192.168.0.1

Gibt es mehrere Optionen, fügen Sie die jeweils nächste Option nach dem Ende der vorherigen an. Je nach DHCP-Server müssen Sie Option 43 mit „FF“ abschliessen.

Unterstützt werden Töne für die folgenden Länder:

Landescode	Land
1	Deutschland
2	Grossbritannien
3	Schweiz
4	Spanien
6	Italien
7	Russland
8	Belgien
9	Niederlande
10	Tschechisch
11	Österreich
12	Dänemark
13	Slowakei
14	Finnland
15	Ungarn
16	Polen
17	Weissrussland
18	Estland
19	Lettland
20	Litauen
21	Ukraine
22	Norwegen
24	Schweden
25	Taiwan
100	Nordamerika
101	Frankreich
102	Australien

3.1.4.1 Booter-Update

Jede Anwendungssoftware wird mit der neuesten freigegebenen Booter-Software geliefert. Die Anwendungssoftware aktualisiert den Booter automatisch.

WARNUNG: Nach einem Upgrade von OpenMobility Release 1.1.x auf 1.7.x wird der Booter der RFPs auf Version 3.3.x aktualisiert. OpenMobility Configurator 1.7.x wird benötigt, um RFPs mit dieser neuen Booter-Version zu konfigurieren. Bei einem RFP-Downgrade auf eine ältere Version wird kein automatisches Downgrade auf eine ältere Booter-Version durchgeführt.

3.1.4.2 Auswahl des richtigen DHCP-Servers

Der DHCP-Client fordert mit Code 50 seine eigene IP-Adresse an. Der DHCP-Client wählt den DHCP-Server aus, der die aktuell verwendete IP-Adresse anbietet. Zusätzlich muss er die zwingend erforderlichen Optionen anbieten, ansonsten wird das DHCP-Angebot vom DHCP-Client ignoriert.

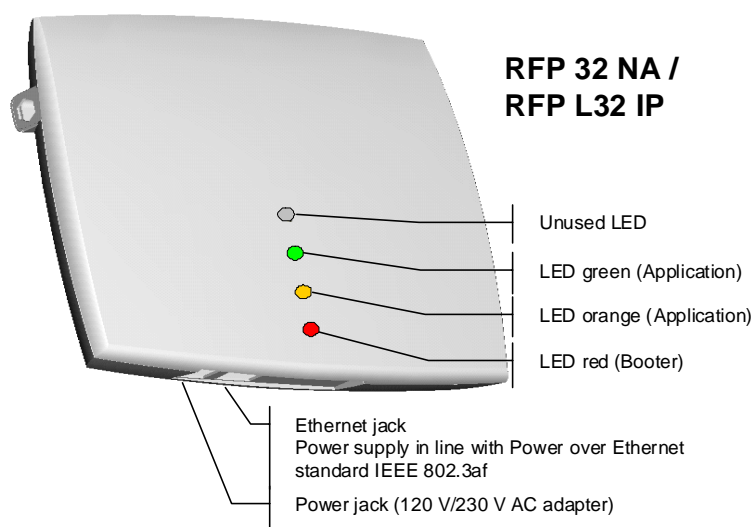
Wird keine passende Antwort empfangen, sendet der DHCP-Client die Anforderung nach jeweils einer Sekunde zwei Mal erneut. Anschliessend wartet der DHCP-Client eine Minute lang, bevor er erneut drei Anforderungen sendet.

Kann der DHCP-Client innerhalb von drei Minuten kein DHCP-Angebot annehmen, wird das RFP neu gestartet.

3.1.5 LED-Status des RFP

Die folgenden Abbildungen zeigen die LED-Anzeigen eines RFP während der einzelnen Zustände beim Starten.

Das RFP IP L32 besitzt drei LEDs, rot, orange und grün, die die einzelnen Zustände beim Starten anzeigen.

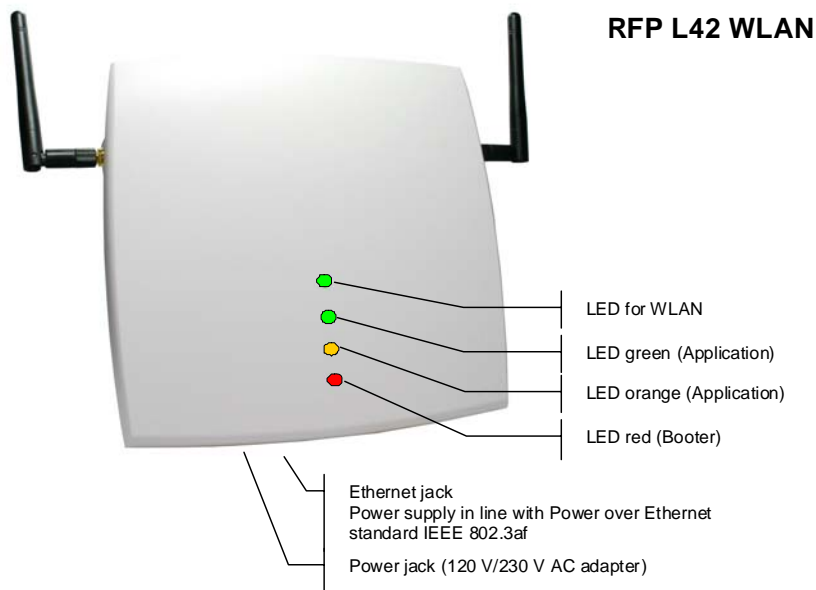


Zustand	LED-Status	Hinweise
Booter (Starten)	rot leuchtet	wartet auf eine Verbindung
Booter DHCP	rot blinkt, 0,5 Hz	startet eine DHCP-Anforderung und wartet auf ein DHCP-Angebot
Booter (TFTP)	rot blinkt, 2.5 Hz	lädt das Anwendungs-Image herunter
Anwendung (DHCP)	orange leuchtet	startet eine DHCP-Anforderung und wartet auf eine DHCP-Antwort
Anwendung (Initialisierung)	grün blinkt, 0.5 Hz	RFP initialisiert seine internen Komponenten
Anwendung (Initialisierung)	grün blinkt, 1 Hz	RFP versucht, zum OMM zu verbinden
Anwendung (Initialisierung)	grün blinkt (2 s an, 0.5 s aus)	Der DECT-Teil des RFP funktioniert nicht (entweder nicht konfiguriert oder nicht mit

Zustand	LED-Status	Hinweise
		anderen RFPs synchronisiert).
Anwendung (Initialisierung)	grün	RFP ist gestartet und funktioniert

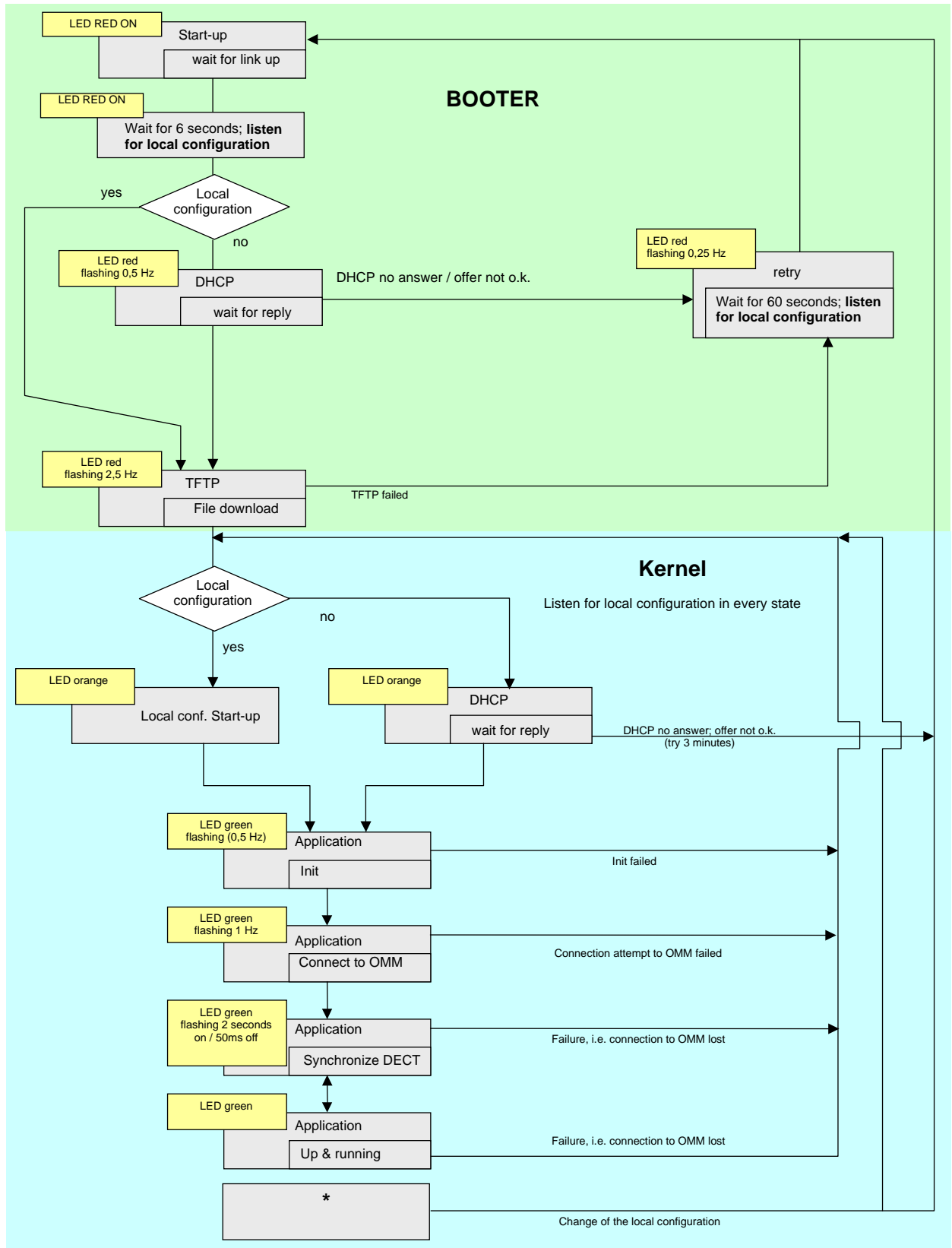
Das RFP L42 WLAN verfügt über eine zusätzliche LED, die den WLAN-Status anzeigt:

Zustand	WLAN-LED-Status
WLAN-Modul nicht gefunden	rot leuchtet
WLAN deaktiviert, da OMM ausgeführt wird.	aus
WLAN durch Konfiguration deaktiviert	aus
WLAN deaktiviert, wegen 10 Mb/s ¹	grün blinkt, 1 Hz
WLAN gestartet und in Betrieb	Grün ein



¹ Das RFP L42 WLAN muss an ein 100BaseT-Ethernet angeschlossen werden, damit das WLAN betriebsbereit ist.

3.1.6 Zustandsdiagramm der einzelnen Startphasen



3.2 Statische lokale Konfiguration eines RFP

Alternativ zur DHCP-Konfiguration können RFPs/OMM mit dem Tool OM Configurator individuell statisch konfiguriert werden.

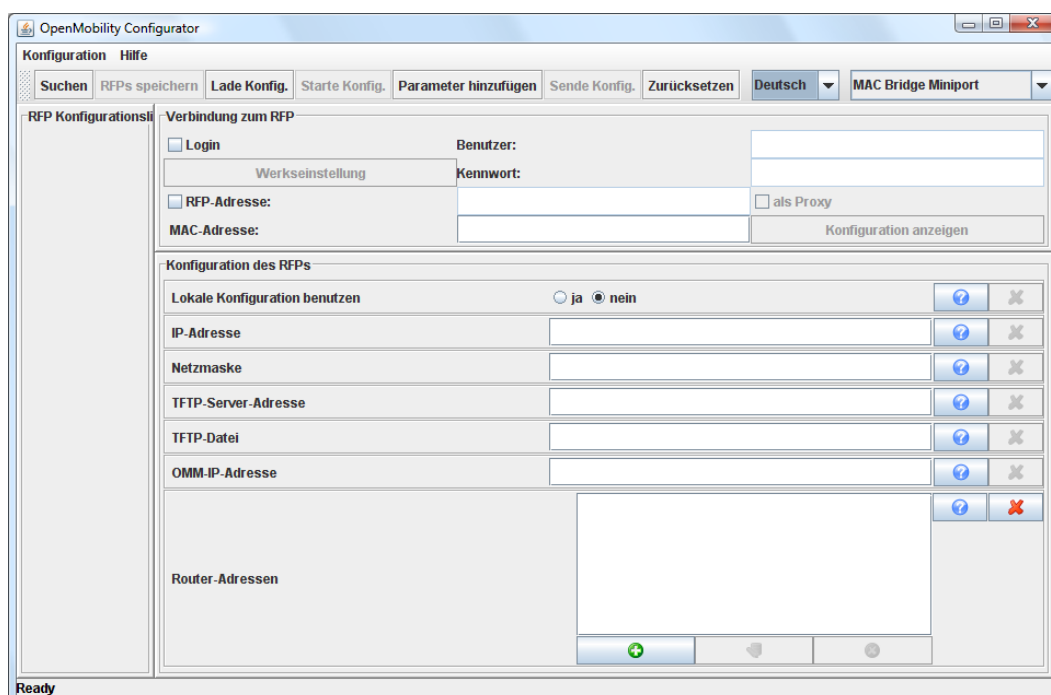
Der OM Configurator benötigt Java Runtime Environment Version 1.6 oder höher.

Die mit dem Tool OM Configurator in das RFP konfigurierten Einstellungen werden dauerhaft im internen Flash-Speicher des RFP gespeichert.

Mit dem OM Configurator können die gleichen Parameter konfiguriert werden wie per DHCP. Einzelheiten finden Sie in Teil 3.1.4.

Wenn eine lokale statische Konfiguration durchgeführt wurde, wird DHCP nicht mehr verwendet.

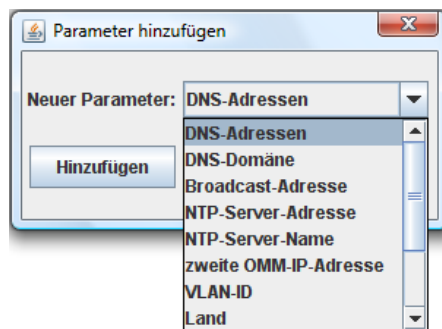
Die folgende Abbildung zeigt den OM Configurator.



Wählen Sie auf Systemen mit mehreren Ethernet-Adaptern die Schnittstelle, die für die Konfiguration der RFPs verwendet werden soll. Um ein RFP zu konfigurieren, müssen mindestens die MAC-Adresse und alle zwingend erforderlichen Optionen (siehe Tabelle unten) eingerichtet werden. Die MAC-Adresse muss in einem Format wie dem folgenden eingegeben werden: xx-xx-xx-xx-xx-xx.

Hat das RFP bereits eine IP-Adresse, geben Sie diese in das entsprechende Feld ein. Sie können das RFP in diesem Fall von ausserhalb des lokalen LAN-Segments erreichen. Optional.

Klicken Sie auf die Schaltfläche „Parameter hinzufügen“, um zusätzliche Parameter einzurichten und wählen Sie dann den gewünschten Parameter.



WICHTIG: Aktivieren Sie unter „Lokale Konfiguration benutzen“ das Kontrollkästchen „ja“, um für den RFP die lokale Konfiguration zu verwenden. Ansonsten wird DHCP verwendet.

Klicken Sie auf die Schaltfläche „Konfiguration senden“, um die Parameter an ein RFP zu senden.

Bootparameter (gemäss DHCP-Optionen)

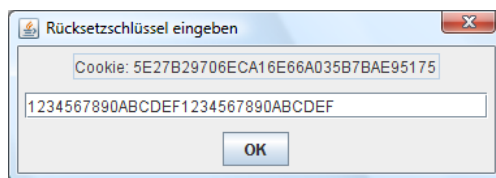
Parameter	Typ	Bedeutung
Lokale Konfiguration benutzen	vorgeschrieben	Dieser Parameter legt fest, ob beim Booten die lokalen Konfigurationseinstellungen verwendet werden sollen oder nicht.
IP-Adresse	vorgeschrieben	IP-Adresse des RFP
Netzmaske	vorgeschrieben	Subnetzmaske des IP-Netzwerks
TFTP-Server-Adresse	vorgeschrieben	IP-Adresse des TFTP-Servers
TFTP-Datei	vorgeschrieben	Boot-Datei, die beim Hochfahren vom TFTP-Server gelesen wird
OMM-IP-Adresse	vorgeschrieben	IP-Adresse des OpenMobility Manager
Routeradressen	optional	IP-Adresse des Standard-Gateway
DNS-Adressen	optional	IP-Adresse des DNS-Servers
DNS-Domäne	optional	Domänenname des Netzwerks
Broadcast-Adresse	optional	Broadcast-Adresse des Netzwerks
zweite OMM-IP-Adresse	optional	IP-Adresse des Standby-OMM
Land	optional	legt landesspezifische Einstellungen (landesspezifische Anruftöne) für den OMM fest
NTP-Server-Adresse	optional	IP-Adresse eines NTP-Servers
NTP-Servername	optional	Name eines NTP-Servers
VLAN ID	optional	VLAN-Kennung
Syslog IP-Adresse	optional	Ziel-IP-Adresse für den Syslog
Syslog-Port	optional	Zielport für den Syslog
URL wiederherstellen	optional	URL für den automatischen OMM-Datenbankimport (siehe Kapitel 3.3.2.5)
OMM im Proxy-Betrieb	optional	Experten-Modus

Die Konfiguration kann nur nach dem Einschalten oder während der Wiederholversuchphase (LED blinkt mit 0.25 Hz) oder in der Kernel-Betriebsart eingestellt werden. Einzelheiten finden Sie in Teil 3.1. Das Konfigurator-Tool wartet zwei Sekunden und versucht dann drei Mal, die Daten erneut zu senden.

Wenn Sie die Konfigurationsparameter eines RFP auslesen möchten, stellen Sie die MAC-Adresse und zusätzlich die IP-Adresse ein und drücken Sie dann die Schaltfläche „Konfiguration laden“. Alle Parameter werden im Tool OM Configurator aufgelistet.

Klicken Sie auf die Schaltfläche „Konfiguration zurücksetzen“, um alle Eingabefelder und zusätzlichen Parameter zu löschen.

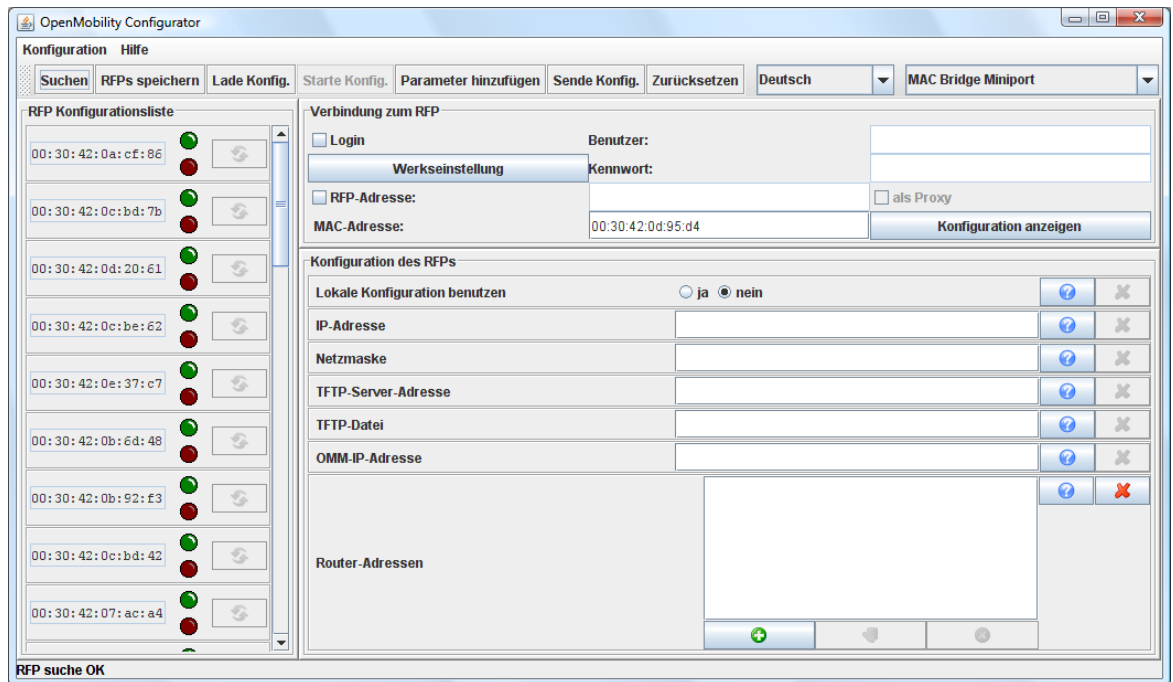
Ab OpenMobility Version 1.5 können Anmeldedaten dazu verwendet werden, unbefugte Konfigurationsänderungen zu verhindern. Bei Verwendung einer Berechtigung, aktivieren Sie das Kontrollkästchen 'Anmelden' und geben Sie den Benutzernamen und das Passwort in die Felder 'Benutzer' und 'Passwort'. Dieser OM-Konfigurator ist abwärts kompatibel zu den vorangehenden OpenMobility-Versionen ohne Anmeldungsunterstützung.



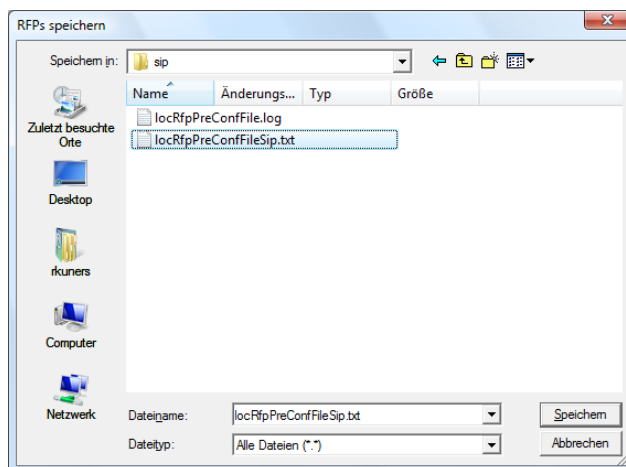
Ein vergessenes Passwort kann nicht wieder hergestellt werden, sondern muss mithilfe der Schaltfläche 'Werkseinstellungen' gelöscht werden. Senden Sie das angezeigte Cookie an den OpenMobility-Herstellersupport. Geben Sie nach Empfang des Passwort-Zurücksetzen-Schlüssels vom Support den Schlüssel in den '„Zurücksetzen-Schlüssel Eingeben“-Dialog ein. Dadurch wird auch die komplette lokale Konfiguration des aus dem internen Flash-Speicher des RFP gelöscht!

WARNUNG: Wird das Passwort gelöscht, werden auch alle lokalen Konfigurationen einschliesslich etwaiger OpenMobility-Konfigurationen gelöscht.

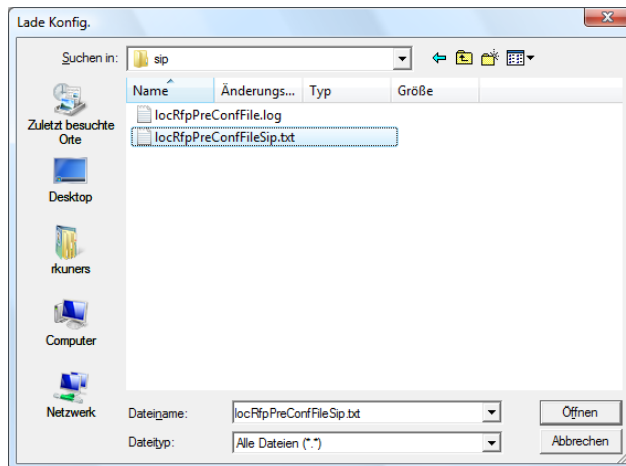
Ein RFP ausserhalb des lokalen LAN-Segments kann auch als Proxy fungieren. Markieren Sie das Kontrollkästchen "als Proxy", um diese Funktionalität zu aktivieren. Dann wird die MAC-Adresse verwendet, um ein RFP im LAN-Segment des Proxy-RFPs zu adressieren. Beim Proxy-Mechanismus könnte auch der Scan-Vorgang nach verfügbaren RFPs und die Konfiguration mehrerer RFPs durch eine Konfigurationsdatei verwendet werden.



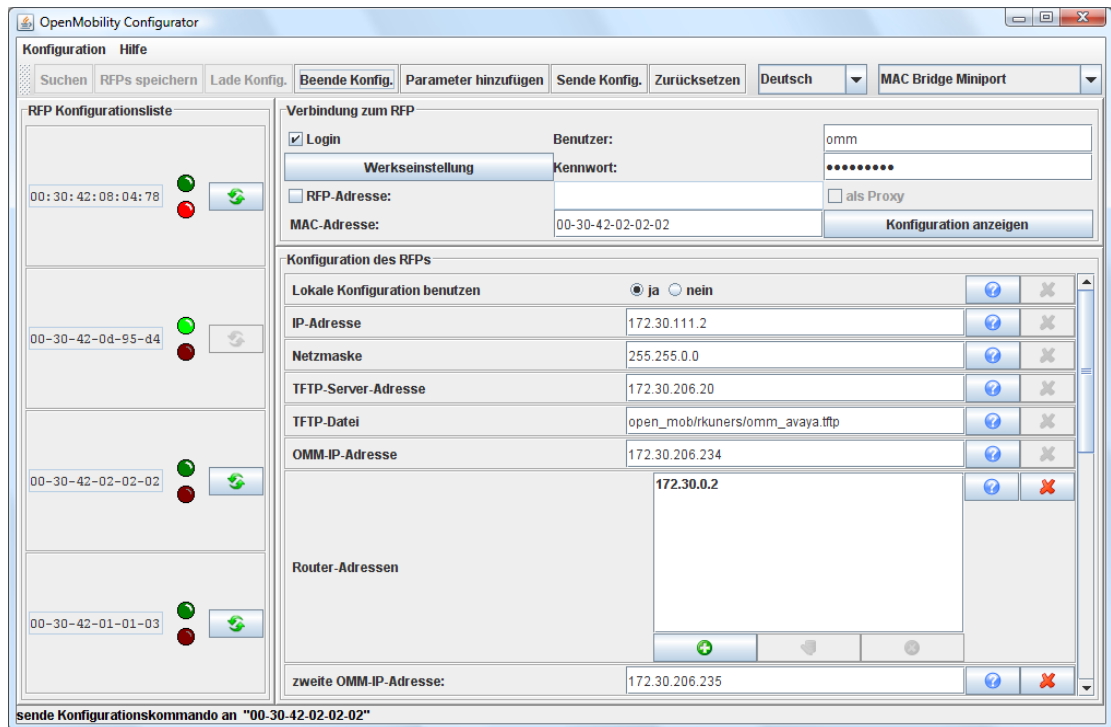
Verwenden Sie die 'Scan-Schaltfläche zur Suche nach verfügbaren RFPs im lokalen LAN-Segment oder mittels Proxy-Mechanismus in externen LAN-Segmenten. Alle MAC-Adressen der gefundenen RFPs werden in der linken RFP-Liste angezeigt. Die Status LEDs und die Aktualisierungsschaltfläche sind nach dem Scannen nach RFPs deaktiviert.



Die Liste der RFPs könnte mithilfe der Schaltfläche "RFPs speichern" gespeichert werden. So kann ein Administrator die Konfigurationsdaten mehrerer RFPs mithilfe eines Texteditors oder eine Tabellenkalkulationsanwendung, wie in Kapitel 8.3.3 beschrieben, bearbeiten.



Die erstellte Konfigurationsdatei könnte mithilfe der Schaltfläche ‘„Konfig. Laden“ geladen werden. Logdateien mit Statusinformationen über das Parsen und Ausführung der Konfigurationsdatei und -daten werden im gleichen Verzeichnis gespeichert.



Verwenden Sie die Schaltfläche “Konfig. Ausführen“, um die iterative Konfiguration mehrerer RFPs mithilfe der erstellten und geladenen Konfigurationsdatei zu starten. Die LEDs zeigen an, ob die Konfiguration erfolgreich war oder fehlgeschlagen ist. Weitere Informationen entnehmen Sie dem Logdatei-Inhalt. Wenn die Konfiguration bei einem RFP fehlgeschlagen ist, könnte sie mithilfe der Aktualisierungsschaltfläche neben den LEDs wiederholt werden.

Beachten Sie, dass die Anmelde- und Proxy-Daten für die gesamte Konfigurationsdatei verwendet werden!

3.3 OpenMobility Manager konfigurieren

Der OMM läuft auf einem dafür vorgesehenen RFP innerhalb einer SIP-DECT-Installation. Der OMM wird über DHCP-Optionen oder statisch über das Tool OM Configurator festgelegt. Alle anderen RFPs in der Installation sind so konfiguriert, dass sie auf den OMM dieser Installation zurückverweisen.

Der OMM kann über HTTP/HTTPS konfiguriert werden. Der OMM fungiert als HTTP-/HTTPS-Server. Der HTTP-Server bindet sich standardmässig an Port 80, HTTPS bindet sich standardmässig an Port 443. Die Konfigurationsdaten werden direkt aus dem internen Flash-Speicher gelesen.

Die Konfigurationsdatei ist eine ASCII-Datei (Klartext). Die Konfigurationsdatei darf nicht ausserhalb des OMM geändert werden.

Sie kann über die Webschnittstelle herunter- und hochgeladen werden.

Der Zugriff auf den Dienst ist auf jeweils eine aktive Sitzung gleichzeitig beschränkt und mit einem Passwort geschützt.

Für den Zugriff auf den Dienst muss mindestens der Browser Microsoft Internet Explorer 6.0, oder Mozilla Firefox 1,5 verwendet werden. Der Browser muss Frames unterstützen. JavaScript und Cookies müssen aktiviert sein.

3.3.1 Anmeldeprozedur für den Dienst

Der OMM ermöglicht nur einem Benutzer gleichzeitig, das System zu konfigurieren. Der Benutzer muss sich mit Benutzername und Kennwort authentifizieren. Bei beiden Zeichenketten ist Gross- und Kleinschreibung relevant.

Nach der ersten Installation oder nach Entfernen der Konfigurationsdatei ist der Dienst OpenMobility über ein integriertes Benutzerkonto als Benutzer "omm" mit dem Kennwort "omm" zugänglich.



OpenMobility Manager



Anmeldung	
System	-
PARK	-
Benutzername	<input type="text" value="omm"/>
Kennwort	<input type="password" value="..."/>

OK




Bei der ersten Anmeldung an eine neue OpenMobility-Version muss der Benutzer die Endbenutzer-Lizenzvereinbarung (EULA) annehmen.

Ist das integrierte Standard-Benutzerkonto aktiv, muss der Administrator das Kennwort des Kontos für „vollständigen Zugang“ und „root“ ändern. Die einzelnen Kontenarten sind in den Kapiteln 4.2 und 4.3 beschrieben.

Nach dem Einloggen stehen folgende Optionen zur Verfügung:

- Systemstatus anzeigen
- Konfiguration allgemeiner SIP-DECT-Systemparameter
- Verwaltung der angeschlossenen RFPs
- Verwaltung der PPs
- WLAN-Parameter konfigurieren
- Systemfunktionen wie Stellenbehandlung und Verzeichnis verwalten
- Endbenutzer-Lizenzvereinbarung (EULA) anzeigen


OpenMobility Manager

Abmelden

Status

System

Basisstationen

Endgeräte

WLAN

Systemmerkmale

Info

Status


Allgemein

OpenMobility Manager

Laufzeit: 0:47

Flash-Speicherauslastung: 2%

Standby-OMM

Zustand:  Es ist kein OpenMobility Manager im Standby-Modus eingerichtet!

Basisstationen

Gesamtanzahl: 0

Endgeräte

Gesamtanzahl: 0

Anmelden erlaubt: ✗

Download neuer Firmware in die Endgeräte

Aktiv: ✗

Laden der Firmware von:

Bleibt der Benutzer fünf Minuten lang untätig, wird er vom OMM abgemeldet.

Mit der Schaltfläche „Abmelden“ melden Sie sich selbst vom System ab.

Hinweis: Wenn Sie den Browser schliessen, ohne sich zuvor abzumelden, ist der Dienst fünf Minuten lang für andere Clients gesperrt.

3.3.2 System

3.3.2.1 Systemeinstellungen

Die Systemeinstellungen enthalten globale Einstellungen für den OpenMobility Manager wie:

- Systemname
- Fernzugang
schaltet den ssh-Zugang für alle RFPs des DECT-Systems ein/aus
- DECT-Authentifizierungscode

Während der ersten PP-Anmeldung wird der Authentifizierungscode als Sicherheitsoption verwendet (siehe Kapitel 3.3.4). Ein hier eingegebener Code ist der standardmässige DECT-Authentifizierungscode für alle neu eingerichteten PP (siehe Kapitel 3.3.4.1). Diese Eingabe ist optional.

- PARK

Jedes DECT-Netzwerk benötigt einen eindeutigen PARK-Schlüssel.
Geben Sie den PARK-Schlüssel auf der OpenMobility-CD ein..
Diese Eingabe ist unbedingt notwendig.

- Verschlüsselung, wie in Kapitel 3.3.2.1.2 beschrieben

- Regulierungsdomäne, wie in Kapitel 3.3.2.1.3 beschrieben

- DECT-Monitor

Für die Überwachung des Verhaltens des OpenMobility Managers im DECT-System gibt es eine getrennte Anwendung. Dieses Tool benötigt einen Zugang zum OpenMobility Manager, der standardmäßig deaktiviert ist und auf der Systemseite aktiviert werden kann. Das markierte Kontrollkästchen DECT Monitor wird aus Sicherheitsgründen nicht dauerhaft im integrierten Flash-Speicher des OMM/RFP gespeichert. Die Markierung des Kontrollkästchens DECT-Monitor wird bei jedem Rücksetzen gelöscht.

- ToS- und TTL-Parameter

Um die Priorisierung von Sprachpaketen und/oder Signalisierungspaketen (SIP) innerhalb des verwendeten Netzwerks zu ermöglichen, muss hier der IP-Parameter ToS (Type of Service) konfiguriert werden.

- Syslog-Parameter

Der OpenMobility Manager und die RFPs können Syslog-Nachrichten weiterleiten. Dieses Merkmal kann zusammen mit der IP-Adresse eines Host konfiguriert werden, der diese Nachrichten sammelt.

- Parameter unter „Datum und Uhrzeit“

Wird SNTP nicht verwendet, können Datum und Uhrzeit im OMM konfiguriert werden. Dies ist nötig, um das DECT 142 Handset / Aastra 142d mit Uhrzeit- und Datumsinformationen zu versorgen.

Die auf dieser Website angezeigten Zeitzoneeregeln können im Bereich *Zeitzone* des Webdienstes konfiguriert werden (siehe Kapitel 3.3.2.4).

Bitte beachten Sie, dass Datum und Uhrzeit bei jedem Neustart des RFP, auf dem der OpenMobility Manager läuft, neu eingestellt werden müssen, falls nicht SNTP verwendet wird.

Der OpenMobility Manager liefert Datums- und Uhrzeitinformationen an das Endgerät DECT 142 Handset / Aastra Phone 142, wenn dieses eine DECT-Standortregistrierung vornimmt. Dies geschieht in folgenden Fällen:

- beim Einbuchen in den OMM

- beim erneuten Eintritt in das Netzwerk nach einem Verlust des DECT-Signals
- beim Einschalten
- wenn das lautlose Laden am Telefon aktiviert ist und das Telefon aus der Ladeschale genommen wird
- nach einer bestimmten Zeit, um Datum und Uhrzeit zu aktualisieren

Systemeinstellungen

OK Abbruch Neustart

Allgemeine Einstellungen

Systemname OM SIP

Fernzugriff ☒

IP-Parameter

ToS für Sprachpakete B0

ToS für Signalisierungspakete B0

TTL (Time to live) 32

Wenn Sie die DECT-Regulierungsdomäne ändern, werden alle Basisstationen neu gestartet.

DECT-Einstellungen

PARK

Verschlüsselung ☐

DECT-Monitor ☐

Regulierungsdomäne EMEA (ETSI)

DECT-Authentifizierungscode

Download neuer Firmware in die Endgeräte

Aktiv ☐

Syslog

IP-Adresse

Port 0 Standard

Wenn Sie die WLAN-Regulierungsdomäne ändern, werden alle Access-Points deaktiviert.

WLAN-Einstellungen

Regulierungsdomäne Kein(e)

Datum und Uhrzeit

Zeitzone Central European (CET UTC+1 DST)

Lokale Uhrzeit im Format HH:MM:SS 12 : 47 : 08

Lokales Datum im Format DD-MM-YYYY 02 - 12 - 2008

Please, enter the PARK key as labelled on the OpenMobility CD

3.3.2.1.1 Neustart des OMM

Um den OMM neu zu starten, wählen Sie im Navigationsbaum „Systemeinstellungen“ und dann „Neustart“. Es ist hier auch möglich, die Konfigurationsdaten zurückzusetzen.

Neustart

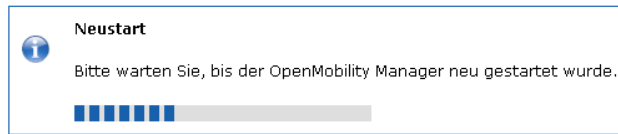
Wenn Sie den OpenMobility Manager neu starten, werden alle laufenden Gespräche beendet. Sind Sie sicher?

System

Alle Einstellungen löschen ☐

OK Abbruch

Dafür wird eine spezielle Website geladen, auf der ein Fortschrittsbalken angezeigt wird. Sobald der OMM wieder erreichbar ist, wird automatisch die Webseite „Anmelden“ geladen.



3.3.2.1.2 Verschlüsselung

Verschlüsselung steht nur bei Produkten des Typs RFP32/34/42 zur Verfügung. Sie kann also nur dann auf der Webseite „Systemeinstellungen“ aktiviert werden, wenn keine anderen Aastra RFP-Varianten an den OMM angeschlossen sind.

Ist die Verschlüsselung aktiviert und stellt eine andere RFP-Variante eine Verbindung zum OMM her, wird deren DECT-Funkschnittstelle nicht aktiviert.

Hinweis: Die PPs müssen DECT-Verschlüsselung unterstützen. Dies ist kein zwingend vorgeschriebenes Merkmal.

3.3.2.1.3 Regulierungsdomäne

Mithilfe der Regulierungsdomäne muss festgelegt werden, wo das IP-DECT-Telefon verwendet wird. Bestehende Installationen werden auf den Standardwert „EMEA (ETSI)“ aktualisiert.

Um eine nordamerikanische, FCC-konforme Installation zu erhalten, muss der Wert auf „US (FCC/CI)“ gesetzt werden.

In einer nordamerikanischen Installation in den USA (FCC/CI), werden ETSI-konforme RFPs deaktiviert. Sie können nicht aktiviert werden, solange die Regulierungsdomäne auf „US (FCC/CI)“ gesetzt ist. Dies gilt sinngemäss auch umgekehrt.

Nur US-konforme (FCC/CI) Endgeräte des Typs DECT 142 können Verbindungen mit RFPs/OMM herstellen, die für den US-Markt gedacht und für die US-Regulierungsdomäne (FCC/CI) eingerichtet sind.

3.3.2.2 SIP

Die SIP-Einstellungen enthalten alle globalen Einstellungen zu SIP-Signalisierung und RTP-Sprach-Streams.

- **Proxy-Server**
IP-Adresse oder Name des SIP-Proxyservers. Wenn Sie als Parameter Proxy Server einen Hostnamen und eine Domäne verwenden, stellen Sie sicher, dass für Ihr SIP-DECT-System ein DNS-Server und eine Domäne über DHCP oder das Tool OM Configurator vergeben sind.
- **Proxy-Port**
Portnummer des SIP-Proxy-Servers. Voreingestellt ist 5060. Um die DNS-Serverunterstützung für die Suche nach einem Proxy zu aktivieren, geben Sie für den Proxy-Port „0“ ein.
- **Registrar-Server**
P-Adresse oder Name des SIP-Registrars. Ermöglicht die

Registrierung der PPs bei einem Registrar. Wenn Sie als Parameter Proxy Server einen Hostnamen und eine Domäne verwenden, stellen Sie sicher, dass für Ihr SIP-DECT-System ein DNS-Server und eine Domäne über DHCP oder das Tool OM Configurator vergeben sind.

- **Registrar-Port**
Portnummer des SIP-Registrars. Voreingestellt ist 5060. Um die DNS-Serverunterstützung für die Suche nach einem Registrar zu aktivieren, geben Sie für den Proxy-Port „0“ ein.
- **Registration-Period**
Der vom Registrar angeforderte Registrierungszeitraum in Sekunden. Der Standardwert beträgt 3600.
- **Outbound-Proxy**
Adresse des Proxy-Servers für abgehende Nachrichten. Alle vom OMM kommenden SIP-Nachrichten werden an diesen Server geschickt. Gibt es in Ihrem Netzwerk beispielsweise einen Session Border Controller, geben sie in der Regel hier dessen Adresse ein. Optional.
- **Outbound-Proxy-Port**
Der Proxy-Port des Proxy-Servers, an den der OMM alle SIP-Nachrichten schickt. Optional.
- **Explizite Nachrichtensignalisierung**
Manche Media-Server wie Asterisk unterstützen die Anzeige wartender Nachrichten (Message Waiting Indication, MWI) basierend auf /15/. Die Endgeräte Aastra DECT 142 Handset / Aastra 142d zeigen ein entsprechendes Symbol an, wenn der Benutzer eine Sprachnachricht auf seiner Voice-Box hat, die vom Media-Server unterstützt wird. Bei aktivierter Expliziter Nachrichtensignalisierung sendet der OMM für jedes PP eine entsprechende Meldung an den Proxy-Server oder Proxy-Server für abgehende Nachrichten.
- **User-Agent-Info**
Bei Aktivierung sendet der OMM Informationen über seine Version in den SIP-Headern *User-AgentServer* aus.
- **Wahlabschluss senden**
Ist dies aktiviert, versucht der OMM nicht, die Vollständigkeit einer vom Benutzer gewählten Nummer mithilfe des Zeichens `#` zu erkennen. Der OMM wartet stattdessen nach jeder vom Benutzer gedrückten Wahl Taste vier Sekunden lang auf weitere Benutzereingaben. Bei aktivierter Option kann das Zeichen `#` Teil der Eingabe sein.
- **Registration Retry Timer**
Bestimmt, wie lange, in Sekunden, der OMM zwischen den Registrierversuchen wartet, wenn die Registrierung vom Registrar zurückgewiesen wird.
- **Transaction Timer**
Zeit in Millisekunden, die der OMM einem Call-Server (Proxy/Registrar) zur Antwort auf die von ihm gesendeten SIP-

Nachrichten erlaubt. Erhält der OMM keine Antwort innerhalb der für diesen Parameter bestimmten Zeit, geht der OMM davon aus, dass eine Zeitüberschreitung der Nachricht vorliegt. In diesem Fall wird der Call-Server in der Blacklist aufgezeichnet. Gültige Werte sind 4000 bis 64000. Der Standardwert beträgt 4000.

- **Blacklist Time Out**

Die Zeitdauer in Minuten, die ein unerreichbarer Call-Server in der Blacklist verweilt. Gültige Werte sind 0 bis 1440. Der Standardwert beträgt 5.

- **RTP-Port-Basis**

Jedes RFP benötigt für das RTP-Sprach-Streaming einen durchgehenden Portbereich von 68 UDP-Ports. Die RTP-Port-Basis ist die Portnummer, mit der dieser Bereich beginnt. Der Standardwert beträgt 16320.

- **Bevorzugter Codec 1 – 5**

Legt eine kundenspezifische Liste bevorzugter Codecs fest, mit deren Hilfe Sie bestimmte Codecs verwenden können. *Codec 1* hat die höchste, *Codec 5* hat die niedrigste Priorität.

- **Silence-Suppression**

Stellen Sie hier ein, ob Sie Ruheunterdrückung wünschen oder nicht.

- **DTMF Out-of-Band**

Hier wird eingestellt, ob DTMF Out-of-Band bevorzugt wird oder nicht

.

- **DTMF-Methode**

Der OMM unterstützt die folgenden Methoden für DTMF Out-of-Band:

- RFC 2833

Sendet DTMF als RTP-Ereignisse gemäss RFC 2833 (/9/) nach Verhandlung des Nutzlast-Typs über SIP/SDP. Ist der Nutzlast-Typ nicht verhandelt, wird automatisch „inband“ verwendet.

- INFO

Bei der SIP-Methode INFO werden DTMF-Töne als Telefon-Ereignisse übertragen (application/dtmf-relay). Diese Einstellung muss verwendet werden, wenn RFC 2833 nicht unterstützt wird.


- BEIDES

DTMF-Telefon-Ereignisse werden gemäss RFC 2833 und der SIP-Methode INFO gesendet.
Hinweis: Es ist möglich, dass die Gegenstelle Ereignisse doppelt erkennt.

DTMF Nutzlast-Typ

Ist Out-of-Band aktiviert, legt *Nutzlast-Typ* die Art der Nutzlast fest, die für das Senden von DTMF-Ereignissen gemäss Teil 1.3, Referenz /9/ verwendet wird.

SIP

 Das Ändern dieser Einstellungen kann zu einem Neustart des OpenMobility-Managers führen.

OK
Abbruch

Basiseinstellungen		
Proxy-Server	<input type="text" value="172.30.206.90"/>	
Proxy-Port	<input type="text" value="5060"/>	
Registrar-Server	<input type="text" value="172.30.206.90"/>	
Registrar-Port	<input type="text" value="5060"/>	
Registration-Period	<input type="text" value="3600"/>	s

Erweiterte Einstellungen		
Outbound-Proxy-Server	<input type="text"/>	
Outbound-Proxy-Port	<input type="text" value="5060"/>	
Explizite Nachrichtensignalisierung	<input type="checkbox"/>	
User-Agent-Info	<input checked="" type="checkbox"/>	
Sende Wahlendezeichen	<input type="checkbox"/>	
Registration-Retry-Timer	<input type="text" value="1200"/>	s
Transaction-Timer	<input type="text" value="4000"/>	ms
Zeitlimit der Sperrliste	<input type="text" value="5"/>	min

RTP-Einstellungen		
RTP-Port-Basis	<input type="text" value="16320"/>	
Bevorzugter Codec 1	<input type="text" value="G.711 u-law"/>	
Bevorzugter Codec 2	<input type="text" value="G.711 A-law"/>	
Bevorzugter Codec 3	<input type="text" value="G.729 A"/>	
Bevorzugter Codec 4	<input type="text" value="G.723-63"/>	
Bevorzugter Codec 5	<input type="text" value="G.723-53"/>	
Bevorzugte Paketzeit	<input type="text" value="30"/>	ms
Silence-Suppression	<input checked="" type="checkbox"/>	

DTMF-Einstellungen		
Out-of-Band	<input checked="" type="checkbox"/>	
Methode	<input type="text" value="RTP(RFC 2833)"/>	
Nutzlast-Typ	<input type="text" value="101"/>	

3.3.2.3 Benutzerverwaltung

Nach der ersten Installation oder nach Entfernen der Konfigurationsdatei ist der Dienst OpenMobility über ein integriertes Benutzerkonto als Benutzer "omm" mit dem Kennwort "omm" zugänglich. Diese Einstellungen sind gross- und kleinschreibungssensitiv und können auf der Webseite „Benutzerverwaltung“ geändert werden.

Die einzelnen Kontenarten sind in den Kapiteln 4.2 und 4.3 beschrieben.

3.3.2.4 Zeitzonen

Die Zeit- und Datums-Nachsynchronisierung der Aastra DECT 142/Aastra 142d-Geräte ist in Kapitel 3.3.2.1 beschrieben.

Im Bereich „Zeitzone“ des OpenMobility Manager sind alle verfügbaren Zeitzone aufgelistet. Die Einstellung erfolgt unter Berücksichtigung bekannter Sommerzeitregelungen, standardmässig angepasst an die koordinierte Weltzeit (Universal Coordinated Time, UTC). Die Differenz zur UTC-Zeit wird in der Spalte „UTC-Differenz“ angezeigt. Falls eine Sommerzeitregelung berücksichtigt wird, ist dies bei der betreffenden Zeitzone angegeben.

Die Zeitzoneregeln können bei maximal fünf Zeitzone geändert werden. Die Namen der Zeitzone mit geänderten Regeln werden in Fettschrift angezeigt. Die Änderungen werden in der Konfigurationsdatei gespeichert und nach jedem Start des OpenMobility Manager wiederhergestellt. Die Schaltfläche „Standard“ setzt alle Zeitzone auf ihre Standardwerte zurück und löscht geänderte Zeitzoneregeln aus der Konfigurationsdatei.

Name	ID	UTC-Differenz	DST
Africa Central West	AFC	+1 h	✗
Africa Central East	AFD	+2 h	✗
Africa East	AFE	+3 h	✗
Afghanistan	AFG	+4.50 h	✗
Africa West	AFW	0 h	✗
Alaska	AK	-9 h	✓
Aleutian Islands	AKW	-10 h	✗
Armenian Standard Time	ARM	+4 h	✓
Asia UTC+4	AS4	+4 h	✗
Asia UTC+5	AS5	+5 h	✗
Asia UTC+6	AS6	+6 h	✗
Asia UTC+7	AS7	+7 h	✗
Asia UTC+8	AS8	+8 h	✗
Asia UTC+9	AS9	+9 h	✗
Atlantic	ATL	-4 h	✓
Australia East	AUE	+10 h	✓

Im Dialog „Konfigurieren der Zeitzone“ lassen sich die normale und die Sommerzeit einer Zeitzone ändern. Bei Zeitzonen ohne Sommerzeit kann nur die UTC-Differenz konfiguriert werden. Für eine Sommerzeiteinstellung müssen beide Umstellungszeitpunkte (Beginnt der normalen Zeit und Beginn der Sommerzeit) genau angegeben werden. Dafür kann ein bestimmter Tag des Monats oder ein bestimmter Wochentag in einem Monat genannt werden. Das folgende Screenshot zeigt dies beispielhaft.

Konfigurieren der Zeitzone

Zeitzone	
Name	Africa Central East
ID	AFD
Standardzeit	
UTC-Differenz	120 min
Monat	0 (0 = Nicht verwendet)
Tag	0 (0 = Nicht verwendet)
Wochentag	0 (0 = Nicht verwendet 1 = Sonntag 7 = Sonnabend)
Woche	0 (0 = Nicht verwendet, 1 = Erste, 5 = Letzte)
Stunde	0
Minute	0
Sommerzeit	
Standardzeit-Differenz	0 min
Monat	0 (0 = Nicht verwendet)
Tag	0 (0 = Nicht verwendet)
Wochentag	0 (0 = Nicht verwendet 1 = Sonntag 7 = Sonnabend)
Woche	0 (0 = Nicht verwendet, 1 = Erste, 5 = Letzte)
Stunde	0
Minute	0

OK Abbruch

Konfigurieren der Zeitzone

Zeitzone	
Name	Africa Central East
ID	AFD
Standardzeit	
UTC-Differenz	60 min
Monat	10 (0 = Nicht verwendet)
Tag	0 (0 = Nicht verwendet)
Wochentag	0 (0 = Nicht verwendet 1 = Sonntag 7 = Sonnabend)
Woche	0 (0 = Nicht verwendet, 1 = Erste, 5 = Letzte)
Stunde	0
Minute	0
Sommerzeit	
Standardzeit-Differenz	60 min
Monat	2 (0 = Nicht verwendet)
Tag	1 (0 = Nicht verwendet)
Wochentag	0 (0 = Nicht verwendet 1 = Sonntag 7 = Sonnabend)
Woche	0 (0 = Nicht verwendet, 1 = Erste, 5 = Letzte)
Stunde	0
Minute	0

OK Abbruch

3.3.2.5 Datenbank-Management

Das Datenbank-Management bietet eine flexible Datensicherungs- und Wiederherstellungs-Verwaltung der OMM-Datenbank. Die OMM-Datenbank enthält alle Konfigurationseinstellungen, die über die WEB-Serviceschnittstelle konfiguriert werden können.

Die OMM-Datenbank kann

- manuell über das Webbrowser-Dateisystem oder von einem externen Server importiert werden
- automatisch von einem externen Server importiert werden
- manuell in das Webbrowser-Dateisystem oder zu einem externen Server exportiert werden
- automatisch zu einem externen Server exportiert werden, nachdem die Konfiguration geändert wurde

Verwaltung der Datenbank

Manueller Import	
Protokoll	FILE <input type="button" value="v"/>
Server	<input type="text"/>
Benutzername	<input type="text"/>
Kennwort	<input type="text"/>
Datei	<input type="text"/> <input type="button" value="Durchsuchen..."/>
<input type="button" value="Laden"/>	

Automatischer Import	
Nur Hochlauf	<input checked="" type="radio"/>
Hochlauf und periodisch	<input type="radio"/>
Uhrzeit	<input type="text" value="00"/> : <input type="text" value="00"/>
URL	-
<input type="button" value="OK"/>	

Manueller Export	
Protokoll	FILE <input type="button" value="v"/>
Server	<input type="text"/>
Benutzername	<input type="text"/>
Kennwort	<input type="text"/>
Datei	OMM_SIP_1F10187322_omm_conf.gz
<input type="button" value="Sichern"/>	

Automatischer Export	
Aktiv	<input type="checkbox"/>
Protokoll	HTTP <input type="button" value="v"/>
Server	<input type="text"/>
Benutzername	<input type="text"/>
Kennwort	<input type="text"/>
Datei	/081205_OMM_SIP_1F10187322_omm_conf.gz
<input type="button" value="OK"/>	

Die OMM-Datenbank wird komprimiert in einem proprietären Format abgespeichert. Änderungen an dieser Datei dürfen nur innerhalb von OMM durchgeführt werden.

Die folgenden Transportprotokolle zu bzw. von externen Servern werden unterstützt:

- FTP
- TFTP
- FTPS
- HTTP

- HTTPS

3.3.2.5.1 Manueller Datenbankimport

Um eine Datenbank über das Webbrowser-Dateisystem zu importieren, muss das Protokoll FILE ausgewählt werden.

Geben Sie den Pfad zur OMM-Datenbank und den Dateinamen ein, und drücken Sie die Schaltfläche „Laden“. Der OMM führt vor dem Import eine Prüfung der Datenbank durch. Wenn die Datenbank als gültig erkannt wurde, wird der OMM neu gestartet, um die neue Datenbank zu aktivieren.

Nach dem Neustart sind mit Ausnahme der Benutzerkonteneinstellungen alle Konfigurationsoptionen der wiederhergestellten Datenbank aktiv. Die Benutzerkonteneinstellungen können nur lokal über den OMM-WEB-Service geändert werden. Bei einem Datenbankimport werden sie nicht wiederhergestellt.

Manueller Import	
Protokoll	FILE <input type="button" value="v"/>
Server	<input type="text"/>
Benutzername	<input type="text"/>
Kennwort	<input type="text"/>
Datei	P:\open_mob\OMM_SIP_1F10187322_omm_conf.gz <input type="button" value="Browse..."/>
<input type="button" value="Laden"/>	

WARNUNG:Ein manueller oder automatischer Datenbankimport führt zu einem Neustart des OMM, damit die Änderungen aktiviert werden können.

Beim Import einer Datenbank von einem externen Server wird das bevorzugte Protokoll ausgewählt und die IP-Adresse oder der Name des externen Servers angegeben. Falls erforderlich, geben Sie die Kontodaten (Benutzername / Kennwort) des Servers ein und wählen Sie den Pfad und Namen der Datenbankdatei, die Sie wiederherstellen möchten. Anschliessend drücken Sie die Schaltfläche „Laden“.

Manueller Import	
Protokoll	HTTP <input type="button" value="v"/>
Server	172.30.206.29
Benutzername	horst
Kennwort	••••••••
Datei	/open_mob/OMM_SIP_1F10187322_omm_conf.gz
<input type="button" value="Laden"/>	

3.3.2.5.2 Manueller Datenbankexport

Beim manuellen Export einer Datenbank zu einem externen Server wird das bevorzugte Protokoll ausgewählt und die IP-Adresse oder der Name des Servers angegeben. Falls erforderlich, geben Sie die Kontodaten (Benutzername / Kennwort) des Servers ein und wählen Sie den Pfad und

Namen der Datenbankdatei, die Sie sichern möchten. Anschliessend drücken Sie die Schaltfläche „Sichern“.

Manueller Export	
Protokoll	HTTP
Server	172.30.206.29
Benutzername	horst
Kennwort	••••••••
Datei	/open_mob/OMM_SIP_1F10187322_omm_conf.gz
<input type="button" value="Sichern"/>	

Beim Export der Datenbank in das Dateisystem des Webbrowsers (Protokoll: FILE) wird die Datenbank in die vom Benutzer angegebene Datei gespeichert.

3.3.2.5.3 Automatischer Datenbankimport

Die Funktion für den automatischen Datenbankimport erleichtert das Wiederherstellen einer vorbereiteten OMM-Datenbank in den OMM zwecks Erstkonfiguration oder wegen eines Updates.

Der Pfad zu der für den automatischen Import vorgesehenen Datenbankdatei muss wie folgt angegeben werden:

{ftp|https|http|https}://[[Benutzer:Kennwort@]Server]/[Verzeichnis]/Datei

oder

tftp://Server]/[Verzeichnis]/Datei

Um sowohl während des OMM-Startvorgangs verfügbar zu sein als auch um eine Erstkonfiguration über den automatischen Import zu ermöglichen, muss diese URL über DHCP (Option 24 / siehe Kapitel 3.1.4) oder OM Configurator (siehe Kapitel 3.2) eingerichtet werden.

Wenn eine solche URL über DHCP oder den OM Configurator bereitgestellt wird, versucht der OMM während des OMM-Startvorgangs automatisch, eine konfigurierte Datenbank zu importieren.

Automatischer Import	
Nur Hochlauf	<input type="radio"/>
Hochlauf und periodisch	<input checked="" type="radio"/>
Uhrzeit	00 : 00
URL	http://172.30.206.29/restore/OMM_SIP_1F10187322_omm_config.gz
<input type="button" value="OK"/>	

Zusätzlich zum Import während des Startvorgangs ermöglicht der WEB-Service, den automatischen Datenbankimport zu einer konfigurierbaren Tageszeit zu aktivieren bzw. zu deaktivieren. Falls „Hochlauf und periodisch“ aktiviert wurde, versucht der OMM, die konfigurierte Datenbank sowohl während des Startvorgangs als auch zu der konfigurierten Tageszeit zu importieren.

Die über DHCP oder OM Configurator konfigurierte URL zu der Datei wird immer angezeigt.


WARNUNG: Beim automatischen Datenbankimport zu einer konfigurierten Tageszeit wird empfohlen, einen NTP-Server für die Zeitsynchronisation einzusetzen. Informationen zum Einrichten eines NTP-Servers finden Sie in den Kapiteln 3.1.4 und 3.2.

Bevor eine Datenbank als gültig akzeptiert und durch den automatischen Import ersetzt wird, führt der OMM folgende Prüfungen durch:





- Die Integrität der Datei muss gewährleistet sein
- Um zu verhindern, dass eine Datei mehrfach importiert wird, müssen sich die Prüfsummen der neuen Datenbankdatei und der zuletzt importierten Datenbankdatei (im Flash-Speicher hinterlegt) voneinander unterscheiden
- Bezüglich Berechtigungen/Authentifizierung:
Der PARK der neuen Datenbankdatei muss mit dem PARK der aktuellen Konfiguration übereinstimmen.
- Das Konto für den Administrator/vollständigen Zugriff der neuen Datenbankdatei muss mit dem der aktuellen Konfiguration übereinstimmen

Die Datenbankdatei wird nur dann akzeptiert, wenn alle Prüfungen erfolgreich abgeschlossen wurden.

Falls die Datenbankdatei abgelehnt oder nicht gefunden wurde, wird auf der Statusseite des OMM-WEB-Service eine Fehlermeldung angezeigt.


OpenMobility Manager

Abmelden

Status

- System
- Basisstationen
- Endgeräte
- WLAN
- Systemmerkmale
- Info

Status

Allgemein

OpenMobility Manager		
Laufzeit	0:11	
Flash-Speicherauslastung	2%	<div style="width: 2%; height: 10px; background-color: green;"></div>
Automatischer Datenbankimport	⚠ Fehlgeschlagen. 2008-12-02 15:16	

Standby-OMM

Zustand i Es ist kein OpenMobility Manager im Standby-Modus eingerichtet!

Basisstationen

Gesamtanzahl	2
Verbunden	1 <div style="width: 50%; height: 10px; background-color: blue;"></div>

WARNUNG: Ein manueller oder automatischer Datenbankimport führt zu einem Neustart des OMM, damit die Änderungen aktiviert werden können.

Der automatische OMM-Datenbankimport ermöglicht die Änderung aller Konfigurationseinstellungen mit Ausnahme der Kontoeinstellungen und PARK. Es gibt nur eine Ausnahme: Bei der Erstkonfiguration ist das Ändern des Standard-Benutzerkontos und des PARK möglich. Nach erfolgter

Erstkonfiguration können Benutzerkonten-Einstellungen und PARK nur über den WEB-Service des entsprechenden OMM selbst geändert werden.

3.3.2.5.4 Automatischer Datenbankexport

Die Funktion für den automatischen Datenbankexport ermöglicht die automatische Sicherung einer Datenbank auf einen externen Server nach jeder Konfigurationsänderung.

Bei Aktivierung dieser Funktion sendet der OMM eine Sicherungsdatei an einen konfigurierten externen Server, sobald eine Konfigurationsänderung erfolgt, zum Beispiel bei Anmeldung eines Endgerätes. Erfolgt keine Konfigurationsänderung, wird auch keine Sicherung durchgeführt. Eine Sicherungsdatei wird innerhalb eines Tages überschrieben, wenn mehr als eine Änderung erfolgte. Eine neue Datei wird angelegt, sobald die erste Konfigurationsänderung eines Tages erfolgt.

Der OMM schreibt die Datenbank in eine Datei auf dem externen Server, wobei folgende Namenskonvention gilt:

<jjmmmt>_<system_name>_<PARK>_omm_conf.gz

Automatischer Export	
Aktiv	<input checked="" type="checkbox"/>
Protokoll	HTTP
Server	172.30.206.29
Benutzername	horst
Kennwort	••••••
Datei	/backup /081202_OMM_SIP_1F10187322_omm_conf.gz
OK	

WARNUNG: Bei automatischen Datenbankexporten ist die Zeitsynchronisation mit einem NTP-Server zwingend erforderlich. Informationen zum Einrichten eines NTP-Servers finden Sie in den Kapiteln 3.1.4 und 3.2.

3.3.3 Konfigurieren der Basisstation

Alle konfigurierten RFPs sind in den Tabellen, in denen sie aufgeführt sind, abhängig von ihrer topographischen Lage in Cluster gruppiert. Die RFPs sind nach ihren Ethernet-Adressen (MAC-Adressen) sortiert.

Um das korrekte Handover eines PP während eines Anrufs sicherzustellen, müssen alle betreffenden RFPs das gleiche Taktsignal an das PP senden. Die RFPs müssen hierfür synchronisiert sein. Für die Synchronisation

werden die RFPs so nahe aneinander platziert, dass jedes RFP über seine Funkschnittstelle mindestens ein anderes RFP erkennt.

Unter bestimmten Bedingungen, beispielsweise bei weit entfernten RFPs, ist keine Synchronisation möglich. Die RFPs werden in diesem Fall unterschiedlichen Clustern zugeordnet. Der OpenMobility Manager versucht nicht, RFPs, die sich in unterschiedlichen Clustern befinden, miteinander zu synchronisieren.

Alle verwendeten Cluster werden in der Navigationsleiste links angezeigt. Das OMM-RFP erscheint in Fettdruck.

OpenMobility Manager

Abmelden

Status

System

Basisstationen

DECT-Cluster 1

DECT-Cluster 2

Endgeräte

WLAN

Systemmerkmale

Info

Basisstationen

Neu Importieren

Sortiert nach DECT-Cluster

Erfassen nicht konfigurierter Basisstationen

Start

Erfassung erlaubt: ✗

DECT-Cluster 1: 2 Basisstationen

Basisstation-ID	Standort	MAC-Adresse	IP-Adresse	HW-Typ	Verbunden	Aktiv
00	Aastra 31/314	00:30:42:0C:BE:04	172.30.206.94	RFP32	✓	✓
01	Aastra 31/316	00:30:42:0D:EE:67	-	-	✗	-

DECT-Cluster 2: 1 Basisstation

Basisstation-ID	Standort	MAC-Adresse	IP-Adresse	HW-Typ	Verbunden	Aktiv
02	Lab 1	00:30:42:0D:D4:7F	172.30.206.41	RFP42	✓	✓

RFPs, die eine Verbindung zum OMM herstellen, melden den Typ ihrer Hardware. Dieser Typ wird auf der Webseite mit der Liste der Basisstationen angezeigt.

3.3.3.1 Erzeugung und Änderung von RFPs

3.3.3.1.1 Schaltfläche "Neu". "Ändern" und "Löschen"

Mit der Schaltfläche „Neu“ können neue RFPs zum System hinzugefügt werden. In einem Popup-Fenster wird die Konfiguration des neuen RFP angezeigt.

Konfigurieren der Basisstation

Allgemeine Einstellungen	
MAC-Adresse	00:30:42:0D:EE:67
Standort	Aastra 31/434

DECT-Einstellungen	
DECT-Cluster	1

WLAN-Einstellungen	
WLAN-Profil	1
Antenna-Diversity	✓
Antenne	1
802.11b/g-Kanal	6
Ausgangsleistung	Voll

OK Abbruch

Jedes RFP ist durch seine MAC-Adresse (sechs Bytes im Hexadezimalformat, durch Doppelpunkte getrennt) gekennzeichnet. Die

Ethernet-Adresse ist eindeutig und auf der Rückseite des Gehäuses vermerkt.

Um die Verwaltung zu vereinfachen, kann jedem RFP eine Standort-Zeichenkette zugewiesen werden. Diese Standort-Zeichenkette kann bis zu 20 Zeichen lang sein.

Die DECT-Funktionen der einzelnen RFPs lassen sich ein- und ausschalten. RFPs mit aktivierten DECT-Funktionen können Clustern zugeordnet werden.


Der WLAN-Bereich steht nur dem RFP L42-WLAN zur Verfügung. Im Bereich 'WLAN-Einstellungen' der Seite können Sie Profil, Antennenvielfalt, Antenne, Ausgangsleistung und Kanal auswählen. Die Antennenvielfalt sollte generell aktiviert werden (d.h. angekreuzt), sodass der AP automatisch die Antenne mit den besten Übertragungs- und Empfangsmerkmalen auswählen kann.

Wichtiger Hinweis:

Ein RFP, das als OMM konfiguriert ist, kann nicht gleichzeitig als ein WLAN-Access Point betrieben werden.

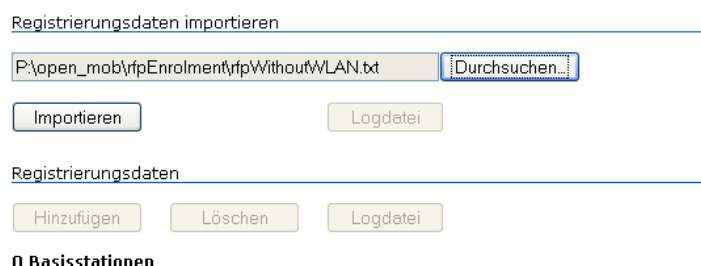
Einzelheiten zur WLAN-Konfiguration finden Sie in Kapitel 3.3.5.

Für bestehende RFPs lässt sich dieses Popup-Fenster durch Drücken des Werkzeugsymbols  des betreffenden RFP öffnen.

Mit dem Papierkorb-Symbol können RFPs gelöscht werden . Ein ähnliches Popup-Fenster bittet um Bestätigung und zeigt die aktuelle Konfiguration des betreffenden RFP an.

3.3.3.1.2 Import durch Konfigurationsdateien

Eine Reihe von RFPs kann auch halbautomatisch durch Import einer Konfigurationsdatei konfiguriert werden. Drücken Sie die Schaltfläche "Importieren", um in das entsprechende Untermenü zu wechseln.



Wählen Sie Ihre Konfigurationsdatei aus und drücken Sie die Schaltfläche "Importieren" (Informationen über das Dateilayout entnehmen Sie 8.3.2). Durch Drücken der entsprechenden "Logdatei"-Schaltfläche kann ein Parsingprotokoll gelesen werden. Alle erfolgreich importierten Datensätze werden in einer Liste angezeigt:

Registrierungsdaten importieren

Registrierungsdaten

3 Basisstationen

<input checked="" type="checkbox"/>	Standort	MAC-Adresse	DECT-Cluster	WLAN-Profil	Eingerichtet
<input checked="" type="checkbox"/>	142(Mirko)	00:30:42:08:31:A2	1	-	-
<input checked="" type="checkbox"/>	Lab1	00:30:42:0D:95:E0	1	-	-
<input checked="" type="checkbox"/>	Lab2(kiel)	00:30:42:0A:C5:40	2	-	-

Wählen Sie RFPs mit dem Optionsfeld aus und drücken Sie "Hinzufügen", um sie zur OMM-Datenbank hinzuzufügen.

Registrierungsdaten importieren

Registrierungsdaten

3 Basisstationen

<input type="checkbox"/>	Standort	MAC-Adresse	DECT-Cluster	WLAN-Profil	Eingerichtet
<input type="checkbox"/>	142(Mirko)	00:30:42:08:31:A2	1	-	✓
<input type="checkbox"/>	Lab1	00:30:42:0D:95:E0	1	-	✓
<input type="checkbox"/>	Lab2(kiel)	00:30:42:0A:C5:40	2	-	✓

Alle erfolgreich gespeicherten Sätze sind in der Spalte "hinzugefügt" grün gekennzeichnet (fehlgeschlagene Sätze erhalten einen roten Stern, Fehlerhinweise können in der entsprechenden Logdatei oder in einem Syslog-Trace gelesen werden.

3.3.3.1.3 Erfassung von RFPs

RFPs, die dem OMM über DHCP-Optionen oder OM-Configurator-Einstellungen zugewiesen werden, können an das System angeschlossen werden. Drücken Sie die entsprechende Schaltfläche "Start" auf der Webseite mit der RFP-Liste.

Nach einer Weile ist die Liste mit den MAC-Adressen derjenigen RFPs gefüllt, die versucht haben, sich beim OMM zu registrieren.

Basisstationen

Sortiert nach

Erfassen nicht konfigurierter Basisstationen

Erfassung erlaubt: ✓

Nicht konfiguriert: 2 Basisstationen

	Basisstation-ID	Standort	MAC-Adresse	IP-Adresse	HW-Typ	Verbunden	Aktiv
	-	-	00:30:42:0D:D4:7F	172.30.206.41	RFP42	-	-
	-	-	00:30:42:0C:BD:CA	172.30.206.97	RFP32	-	-

Beachten Sie bitte, dass diese Einträge nicht wirklich gespeichert werden (sie gehen nach dem Zurücksetzen verloren). Durch Drücken des Werkzeugsymbols des entsprechenden RFP können Sie weitere Daten hinzufügen und das RFP speichern.

3.3.3.2 RFP-Betriebszustände


Hier werden die Zustände der DECT-Subsysteme der einzelnen RFPs angezeigt. Folgende Zustände sind möglich:

Synchron

	Basisstation-ID	Standort	MAC-Adresse	IP-Adresse	HW-Typ	Verbunden	Aktiv
 	00	Aastra 31/314	00:30:42:0C:BE:04	172.30.206.94	RFP32	✓	✓



Das RFP ist gestartet und in Betrieb. Das RFP erkennt über seine Funkschnittstelle andere RFPs in seinem Cluster und wird von diesen erkannt. Es sendet ein synchrones Taktsignal an die PPs.

Asynchron

	Basisstation-ID	Standort	MAC-Adresse	IP-Adresse	HW-Typ	Verbunden	Aktiv
 	00	Aastra 31/314	00:30:42:0C:BE:04	172.30.206.94	RFP32	✓	✗



Das RFP konnte sich noch nicht mit seinen Nachbarn synchronisieren. Es ist keine DECT-Kommunikation möglich. Das RFP konnte jedoch bereits eine Verbindung zum OMM herstellen. Diese Phase sollte in der Regel nur einige Sekunden nach dem Start von RFP oder OMM andauern. Bleibt dieser Zustand längere Zeit bestehen, ist dies ein Anzeichen für einen Hardware- oder Netzwerkfehler.

Sucht

	Basisstation-ID	Standort	MAC-Adresse	IP-Adresse	HW-Typ	Verbunden	Aktiv
 	00	Aastra 31/314	00:30:42:0C:BE:04	172.30.206.94	RFP32	✓	🔍



Das RFP hat die Synchronisation mit seinen Nachbarn verloren. Es ist keine DECT-Kommunikation möglich. Diese Phase sollte in der Regel nur einige Sekunden nach dem Start von RFP oder OMM andauern. Bleibt dieser Zustand längere Zeit bestehen oder tritt er nach erfolgter Synchronisation erneut auf, ist dies ein Zeichen für einen schlecht gewählten RFP-Standort.

Inaktiv

	Basisstation-ID	Standort	MAC-Adresse	IP-Adresse	HW-Typ	Verbunden	Aktiv
 	00	Aastra 31/314	00:30:42:0C:BE:04	172.30.206.94	RFP32	✓	–

Das RFP hat die Verbindung zum OMM hergestellt, die Funkschnittstelle jedoch noch nicht eingeschaltet. Bei RFPs mit aktivierten DECT-Funktionen darf diese Phase nur einige Sekunden nach Start des RFP andauern. Bleibt dieser Zustand längere Zeit bestehen, ist dies ein Anzeichen für einen Hardwarefehler.

Nicht verbunden

	Basisstation-ID	Standort	MAC-Adresse	IP-Adresse	HW-Typ	Verbunden	Aktiv
 	00	Aastra 31/314	00:30:42:0C:BE:04	–	RFP32	✗	–

Das RFP wurde konfiguriert, hat jedoch noch keine Verbindung zum OMM hergestellt. Die Spalte „IP-Adresse“ ist deshalb leer.

3.3.3.3 Hardwaretyp des RFP


RFPs, die eine Verbindung zum OMM herstellen, melden den Typ ihrer Hardware. Dieser Typ wird auf der Webseite mit der Liste der Basisstationen angezeigt.

3.3.3.4 OMM-/RFP-Software-Versionsprüfung

RFPs, die eine Verbindung zum OMM herstellen, melden ihre Softwareversion. Weicht diese Version von der der OMM-Software ab, wird der Verbindungsversuch des RFP zurückgewiesen. Dies kann passieren, wenn Sie mehrere DHCP-Server mit unterschiedlichen Versionen der OpenMobility-Software verwenden. Das RFP wird in diesem Fall mit einer Fehlermeldung gekennzeichnet. Ausserdem wird auf der Webseite mit der RFP-Liste eine globale Fehlermeldung angezeigt, wenn mindestens eine Versionsabweichung erkannt wurde.

Basisstationen

Status

 Bitte Status-Seite überprüfen.


Neu

Importieren





Sortiert nach DECT-Cluster

Erfassen nicht konfigurierter Basisstationen

Start

Erfassung erlaubt: 

DECT-Cluster 1: 2 Basisstationen

	Basisstation-ID	Standort	MAC-Adresse	IP-Adresse	HW-Typ	Verbunden	Aktiv
	00	Aastra 31/314	00:30:42:0C:BE:04	172.30.206.94	RFP32		
	02	Lab	00:30:42:0D:D4:7F	172.30.206.41	Falsche Version (1.6.6)		

3.3.4 Endgeräte konfigurieren

Auf der Webseite „Endgeräte“ (PPs) sind alle konfigurierten DECT-Endgeräte nach Nummern sortiert aufgelistet. Um die Liste prägnant zu halten, ist sie in Unterlisten unterteilt, die bis zu 100 Endgeräte enthalten können. Der Benutzer kann in Schritten zu 100 Endgeräten vor- und zurückgehen. Da mit den Browserfunktionen keine Suche nach einem bestimmten Endgerät in allen Unterlisten möglich ist, steht eine Suchfunktion zur Verfügung, mit der Endgeräte nach einer bestimmten Nummer oder nach IPEI gesucht werden können.

Abmelden
 Status
 System
 Basisstationen
Endgeräte
 WLAN
 Systemmerkmale
 Info

Neu
 Importieren
 Suchen

Anmelden mit eingerichteten IPEIs

Stop

 PARK: 31100303462104

Anmelden ohne eingerichtete IPEIs

2 min

Start

 Anmelden erlaubt: ✓

1 - 5 (5) Endgeräte

Name	Rufnummer	IPEI	Eingebucht	Download
Manuela Mustermann	5140	-	✗	-
Daniel	5143	00750 0358349 4	✓	-
James B.	5144	00750 0290968 5	✓	-
Otto	5145	01271 0573185 9	✓	-
Isabelle	5146	01271 0562059 8	✓	-

Die Spalte „Download“ wird nur dann angezeigt, wenn die Funktion „Download neuer Firmware in die Endgeräte“ erfolgreich gestartet wurde. In dieser Spalte werden Informationen über den Downloadstatus angezeigt (siehe Kapitel 6).

3.3.4.1 Erzeugung und Änderung von PPs

3.3.4.1.1 Schaltfläche "Neu". "Ändern" und "Löschen"

Endgeräte zum SIP-DECT-System hinzufügen

Mit der Schaltfläche „Neu“ können neue PPs zum System hinzugefügt werden. Das neue PP kann dann in folgendem Popup-Fenster konfiguriert werden.

Neues Endgerät

Allgemeine Einstellungen	
Name	Tony
Rufnummer	5147
IPEI	0358600083186
DECT-Authentifizierungscode	1234
Zusatz-ID	101

SIP-Authentifizierung	
Benutzername	5147
Kennwort	••••
Kennwort-Bestätigung	••••

OK
 Abbruch

Der Parameter „Name“ entspricht dem SIP-Displaynamen. Dieser Parameter ist optional, sollte aber eingegeben werden.

Die „Nummer“ ist die SIP-Kontonummer oder der Anschluss des PP.

„IPEI“ ist die IPEI-Nummer des Endgeräts DECT 142. Sie finden sie im Menü Systemoptionen des Endgeräts DECT 142.

Während der ersten DECT-Anmeldung wird der DECT-Authentifizierungscode als Sicherheitsoption verwendet. Er kann hier für jedes PP getrennt eingestellt werden. Wurde auf der Webseite


„Systemeinstellungen“ ein globaler DECT-Authentifizierungscode eingegeben, wird dieser hier als Standardwert vorgegeben. Dieser Parameter ist optional.

Hinweis: Der Authentifizierungscode kann nur geändert werden, wenn das PP nicht angemeldet ist. Der Name des PP kann geändert werden. Dies wirkt sich jedoch erst aus, wenn das PP erneut angemeldet wird.

Die zusätzliche ID kann für die Datensuche innerhalb der Wildcard-Anmeldung verwendet werden (weil die IPEI, die die Daten sonst auswählt, nicht konfiguriert ist).

Der Benutzername unter „SIP-Authentifizierung“ ist optional, sollte aber eingegeben werden. Dies ist der Name, der für SIP-Registrierung und -Authentifizierung verwendet wird. Wird kein Name vergeben, wird standardmässig die Nummer verwendet. Das Kennwort wird für SIP-Registrierung und -Authentifizierung verwendet.

Endgeräte im SIP-DECT-System bearbeiten

Drücken Sie das Werkzeugsymbol , um ein vorhandenes PP zu konfigurieren. Ein Popup-Fenster wird angezeigt. Der einzige Unterschied zwischen diesem Fenster und dem für das Hinzufügen und Bearbeiten von Endgeräten ist das Kontrollkästchen „Anmeldung löschen“. Ist diese Option ausgewählt, wird das PP abgemeldet.

Endgeräte im SIP-DECT-System löschen

Mit dem Papierkorb-Symbol  können PPs gelöscht werden. Sie müssen diesen Vorgang in einem Popup-Fenster bestätigen.

3.3.4.1.2 Import durch Konfigurationsdateien

Eine Reihe von PPs kann auch halbautomatisch durch Import einer Konfigurationsdatei konfiguriert werden. Drücken Sie die Schaltfläche „Importieren“, um in das entsprechende Untermenü zu wechseln.

Endgeräte-Registrierung

Registrierungsdaten importieren

P:\open_mob\ppEnrolment\ppEnrolment.txt

Wählen Sie Ihre Konfigurationsdatei aus und drücken Sie die Schaltfläche „Importieren“ (Informationen über das Dateilayout entnehmen Sie 8.3.1). Durch Drücken der entsprechenden "Logdatei"-Schaltfläche kann ein Parsingprotokoll gelesen werden. Alle erfolgreich importierten Datensätze werden in einer Liste angezeigt:

Endgeräte-Registrierung

Registrierungsdaten importieren

Registrierungsdaten

12 Endgeräte

<input checked="" type="checkbox"/> Name	Rufnummer	IPEI	DECT-Authentifizierungscode	Zusatz-ID	Eingerichtet
<input checked="" type="checkbox"/> PP 1	101	0081008625768	1001	101	-
<input checked="" type="checkbox"/> PP 4	104	0007701154842	1002	104	-
<input checked="" type="checkbox"/> Kiel Phone1	5401	0127105395099	1003	5401	-
<input checked="" type="checkbox"/> Karl May	5402	-	1004	5402	-
<input checked="" type="checkbox"/> Karl Valentin	5403	-	1005	5403	-
<input checked="" type="checkbox"/> Karl Heinz	5404	-	1006	5404	-
<input checked="" type="checkbox"/> Radi Radenkowicz	5405	-	1007	5405	-
<input checked="" type="checkbox"/> Radi Rettich	5406	-	1008	5406	-
<input checked="" type="checkbox"/> Wadi Wade	5407	-	1009	5407	-
<input checked="" type="checkbox"/> Stephan	5408	0127105314450	1010	5408	-
<input checked="" type="checkbox"/> Waldi Hartmann	5409	-	1011	5409	-
<input checked="" type="checkbox"/> -	5410	-	1012	5410	-

Wählen Sie PPs mit dem Optionsfeld aus und drücken Sie "Hinzufügen", um sie zur OMM-Datenbank hinzuzufügen.

Endgeräte-Registrierung

Registrierungsdaten importieren

Registrierungsdaten

12 Endgeräte

<input type="checkbox"/> Name	Rufnummer	IPEI	DECT-Authentifizierungscode	Zusatz-ID	Eingerichtet
<input type="checkbox"/> PP 1	101	0081008625768	1001	101	✓
<input type="checkbox"/> PP 4	104	0007701154842	1002	104	✓
<input type="checkbox"/> Kiel Phone1	5401	0127105395099	1003	5401	✓
<input type="checkbox"/> Karl May	5402	-	1004	5402	✓
<input type="checkbox"/> Karl Valentin	5403	-	1005	5403	✓
<input type="checkbox"/> Karl Heinz	5404	-	1006	5404	✓
<input type="checkbox"/> Radi Radenkowicz	5405	-	1007	5405	✓
<input type="checkbox"/> Radi Rettich	5406	-	1008	5406	✓
<input type="checkbox"/> Wadi Wade	5407	-	1009	5407	✓
<input type="checkbox"/> Stephan	5408	0127105314450	1010	5408	✓
<input type="checkbox"/> Waldi Hartmann	5409	-	1011	5409	✓
<input type="checkbox"/> -	5410	-	1012	5410	✓

Alle erfolgreich gespeicherten Sätze sind in der Spalte "hinzugefügt" grün gekennzeichnet (fehlgeschlagene Sätze erhalten einen roten Stern, Fehlerhinweise können in der entsprechenden Logdatei oder in einem Syslog-Trace gelesen werden.

3.3.4.2 Anmeldung

Vorbereitung durch OMM-WEB-Service

Nachdem ein PP mit dem OMM konfiguriert wurde, muss es angemeldet werden. Zunächst muss der OMM so eingerichtet werden, dass er Anmeldungen von Endgeräten entgegennimmt. Dies geschieht durch Drücken der folgenden Schaltfläche auf der Webseite „Endgeräte“ des OMM.

- Start-Schaltfläche des Bereichs „Anmelden mit konfigurierten IPEIs“
Diese Schaltfläche aktiviert die Anmeldung für die nächsten 24 Stunden.

oder

- Start-Schaltfläche und Zeitintervall des Bereichs „Wildcard-Anmeldung“
Diese Schaltfläche aktiviert die „Wildcard-Anmeldung“ für den gewählten Zeitraum. Nach Ablauf ist die „Anmeldung mit konfigurierten IPEIs“ weiterhin für 24 Stunden aktiv.

Um die Erstinstallation eines DECT-Systems zu erleichtern, wird die Anmeldung dauerhaft aktiviert, wenn mindestens ein PP (mit IPEI) in der Datenbank eingerichtet ist und kein PP angemeldet ist. Nach erfolgreicher Anmeldung des ersten PP ist die Anmeldung weiterhin für 24 Stunden aktiv.

Anmeldeschritte, durchgeführt von PP

Jedes PP muss nach Abschluss seiner Konfiguration im OMM und bei für neue Anmeldungen freigeschaltetem OMM am System angemeldet werden.

Der Administrator oder der Benutzer muss jedes Endgerät im Menü „System/Anmeldungen“ am SIP-DECT-System anmelden. Für diese Anmeldung sollte der zum SIP-DECT-System gehörende, spezielle PARK-Code eingegeben werden.

WICHTIG: Der PARK-Code in numerischem Format steht in der oberen rechten Ecke der OMM-Webseite „Endgeräte“. Jede SIP-DECT-Installation besitzt einen eindeutigen PARK-Code, der mit dem OMM-Aktivierungskit mitgeliefert wird.

Hat der Administrator einen globalen oder individuellen DECT-Authentifizierungscode für die Endgeräte eingerichtet, muss der Administrator oder Benutzer diesen Code eingeben, bevor das Endgerät am System angemeldet werden kann.

Bei einer Wildcard-Anmeldung beachten Sie bitte, dass eine zusätzliche ID konfiguriert werden kann (siehe Unterkapitel "Wildcard-Anmeldung"), die dann eingegeben werden muss.

Treten beim Anmelden am SIP-DECT-System durch Administrator oder Benutzer Probleme auf, empfiehlt es sich, das Endgerät auszuschalten und die Anmeldung dann erneut zu versuchen.

Der Anmeldeprozess für das jeweilige Endgerät am SIP-DECT-System wird dadurch abgeschlossen.

3.3.4.2.1 Anmeldung mit konfigurierter IPEI

Die PP-Daten, die dem anmeldenden PP zuzuweisen sind, werden von der IPEI identifiziert. Des Weiteren sorgt die IPEI dafür, dass auch dann keine nicht autorisierten Anmeldungen empfangen werden, wenn keine Einstellung von AC zur Gewährleistung der Sicherheit vorgenommen wurde.

Drücken Sie die Schaltfläche "Start" des Bereichs "Anmeldung mit konfigurierten IPEIs":

- Der OMM lässt nun ausschließlich innerhalb der kommenden Stunde die Anmeldung eines konfigurierten aber noch nicht angemeldeten PP zu. Der Administrator muss die Schaltfläche „Anmelden“ erneut drücken, wenn er weitere Endgeräte an das SIP-DECT-System anmelden möchte.

3.3.4.2.2 Wildcard-Anmeldung

Zur Minimierung des Administrationsaufwands kann eine Anmeldung auch dann erfolgen, wenn die IPEI nicht konfiguriert ist. Da durch die IPEI-Prüfung die Sicherheit weiter verringert wird, ist diese Art der Anmeldung nur innerhalb eines kurzen voreingestellten Zeitintervalls von 2 Minuten erlaubt.

Drücken Sie zur Aktivierung von Anmeldungen die Schaltfläche „Start“ im Bereich „Wildcard-Anmeldung“ und erhöhen Sie bei Bedarf den Zeitintervall (oder aktualisieren Sie rechtzeitig die Anmeldegenehmigung).

- Mithilfe des OMM kann eine Wildcard-Anmeldung während des eingestellten Zeitintervalls durchgeführt werden. Bei Zeitüberschreitungen geht die Genehmigung verloren. Nur eine Anmeldung mit IPEI bleibt innerhalb einer festen zeitlichen Begrenzung von einer Stunde zulässig (siehe vorangehendes Kapitel).

Um eine Auswahl von Daten während der Anmeldung durchzuführen zu können (z.B. der Zuweisung des Benutzernamens zum PP); kann das Feld „Zusätzliche ID“ in OMM-Daten eingestellt werden. Wenn der OMM eine gültige "zusätzliche ID" während der Anmeldung erhält, werden die entsprechenden Daten dem PP zugewiesen.

Wird die zusätzliche ID für einen Datensatz angefordert wird, muss der PP-Benutzer diese eingeben. Die "zusätzliche ID" kann innerhalb der Menüs "Authentifizierungscode" eingestellt werden. Drücken Sie die Taste „R“ und geben Sie die zusätzliche ID ein.

WARNUNG:Nur bei Aastra DECT 142 / Aastra 142d kann eine zusätzliche ID eingegeben werden. Es besteht keine Möglichkeit, den Wert von dritten GAP-Telefonen einzugeben. Wenn GAP-Telefone Wildcard-Anmeldungen durchführen, wird der erste freie PP-Datensatz ohne zusätzliche ID ausgewählt und zugewiesen.

3.3.4.3 Suche innerhalb der PP-Liste

Endgeräte im SIP-DECT-System suchen

Mit der Suchfunktion kann der Benutzer ein bestimmtes Endgerät suchen. Mit der Schaltfläche „Suchen“ gelangt man zu folgendem Pop-up-Fenster.

Endgerät suchen

Allgemeine Einstellungen	
Rufnummer	104
IPEI	

OK Abbruch

Endgerät suchen

Allgemeine Einstellungen	
Rufnummer	
IPEI	0007701154842

OK Abbruch

Der Benutzer kann hier die Nummer oder IPEI des Endgeräts eingeben. Mindestens einer der Parameter muss angegeben werden. Die eingegebene Nummer oder IPEI muss genau mit der Nummer oder IPEI des Endgeräts übereinstimmen. Bei der Suche mit Nummer und IPEI muss das jeweilige Endgerät mit passender Nummer und mit dieser IPEI in der OMM-Datenbank eingetragen sein. Ansonsten wird es nicht gefunden.

Wird ein Endgerät mit angegebener Nummer und/oder IPEI gefunden, wird eine Liste angezeigt, in der das betreffende Endgerät an erster Stelle steht. Die Suchfunktion kann auch dazu verwendet werden, in einem einzigen Schritt die gewünschte Unterliste zu erhalten.

Endgeräte

Neu Importieren Suchen

Anmelden mit eingerichteten IPEIs

Stop PARK: 31100303462104

Anmelden ohne eingerichtete IPEIs

2 min Start Anmelden erlaubt: ✓

← Vorherige Seite 2 - 19 (19) Endgeräte

Name	Rufnummer	IPEI	Eingebucht	Download
PP 4	104	00077 0115484 2	✗	-
PP 5	105	00077 0115817 1	✗	-
PP 6	106	00077 0115822 7	✗	-

3.3.5 WLAN-Konfiguration (nur RFP L42-WLAN)

Für die richtige Konfiguration eines RFP mit einem WLAN-Teil muss der DECT-Teil richtig konfiguriert werden. Im zweiten Schritt wird die Regulierungsdomäne des WLAN-Netzwerks auf der System-Webseite des OMM-Webservice festgelegt.

Regulierungsdomäne	Land
0x10: FCC	USA, Australien
0x20: IC	Kanada
0x30: ETSI	Europa (ausgenommen Spanien, Frankreich)
0x31: SPANIEN	Spanien
0x32: FRANKREICH	Frankreich
0x40: MKK	Japan
0x41: MKK1	Japan (MKK1)

Diese Einstellung hängt von dem Land ab und unterliegt den gesetzlichen Vorschriften dieses Landes. Nur die für dieses Land vorgeschriebene Einstellung darf verwendet werden.



OpenMobility Manager

Abmelden

Status

- ▼ System
- Systemeinstellungen**
- SIP
- Benutzerverwaltung
- Zeitzone
- Verwaltung der DB
- Basisstationen
- Endgeräte
- WLAN
- Systemmerkmale
- Info

Port

Wenn Sie die WLAN-Regulierungsdomäne ändern, werden alle Access-Points deaktiviert.

WLAN-Einstellungen

Regulierungsdomäne

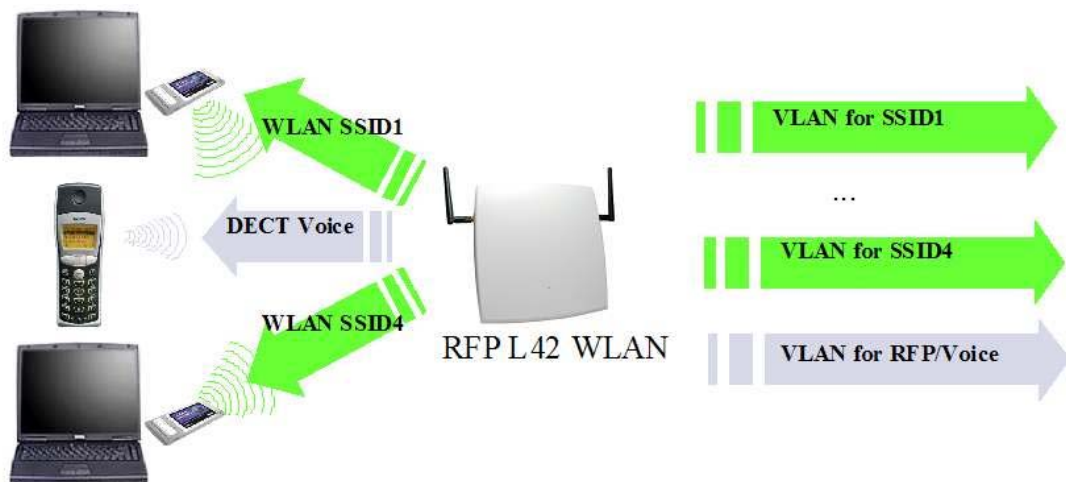
Datum und Uhrzeit

Zeitzone

Lokale Uhrzeit im Format HH:MM:SS : :

Lokales Datum im Format DD-MM-YYYY - -

Der dritte Schritt ist die Festlegung der WLAN-Parameter in einem Profil. Hier tragen Sie den Namen (SSID) des WLAN-Netzwerks und andere Parameter ein. Die Verschlüsselungs- und Authentifizierungsverfahren sind besonders wichtig und müssen vorab sorgfältig geplant werden.



Der Access Point kann einen VLAN zugewiesen werden, das 802.1q entspricht. Alle Daten, die von den WLAN-Clients empfangen werden und an sie weitergeleitet werden sollen, werden von einem VLAN übertragen. Alle Daten, die diese Bedingung nicht erfüllen, wie beispielsweise VoIP-Pakete, Konfigurations- oder Authentifizierungsdaten (Radius) erhalten den VLAN-Code des RFP. Der Port der Netzwerkkomponente, an die der Access Point angeschlossen ist, muss als Trunk-Port konfiguriert werden. Die Werte der Profilparameter sind voreingestellt.

Parameter	Bereich	Notizen
Bakenzeitraum	50 – 65.535 Millisekunden	Die Länge des Intervalls zwischen Baken
DTIM-Zeitraum	1 - 255 Baken	Die Anzahl der Baken zwischen zwei DTIM-Übertragungen (Delivery Traffic Indication Map).
RTS-Schwellenwert	0 – 4.096 Bytes	Unicast- und Management-Frames, die den hier spezifizierten Schwellenwert überschreiten, werden durch ein RTS/CTS-Handshake-Verfahren übertragen.
Fragmentierungsschwellenwert	0 – 4.096 Bytes	Unicast-Frames, die den hier spezifizierten Schwellenwert überschreiten, werden fragmentiert.
Maximale Rate	1; 2; 5,5; 6; 9; 11; 12; 18; 22; 24; 36; 48; 54 Mbps	Die maximale Übertragungsrate zwischen WLAN AP und dem WLAN-Client
802.11 b/g-Modus	Gemischt, nur b, nur g	802.11-Verbindungsmodus.
Versteckte SSID	Ja/Nein	Unterdrückt Übertragung der SSID.
Störungsvermeidung	Ja/Nein	Ein Verfahren zu Vermeidung von Störungen.
Sicherheitseinstellungen		Verschlüsselungseinstellungen (siehe unten)
MAC-Zugangsfiler	1 – 64	Autorisierte Clients (Whitelist)
BSS Isolierung	Ja/Nein	Verhindert, dass WLAN-Clients sich gegenseitig entdecken.
Chiffrelänge	64 / 128 / 256 Bits	Die Länge des Schlüssels, der in den Sicherheitsmodi verwendet wird.
Verteilungsintervall	Sekunden	Der Intervall zwischen Schlüsselaustauschereignissen.
Radiuseinstellungen	IP-Adresse, Port, Geheim	Radius-Servereinstellungen

Mehrfach-SSID-Einstellungen	SSID Name, VLAN- und Sicherheitseinstellungen	1 bis 3 zusätzliche SSIDs
-----------------------------	---	---------------------------

Sie konfigurieren ein offenes System, d.h. ein System, in dem alle Authentifizierungs- und Verschlüsselungsverfahren deaktiviert sind, durch Auswahl des Menüpunkts "Offenes System".

Der „BSS-Isolationsparameter“ verhindert, dass WLAN-Clients sich gegenseitig **mittels ein und desselben AP** kontaktieren.

Hinweis: Das RFP L42 WLAN muss an ein 100BaseT-Ethernet angeschlossen werden, damit das WLAN betriebsbereit ist.

3.3.5.1 Optimierung des WLAN

Bakenintervall

Für die Übertragung von Baken wird Übertragungskapazität benötigt. Durch die Verringerung des Bakenintervalls ist das WLAN-Netzwerk besser in der Lage, Signale zu erkennen und seine Verfügbarkeit wird verbessert. Gleichzeitig kann das Netzwerk die gegenseitig ausgehandelte Signalstärke besser anpassen. Ein höherer Wert, d.h. ein längerer Bakenintervall, verringert indirekt den Stromverbrauch des WLAN-Clients.

RTS-Schwellenwert

Wenn der Netzwerkdurchsatz gering ist oder viele Übertragungswiederholungen erfolgen, kann durch die Verringerung des RTS-Schwellenwerts eine RTS-Reinigung aktiviert werden. Dies kann zu einer Verbesserung des Durchsatzes führen, insbesondere in Umgebungen, wo Reflexion und Dämpfungen Probleme für HF verursachen.

Fragmentierungsschwellenwert

In Umgebungen, die durch viele Störungen und schlechte Funkqualität gekennzeichnet sind, kann die Verringerung der Fragmentgröße den effektiven Durchsatz verbessern. In diesem Fall müssen die übertragenen Frames jedoch häufiger fragmentiert werden. Dies bedeutet eine höhere Belastung des AP-Prozessors.

DTIM-Zeitraum

Der DTIM-Zeitraum bestimmt den Intervall zwischen Übertragungen der Broadcast- und Multicast-Pakete. Alle WLAN-Clients müssen während diesem Intervall aktiv sein. Durch Verlängerung des DTIM-Zeitraums wird der Stromverbrauch der Clients leicht verringert. Allerdings sind nicht alle Programme in der Lage, die Steigerung bei den Antwortzeiten zu bewältigen.

3.3.5.2 Sicherstellung des WLAN mit Radius

Um sicherzustellen, dass die Kommunikation im WLAN-Netzwerk sicher ist, sind verschiedene Maßnahmen zu ergreifen. Als erstes müssen Datenpakete durch öffentlich sichtbaren Funkschnittstelle verschlüsselt werden und dann

sollten sich alle Komponenten, die Teil des Netzwerks sind oder Dienste bereitstellen, selbst authentifizieren müssen.

Hierzu erstellen Sie ein sogenanntes “AAA”-System (Authentifizierung, Autorisierung, Abrechnung). Das RFP L42-WLAN dient als Netzwerkzugangsserver und ein Radius-Server dient als AAA-Server.

Das RFP L42-WLAN dient als Netzwerkzugangsserver und kann die Authentifizierung an einen Radiusserver im Netzwerk weiterleiten.

Die Verschlüsselung der zwischen dem RFP L42 WLAN und dem WLAN-Client übertragenen Daten erfolgt entweder mittels WPA (Wi-Fi Protected Access) mit 802.1x (Radius) oder „802.1x (Radius)“ mit WEP-Verschlüsselung. Die Server-IP-Adresse, der IP-Port und das gemeinsame Passwort müssen in das Radius-Profil eingegeben werden.

Ein Radius-Server (Remote Authentication Dial in User Service) übernimmt die 802.1x-Authentifizierung und Client-Autorisierung.

Wir empfehlen die Verwendung eines Radius-Servers mit EAP-TLS (z.B. FreeRadius oder MS Windows 2003 IAS Server) und eine Zertifizierungsstelle (CA).

Ihr WLAN-Client muss diese Authentifizierungsmethode unterstützen und die entsprechenden Zertifikate besitzen (trifft auf die meisten WLAN-Clients zu). Zur Erzeugung der Schlüssel wird eine Zertifizierungs-Site benötigt, die dem WLAN-Client und dem Radius-Server bekannt gemacht werden muss.

Sie müssen die IP-Adresse des Radius-Servers, den IP-Port und den gemeinsamen geheimen Schlüssel im Radiuseinstellungsbereich eingeben.

Abmelden

Status

System
Basisstationen
Endgeräte
WLAN
WLAN-Profil
WLAN-Stationen
Systemmerkmale
Info

WLAN-Profil 1: 0 Access-Points

OK

Abbruch

Allgemeine Einstellungen

☒ Profil aktiv

SSID

RFPL42SipTest

VLAN-Tag

[1 .. 4094]

Beacon-Periode

100

ms [50 .. 65535]

DTIM-Periode

5

Beacon(s) [1 .. 255]

RTS-Schwellwert

2346

Byte(s) [0 .. 4096]

Fragmentierungsschwellwert

2346

Byte(s) [0 .. 4096]

Maximale Bitrate

54

MBit/s

802.11b/g-Modus

Mixed

Versteckter SSID-Modus

☐

Vermeiden von Interferenzen

☐

Sicherheitseinstellungen

☐ Open-System

☐ Wired-Equivalent-Privacy (WEP)

Authentifizierung

☐

Anzahl der Tx-Keys

1

als Text

Standard-Tx-Key

1

Key #1

Erzeugen

Key #2

Erzeugen

Key #3

Erzeugen

Key #4

Erzeugen

☒ WiFi-Protected-Access (WPA)

Typ

WPA beliebig

802.1x (Radius)

☒

Pre-Shared-Key

☐

Wert

E008A2CBB57852C2AA4A

als Text

Erzeugen

☐ 802.1x (Radius)

☐ MAC-Access-Filter

Konfigurieren

☐ BSS-Isolation

Key-Konfiguration

Cipher-Länge

256 Bits

Distributionsintervall

120

s [1 .. 65535]

Radius-Konfiguration

IP-Adresse

172.30.51.123

Port

1812

Standard

Schlüssel

12Wedstr.

QoS-Konfiguration

☐ WME mit

VLAN

Mehrfach-SSID

☐ SSID2

☐ SSID3

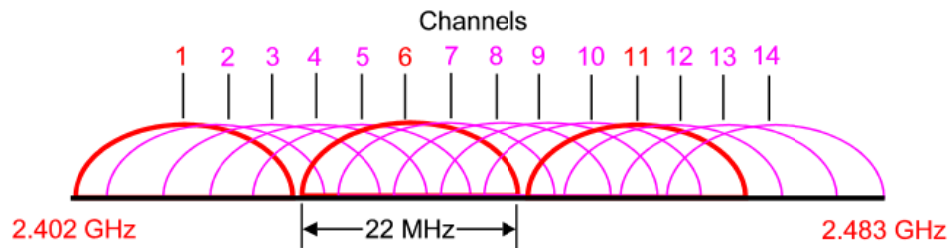
☐ SSID4

Als letztes muss den RFPs / Access Points (APs) ein Profil zugewiesen werden. Jeder AP muss für einen Kanal konfiguriert sein. Stellen Sie hierfür sicher, dass sich die Frequenzen der AP-Kanäle nicht überlappen. APs, die sich innerhalb des Bereichs anderer APs befinden, müssen mindestens fünf Kanäle voneinander entfernt sein. Dies wird im AP-Konfigurationsbildschirm konfiguriert. Bei der Planung des Funkfelds müssen die APs aller anderen WLANs die in der nahen Umgebung in Betrieb sind, berücksichtigt werden.

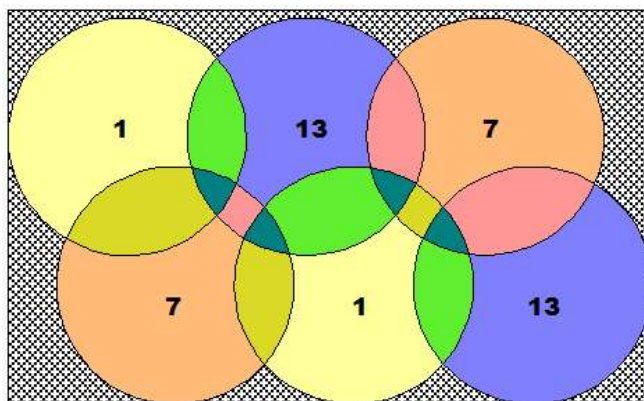
Aastra

depl-0900/1.8

Seite: 64 (107)



Denken sie bei der Planung der Funkübertragung für einen zweidimensionalen Bereich daran, dass der Abstand zwischen zwei Basisstationen, die auf der gleichen Frequenz arbeiten, mindestens doppelt so groß wie ihre Reichweite sein muss. Die Reichweite kann mithilfe des Ausgangsleistungsstufenparameters angepasst werden.



Neue APs können hinzugefügt und konfigurierte RFPs können einem WLAN-Netzwerk mithilfe des Menüs "Basisstationen" zugewiesen werden. Wählen Sie hierfür unter „Sortiert nach“ den Eintrag „WLAN-Profil“.

Abmelden

- Status
- System
- Basisstationen**
 - WLAN-Profil 1
 - Inaktiv
 - Endgeräte
- WLAN
- Systemmerkmale
- Info

Access-Points

Neu Importieren

Sortiert nach WLAN-Profil

Erfassen nicht konfigurierter Access-Points

Start Erfassung erlaubt: ✗

WLAN-Profil 1: 1 Access-Point

Standort	MAC-Adresse	IP-Adresse	HW-Typ	Sender aktiv	Kanal
Lab	00:30:42:0D:D4:7F	172.30.206.41	RFP42	✓	6

Inaktiv: 1 Access-Point

Standort	MAC-Adresse	IP-Adresse	HW-Typ	Sender aktiv	Kanal
Aastra 31/314	00:30:42:0C:BE:04	172.30.206.94	RFP32	–	–

Konfigurieren der Basisstation	
Allgemeine Einstellungen	
MAC-Adresse	00:30:42:0D:D4:7F
Standort	Lab
<input checked="" type="checkbox"/>	DECT-Einstellungen
DECT-Cluster	1
<input checked="" type="checkbox"/>	WLAN-Einstellungen
WLAN-Profil	1
Antenna-Diversity	<input checked="" type="checkbox"/>
Antenne	1
802.11b/g-Kanal	6
Ausgangsleistung	Voll
<input type="button" value="OK"/> <input type="button" value="Abbruch"/>	

Im Bereich “WLAN-Einstellungen” der Seite können Sie Profil, Antennenvielfalt, Antenne, Ausgangsleistungsstärke und Kanal auswählen. Die Antennenvielfalt sollte generell aktiviert werden (d.h. angekreuzt), sodass der AP automatisch die Antenne mit den besten Übertragungs- und Empfangsmerkmalen auswählen kann. Der WLAN-Bereich steht nur dem RFP L42-WLAN zur Verfügung.

WICHTIG: Ein RFP, das als OMM konfiguriert ist, kann nicht gleichzeitig als ein WLAN-Access Point betrieben werden.

3.3.5.3 Anforderungen für das WLAN

WLAN-Adapter nach den Standards 802.11b oder 802.11g sind eine Voraussetzung für den Betrieb von WLAN-Clients. In Bezug auf WEP- und WPA-Verschlüsselung und die Verwendung einer Radius-Infrastruktur muss sichergestellt werden, dass die WLAN-Netzwerkadapter, die unter dem Client-Betriebssystem betrieben werden, die entsprechenden Modi unterstützen. Die Funktionsfähigkeit der Adapter muss jedoch vor ihrem Einsatz stets geprüft werden.

3.3.6 Systemfunktionen

3.3.6.1 Zentrale Konfiguration des LDAP-Zugangs

Folgende Parameter werden über den OMM-Webdienst eingestellt. Die Konfiguration betrifft alle Endgeräte, für die Namenwahl über LDAP aktiviert ist. Der OMM unterstützt LDAP Simple Bind.

Abmelden

- Status
- System
- Basisstationen
- Endgeräte
- WLAN
- Systemmerkmale
 - Digit-Treatment
 - Telefonbuch**
 - Service-Codes
 - Info

Telefonbuch

OK Abbruch

Allgemeine Einstellungen	
Typ	LDAP ▼
LDAP	
Server-Name	my.ldap.com
Server-Port	389
Suche-Optionen	ou=people,o=my.com
Benutzername	cn=that's me,ou=people,o=my.com
Kennwort	••••••••
Suche-Typ	Nachname ▼
Anzeige-Typ	Nachname, Vorname ▼
Timeout für Server-Suche	10 s

Feldbeschreibung:

- **Servername und Serverport** (erforderlich)
 - Name oder IP-Adresse des Servers
 - Serverport (Standardeinstellung: 389)Hinweis: SSL (Standardport 689) wird nicht unterstützt
- **Root-Verzeichnis**

Die Suchbasis muss bearbeitet werden (z.B. „ou=people,o=my com“).
- **Benutzername und Benutzer-Passwort**

Falls vom LDAP-Server angefordert, kann hier ein Benutzername (eindeutig) und ein Passwort eingegeben werden. Ansonsten wird eine anonyme Bindung hergestellt.

Hinweis: Der DECT-IP-OMM unterstützt LDAP Simple Bind.
- **Suchattribut**

Gesucht wird nach einem der folgenden Attribute:

 - Name (Nachname) -> (Standardeinstellung) // Nachname
 - Vorname (Vorname)
- **Anzeigeattribute**

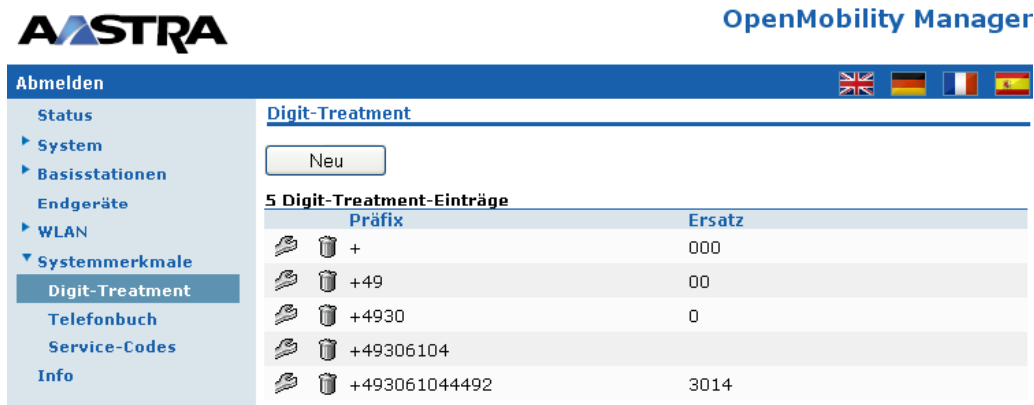
Folgende beiden Alternativen sind möglich:

 - Name (Nachname), Vorname (Vorname) -> Standardeinstellung
 - Vorname (Vorname) und Name (Nachname)
- **Such-Timeout des Servers**

(Werte zwischen: 1 und 99 s)

Suchergebnisse werden während der Suchzeit akzeptiert.

3.3.6.2 Stellenbehandlung



Präfix	Ersatz
+	000
+49	00
+4930	0
+49306104	
+493061044492	3014

Die Stellenbehandlung ersetzt, löscht oder ergänzt Stellen in Nummern, die vom LDAP-basierten Unternehmens-Telefonbuch geliefert werden.

Die Nummern werden in zwei Schritten bearbeitet:

- Zunächst werden alle ungültigen Zeichen wie Leerstellen oder Bindestriche aus der Nummer gelöscht (Beispiel: „+49 (30) 6104 4492“ wird zu +493061044492).
- Im zweiten Schritt wird in der eingerichteten Vorwahlliste die beste Übereinstimmung gesucht. Die Vorwahl wird ersetzt. (Beispiel: Die beste Übereinstimmung für „+493061044492“ ist die Vorwahl „+49306104“, die durch „“ ersetzt wird. Das Ergebnis ist „4492“.)

Die Stellenbehandlung erfolgt vor dem Weiterleiten der Nummer an das Endgerätemenü.

Wertebereiche und Höchstwerte:

- Es sind bis zu 128 Einträge möglich, wenn der OMM auf einer IP-DECT-Basisstation läuft. Läuft der OMM auf einem Linux-Server, sind bis zu 750 Einträge möglich.
- Jede Vorwahl kann aus den Ziffern 0 bis 9 und den Zeichen ‘*’ und ‘#’ bestehen. Gemäss LDAP-Standard kann das erste Zeichen ein ‘+’ sein. Pro Sequenz sind bis zu 15 Stellen zulässig. Leerzeichen sind nicht erlaubt.
- Jede ersetzte Nummer kann aus den Ziffern 0 bis 9 und den Zeichen ‘*’ und ‘#’ bestehen.

3.3.6.3 Service-Codes

Durch Service-Codes können mit jedem angemeldeten DECT-Endgerät bestimmte Aktionen auf dem OMM ausgeführt werden.

Abmelden

Status

System

Basisstationen

Endgeräte

WLAN

Systemmerkmale

Digit-Treatment

Telefonbuch

Service-Codes

Info

Service-Codes

Status

⚠

Bitte Status-Seite überprüfen.

OK

Abbruch

Allgemeine Einstellungen

Service-Code-Nummer

99999

Service-Code-Aktion

Anmelden erlaubt

☒

*4701#

Anmelden ohne eingerichtete IPEI erlaubt

☒

*4702#

Anmelden gesperrt

☒

*4799#

Um einen Service-Code zu aktivieren, wählen Sie eine eindeutige Service-Code-Nummer aus, markieren das entsprechende Kontrollkästchen und weisen einen Aktions-Code zu.

Daraufhin kann die entsprechende Aktion durch Wählen der „Service-Code-Nummer“ gefolgt von dem „Service-Aktions-Code“ (als Ganzes einzugeben) mit jedem angemeldeten DECT-Endgerät durchgeführt werden.

Im oben dargestellten Beispiel kann ein angemeldeter Benutzer die OMM-DECT-Anmeldung durch Wählen von „99999*4701#“ aktivieren.

WARNUNG: Overlap-Sending wird bei Service-Codes nicht unterstützt. Die „Service-Code-Nummer“ und der „Service-Aktions-Code“ müssen zusammenhängend eingegeben werden.

Die Ausführung von Service-Code-Funktionen wird dem Benutzer durch ein akustisches Signal mitgeteilt (Innenband-Signale).

Aastra

depl-0900/1.8

Seite: 69 (107)

4 Sicherheit

4.1 Das Sicherheitskonzept

Zusätzlich zum https-Zugang des OMM verfügt jedes einzelne RFP über zwei Zugangsmöglichkeiten: den OM Configurator und einen ssh-Zugang. Jeder dieser 3 unabhängigen Zugangstypen verwendet die gleichen Kontodaten.

Die Kontodaten können an der https-Schnittstelle des OMM geändert werden. Das OMM liefert alle erforderlichen Kontendaten an alle angeschlossenen RFPs. Die RFPs speichern die Kontendaten in ihrem permanenter Speicher.

Dies hat einige Auswirkungen:

- Ein RFP im Auslieferungszustand verwendet die Standardkontendaten solange die RFP noch nicht an den OMM angeschlossen ist.
- Ein RFP, das bereits mindestens einmal an das OMM angeschlossen wurde, verwendet die Kontendaten aus dem OMM.
- Bei Änderung der Kontodaten auf dem OMM verwenden alle nicht angeschlossenen RFPs die alten Passwörter weiter.

4.2 Kontotypen

Es gibt 3 verschiedene Kontotypen:

1. Vollzugang

Dieser Zugangstyp ist der "normale" Zugang für alle Konfigurationen. Bei Verwendung dieses Zugangs dürfen der OMM und jedes RFP konfiguriert werden. Der Zugangstyp ermöglicht die Anmeldung auf der ssh-Schnittstelle eines RFP für Debug-Informationen wie z.B. "Pingen" eines anderen RFPs, um die Sichtbarkeit zu prüfen.

Die werkseitige Einstellung für dieses Konto lautet

Name: 'omm'
Passwort: 'omm'
Aktiv: 'n/a'

2. Nur-Lese-Zugriff

Wie der Name schon sagt, ist die Zugangstyp für keine Konfigurierung auf der OMM-Installation zulässig. Dieser Zugangstyp ist nur auf der https-Schnittstelle zulässig. Das Konto kann deaktiviert werden.

Die werkseitige Einstellung für dieses Konto lautet

Name: 'user'
Passwort: 'user'
Aktiv: 'ja'

3. Root-Zugang

Dieser Zugangstyp ist nur auf der ssh-Schnittstelle eines RFPs anwendbar. Mit ihm sollen detaillierte Informationen erhalten werden, z.B. Parameter aus dem Kernel. Zugänge, die diesen Kontotyp verwenden, können von anderen Hosts nicht erreicht werden, da für die Verwendung des vollen Zugangstyps eine Anmeldung erforderlich

ist.

WICHTIG: Es wird dringend empfohlen, diesen Kontotyp nicht zu benutzen. Er ist nur für den technischen Support bestimmt.

Die werkseitige Einstellung für dieses Konto lautet

Name: 'root'
 Passwort: '22222'
 aktiv: 'n/a'

	https	OM Configurator	ssh
Vollständiger Zugang	zugelassen	zugelassen	zugelassen
Schreibgeschützter Zugang	Zugelassen (aber nicht erlaubt, um Konfiguration zu ändern)	Nicht zugelassen	Nicht zugelassen
Root-Zugang	Nicht zugelassen	Nicht zugelassen	Zugelassen (aber nicht direkt von anderen Hosts)

4.3 Änderung von Kontodaten

Der OMM zwingt den Benutzer die voreingestellten Benutzerdaten in seine eigenen Einstellungen zu ändern. Solange die Passwörter nicht geändert werden, erlaubt der OMM keine andere Konfiguration.



Zur Änderung des Passworts muss das alte Passwort wieder eingegeben werden. Das OMM verfügt über verschiedene Regeln zur Prüfung der Komplexität eines neuen Passworts, somit wird ein neues Passwort nicht akzeptiert, wenn irgendeine dieser Regeln verletzt wird.

- Das neue Passwort ist nicht 5 oder mehr Zeichen lang,
- Das neue Passwort enthält keine Zeichen aus mindestens 3 der folgenden Gruppen: Kleinschrift, Großschrift, Ziffern oder sonstige Zeichen,

- Mindestens 50% des neuen Passwort bestehen aus dem gleichen Zeichen ('World11111' oder 'W1o1r1l1d1')
- Das neue Passwort enthält eines der folgenden Elemente (entweder in Groß- oder Kleinschrift sowie vorwärts oder rückwärts).
 - Kontoname
 - Hostname (IP-Adresse)
 - Altes Passwort oder
 - einige nebeneinander liegende Tastenanschläge (z.B. "qwert").

4.4 Potenzielle Fallgruben

Wird ein über OM Configurator konfiguriertes RFP aus einer Installation entfernt, kann es unbenutzbar werden.

- Ein solches RFP findet in seinem permanenten Speicher eine gültige Konfiguration. Es wird also DHCP für den Bootvorgang überspringen.
- Wenn diese Konfiguration allerdings nicht mehr gültig ist (z.B. der TFTP-Server hat inzwischen eine neue IP-Adresse, ist das RFP nicht in der Lage, den Bootvorgang abzuschließen, und kann somit keine Verbindung zum OMM herstellen.
- Der RFP erhält keine neueren Passwörter aus dem OMM.

Es wird daher empfohlen, die OM-Konfiguration auszuschalten, bevor ein RFP aus einer Installation entfernt wird. Dennoch kann mithilfe des OM Configurator der permanente Speicher eines RFP zurückgesetzt werden (die Verbindung zum Aastra DeTeWe-Support muss hergestellt sein).

5 OMM-Resiliency

Um die Funktion OMM-Resiliency auszuführen, müssen zwei OpenMobility Manager in einem OMM-Netzwerk bereitgestellt werden. Einer arbeitet als "Master"-OMM und der andere als fehlertoleranter oder Standby-OMM.

Falls das als OMM bestimmte RFP ausfällt, übernimmt das andere RFP, das als sekundärer OMM bestimmt wurde, automatisch die Rolle des OpenMobility Managers.

5.1 Wie OMM Resiliency (Fehlertoleranz) arbeitet

Während des Systemanlaufs ruft jedes IP-RFP entweder eine (bei keiner OMM-Fehlertoleranz) oder zwei (bei Konfiguration von OMM-Resiliency) OMM IP-Adressen auf und beide versuchen, miteinander eine Verbindung herzustellen. Der aktive oder „Master“-OMM bedient alle Verbindungen von den RFPs. Der Reserve- oder Standby-OMM verweigert alle Verbindungsversuche von RFPs.

5.2 Einleitung

Während des Normalbetriebs ist der aktive und der Standby-/Reserve-OMM in Kontakt und überwachen gegenseitig ihren Betriebszustand. Sie tauschen ständig ihre aktuellen Fehlertoleranz-Zustände und der Standby-OMM empfängt eine Kopie aller Konfigurationsänderungen auf dem aktiven OMM. Wenn sich beide OMMs miteinander in Kontakt befinden, werden ihre Datenbanken automatisch synchronisiert.

Wenn der Haupt-OMM ausfällt, werden die OMM-Aufgaben vom Standby-OMM zur Aufrechterhaltung des Betriebs übernommen. Auf der OMM-Webschnittstelle wird eine "No Resiliency"-Warnung ("Keine Fehlertoleranz") angezeigt, die darauf hinweist, dass sich im Netzwerk oder Cluster nicht mehr länger zwei funktionierende OMMs befinden. Konfigurationsänderungen können in diesem Zustand nicht sicher durchgeführt werden.

Der Ausfall des aktiven OMM wird vom inaktiven OMM erkannt. Dieser beginnt als aktiver OMM zu arbeiten und der Webservice wird gestartet. Alle vom OMM gepflegten IP RFPs werden neu gestartet und alle Endgeräte werden neu synchronisiert. Wenn die Verbindung zwischen den beiden OMMs ausfällt, teilt sich das Netzwerk oder der Cluster im Wesentlichen in zwei betriebsfähige Teile. Der fehlertolerante oder Standby-OMM wird jetzt der aktive OMM. Zu diesem Zeitpunkt können sich die OMMs nicht gegenseitig entdecken und somit keine Synchronisation durchführen. Wenn die Verbindung zwischen den beiden OMMs wiederhergestellt wurde, zwingt die Synchronisation der OMMs ein OMM, wieder zum Standby-OMM zu werden. Nach dem der zuvor ausgefallene OMM wieder seinen Betrieb aufgenommen hat, wird er zum inaktiven OMM. Er nimmt seine Funktion als aktiver OMM nicht wieder auf.

5.3 Konfigurierung der OMM-Fehlertoleranz (Resiliency)

Jedes RFP des DECT-Systems muss mit zwei OMM-IP-Adressen konfiguriert werden. Diese beiden OMM-Adressen können entweder mittels

DHCP (siehe Kapitel 3.1.1) oder mit dem OM Configurator (siehe Kapitel 3.2) konfiguriert werden.

5.4 Absturzsituationen

Abstürze treten in den folgenden Fällen ein:

- Im aktiven OMM tritt ein OMM-Fehler auf.
- Das RFP, das als aktives OMM fungiert, ist ausgeschaltet oder wird auf der ssh-Konsole neu gebootet.
- Der OMM wird im Webbrowser-Menü neu gebootet.
- Der aktive OMM kann nicht erreicht werden.

Der fehlertolerante oder Standby-OMM wird in den folgenden Fällen zum aktiven OMM:

- Der konfigurierte SIP-Proxy/Registrar ist erreichbar
- Der andere OMM hat eine größere IP-Adresse, während kein OMM aktiv ist und beide OMMs miteinander Kontakt haben (in der Regel beim Systemanlauf).

Wenn die OMMs wieder in Kontakt kommen:

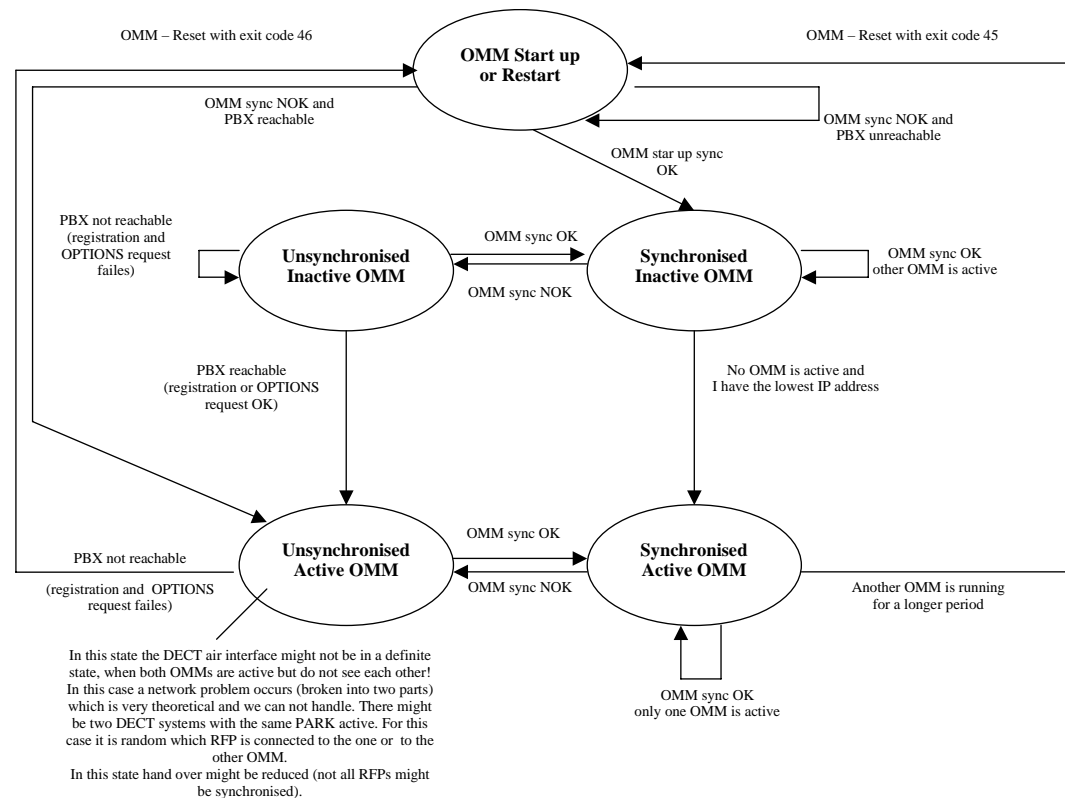
- Beide OMMs prüfen, welcher von beiden länger gelaufen ist. Dieser wird zum aktiven OMM. Der andere wird nur zum Standby-OMM.

5.5 Absturz-Fehlschlagsituationen

Absturz-Fehlschläge treten in den folgenden Fällen ein:

- Die IP-Verbindung zwischen den OMMs schlägt fehl und der konfigurierte SIP Proxy/Registrar ist nicht erreichbar.
In diesem Fall muss der aktive OMM warten, bis der SIP-Proxy/Registrar erreichbar ist..

Das folgende Statusdiagramm zeigt die OMM-Fehlertoleranz-Zustände:



„OMM sync OK“ means: OMMs are synchronised with each other and are able to exchange their operational states
 „OMM sync NOK“ means: OMMs are not synchronised with each other and are not able to exchange their operational states

5.6 Spezifische fehlertolerante Zustände

Einige Aspekte müssen beachtet werden, falls der OMM-Zustand sich dann ändert, wenn sie nicht synchronisiert sind.

5.6.1 Wie ein fehlertoleranter OMM aktiv wird

Wie die vorstehenden Abbildung zeigt, muss der Standby-OMM im Falle eines unsynchronisierten OMM-Zustands entscheiden, ob er aktiv wird oder nicht.

Zu diesem Zweck versucht der OMM Kontakt zum konfigurierten SIP-Proxy und Registrar aufzunehmen. Der OMM startet eine SIP-Registrierung für das Engegerät mit der niedrigsten Telefonnummer und sendet eine Anforderungen „OPTIONS“ an den konfigurierten Proxy. Bei Antwort wird der SIP-Proxy/Registrar als erreichbar betrachtet und der OMM wird aktiv.

5.6.2 Behandlung, wenn beide OMMs nicht synchronisiert sind

In einem unsynchronisierten OMM-Fehlertoleranz-Zustand ist die Verbindung zwischen den OMMs unterbrochen. Bei einem Netzwerkproblem können beide OMMs in diesem Zustand sein. Während dieser Zeit arbeitet ein inkonsistentes OpenMobility-System unter einigen Einschränkungen.

Der WEB-Service meldet die Warnung „No Resiliency“ (keine Fehlertoleranz) für beide OMMs. Konfigurationsänderungen, die in dieser Situation vorgenommen werden, sind nicht sicher.

Auf jeden Fall wird, wenn beide OMMs den Kontakt zueinander wieder herstellen, der länger laufende OMM zum aktiven OMM. Die Datenbankdatei im Standby-OMM wird dadurch überschrieben. Konfiguration, die in diesen künftigen Standby-OMMs vorgenommen werden, würden verloren gehen!

5.6.2.1 Zwei DECT-Funkschnittstellen

Wenn beide OMMs in einem unsynchronisierten und aktiven Zustand sind, sind sie vollständig in Betrieb. RFPs, die aufgrund eines Netzwerkausfalls die Verbindung zum OMM verlieren, können mit dem anderen OMM eine Verbindung herstellen. Zwei DECT-Funkschnittstellen sind vorhanden, arbeiten jedoch parallel.

Hinweis: Beide Funkschnittstellen verwenden den gleichen PARK. So kann nicht bestimmt werden, für welchen OMM eine Standortregistrierung erfolgreich ist.

Bei PPs sind verschiedene Situationen möglich:

- Sie bemerken diese Situation nicht
 - o Aktive Anrufe bleiben aufgebaut, je nach Netzwerkbedingungen
 - o PPs können neue Anrufe tätigen und empfangen, je nach verfügbarer PBX-Verbindung
 - o PPs können an RFPs, die an den gleichen OMM angeschlossen sind, weitergeben
 - o PPs könne PPs anrufen, die beim anderen OMM registriert sind
- Sie alle verlieren ihre RFP-Basisstation und führen eine neue Standortregistrierung durch.
 - o Aktive Anrufe werden unterbrochen
 - o PPs können neue Anrufe tätigen und empfangen, je nach verfügbarer PBX-Verbindung
 - o PPs können an RFPs, die an den gleichen OMM angeschlossen sind, weitergeben
 - o PPs könne PPs anrufen, die beim anderen OMM registriert sind
- Sie verlieren ihre RFP-Basisstation und durchsuchen das DECT-Netzwerk ohne eine andere zu finden
 - o Aktive Anrufe werden unterbrochen
 - o PPs suchen weiterhin nach einem Netzwerk bis wieder eine Funkschnittstelle zur Verfügung steht

Hinweis: Übergabe zwischen PPs, die sich bei RFPs befinden, die von verschiedenen OMMs gesteuert werden, ist nicht möglich.

Wenn die OMMs wieder miteinander Kontakt haben, endet diese inkonsistente OpenMobility-Situation.

6 Download neuer Firmware in die Endgeräte

Das Leistungsmerkmal „Download neuer Firmware in die Endgeräte“ ermöglicht die Aktualisierung der Endgeräte-Firmware, ohne dass der Benutzer eingreifen muss oder über die bestehende DECT-Funkschnittstelle laufende Telefoniedienste unterbrochen werden.

Dieses Leistungsmerkmal ist gegenwärtig für die Endgeräte 610d, 620d und 630d verfügbar.

6.1 So funktioniert der Download neuer Firmware in die Endgeräte

Bei aktivierter Funktion „Download neuer Firmware in die Endgeräte“ agiert der OMM als Download-Server, der die Firmware für Downloads zur Verfügung stellt.

Das PP sendet seine aktuelle Firmwareversion während der Einbuchung in das DECT-System. Stimmt die aktuelle Firmwareversion nicht mit der vom OMM bereitgestellten Version überein, wird das PP zur Update-Warteschlange hinzugefügt.

Danach werden in der Warteschlange befindliche PPs per Funkruf kontaktiert und eine Download-Verbindung hergestellt. Nachdem die Verbindung hergestellt wurde, sendet der OMM seine PP-Firmwareversion und das PP fordert eine *Endgeräte-Beschreibungsdatei* an. Nach dem Empfang der Endgeräte-Beschreibungsdatei prüft das PP, welche Dateien fehlen oder aktualisiert werden müssen.

Falls Dateien fehlen oder aktualisiert werden müssen, leitet das PP den Download-Vorgang ein.

Folgende Download-Szenarien werden vom OMM automatisch gehandhabt:

- Kann ein Endgerät nicht mehr erreicht werden (z.B. durch Ausschalten), wird der OMM es aktualisieren, sobald es wieder erreichbar ist.
- Der OMM kümmert sich um den Softwaredownload, während der Benutzer zwischen verschiedenen Basisstationen (Roaming) und Orten pendelt.
- Der OMM kann im Falle eines Verbindungsabbruchs einen Download an der unterbrochenen Stelle wieder aufnehmen, zum Beispiel wenn der Benutzer während des Downloads den Empfangs- und Sendebereich verlassen hat oder der Akku des Endgerätes zwischenzeitlich geleert wurde.
- Der OMM aktualisiert neu an das System angemeldete Endgeräte.
- Der Download wird auf einen späteren Zeitpunkt verschoben, falls das Endgerät gesperrt ist (zum Beispiel wegen eines zu niedrigen Akkuladestands, oder weil der Firmware-Download im lokalen Menü deaktiviert wurde).

Der Download erfolgt ohne jedes Eingreifen des Benutzers. Während des Downloads stehen Telefoniedienste, Roaming- und Handover-Prozeduren

weiterhin zur Verfügung. Der Download wird automatisch angehalten, falls das PP zum Beispiel den Empfangs- und Sendebereich verlässt oder das RFP besetzt ist. Der Download wird automatisch wieder aufgenommen, wenn die Ursache für die Unterbrechung behoben wurde.

Die Endgeräte 610d / 620d / 630d sind mit zwei Partitionen im internen Flash-Speicher ausgestattet, um zwei verschiedene Softwareversionen speichern zu können. Während eines Downloads wird die neue Firmware in eine der beiden Partitionen geschrieben, und das PP wird mit der Firmware der anderen Partition betrieben.

Die neue Firmware wird erst aktiviert, nachdem

- der Firmware-Download vollständig abgeschlossen wurde,
- eine Konsistenzprüfung erfolgreich durchgeführt wurde und
- das Endgerät in den Ruhezustand gesetzt wurde.

Der Download einer PP-Firmware von 1 MB dauert ungefähr 90 Minuten.

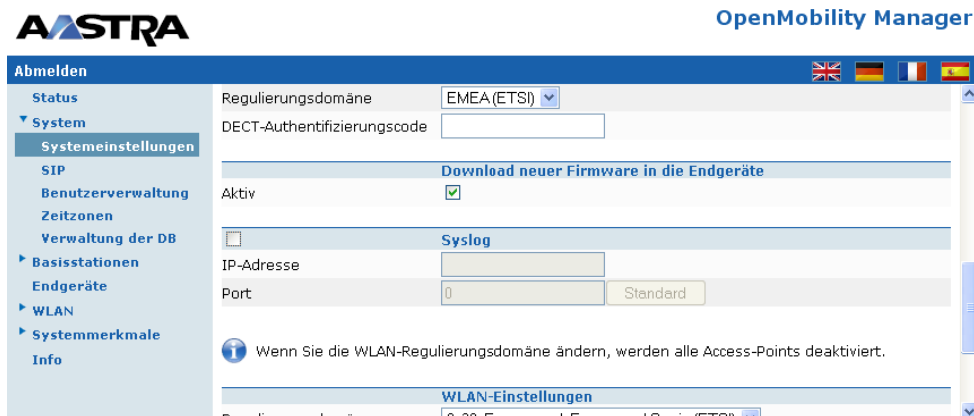
Das Endgerät kann den Download aus mehreren Gründen unterbinden:

- Niedriger Akkuladestand
Der Akkuladestand beträgt weniger als 50 %, und das PP ist weder an die Docking-Station noch über die USB-Schnittstelle angeschlossen.
- Software gesperrt
Der Firmware-Download wurde im lokalen Menü des Endgerätes deaktiviert
- Download fehlgeschlagen
Es traten zu viele Downloadfehler auf
- Mehrere Systeme
Ein PP kann an mehrere OpenMobility-Systeme angemeldet sein. Das erste System, an das ein Endgerät angemeldet wird, wird automatisch zum „Master-System“. Das PP wird nur vom „Master-System“ heruntergeladen. Im lokalen Menü des Endgerätes kann ein anderes „Master-System“ ausgewählt werden.

Die Anzahl der herunterladbaren PPs hängt von den verfügbaren Systemressourcen ab.

6.2 Download neuer Firmware konfigurieren

Das Leistungsmerkmal „Download neuer Firmware in die Endgeräte“ kann auf der Webseite „Systemeinstellungen“ aktiviert bzw. deaktiviert werden.



Die PP-Firmware ist Teil jedes OpenMobility-Softwarepaketes, das von Aastra bereitgestellt wird.

Die PP-Firmware befindet sich in der Paketdatei *aafon6xxd.dnld*. Diese Paketdatei muss sich auf demselben TFTP-Server in dem Pfad befinden, von dem auch das OMM-RFP seine Boot-Imagedatei bezieht (zum Beispiel *omm_ffsip.tftp*).


Wichtig: Das Leistungsmerkmal „Download neuer Firmware in die Endgeräte“ muss über die Webseite **Systemeinstellungen** deaktiviert werden, bevor eine neue Endgeräte-Firmware auf den TFTP-Server geladen wird. Nach dem Kopier- oder Installationsvorgang kann der Firmware-Download wieder aktiviert werden.

Nach einem Systemstart wird der Start des Dienstes „Download neuer Firmware in die Endgeräte“ für eine Weile verzögert, damit erst das gesamte DECT-System starten kann. Dieser Vorgang kann mehrere Minuten in Anspruch nehmen.

Ist der Download neuer Firmware in die Endgeräte aktiviert, wird der Status des Firmware-Download-Dienstes zusammen mit einer Statistik auf der Webseite „Status“ angezeigt.



Der Status der jedes einzelnen PP-Downloads wird auf der Webseite „Endgeräte“ angezeigt.


OpenMobility Manager

Abmelden

- Status
- System
- Basisstationen
- Endgeräte**
- WLAN
- Systemmerkmale
- Info

Endgeräte

Status

⚠ Bitte Status-Seite überprüfen.

Anmelden mit eingerichteten IPEIs

PARK: 31100303462104

Anmelden ohne eingerichtete IPEIs







2 min
Anmelden erlaubt: ✖

1 - 7 (7) Endgeräte

Name	Rufnummer	IPEI	Eingebucht	Download
Manuela Mustermann	5140	03586 0008318 6	✓	-
Daniel	5143	00750 0358349 4	✓	🔍
James B.	5144	00750 0290968 5	✓	✓
Otto	5145	01271 0573185 9	✓	9.7 kBytes left
Isabelle	5146	01271 0562059 8	✓	🔄
Henrik	5147	01271 0710479 4	✓	⚠
pp55	5148	00077 0115822 7	✖	-

Das Endgerät ist beschäftigt.

Die verschiedenen Symbole und Textmeldungen in der Spalte „Download“ haben folgende Bedeutung:

Download	Bedeutung
-	Download der Firmware auf dieses Endgerät nicht möglich (zum Beispiel, da kein 610d, 620d oder 630d)
	Das PP wird per Funkruf kontaktiert, um eine Downloadverbindung herzustellen. Nach erfolgreicher Verbindung berechnet das PP die zu ladende Datenmenge. Dieser Vorgang kann mehrere Sekunden in Anspruch nehmen.
xx kbytes left	Der Download ist noch nicht abgeschlossen; xx Kilobyte sind noch zu laden.
	Die Firmware dieses PP's ist aktuell.
	Der PP-Download befindet sich in der Warteschlange für Updates (ausstehend).
	Warnung. Der Download wurde aus einem der folgenden Gründe blockiert: <ul style="list-style-type: none"> - das PP ist besetzt (vorübergehender Status) - niedriger Akkuladestand - dies ist nicht das Master-Downloadsystem - der Download wurde im Endgerät deaktiviert Der spezielle Grund wird als Tooltip angezeigt.
	Fehler Der Download schlug aus einem der folgenden Gründe fehl: <ul style="list-style-type: none"> - Prüfsummen-Fehler - Dateisystem-Fehler - Fehler beim Schreiben der Firmware in den Flash-Speicher - Versionen stimmen nicht überein - Firmware-Container konnte nicht erweitert werden Der spezielle Grund wird als Tooltip angezeigt.
	Info Download nicht möglich, da <ul style="list-style-type: none"> - das Endgerät nicht erreichbar ist - das Endgerät nicht angeschlossen ist Der spezielle Grund wird als Tooltip angezeigt.

7 Wartung

7.1 Messausrüstung für die Standortaufnahme

Bei der Planung einer SIP-DECT-Installation ist auf eine ausreichende Verteilung der einzelnen RFPs zu achten, sodass die Anforderungen für eine zuverlässige Synchronisation und zuverlässige Verbindungen zu den Endgeräten erfüllt werden. Hierbei kann Ihnen das Standortaufnahme-Kit helfen. Es besteht aus:

- Mess-RFP mit eigener Spannungsversorgung
- Stativ und Batterie für das RFP
- zwei Referenz-PPs mit Ladeschalen
- Ladegeräte
- Optionales Mess-Endgerät, mit dem die Funksignale von DECT-Geräten anderer Hersteller überwacht werden können

7.2 Firmware-Version des Aastra DECT 142 / Aastra 142d Handset prüfen

Die Versionsinformationen des Aastra DECT 142 Handset / Aastra 142d lassen sich mit einigen wenigen Tastendrücken anzeigen. Prüfen Sie die Firmware-Version, um festzustellen, ob Sie eine Aktualisierung vornehmen müssen, mit der etwaige Benutzerprobleme beseitigt werden.

1. Drücken Sie den Softkey „**Menu**“.
2. Wählen Sie System „**System**“ (nur markieren).
3. Drücken Sie „**OK**“.
4. Wählen Sie „**Version Number**“.
5. Drücken Sie „**OK**“.

Im Display werden nun Software- und Hardware-Version des Aastra DECT 142 Handset / Aastra 142d angezeigt.

7.3 Diagnosefunktionen

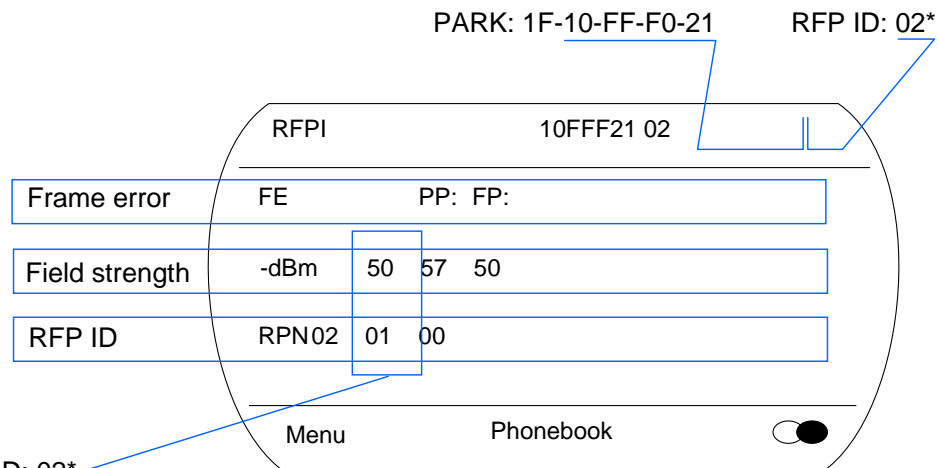
7.3.1 Standortaufnahme-Betriebsart des Aastra DECT 142 / Aastra 142d

Sie gelangen mit wenigen Tastendrücken in die “Standortaufnahme-Betriebsart” des Aastra DECT 142 / Aastra 142d. Das Telefon zeigt in dieser Betriebsart die RFPs sowie die tatsächliche Feldstärke des empfangenen Signals in dBm an.

- 1) Drücken Sie den Softkey „**Menu**“.
- 2) Geben Sie folgende Sequenz ein: „**R***76#**“.
- 3) Wählen Sie „**Site Survey**“.
- 4) Drücken Sie „**OK**“.

Um die Standortaufnahme-Betriebsart wieder zu verlassen, schalten Sie das Telefon aus und wieder ein.

Am Endgerät Aastra DECT 142 Handset / Aastra Phone 142 wird Folgendes angezeigt:



RFP ID: 02*

*The ID of RFP to which the PP is currently associated to.

In diesem Beispiel ist das PP aktuell mit dem RFP mit den Nummer 02 verbunden. Das RFP 01 und 00 sind ebenfalls sichtbar. Die Nummer „10FFF21 02“ oben rechts bezieht sich auf den PARK (Beispiel 1F-10-F2-21) des SIP-DECTSystems und das RFP, mit dem das Telefon aktuell verbunden ist.

7.3.2 Anruftest-Betriebsart des Aastra DECT 142 / Aastra 142d

Sie gelangen mit wenigen Tastendrücken in die „Anruftest-Betriebsart“ des Aastra DECT 142 / Aastra 142d. Das Telefon wählt in dieser Betriebsart fortwährend eine festgelegte Nummer. Sie können dieses Merkmal nutzen, um zu Testzwecken Verkehr zu generieren. Diese Betriebsart bleibt auch aktiv, wenn sich das Telefon in der Ladeschale befindet.

- 1) Drücken Sie den Softkey „**Menu**“.
- 2) Geben Sie folgende Sequenz ein: „**R***76#**“.
- 3) Wählen Sie „**Auto Call Test**“.
- 4) Drücken Sie „**OK**“.
- 5) Wählen Sie die anzurufende Telefonnummer.
- 6) Drücken Sie „**OK**“.
- 7) Geben Sie den Zeitabstand zwischen zwei Anrufen in Sekunden ein.
- 8) Drücken Sie „**OK**“.
- 9) Geben Sie Dauer der jeweiligen Anrufe in Sekunden ein.
- 10) Drücken Sie „**OK**“. Der Test startet automatisch.

Um den Test zu beenden, schalten Sie das Telefon aus und wieder ein.

7.3.3 Annahmetest-Betriebsart des Aastra DECT 142 / Aastra 142d

Sie gelangen mit wenigen Tastendrücken in die „Annahmetest-Betriebsart“ des Aastra DECT 142 / Aastra 142d. Das Telefon beantwortet in dieser Betriebsart ankommende Anrufe automatisch. Sie können diese Funktion gemeinsam mit der Funktion „Anruftest“ zu Testzwecken nutzen. Diese

Betriebsart bleibt auch aktiv, wenn sich das Telefon in der Ladeschale befindet.

- 1) Drücken Sie den Softkey „**Menu**“.
- 2) Geben Sie folgende Sequenz ein: „**R***76#**“.
- 3) Wählen Sie „**Auto Answer**“.
- 4) Drücken Sie „**OK**“.
- 5) Geben Sie in Sekunden an, wie lange das Telefon läuten soll, bevor es den Anruf annimmt.
- 6) Drücken Sie „**OK**“.
- 7) Geben Sie Dauer der jeweiligen Anrufe in Sekunden ein.
- 8) Drücken Sie „**OK**“. Der Test startet automatisch.

Um den Test zu beenden, schalten Sie das Telefon aus und wieder ein.

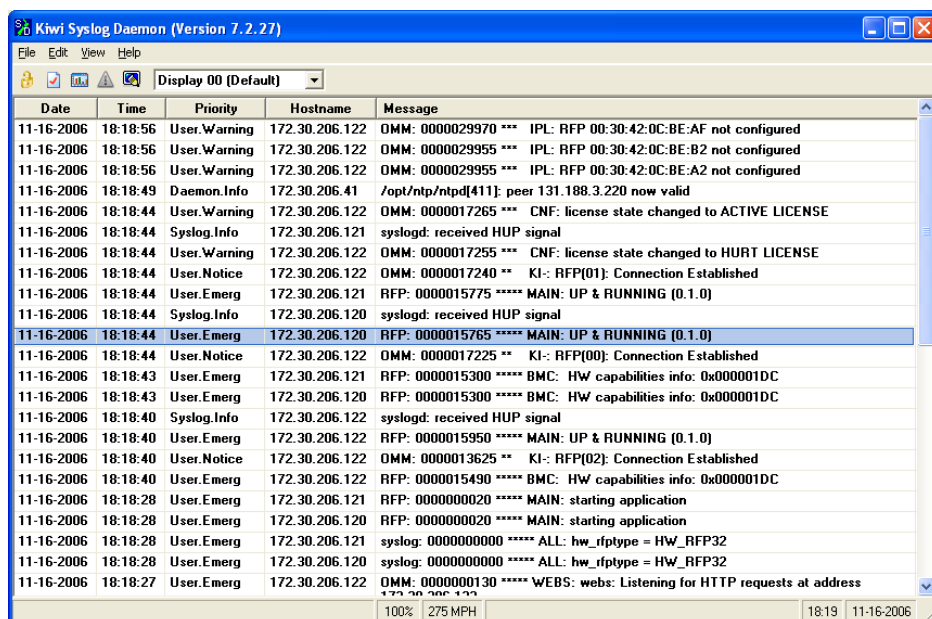
7.3.4 Syslog

Der OpenMobility Manager und die RFPs können Syslog-Nachrichten gemäß /8/ weiterleiten. Dieses Merkmal kann zusammen mit der IP-Adresse eines Host konfiguriert werden, der diese Nachrichten sammelt.

Syslog muss aktiviert sein für:

- DHCP mit den Public Options 227 und 228
- die Einstellung von Syslog-Daemon-Server und -Port über die Webschnittstelle

Das Einrichten des Syslog via DHCP oder OM Configurator hat den Vorteil, dass Syslogs bereits in einem früheren Stadium des Startens des RFP zur Verfügung stehen.



Date	Time	Priority	Hostname	Message
11-16-2006	18:18:56	User.Warning	172.30.206.122	OMM: 0000029970 *** IPL: RFP 00:30:42:0C:BE:AF not configured
11-16-2006	18:18:56	User.Warning	172.30.206.122	OMM: 0000029955 *** IPL: RFP 00:30:42:0C:BE:B2 not configured
11-16-2006	18:18:56	User.Warning	172.30.206.122	OMM: 0000029955 *** IPL: RFP 00:30:42:0C:BE:A2 not configured
11-16-2006	18:18:49	Daemon.Info	172.30.206.41	/opt/ntp/ntpd[411]: peer 131.188.3.220 now valid
11-16-2006	18:18:44	User.Warning	172.30.206.122	OMM: 0000017265 *** CNF: license state changed to ACTIVE LICENSE
11-16-2006	18:18:44	Syslog.Info	172.30.206.121	syslogd: received HUP signal
11-16-2006	18:18:44	User.Warning	172.30.206.122	OMM: 0000017255 *** CNF: license state changed to HURT LICENSE
11-16-2006	18:18:44	User.Notice	172.30.206.122	OMM: 0000017240 ** KI: RFP[01]: Connection Established
11-16-2006	18:18:44	User.Emerg	172.30.206.121	RFP: 0000015775 ***** MAIN: UP & RUNNING (0.1.0)
11-16-2006	18:18:44	Syslog.Info	172.30.206.120	syslogd: received HUP signal
11-16-2006	18:18:44	User.Emerg	172.30.206.120	RFP: 0000015765 ***** MAIN: UP & RUNNING (0.1.0)
11-16-2006	18:18:44	User.Notice	172.30.206.122	OMM: 0000017225 ** KI: RFP[00]: Connection Established
11-16-2006	18:18:43	User.Emerg	172.30.206.121	RFP: 0000015300 ***** BMC: HW capabilities info: 0x000001DC
11-16-2006	18:18:43	User.Emerg	172.30.206.120	RFP: 0000015300 ***** BMC: HW capabilities info: 0x000001DC
11-16-2006	18:18:40	Syslog.Info	172.30.206.122	syslogd: received HUP signal
11-16-2006	18:18:40	User.Emerg	172.30.206.122	RFP: 0000015950 ***** MAIN: UP & RUNNING (0.1.0)
11-16-2006	18:18:40	User.Notice	172.30.206.122	OMM: 0000013625 ** KI: RFP[02]: Connection Established
11-16-2006	18:18:40	User.Emerg	172.30.206.122	RFP: 0000015490 ***** BMC: HW capabilities info: 0x000001DC
11-16-2006	18:18:28	User.Emerg	172.30.206.121	RFP: 0000000020 ***** MAIN: starting application
11-16-2006	18:18:28	User.Emerg	172.30.206.120	RFP: 0000000020 ***** MAIN: starting application
11-16-2006	18:18:28	User.Emerg	172.30.206.121	syslog: 0000000000 ***** ALL: hw_rftype = HW_RFP32
11-16-2006	18:18:28	User.Emerg	172.30.206.120	syslog: 0000000000 ***** ALL: hw_rftype = HW_RFP32
11-16-2006	18:18:27	User.Emerg	172.30.206.122	OMM: 0000000130 ***** WEBS: webs: Listening for HTTP requests at address

Im Standardzustand ist der Umfang der Syslog-Meldungen so eingestellt, dass der Benutzer den allgemeinen Systemzustand und wichtige Fehler erkennen kann.

7.3.5 ssh-Benutzeroberfläche

Über diese Oberfläche mit eine Reihe von Befehlen an die einzelnen RFPs ausgegeben werden. Die meisten dieser Befehle dienen Diagnosezwecken und helfen dem Spezialisten bei der Fehlersuche.

Hinweis: Manche Befehle können den Betrieb des Systems beeinträchtigen.

Der ssh-Zugang zu einem RFP ist offen, wenn

- das RFP an einen OMM angeschlossen ist und „Fernzugang“ eingeschaltet ist;
- das RFP an keinen OMM angeschlossen ist.

Um den ssh-Zugang zu einem an einen OMM angeschlossen RFP freizugeben, aktivieren Sie das Kontrollkästchen „Fernzugang“ auf der OMM-Webseite „Systemeinstellungen“.



7.3.5.1 Anmelden

Beschreibung des Ablaufs:

- Öffnen Sie eine ssh-Sitzung zur IP-DECT-Basisstation. Verwenden Sie den Benutzernamen für vollständigen Zugang
- und geben Sie das Passwort für vollständigen Zugang ein.

Die Ausgabe sollte so aussehen:

```
Willkommen zu IP RFP OpenMobility SIP Only Version 1.6.x
4. Juni 2008 10:12:16
Release
```

```
(BUILD 0)
```

```
letzte Reset-Ursache: Hardware-Reset (Power-on-Reset)
```

```
Passwort des omm@172.30.206.94:
omm@172.30.206.94 >
```

7.3.5.2 Befehlsübersicht

Geben Sie „help“ ein, um eine Befehlsübersicht zu erhalten:

```

exit,quit,bye      : Sitzung beenden
ommconsole         : OMM-Konsole
ip_rfpconsole      : RFP-Konsole
flash              : zeigt Informationen des Flash
link               : zeigt den Status der Ethernet-Schnittstelle
ldb                : lokale Konfiguration anzeigen/einstellen (OM
Configurator)
setconsole         : Nachrichten auf Konsole ausgeben
noconsole          : Nachrichten nicht auf Konsole ausgeben
dmesg              : Meldungen vom letzten Bootvorgang
logread            : letzte Meldungen
su                 : zum Benutzer-Rootverzeichnis
ping               : das bekannte „Ping“
traceroute         : das bekannte „Traceroute“
free               : das bekannte „free“
ps                 : das bekannte „ps“
top                : das bekannte „top“
ifconfig           : das bekannte „ifconfig“
uptime             : das bekannte „uptime“
reboot             : das bekannte „reboot“

```

7.3.5.3 RFP-Konsolenbefehle

Nach Eingabe von „ip_rfpconsole“ können Sie die folgenden Befehle auf die einzelnen RFPs anwenden:

```

heap               - zeigt die Heap-Pufferstatistik
help               - zeigt die Befehlshilfetabelle
lec                - Anpassung der linearen Echo-Canceller-
Parameter
media              - zeigt den Status von Medienkanälen
mutex              - listet alle erstellten MXP-Mutexe
queues             - listet alle erstellten MXP-Warteschlangen
reset              - setzt die IPRFP-Anwendung zurück
rsx                - gibt die RSX-Verbindung zu BMC über TCP frei
sem                - listet alle erstellten MXP-Semaphore
spy                - setzt Beobachtungsebenen und zeigt sie an [
<key #> <level #> ]
tasks              - listet alle laufenden MXP-Tasks
voice              - zeigt den Status der Sprachbehandlung an
exit               - verlässt die IP-RFP-Konsole

```

Hinweis:Mit dem Befehl „spy“ können Sie die Syslog-Benachrichtigungsebene erhöhen. Sie sollten dies nur auf Anweisung des Supports tun, da dies den Betrieb des Systems beeinträchtigen kann.

7.3.5.4 OMM-Konsolenbefehle

Wenn Sie bei geöffneter OMM-RFP-Sitzung „ommconsole“ eingeben, stehen Ihnen folgende Befehle für den OpenMobility Manager (OMM) zur Verfügung:

```

omm@172.30.206.94 > ommconsole
Willkommen zur OMM-Konsole. Mit ? erhalten Sie eine Befehlsliste.

```

omm# help	
Befehl	Erklärung
-----	-----
?	zeigt die Befehlshilfetabelle
cmi	cmi-Befehle
cnf	zeigt Konfigurationsparameter
dsip	dsip-Befehle
help	zeigt die Befehlshilfetabelle
exit	verlässt diese Konsole
heartbeat	konfiguriert den Heartbeat-Mechanismus für
IP-RFPs	
ipc	zeigt die Socket-Kommunikation
ipl	zeigt konfigurierte RFPs
ki	KI-Monitor
quit	verlässt diese Konsole
logger	sendet eine Zeichenkette zum Syslog-Daemon
mon	schaltet die Monitorfunktion um
msm	zeigt Statusinformationen im
MediaStreamManagement	
mutex	listet alle erstellten MXP-Mutexe
queues	listet alle erstellten MXP-Warteschlangen
rsip	Fernkonfiguration der Beobachtungsebenen für
IP-RFPs	
rsx	zeigt konfigurierte RFPs
sem	listet alle erstellten MXP-Semaphore
spy	setzt Beobachtungsebenen und zeigt sie an [
<key #> <level #>]	
standby	zeigt redundante OMMs
sync	Befehle für die RFP-Synchronisation
tasks	listet alle laufenden MXP-Tasks
tasks	listet alle laufenden MXP-Tasks
tzone	tzone-Befehle
uptime	zeigt die Laufzeit des Systems
ver	Versionsinformationen
wlan	zeigt Statusinformationen des WLAN-Management
omm#	

Hinweis: Mit dem Befehl “spy” können Sie die Syslog-Benachrichtigungsebene speziell für Subsysteme des OMM erhöhen. Sie sollten dies nur auf Anweisung des Supports tun, da dies den Betrieb des Systems beeinträchtigen kann.

7.3.6 Erfassung von Core-Dateien

Bei fatalen Fehlern im OMM und einem Absturz der Software kann der OMM Memory-Dumps erstellen. Sie können die so erzeugten Core-Dateien an den Support senden und ihn so bei der Lösung des Problems unterstützen.

Der OMM kann diese Core-Dateien auf einem TFTP-Server in Ihrem lokalen Netzwerk speichern.

Um die Erstellung von Core-Dateien freizugeben, geben Sie in der OMM-Befehlszeile Folgendes ein:

```
local_db core=yes
```

```
local_db core_srv=server-ip – IP-Adresse des TFTP-Servers
```

```
local_db core_path=path – Dateipfad auf dem TFTP-Server (muss Schreibfreigabe besitzen)
```

Werden `local_db_core_srv` und `local_db_core_path` nicht angegeben, versucht der OMM, die Core-Dateien auf den TFTP-Server in das Verzeichnis zu schreiben, von dem aus die OMM-/RFP-Anwendung heruntergeladen wurde.

Nach dem Neustart des OMM werden die Core-Dateien automatisch zum TFTP-Server übertragen.

Hinweis: Der TFTP-Server muss das Erstellen neuer Dateien erlauben. Dies ist in der Regel nicht standardmässig der Fall.

Um die Erstellung von Core-Dateien zu sperren, geben Sie in der OMM-Befehlszeile Folgendes ein:

```
local_db core=
```

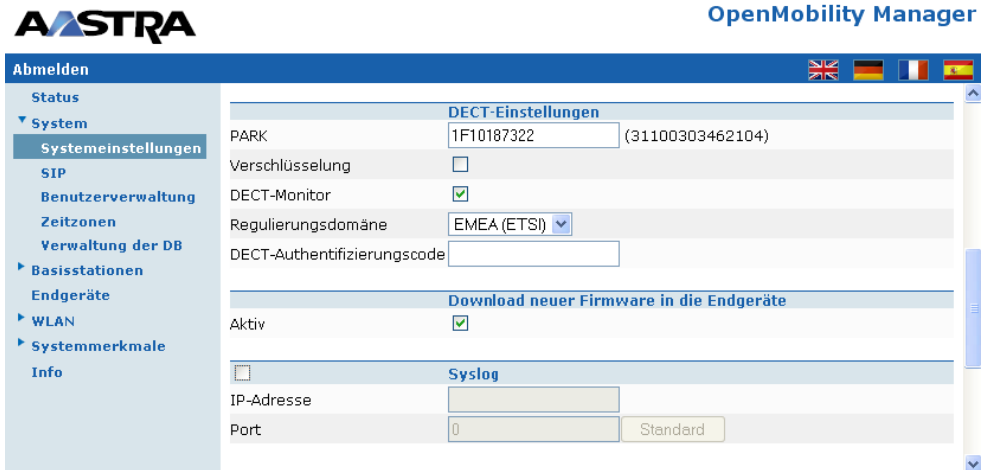
7.3.7 DECT-Monitor

Für die bessere Fehlererkennung im IP-DECT-System kann der DECT-Monitor verwendet werden. Der DECT-Monitor ist ein eigenständiges Programm für MS Windows. Er liefert einen Echtzeit-Überblick über den Status der aktuellen IP-DECT-Basisstation und den Status der einzelnen Telefone im IP-DECT-System.

Der DECT-Monitor besitzt folgende Funktionen:

- Auslesen der DECT-Konfiguration eines IP-DECT-Systems
- Speichern der Konfiguration in einer ASCII-Datei
- Klare, tabellarische Anzeige von DECT-Transaktionen zwischen IP-DECT-Basisstation und Telefon mit Kennzeichnung von Handover-Situationen. Anzeige in Echtzeit.
- Anzeige weiterer Ereignisse, die den Status oder Aktionen von IP-DECT-Basisstationen und Telefonen des IP-DECT-Systems betreffen
- Aufzeichnen aller Events in einer Logbuchdatei
- Anzeigen der Synchronisationszustände zwischen den RFPs
- Überwachen von Systemen mit bis zu 256 IP-DECT-Basisstationen und 512 PPs
- Auslesen und Anzeige von IP-DECT-RFP-Statistikdaten, entweder für ein einzelnes IP-DECT-RFP oder für alle IP-DECT-RFPs
- Anzeige wichtiger DECT-Daten des IP-DECT-Systems

Das Programm DECT Monitor kann nur verwendet werden, wenn das Kontrollkästchen DECT-Monitor in der OMM-Konfiguration aktiviert ist.



Hinweis: Das markierte Kontrollkästchen DECT Monitor wird aus Sicherheitsgründen nicht dauerhaft im integrierten Flash-Speicher des OMM/RFP gespeichert. Das markierte Kontrollkästchen DECT-Monitor wird beim Rücksetzen gelöscht.

Das Programm DECT Monitor wird zusammen mit dem IP-DECT-System benutzt.

Beim Start des Programms wird der Benutzer aufgefordert, die IP-Adresse des IP-DECT-RFP oder des Servers einzugeben, auf dem die Software OpenMobility Manager (OMM) läuft.

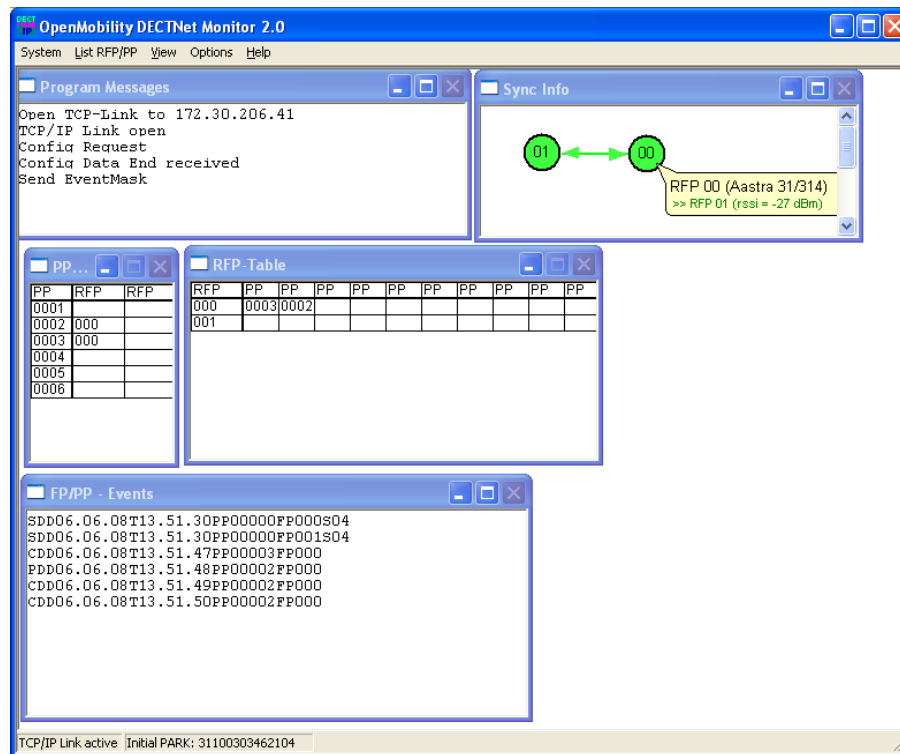
Kann die Verbindung nicht aufgebaut werden, kommen mehrere Gründe infrage:

- Der Betrieb des DECT-Monitors ist in der OMM nicht freigegeben. Ermöglichen Sie den Betrieb des DECT Monitor mithilfe des Webdienstes.
- Die IP-Adresse stimmt nicht. Sie müssen die IP-Adresse des RFP angeben, auf dem der OMM läuft.
- Eine Verbindung zum RFP wird nicht unterstützt.

Das Programm zeigt die IP-Adresse an, die beim letzten Mal benutzt wurde.

Beim Start des Programms, wird automatisch eine Verbindung zum OMM aufgebaut und alle vom Benutzer konfigurierten Unterfenster und Tabellen werden in einem Programmfenster angezeigt.

Sind alle Verbindungen aufgebaut, werden automatisch die DECT-Daten des Systems ausgelesen und in die Tabellen „RFP-Tabelle“ und „PP-Tabelle“ übernommen. Diese Prozedur wird „Konfigurationsabfrage“ genannt.



Anschliessend werden die festgelegten Trace-Optionen (Ereignismaske) an den OMM gesendet. Es werden immer die Optionen an den OMM gesendet, die beim letzten Verlassen des Programms aktiv waren.

Ist die Trace-Option „Transaktion erstellen/freigeben“ aktiviert, liefert der OMM alle vorhandenen Transaktionen.

Anschliessend liefert das OMM-System die gewünschten Trace-Daten. Der Benutzer kann entweder interaktiv mit dem System kommunizieren (siehe unten) oder einfach eine Logbuchdatei angeben, in der die Daten gespeichert werden sollen.

Nach dieser Initialisierung kann der Benutzer folgende Änderungen durchführen:

- Die Trace-Einstellungen können mit dem Menüpunkt Optionen – Ereignismaske angepasst werden. Nach Bestätigung der Einstellungen mit <OK> werden diese an den OMM gesendet.
- Eine erneute Konfigurationsabfrage kann an den OMM gesendet werden.
- Eine Logbuchdatei kann aktiviert werden.
- Die Konfigurationsdaten von Telefonen, RFPs und Steuerungsmodulen können mithilfe verschiedener Dialoge angezeigt und in ASCII-Dateien gespeichert werden.

Die folgenden Informationen werden in den Tabellen dynamisch angezeigt:

- Transaktionen zwischen Telefon und DECT-System. Diese werden in beiden Tabellen angezeigt. Einfache Transaktionen werden schwarz auf weissem Hintergrund angezeigt. Beim Handover werden beide betreffenden Transaktionen weiss auf rotem Hintergrund angezeigt.
- Ihre Ereignisse „Location Registration“ und „Detach“ werden falls möglich etwa ein bis zwei Sekunden nach ihrem Auftreten in den Tabellen

angezeigt (hellgrüner Hintergrund). Ist für die Anzeige keine Spalte frei, werden sie in der FP-Tabelle nicht angezeigt. Bereits angezeigte Ereignisse können jederzeit überschrieben werden. Ereignisse, die während einer laufenden Transaktion stattfinden, werden nicht angezeigt. Ereignisse werden immer in Fenster „FP/PP-Ereignisse“ und in die Logbuchdatei übernommen (vorausgesetzt, diese ist geöffnet), unabhängig davon, ob sie in den Tabellen angezeigt werden.

Für RFPs in der RFP-Tabelle wird folgendes Farbschema verwendet:

- RFP graublau
Die IP-DECT-Basisstation ist nicht aktiv (nicht verbunden oder Störung).
- RFP schwarz
Die IP-DECT-Basisstation ist aktiv.

Die Daten eines RFP werden durch Klicken auf das jeweilige RFP-Feld in der RFP-Tabelle in einem Dialog angezeigt. Dieser Dialog zeigt Statistikdaten des jeweiligen RFP.

Für Telefone in der PP-Tabelle wird folgendes Farbschema verwendet:

- PP schwarz
Das Endgerät ist angemeldet. Es wird vorausgesetzt, dass das Telefon erreichbar ist.
- PP blau
Das Endgerät ist wahrscheinlich nicht erreichbar. Ein „Detach“ wurde empfangen oder das Endgerät hat auf einen Versuch, es zu erreichen, nicht geantwortet.
- PP graublau
Das Endgerät ist nicht angemeldet.

Die Daten eines Telefons werden durch Klicken auf das jeweilige Telefon-Feld in der FP-Tabelle in einem Dialog angezeigt.

Das Unterfenster „Sync Info“ zeigt alle IP-DECT-Basisstationen sowie ihre Synchronisation und gegenseitigen Beziehungen. Durch Auswahl der IP-DECT-Basisstationen mit der rechten Maustaste lassen sich die sichtbaren Anzeigen ändern. Ausserdem kann eine erneute Synchronisation mit der IP-DECT-Basisstation erzwungen werden.

Es können mehrere, unten aufgelistete, Unterfenster gewählt werden. in denen zusätzliche Informationen zu den IP-DECT-Systemen angezeigt werden. Meist handelt es sich um Statistiken ausschliesslich zur internen Verwendung.

Central DECT Data

DMM - Version:

Common Par: PL:

Encryption:

Statistic Data Counter of RFP

FP-Nr	Reset Time	Data
000	03.09.2007 12:55	62114 30063 1763 0 32054 24056 5523 2 1551 0 0 0
001	unknown	12036 0 0 0 8687 0 0 0 142 0 0 0 0 0 0

Event Counter

Counter	Value
Transaction established	3
Transaction released	0
Handover situations	0
PP not found	0
Paging started	1
Release from PP	0
PP_setup rejected	0
Location Registration	0
Detach	0
Location Update	0
Enrolment	0
failed Enrolment	0
FP state	2
FP error	0
ADLC info	0
other messages	0

List Other RFP 101 found, 63 > -70 ...

- + 10 0C F0 9A A0
- + 10 0C FF B0 60
- + 10 10 FF F5 01
- + 10 10 FF F5 40
- + 10 10 FF F5 27
- + 10 18 73 27 03
- + 00 51 A0 53 F0
- + 10 10 FE F9 02
- + 10 1A 75 2D 84
- + 10 18 D6 8F 01
- + 10 14 5C BF 0F
- + 10 0E 91 A4 90
- + 10 1A 7A BD 81
- + 10 11 22 67 00
- + 10 10 FF F5 33
- + 10 10 FE F0 00
- + 10 1A 75 2D 80
- + 00 5F B8 33 80
- + 10 10 FE 9C B8
- + 00 44 EC 22 D0
- + 00 80 DC 98 00
- + 10 0C F0 A3 00
- + 10 10 FF F5 24
- + 10 14 5C D1 03
- + 00 CA 81 BC 18
- + 10 18 70 4E 00

8 Anhang

8.1 Fernmelderechtliche Informationen zu Aastra DECT 142 US

FCC-Hinweise (nur USA)

Dieses Gerät erfüllt Teil 15 der FCC-Richtlinien. Sein Betrieb unterliegt den folgenden zwei Bedingungen: (1) Dieses Gerät darf keine schädlichen Störungen verursachen und (2) dieses Gerät muss sämtliche empfangene Störungen vertragen können, einschließlich Störungen, die zum unerwünschten Betrieb des Geräts führen können.

Änderungen, die nicht ausdrücklich von diesem Unternehmen genehmigt wurden, können die Berechtigung des Benutzers zum Betrieb der Ausrüstung ungültig machen.

HINWEIS: Dieses Gerät wurde getestet und entspricht somit den empfohlenen Höchstgrenzen eines digitalen Gerätes der Klasse B in Übereinstimmung mit Teil 15 der FCC Bestimmungen. Diese Grenzen sollen angemessenen Schutz gegen störende Auswirkungen auf Einrichtungen in Wohnbereichen bieten. Dieses Gerät erzeugt, verwendet und strahlt möglicherweise Hochfrequenzenergie ab. Falls das Gerät nicht bestimmungsgemäß installiert und verwendet wird, kann es sich störend auf Funkübertragungen auswirken. Jedoch kann eine Störung auf bestimmte Einrichtungen nicht ausgeschlossen werden. Falls sich das Gerät störend auf Funk- oder Fernsehempfang auswirkt - dies kann durch An- und Abschalten des Gerätes festgestellt werden - kann der Benutzer die Störung durch eine der folgenden Maßnahmen beheben:

- Neueinstellung oder Versetzung der Empfangsantenne
- Vergrößern des Abstands zwischen dem Gerät und dem Empfänger.
- Anschluss des Geräts an einen Stromkreis mit dem der Empfänger nicht verbunden ist.
- Wenden Sie sich an Ihren Händler oder erfahrenen Radio-/Fernsehtechniker, wenn Sie weitere Hilfe benötigen.

Gesundheits- und Sicherheitsinformationen

Einwirkung von Hochfrequenz (HF)-Signalen:

Das Mobiltelefon ist ein Funksender und -empfänger. Die Konstruktion und Herstellung des Geräts gewährleistet, dass die von der Federal Communications Commission (FCC) der US-Regierung festgelegten Emissionsgrenzen für die Belastung durch Hochfrequenzenergie (HF) nicht überschritten werden. Diese Grenzen sind Teil umfassender Richtlinien und legen die zulässigen HF-Energiemengen für die allgemeine Bevölkerung fest. Die Richtlinien basieren auf Sicherheitsstandards, die vorher sowohl von US- als auch von internationalen Normbehörden festgelegt werden. Diese

Normen beinhalten eine erhebliche Sicherheitsspanne zur Gewährleistung der Sicherheit aller Personen, unabhängig von Alter und Gesundheitszustand.

Dieses Gerät und seine Antenne dürfen nicht gemeinsam mit anderen Antennen oder Transmittern aufgestellt oder in Verbindung mit diesen Geräten betrieben werden.

Dieser EUT ist nachweislich in der Lage, die örtlich spezifische Absorptionsrate (SAR) für unkontrollierte Umwelt-/Bevölkerungs-Strahlungsgrenzen zu erfüllen, die im ANSI/IEEE-Standard C95.1-1992 festgelegt sind und wurde in Übereinstimmung mit den in FCC/OET Bulletin 65 Supplement C (2001) und IEEE 1528-2003 festgelegten Messverfahren getestet.

Industrie Kanada (nur Kanada)

Der Betrieb dieses Geräts unterliegt den folgenden zwei Bedingungen: (1) Dieses Gerät darf keine Störungen verursachen und (2) dieses Gerät muss sämtliche empfangene Störungen vertragen können, einschließlich Störungen, die zum unerwünschten Betrieb des Geräts führen können.

Durch Verwendung dieses Telefons kann der Schutz der Privatsphäre nicht gewährleistet werden.

Einwirkung von Hochfrequenz (HF)-Signalen:

Das Mobiltelefon ist ein Funksender und -empfänger. Die Konstruktion und Herstellung des Geräts gewährleistet, dass die von der Federal kanadischen Gesundheitsministerium, Safety Code 6, festgelegten Emissionsgrenzen für die Belastung durch Hochfrequenzenergie (HF) nicht überschritten werden. Diese Grenzen sind Teil umfassender Richtlinien und legen die zulässigen HF-Energiemengen für die allgemeine Bevölkerung fest. Diese Richtlinien basieren auf den Sicherheitsnormen, die vorher von internationalen Normierungsstellen festgelegt wurden. Diese Normen beinhalten eine erhebliche Sicherheitsspanne zur Gewährleistung der Sicherheit aller Personen, unabhängig von Alter und Gesundheitszustand.

Dieses Gerät und seine Antenne dürfen nicht gemeinsam mit anderen Antennen oder Transmittern aufgestellt oder in Verbindung mit diesen Geräten betrieben werden.

Dieses Gerät ist nachweislich in der Lage, die örtlich spezifische Absorptionsrate (SAR) für unkontrollierte Umwelt-/Bevölkerungs-Strahlungsgrenzen zu erfüllen, die im ANSI/IEEE C.95.1-1992 festgelegt sind und wurde in Übereinstimmung mit den in IEEE 1528-2003 festgelegten Messverfahren getestet.

8.2 Fernmelderechtliche Informationen zu RFP 32 bzw. RFP 34 (NA)

FCC-Hinweise (nur USA)

Dieses Gerät erfüllt Teil 15 der FCC-Richtlinien. Sein Betrieb unterliegt den folgenden zwei Bedingungen: (1) Dieses Gerät darf keine schädlichen Störungen verursachen und (2) dieses Gerät muss sämtliche empfangene Störungen vertragen können, einschließlich Störungen, die zum unerwünschten Betrieb des Geräts führen können.

Änderungen, die nicht ausdrücklich von diesem Unternehmen genehmigt wurden, können die Berechtigung des Benutzers zum Betrieb der Ausrüstung ungültig machen.

HINWEIS: Dieses Gerät wurde getestet und entspricht somit den empfohlenen Höchstgrenzen eines digitalen Gerätes der Klasse B in Übereinstimmung mit Teil 15 der FCC Bestimmungen. Diese Grenzen sollen angemessenen Schutz gegen störende Auswirkungen auf Einrichtungen in Wohnbereichen bieten. Dieses Gerät erzeugt, verwendet und strahlt möglicherweise Hochfrequenzenergie ab. Falls das Gerät nicht bestimmungsgemäß installiert und verwendet wird, kann es sich störend auf Funkübertragungen auswirken. Jedoch kann eine Störung auf bestimmte Einrichtungen nicht ausgeschlossen werden. Falls sich das Gerät störend auf Funk- oder Fernsehempfang auswirkt - dies kann durch An- und Abschalten des Gerätes festgestellt werden - kann der Benutzer die Störung durch eine der folgenden Maßnahmen beheben:

- Neueinstellung oder Versetzung der Empfangsantenne
- Vergrößern des Abstands zwischen dem Gerät und dem Empfänger.
- Anschluss des Geräts an einen Stromkreis mit dem der Empfänger nicht verbunden ist.
- Wenden Sie sich an Ihren Händler oder erfahrenen Radio-/Fernsehtechniker, wenn Sie weitere Hilfe benötigen.

Einwirkung von Hochfrequenz (HF)-Signalen:

Das Mobiltelefon ist ein Funksender und -empfänger. Die Konstruktion und Herstellung des Geräts gewährleistet, dass die von der Federal Communications Commission (FCC) der US-Regierung festgelegten Emissionsgrenzen für die Belastung durch Hochfrequenzenergie (HF) nicht überschritten werden. Diese Grenzen sind Teil umfassender Richtlinien und legen die zulässigen HF-Energiemengen für die allgemeine Bevölkerung fest. Die Richtlinien basieren auf Sicherheitsstandards, die vorher sowohl von US- als auch von internationalen Normbehörden festgelegt werden. Diese Normen beinhalten eine erhebliche Sicherheitsspanne zur Gewährleistung der Sicherheit aller Personen, unabhängig von Alter und Gesundheitszustand.

Dieses Gerät und seine Antenne dürfen nicht gemeinsam mit anderen Antennen oder Transmittern aufgestellt oder in Verbindung mit diesen Geräten betrieben werden.

Das Funkwellen emittierende Element des RFP muss während des Betriebs weiter als 20 cm vom Benutzer entfernt sein. Das Gerät entspricht den Bestimmungen für routinemässige Bemessungsgrenzwerte.

Industrie Kanada (nur Kanada)

Der Betrieb dieses Geräts unterliegt den folgenden zwei Bedingungen: (1) Dieses Gerät darf keine Störungen verursachen und (2) dieses Gerät muss sämtliche empfangene Störungen vertragen können, einschließlich Störungen, die zum unerwünschten Betrieb des Geräts führen können.

Durch Verwendung dieses Telefons kann der Schutz der Privatsphäre nicht gewährleistet werden.

Einwirkung von Hochfrequenz (HF)-Signalen:

Das Mobiltelefon ist ein Funksender und -empfänger. Die Konstruktion und Herstellung des Geräts gewährleistet, dass die von der Federal kanadischen Gesundheitsministerium, Safety Code 6, festgelegten Emissionsgrenzen für die Belastung durch Hochfrequenzenergie (HF) nicht überschritten werden. Diese Grenzen sind Teil umfassender Richtlinien und legen die zulässigen HF-Energiemengen für die allgemeine Bevölkerung fest. Diese Richtlinien basieren auf den Sicherheitsnormen, die vorher von internationalen Normierungsstellen festgelegt wurden. Diese Normen beinhalten eine erhebliche Sicherheitsspanne zur Gewährleistung der Sicherheit aller Personen, unabhängig von Alter und Gesundheitszustand.

Dieses Gerät und seine Antenne dürfen nicht gemeinsam mit anderen Antennen oder Transmittern aufgestellt oder in Verbindung mit diesen Geräten betrieben werden.

Das Funkwellen emittierende Element des RFP muss während des Betriebs weiter als 20 cm vom Benutzer entfernt sein. Das Gerät entspricht den Bestimmungen für routinemässige Bemessungsgrenzwerte.

8.3 Regeln für Dateien vor der Konfiguration

Die Struktur der Textdatei folgt streng definierten Regeln.

Die Hauptstruktur besteht aus zwei Teilen:

1. Ein **Anweisungsbereich** wird zur Steuerung der generischen Datenerzeugung derjenigen Felder, die nicht im Datensequenzbereich gefüllt werden, verwendet.
2. Ein **Datensequenzbereich** definiert die Datensatzfelder. Jedes von ihnen wird ausdrücklich festgelegt

Im einzelnen lauten die Auszeichnungsregelungen:

- Kommentare beginnen mit „#“
- Jeder Datensatz endet mit den regulären Ausdrücken „\r“ oder „\n“
- Befehlseinstellungen erfolgen wie: <tag> = <value>.
- Datensequenzbereiche starten mit dem Schlüsselwort „**data_sequence**“. Dieses Schlüsselwort ist **für die Weiterbearbeitung der Datei unerlässlich**. Alle Anweisungen müssen vor diese Zeile geschrieben werden.
- Datensatzfelder werden durch Komma „,” getrennt. Kommas müssen auch bei leeren Feldern gesetzt werden. wenn mindestens ein nicht leeres Feld folgt. Andernfalls tritt eine falsche Zuordnung der Positionen auf.
- Felder, denen mehrere Werte zugewiesen wurden (dies gilt möglicherweise für ein paar lokale Konfigurationsfelder wie ntp_address), müssen durch Komma getrennt werden „,”.

Hinweise:

- Da Datensequenzfelder durch Komma getrennt werden, wird der Inhalt dieses Bereichs möglicherweise durch einen .csv-Export des Excel-Tabelle erzeugt und an in die Konfigurationsdatei kopiert.
- Anweisungen werden nur in denjenigen Feldern weiter verarbeitet, die innerhalb des Datensequenzbereichs leer gelassen wurden.

8.3.1 PP Konfigurationsdatei (OMM-Datenbank)

8.3.1.1 Unterstützte Anweisungen

- start_number
Zahlen können automatisch erzeugt werden. Diese Anweisung definiert den Startwert
- no_of_number
Bei Erteilung von start_number definiert diese Anweisung die maximale Anzahl der erzeugten Zahlen
- ac (authentication code)
Wenn auf "number" eingestellt, ist ac gleich der Zahl. Bei Angabe eines Werts wird dieser als Startwert, der mit jedem Erzeugungsschritt erhöht wird, genommen.
- additional_pin
siehe ac
- sip_user
siehe ac
- sip_pw
siehe ac

8.3.1.2 Datenbereichsfelder

Die Datenbereichsfelder enthalten die folgende Feldreihenfolge

1. Nummer
2. Name
3. AC
4. IPEI
5. Zusätzliche ID
6. Sip Benutzer Name
7. Sip-Passwort

8.3.1.3 Beispiel

PP-Konfigurationsfeld:

```
# -----#
# instruction section:
# -----#
# -- start_number           = {<start value for numbers to be generated>}
# -- no_of_number          = {<maximum of generated numbers>}
# -- dect authentication code (ac) = {<"number">, <start value for ac's to be generated>}
# -- additionalId/userPin    = {<"number">, <start value for id's to be generated>}
# -- SIP user               = {<"number">, <start value for id's to be generated>}
# -- SIP password           = {<"number">, <start value for id's to be generated>}

start_number = 5401
no_of_number = 10
ac = 1001
additional_pin = number
sip_user = number
```

sip_pw = number

-----#

data sequence:

-----#

number # 2. name # 3. AC # 4. IPEI # 5. additionalId # 6. SIP user # 7. SIP password

data_sequence

101;PP 1;;0081008625768

104;PP 4;;0007701154842

;Kiel Phone1;;0127105395099

;Karl May

;Karl Valentin

;Karl Heinz

;Radi Radenkowicz

;Radi Rettich

;Wadi Wade

;Stephan Fiedler;;0127105314450

;Waldi Hartmann;

Zugehöriges Parsingprotokoll über Anweisungsverarbeitung und Einlesung:

Anweisung Parsing:

ok: start_number = 5401

ok: ac = 1001

ok: additional_pin = number

ok: sip_user = number

ok: sip_pw = number

ok: no_of_number = 10

Verarbeitung des Bereichs:

0 : 101;PP 1;1001;0081008625768;101;101;101

1 : 104;PP 4;1002;0007701154842;104;104;104

2 : 5401;Kiel Phone1;1003;0127105395099;5401;5401;5401

3 : 5402;Karl May;1004;;5402;5402;5402

4 : 5403;Karl Valentin;1005;;5403;5403;5403

5 : 5404;Karl Heinz;1006;;5404;5404;5404

6 : 5405;Radi Radenkowicz;1007;;5405;5405;5405

7 : 5406;Radi Rettich;1008;;5406;5406;5406

8 : 5407;Wadi Wade;1009;;5407;5407;5407

9 : 5408;Stephan Fiedler;1010;0127105314450;5408;5408;5408

10 : 5409;Waldi Hartmann;1011;;5409;5409;5409

11 : 5410;;1012;;5410;5410;5410

8.3.2 PP Konfigurationsdatei/ zentral (OMM-Datenbank)

8.3.2.1 Unterstützte Anweisungen

Alle Anweisungen werden als gemeinsamer Wert genommen, der bei allen Sätzen des Datensequenzbereichs dieser Datei eingestellt wird, wenn das entsprechende Feld leer ist.

- name
Standortname
- aktiv
Aktivierung des DECT: {0=inaktiv, 1=aktiv}
- cluster
Cluster, das RFP wird verwiesen auf: {1..256}
- wlan_profile
Referenzschlüssel für ein bestehendes WLAN-Profil
- wlan_antenna
Antenneneinstellungen: = {0=diversity, 1, 2}
- wlan_channel_bg
{0..14 (grösse ist von Regulierungsdomäne abhängig) }
- wlan_power
{ 6, 12, 25, 50,100 (in Prozent)}
- wlan_act
Aktivierung des WLAN: {0=inaktiv, 1=aktiv}

8.3.2.2 Datenbereichsfelder

Die Datenbereichsfelder enthalten die folgende Feldreihenfolge

1. MAC-Adresse
2. Standortname
3. DECT aktiv
4. Cluster
5. WLAN Profilreferenz
6. WLAN-Antenne
7. Channel_bg
8. WLAN power
9. WLAN active

8.3.2.3 Beispiel

RFP Konfigurationsdatei/zentral:

```
# -----#
# instruction section:
# -----#
# -- name      = {<location name>}
# -- active    = {0,1}
# -- cluster   = {1..256}
```



```
# -- wlan_profile      = <valid reference to an existin WLAN profile>
# -- wlan_antenna      = {0=diversity, 1, 2}
# -- wlan_channel_bg   = {0..13 (size depends on regulatory domain) }
# -- wlan_power        = { 6, 12, 25, 50,100 (in percent)}
# -- wlan_act          = {0,1}
```

```
active = 1
cluster = 1
#wlan_profile = 2
#wlan_antenna = 0
#wlan_channel_bg =5
#wlan_power = 12
#wlan_act = 1
```

```
# -----#
# data sequence:
# -----#
# 1.MAC # 2.Name # 3.active # 4.cluster
# 5.wlanProfile # 6. antenna # 7.channelBg # 8.Power # 9.WlanActive
```

```
data_sequence
00:30:42:08:31:A2;142(Mirko)
00:30:42:0D:95:E0;Lab1
00:30:42:0A:C5:40;Lab2(kiel);;2
```

Zugehöriges Parsingprotokoll über Anweisungsverarbeitung und Einlesung:

Anweisung Parsing:

```
nicht eingestellt: location
ok: active = 1
ok: cluster = 1
nicht eingestellt: wlan_profile
nicht eingestellt: wlan_antenna
nicht eingestellt: wlan_channel_bg
nicht eingestellt: wlan_power
nicht eingestellt: wlan_act
```

Verarbeitung des Bereichs:

```
0 : 00:30:42:08:31:A2;142(Mirko);1;1;;;;
1 : 00:30:42:0D:95:E0;Lab1;1;1;;;;
2 : 00:30:42:0A:C5:40;Lab2(kiel);1;2;;;;
```

8.3.3 RFP-Konfigurationsdatei/lokal (OM Configurator)

8.3.3.1 Unterstützte Anweisungen

Alle Anweisungen werden als gemeinsamer Wert genommen, der bei allen Sätzen des Datensequenzbereichs dieser Datei eingestellt wird, wenn das entsprechende Feld leer ist.

- aktiv
Lokale Konfiguration aktiv: {0=inaktiv (DHCP verwenden), 1=aktiv}
- net_mask
Netzmaske
- tftp_server
IP-Adresse des TFTP-Servers
- tftp_file
Pfad und Name der Boot-Datei
- omm_1
OMM-IP-Adresse
- omm_2
IP-Adresse der Backup-OMM
- Gateway
Standard-Gateway
- dns_server
Bis zu zwei DNS-Server-IP-Adressen
- dns_domain
lokale DNS-Domain
- ntp_address
Bis zu zwei NTP-Server-IP-Adressen
- ntp_name
Bis zu zwei NTP-Servernamen
- syslog_addr
IP-Adresse des Syslog-Daemon
- syslog_port
Listen-Port des Syslog-Daemon
- broadcast_addr
Lokale Broadcast-Adresse
- Land
Landescode

8.3.3.2 Datenbereichsfelder

Die Datenbereichsfelder enthalten die folgende Feldreihenfolge

1. MAC-Adresse des RFP
2. Lokale Konfiguration aktiv-Markierung:
3. IP-Adresse des RFP
4. Net mask
5. TFTP-Server
6. TFTP_FILE
7. OMM-IP-Adresse
8. IP-Adresse der Backup-OMM
9. Standardgateway
10. DNS-Server
11. DNS-Domäne
12. NTP-Server-IP-Adresse
13. NTP-Servername
14. Syslog-Daemon-IP-Adresse
15. Syslog-Listen-Port
16. Broadcast-Adresse
17. Landescode

8.3.3.3 Beispiel

RFP-Konfigurationsdatei/lokal (OM Configurator)

```
# -----#
# instruction section                                #
# -----#

active = 1
net_mask    = 255.255.0.0
tftp_server= 172.30.200.92
tftp_file   = omm_ffsip.tftp
omm_1       = 172.30.111.188
omm_2       = 172.30.11.181
gateway     = 172.30.0.2
dns_server  = 172.30.0.4,172.30.0.21
dns_domain  = detewe.de
ntp_addr    = 192.53.103.108,192.53.103.104
ntp_name    = ptbtimel.ptb.de,ptbtime2.ptb.de
syslog_addr= 172.30.200.92
syslog_port= 512
broadcast_addr = 172.30.255.255
country     = 1

# -----#
# data sequence                                      #
# -----#
# 1. MAC_ADDR           ! keine Anweisung unterstützt!
# 2. ACTIVE_FLAG
# 3. RFPADDR            ! keine Anweisung unterstützt!
# 4. NET_MASK
# 5. TFTP_SERVER
# 6. TFTP_FILE
# 7. OMM1
```

```
# 8. OMM1
# 9. GATEWAY
#10. DNS_SERVER
#11. DNS_DOMAIN
#12. NTP_ADDR
#13. NTP_ADDR
#14. SYSLOG_ADDR
#15. SYSLOG_PORT
#16. BROADCAST_ADDR
#17. COUNTRY

data_sequence
00-30-42-01-01-01;;172.30.111.1
00-30-42-02-02-02;;172.30.111.2
00-30-42-01-01-03;;172.30.111.3;
```

Zugehöriges Parsingprotokoll über Anweisungsverarbeitung und Einlesung:

Anweisung Parsing:

```
ok: active = 1
ok: net_mask = 255.255.0.0
ok: tftp_server = 172.30.200.92
ok: tftp_file = /omm_ffsip.tftp
ok: omm_1 = 172.30.111.188
nicht eingestellt: omm_2
nicht eingestellt: gateway
nicht eingestellt: dns_server
nicht eingestellt: dns_domain
nicht eingestellt: ntp_addr
nicht eingestellt: ntp_name
nicht eingestellt: syslog_addr
nicht eingestellt: syslog_port
nicht eingestellt: broadcast_addr
nicht eingestellt: country
```

:parsing ok:

Verarbeitung des Bereichs:

```
: 0 : 00-30-42-01-01-01; 1;172.30.111.1;255.255.0.0;172.30.200.92;
    /omm_ffsip.tftp;172.30.111.188;;;;;;;;;;
: 1 : 00-30-42-02-02-02;1;172.30.111.2;255.255.0.0;172.30.200.92;
    /omm_ffsip.tftp;172.30.111.188;;;;;;;;;;
: 2 : 00-30-42-01-01-03;1;172.30.111.3;255.255.0.0;172.30.200.92;
    /omm_ffsip.tftp;172.30.111.188;;;;;;;;;;
```

Daten erstellen:

```
0 :hinzugefügt: 00-30-42-01-01-01;1;172.30.111.1;255.255.0.0;172.30.200.92;
    /omm_ffsip.tftp;172.30.111.188;;;;;;;;;;
1 :hinzugefügt: 00-30-42-02-02-02;1;172.30.111.2;255.255.0.0;172.30.200.92;
    /omm_ffsip.tftp;172.30.111.188;;;;;;;;;;
2 :hinzugefügt: 00-30-42-01-01-03;1;172.30.111.3;255.255.0.0;172.30.200.92;
    /omm_ffsip.tftp;172.30.111.188;;;;;;;;;;
```

RFP Konfiguration:

```
0 : MAC-Adresse=00-30-42-01-01-01 : use_local_cfg=1 ip=172.30.111.1
    subnet=255.255.0.0 siaddr=172.30.200.92
    boot_file=/omm_ffsip.tftp ommip1=172.30.111.188
```

```
0 : MAC-Adresse=00-30-42-01-01-01 : timer expired ! !

1 : MAC-Adresse=00-30-42-02-02-02 : use_local_cfg=1 ip=172.30.111.2
  subnet=255.255.0.0 siaddr=172.30.200.92
  boot_file=/omm_ffsip.tftp ommip1=172.30.111.188
1 : MAC-Adresse=00-30-42-02-02-02 : timer expired ! !

2 : MAC-Adresse=00-30-42-01-01-03 : use_local_cfg=1 ip=172.30.111.3
  subnet=255.255.0.0 siaddr=172.30.200.92
  boot_file=/omm_ffsip.tftp ommip1=172.30.111.188
2 : MAC-Adresse=00-30-42-01-01-03 : timer expired ! !
```

8.4 Protokolle und Ports

Protokoll	IP DECT Base Station senden		IP DECT Base Station empfangen		OMM senden		OMM empfangen		Kommentare
	SRC Port	DST Port	SRC Port	DST Port	SRC Port	DST Port	SRC Port	DST Port	
DHCP	68	67	67	68	-	-	-	-	Booter
TFTP	Random	69	Random	Random	-	-	-	-	Booter
OMCFG (UDP)	64000	64000	64000	64000	-	-	-	-	Booter / Anwendung
NTP	123	123	123	123	-	-	-	-	Anwendung
Syslog	514	wie konfiguriert	-	-	-	-	-	-	Anwendung
TFTP	> 1023	69	Random	> 1023	-	-	-	-	Anwendung
OMM-RFP-Protokoll (TCP)	> 1023	16321	16321	> 1023	16321	> 1023	> 1023	16321	Anwendung
RTP / RTCP	Bereich der konfigurierten Port-Basis + 72 sogar Ports für RTP, gelegentliche Ports für RTCP	<i>Je nach Remote-Partei</i>	<i>Je nach Remote-Partei</i>	Bereich der konfigurierten Port-Basis + 72 sogar Ports für RTP, gelegentliche Ports für RTCP	-	-	-	-	Anwendung
SIP (UDP)	-	-	-	-	5060	Konfigurierter Proxy-/Registrar-Port	Konfigurierter Proxy-/Registrar-Port	5060	Anwendung
Resiliency (TCP)	-	-	-	-	> 1023	16322	16322	> 1023	Anwendung
LDAP (TCP)	-	-	-	-	> 1023	konfigurierter Port (Standardeinstellung 389)	konfigurierter Port (Standardeinstellung 389)	> 1023	Anwendung
http Umleitung	-	-	-	-	80	Client-Port	Client-Port	80	Anwendung
Web-IF / HTTPS	-	-	-	-	443	Client-Port	Client-Port	443	Anwendung
DNS	> 1023	53	53	> 1023	> 1023	53	53	> 1023	Anwendung

Protokoll	IP DECT Base Station senden		IP DECT Base Station empfangen		OMM senden		OMM empfangen		Kommentare
	SRC Port	DST Port	SRC Port	DST Port	SRC Port	DST Port	SRC Port	DST Port	
ssh	22	Client-Port	Client-Port	22	-	-	-	-	Anwendung
DECTnetMonitor (TCP)	-	-	-	-	8106	Client-Port	Client-Port	8106	Anwendung
Zusätzliche Protokolle ARP ICMP									