

MITEL

3300 | Integrated Communications Platform

IP-DECT WIRELESS SOLUTION TECHNICAL MANUAL

Release 2.0



MITEL

| it's about **YOU**

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks Corporation (MITEL®). The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

Mitel *is* a registered trademark of Mitel Networks Corporation.

Cisco is a registered trademark of Cisco Systems, Inc.

Windows and Microsoft are trademarks of Microsoft Corporation.

Adobe Acrobat Reader is a registered trademark of Adobe Systems Incorporated.

Other product names mentioned in this document may be trademarks of their respective companies and are hereby acknowledged.

Mitel IP-DECT Wireless Solution Technical Manual

Release 2.0
February 2007

®,™ Trademark of MITEL Networks Corporation
© Copyright 2007, MITEL Networks Corporation
All rights reserved

Introduction	7
Purpose of this Manual	7
Who Should Read this Manual	7
Where to Find More Information	7
Glossary of Terms	9
Regulatory Approvals	11
About the IP-DECT Wireless Solution	12
About the RFPs	13
DECT and IP Functionality	15
Clustering Radio Fixed Parts	16
About the Handsets	17
Local Features	19
3300 ICP System Features	20
OpenMobility Manager	21
Media Stream Management	22
Sync-over-air Management	22
Resiliency	22
SNMP	24
Configuration Management	25
3300 ICP System and IP-DECT Integration	26
IP Phone to OpenPhone Call	26
OpenPhone to IP Phone Call	26
OpenPhone to OpenPhone Call	27
Radio Fixed Part Synchronization	27
RFP Channel Capacity	29
Installation and Configuration	31
Overview	31
Understanding System Requirements	31
Power Considerations	32
RFP Licensing	32
System Capacity	34
Portable Part Connectivity	34
Performing the Site Survey	34
Collecting and Recording Site Data	35
Configuring the 3300 ICP E2T Card DHCP Options	36
Configuring the DHCP Scope for Resiliency	36
Configuring Embedded 3300 DHCP	39
Configuring Windows NT DHCP	41
Configuring Windows 2000 DHCP	43
Mounting the Radio Fixed Parts	48
Configuring the OpenMobility Manager	48
Logging in	48
Configuring the License Key and PARK	49
Configuring System Settings	53
Configuring the RFPs	54

Verifying RFP Functionality	56
Configuring SNMP	57
Configuring OpenPhones (Portable Parts)	59
Configuring Authentication Codes and OpenPhone Resiliency	60
Configuring Multiple OpenPhones (Quicker Installation)	61
Configuring Individual OpenPhones	64
Configuring a Site Name and Number on an OpenPhone (Optional)	68
Configuring a Username for an OpenPhone (Optional)	69
Verifying OpenPhone Functionality	69
Backing up Databases	69
Maintenance	71
Health Checklist	71
Changing the Administrator's Password	71
Removing an OpenPhone from the System	72
Changing the Directory Number of an OpenPhone	72
Changing the Directory Name of an OpenPhone	73
Performing Backups	73
Restarting the OMM	75
Resetting OMM Configuration to Defaults	75
Assigning a Different RFP as the OMM	76
Upgrading RFP Firmware	76
Checking OpenPhone Firmware Versions	76
Setting the RFP Subscription List	77
Upgrading License Requirements	78
Upgrading OpenPhone Firmware	78
Troubleshooting	83
Identifying Faults	83
Using the OMM Command Interface	84
Restoring a Database	84
Checking LEDs	85
Identifying Problem Zones	85
Collecting Syslog Daemon Messages	85
Replacing Failed Licensed RFPs	86
Appendix A: Hardware Specifications	87
Radio Fixed Parts	87
From Release 1.5	89
RFP LED Status	90
RFP Startup Sequence	90
IP RFP Booter	91
Portable Parts (OpenPhones)	92
Handset Display	92
Field Strength Display	94
Battery Charge	94
Power	94

Appendix B: MIB-II	95
System Group (1)	95
Interfaces Group (2)	96
Address Translation (AT) Group (3)	101
IP Group (4)	101
ICMP Group (5)	108
TCP Group (6)	110
UDP Group (7)	113
Exterior Gateway Protocol (EGP) Group (8)	114
Common Management Information Services and Protocol Over TCP/IP (CMOT) Group (9) ..	114
Transmission Group (10)	114
SNMP Group (11)	114
Index	119

Introduction

Purpose of this Manual

The Mitel® IP-DECT Technical Manual guide provides instructions on how to install, configure, maintain, and troubleshoot the Internet Protocol Digital Enhanced Cordless Telecommunications (IP-DECT) Wireless Solution.

Who Should Read this Manual

This manual is intended for qualified technicians who will install and configure the IP-DECT Wireless Solution. To qualify to install the IP-DECT Wireless Solution, you must have successfully completed the following training:

- 3300 Integrated Communications Platform (ICP) system technical training
- IP-DECT Wireless Solution technical training.

Where to Find More Information

You can access technical documentation by visiting Mitel OnLine at **www.mitel.com**.



Note: You must be a registered user to access Mitel OnLine. First-time users will be prompted to register and create a username and password which can be used on all subsequent visits.

To access Mitel OnLine:

1. Navigate to **http://www.mitel.com**.
2. Access Mitel OnLine from the Partners and Resellers selection menu.
3. Login to Mitel OnLine by entering your username and password.
4. To access product documentation, click **Technical Support**, and then click **Product Documentation**.

The following guides provide information related to the IP-DECT Wireless Solution.

Mitel Site Survey Instructions: provides instructions on how to use the Site Survey Kit to determine the most suitable locations for the Radio Fixed Parts (RFPs). This guide is available on the Customer Documentation site of Mitel OnLine.

- From Mitel OnLine, click **Technical Support**, click **Product Documentation**, under the **3300 ICP** heading, scroll down to **IP-DECT Wireless Solution**, and then click **Site Survey Instructions for Mitel Systems**.

Radio Fixed Part Specification: describes the operating conditions of the RFPs and provides mounting instructions. This specification is shipped with the RFPs.

Mitel 3300 ICP System Administration Tool Help: provides instructions on how to configure the DHCP server scope, program the wireless phones, and use the 3300 system features that are supported by the wireless phones.

Mitel OpenPhone (OP) 27 Handset User Guide: provides instructions on how to install the batteries, charge the batteries, customize handset operation, use the handset features and use the 3300 ICP system features. This guide is available from the Mitel Customer Documentation site.

Technical Training Materials

Mitel IP-DECT Training provides practical, "hands-on" training to give you the skills and knowledge to install and configure the Mitel IP-DECT Wireless Solution. You can download the Pre-course learning material from the Mitel UK Training web site. From the Mitel OnLine web page at **www.mitel.com**, click **Training**.

Course prerequisites:

- Mitel DECT Theory Pre-course Learning Document
- Mitel DECT Theory Pre-course Learning Test
- Mitel Networks 3300 Installation and Maintenance course.

Release Notes

Every software release is accompanied by a Release Note (RN). The RN describes software changes, bug fixes, outstanding issues, and hardware compatibility considerations for the new software release. **Read the RN before you begin a software upgrade.** To obtain the latest RN, go to the Mitel OnLine web page at **www.mitel.com**. Click **Technical Support**, and then click **Knowledge Base**. Select **IP-DECT** as the Product type, select **Release Notes** as the Article type, and then click **Search**.

Technical Bulletins

Technical Bulletins (TBs) are issued by Mitel Technical Support to address frequently asked questions regarding software and hardware problems. To obtain the latest TBs, go to the Mitel OnLine web page at **www.mitel.com**. Click **Technical Support**, and then click **Knowledge Base**. Select **IP-DECT** as the Product type, select **Technical Bulletins** as the Article type, and then click **Search**.

Glossary of Terms

AAA	Authentication, Authorization, Accounting
ADPCM	Adaptive Differential Pulse Code Modulation
AP	Access Point
BOOTP	Bootstrap Protocol
CAT 5	Category 5 Ethernet cabling – allows data transfers up to 100 Mbps.
CDP	Cisco® Discovery Protocol
CMI	Customized Mobility Instruction – a Mitel Generic Mobility Instruction
DECT	Digital Enhanced Cordless Telecommunication
DECTnet2	Second-generation DECT technology
DECTnetIP	DECT technology that integrates DECT/GAP cordless telephones and equipment into voice-over-IP infrastructure, achieved by means of IP-capable DECT base stations.
DHCP	Dynamic Host Configuration Protocol
DIWU	DECT Interworking Unit
DSP	Digital Signal Processor – detects and generates tones
E2T	Ethernet to TDM converter – a component of the 3300 ICP controller
Extn	Extension device
G.711	Standard that describes the 64-kbps PCM voice-coding technique
G.729a	Standard for compressing a G.711 payload to 8-kbps
GAP	General Access Profile
GMI	Generic Mobility Instruction
GMS	Global Mobile Communications System
GPRS	General Packet Radio Service
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol – for example, PING
ICP	Integrated Communications Platform, such as MN3300 ICP, which controls phones and other devices to provide call features and IP networking capabilities.
IP	Internet Protocol
IPEI	International Portable Equipment Identity
IPRFP	Internet Protocol Radio Fixed Part
LED	Light Emitting Diode
MAC	Media Access Control – hardware address of a device connected to a network.
MiNET	The master-slave control protocol used between ICPs and IP Phones/Devices.
MIPS	Millions of Instructions Per Second – a measure of processing power.

OMM	OpenMobility Manager – management interface for IP-DECT
OP27	OpenPhone 27 – a Mitel handset (wireless phone)
PARK	Portable Access Rights Key – a key used to license Radio Fixed Parts
POE	Power Over the Ethernet
PP	Portable Part – handset (a generic term for a wireless phone)
RFP	Radio Fixed Part – base station for wireless handset
RTP	Real Time Protocol
RTCP	Real Time Control Protocol
RFP 31 IP	RFPs with internal DECT antennas, designed for indoor operation
RFP 32 IP	
RFP 33 IP	RFPs that connect to DECT antennas with special characteristics, designed for outdoor operation
RFP 34 IP	
RFPI	Radio Fixed Part Identification
RSSI	Received Signal Strength Indicator
RTS	Request To Send
SNMP	Simple Network Management Protocol
Sync Over Air	RFP synchronization method
TAN	Transaction Number
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TOS	Type of Service
UPS	Uninterruptible Power Supply
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WPA	WiFi Protected Access

Regulatory Approvals

The CE marking affixed to this product indicates conformance to the R&TTE Directive 99/05/EC (Radio and Telecommunications Terminal Equipment Directive).



For a copy of the complete Manufacturer's Declaration of Conformity, please contact the Regulatory Approvals Manager at the address below:

Mitel Networks Ltd.
Mitel Business Park
Portskewett, Monmouthshire
NP26 5YR
UK.

About the IP-DECT Wireless Solution

OpenMobility IP provides Voice Over IP (VoIP) networks with complete mobility. DECT radio networks are reliable and provide seamless handover, maintaining voice quality and uninterrupted calls when changing radio cell areas. The RFPs and the Portable Parts communicate over the airwaves by using the standard DECT protocol.

The Mitel IP-DECT Wireless Solution consists of the following components:

- **Mitel 3300 ICP:** system platform
- **Radio Fixed Parts (RFPs):** base stations for wireless phones
- **Portable Parts (PPs):** OP27 wireless phones
- **OpenMobility Manager (OMM):** IP management interface for implementing the IP-DECT Wireless Solution, primary and secondary OMMs are configured for resiliency



Note: IP-DECT Release 2.0 does not support Wireless LANs (WLANs). The OMM management interface has data fields for WLAN parameters. When you configure the IP-DECT Release 2.0 solution, ignore the WLAN data fields.

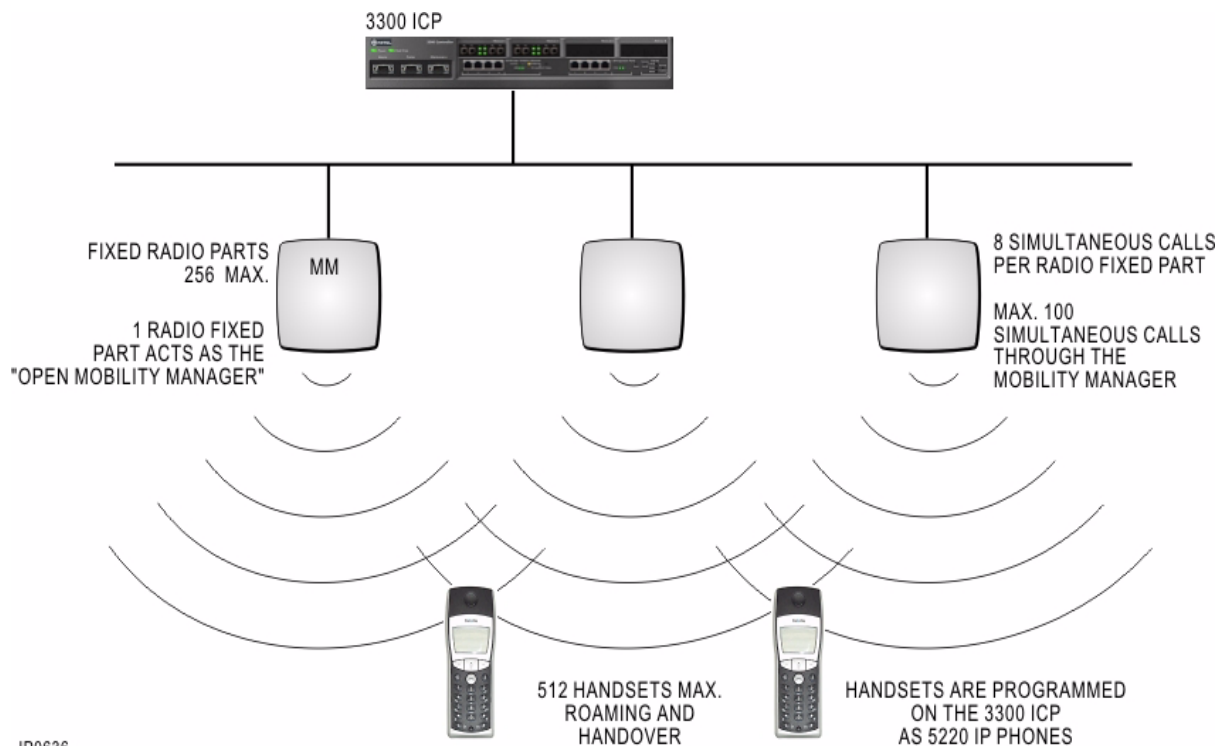


Figure 1: IP-DECT Wireless Solution.

About the RFPs

All RFPs are connected directly to the LAN like a VoIP device and make use of established DECT technology for radio transmission. This ensures full compatibility with cordless DECT terminals, which are available as system telephones and standard GAP terminals.

There are four different models of IP Radio Fixed Parts:

- **RFP 31 IP:** RFP 31 IP has internal DECT antennas and is designed for indoor operation. This RFP has a single signalling LED. If you install this RFP on a wall, the LAN port must face downward for cable connection up from the floor.
- **RFP 32 IP:** RFP 32 IP also has internal DECT antennas and is designed for indoor operation. It has three signalling LEDs that indicate the start-up and operation status of the unit. If you install this RFP on a wall, the LAN port can face upward for cable connection down from the ceiling, or face downward for cable connection up from the floor.
- **RFP 33 IP:** RFP 33 IP is designed for outdoor operation, and/or for the connection of DECT antennas with special characteristics. This RFP has a IP54 class rating and protects against splash water only. It connects to the LAN via an LSA connection module only.
- **RFP 34 IP:** RFP 34 IP is also designed for outdoor operation, and/or for the connection of DECT antennas with special characteristics. This RFP has a IP55 class rating and protects against splash water and jet water. You can connect it to the LAN via an LSA-connection module or via an 8-pole modular jack (RJ45).

The RFPs support two modes of operation: Base Station and OpenMobility Manager (OMM) mode. During installation, you will set one RFP to OMM mode and another to standby OMM mode. Set the remaining RFPs to Base Station mode to act as DECT terminals.

OpenMobility Manager mode

In this mode, an RFP functions as a regular base station, but is also responsible for call setup and management of the IP-DECT solution. You designate one RFP as the OMM and another as the standby OMM by assigning IP Addresses to them in the DHCP scope (see “Configuring the DHCP Scope for Resiliency” on page 36). After an RFP is designated as the OMM, it starts the extra, on-board services (for example, the Web Service that supports the management interface).

Base Station mode

In this mode, an RFP converts IP protocol to DECT protocol and then transmits the traffic to and from the OpenPhones over a 1.8 GHz Media channel. The RFP has 12 available airtime slots, eight of which have associated DSP resources for media streams. The remaining four airtime slots provide control signaling between RFPs and OpenPhones. Each RFP must be able to communicate (sync) with its adjacent RFP to permit call handover when a user crosses from one RFP's zone of coverage to another. The communication between RFPs is serial; that is, it is not necessary for an RFP to communicate directly with all other RFPs in the system. Each RFP only needs to be able to communicate with the next RFP in the chain; however, it is preferable for an RFP to detect more than one RFP to maintain synchronization in the event that one of the RFPs fails. A group of RFPs that can communicate with each other is referred

to as a cluster. (Note that the term cluster is also used by Mitel to identify a group of network elements that share a common Telephone Directory. The two terms should not be confused).

The four control-signaling channels are also used to carry bearer signals that signal the OpenPhone to start the handover process. If the radio signal of another RFP is stronger than that of the current RFP, as the user moves around the site, the OP27 starts the handover process to the RFP that has the stronger signal.

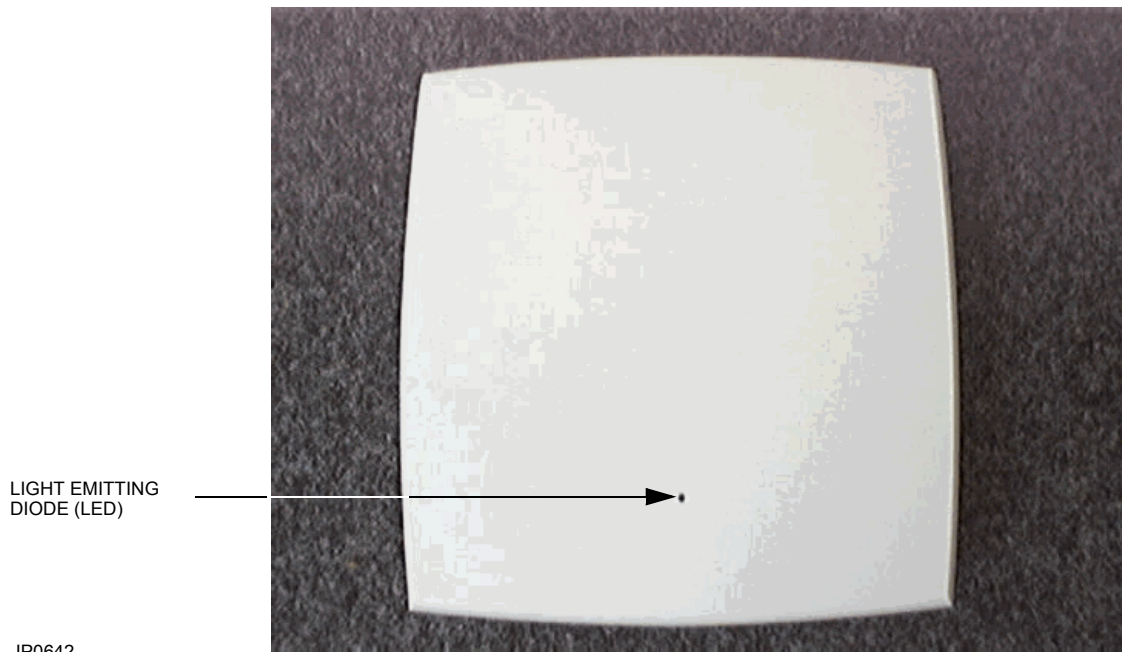


Figure 2: Radio Fixed Part (RFP 31 IP or RFP 33 IP)



Note: The RFP 31 and RFP 33 have one LED that changes color (yellow, orange, and green) to indicate the status of the unit. The RFP 32 and RFP 34 have three separate LEDs (yellow, orange and green) that indicate the status of the unit.

DECT and IP Functionality

The IP RFPs designated as the primary and secondary OpenMobility Managers (OMMs) also provide the following DECT and IP functionality listed in Table 1, “OMM and RFP Features,” on page 15:

Table 1: OMM and RFP Features

Functionality	Feature
DECT	Uses all 120 DECT channels between the base station RFP and the PP
	Provides 8 simultaneous voice channels, plus 4 additional channels for bearer handover and registration
	Synchronizes the IP RFPs via DECT radio interface
	Supports GAP and CAP standards
	Supports connection handover (GAP standard)
IP	Connects via 10/100 BaseT Ethernet
	Supplies Power-over-LAN, in accordance with IEEE 802.3af
	Employs VoIP connection using RTP/RTCP protocol
	Supports network boot, SW download/upgrade capability
	Supports DHCP/ BOOTP capability
	Supports G.711/ G.729 CODEC support, depending on voice quality required and available bandwidth
	Supports Quality of Service by Diffserv/ToS flag
	Supports adaptive jitter compensation
	Supports echo cancellation/ suppression of acoustic and transmission echo
	Supports voice activity detection and Comfort Noise generator
	Supports Media Stream Management
	Supports software download ability upon new system start-up or software upgrade

Clustering Radio Fixed Parts

The IP-DECT Solution is based on the principles of synchronization and cluster management. The DECTnetIP configuration maintains IP RFP synchronization via the radio interface, rather than through the line interface, that was used with the DECTnet2 version of this product. Ideally, all the RFPs within a system should form a single cluster. In configurations that include remote locations, however, remote RFPs must be assigned to their own clusters. If, for example, an RFP cannot detect another RFP located on a different floor of a building or in a completely different building within the same VLAN, then a new cluster is required.

A cluster may consist of one or more RFPs. A network may consist of more than one RFP cluster. The RFPs within a cluster should be synchronized with each other and be able to "see" at least one RFP, but preferably several others, via the radio interface. The limit of the field strength for synchronization between two RFPs is -70 dBm. Handover can occur within the clusters, but cannot span them. If there is more than one cluster, there is no synchronization between clusters, therefore, handover is only possible within a cluster.

The primary OMM has central control over synchronization. The OMM, using information supplied by the RFPs, determines which of the RFPs can see each other. During operation, this information is continually updated in the OMM. The system operates more reliably if every RFP can detect several other RFPs in its cluster. Clusters, in turn, communicate with each other through the OMM over the LAN infrastructure.

On sites where three or more RFPs are used, the best solution is to use three RFPs when licensing to provide some redundancy. RFP redundancy means that no RFP is dependent upon any other RFP. Together, centralized control and redundancy ensure that if one RFP fails, the network, as a whole, will not be affected.

The OMM can handle up to 256 RFPs. These RFPs can be grouped in up to 20 clusters. The number of clusters has no impact on the number of supported RFPs. The OMM synchronizes all RFPs within a cluster, but it does not synchronize clusters.

By default, the OMM chooses one RFP from the cluster to act as the synchronization master for the other RFPs, therefore, you should leave this option disabled. Once the RFPs are synchronized, the 'master' bit in the configuration has no effect.

The example in Figure 3 shows two buildings that are owned by the same company. They have a single DECT Wireless solution spanning two buildings. The circles represent the zones of coverage of the RFPs. The minimum receive signal strength allowed at the Portable Part is -70 dBm. Note that the shape of the signal changes when it has to pass through walls because solid structures absorb the signal. The OMM is situated in the middle of the building and is directly connected over the air to three other RFPs. The RFPs in the larger building cannot

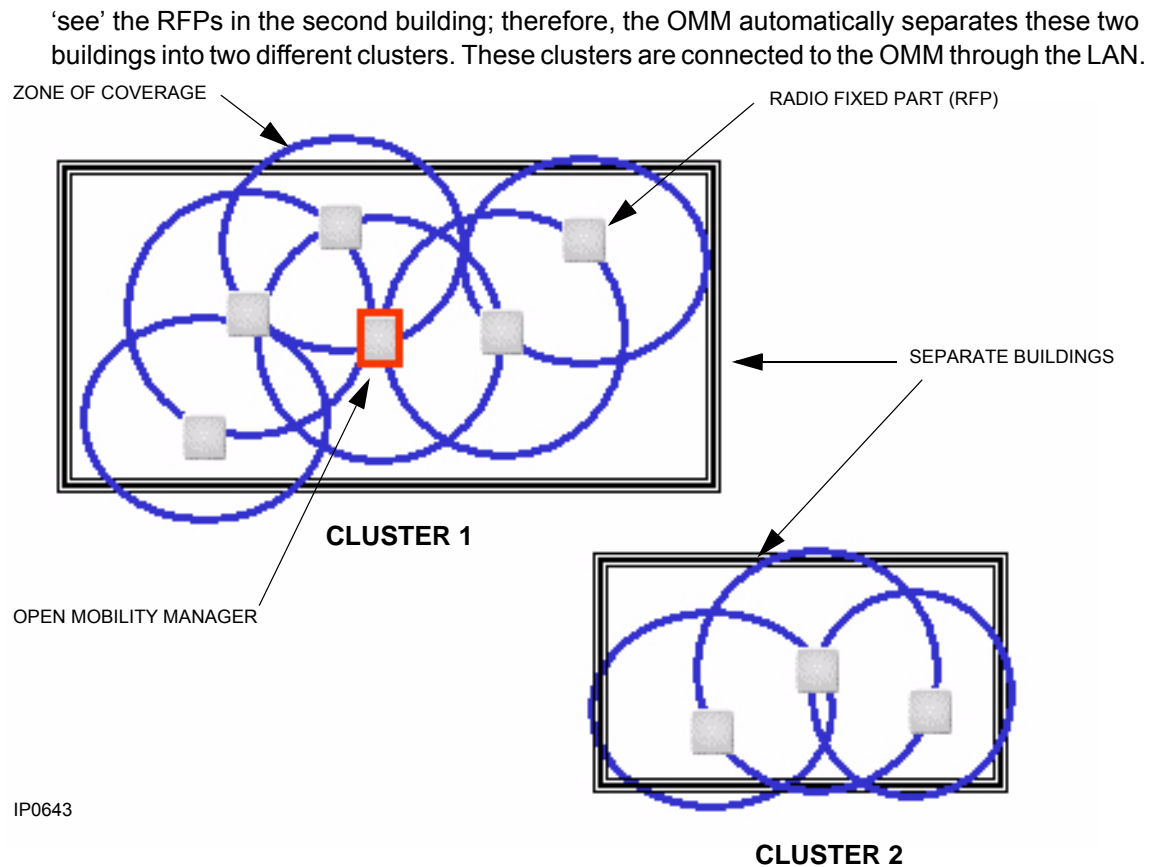


Figure 3: Clustering of Radio Fixed Parts (RFPs)

About the Handsets

OpenPhone 27 (OP27) has a 4-line LCD display, of which two are used to display 3300 ICP system features. The OP27 supports English, French, Dutch, German, Italian and Spanish languages, and G.711 and G.729a compression.



Figure 4: OpenPhone 27 Wireless Handset

The IP-DECT Wireless Solution is supported by the Mitel 3300 ICP (Release 5.0 and later). The OpenPhone 27 is programmed with the device type 'OpenPhone 26/27' within both the 3300 System Administration tool and OPS Manager.





Note: Only the OpenPhone 27 is available as part of the IP-DECT Wireless Solution.



Note: Unlike Mitel IP Phones, OpenPhones do not support Cisco Discovery Protocol (CDP).

Local Features

In local mode, OpenPhone 27 provides the following features:

- **Telephone Book:** Store up to 100 entries, alphabetically sorted. Each entry can contain a maximum of 16 characters for the name and 32 digits for the number. You can search, add, edit, delete the number and name combinations in the book.
- **Menu and Softkeys:** Select functions from menu-driven user interface with three soft keys.
- **Key Lock:** Lock the keypad to prevent accidental dialing with a long press of the # key (or use the Key Lock menu option in local mode). Key Lock is temporarily disabled when a call arrives. To unlock the keypad, press the  softkey and then press #.
- **Auto Key Lock:** Disable the handset keys to prevent accidental dialing. If the Auto Key Lock is enabled, the handset activates the key lock function automatically, if you don't press any key for 1 minute during idle state.
- **Multiple Ringer Settings:**
 - 30 fixed melodies, with various ring tones
 - full melody, single ringing burst or chirp for all incoming traffic
 - enable/disable ringer and trembler
- **Selectable Volume:** 7 levels
- **Key Click:** Enable or disable an audible click for each key press.
- **Alarm Set:** Set an alarm reminder in the 24-hour (hour:minute) format. The 3300 ICP controller must also be using the 24-hour format for this option to work.
- **SOS Number:** Dial a preprogrammed emergency number with a long press of the SOS key (available in idle mode only to prevent accidental usage).
- **Auto Answer:** Automatically answer incoming calls that ring at the handset. You need a headset connected to the handset to use this feature.
- **Silent Charging:** Redirect calls to your extension to your Mitel IP Phone while your OP27 is charging. Use this feature once your Mitel IP Phone has been associated (programmed into a suite on the 3300 ICP) with your OP27 phone. Note that Suite Services is a feature of the 3300 ICP. Check with your system administrator to see if this feature is enabled.
- **Range Warning:** Program 4 short beeps to play whenever you move out of range of the system. When you are out of range of the system, your OpenPhone 27 handset will not function. If you hear the 4 short beeps, move back into range by getting closer to an RFP.
- **RFP Subscription List:** Select from a list of 20 (maximum) installation/sites. Automatic search is supported. If enabled, the OpenPhone supports automatic roaming. If disabled, the handset will always attempt to stay locked to the active selected system.
- **Downloadable FLASH and EPROM:** Upgrade the handset firmware by running an executable on your PC and downloading the software across a mini USB connector interface to the handset (see "Upgrading OpenPhone Firmware" on page 78).
- **Volume Setting:** Set the volume of the ear piece, loudspeaker and the headset during the call by pressing the up- and down-keys (7 levels). You can only set the volume while on a call. To set the volume, a long press of the  key is required.

- **Time:** Display the 3300 ICP system time (24-hour clock only). Note that the 3300 ICP system must be set to 24-hour format.
- **Contrast:** Adjust the contrast of the handset display.
- **Languages:** Choose from a maximum of 8 languages: Dutch, German, Italian, English, French, Spanish, Swedish, Finnish. English is the default.
- **Headset:** Connect a headset using a standard 2.5 mm jack (inline hook switch supported).

Table 2: OpenPhone Local Feature Defaults

Parameter	Default Setting
Key lock	Off
Ringer Settings Internal Melody	1
Ringer Settings External Melody	2
Ringer Settings Type	Full Melody
Ringer Settings Device Buzzer	On
Ringer Settings Device Trembler	Off
Ringer Settings Volume	Level 3
Telephone Options Auto Key Lock	Off
Telephone Options Key Click	On
Telephone Options Alarm	Off
Telephone Options Alarm Time	12:00
Telephone Options SOS Number	<empty>
Telephone Options User Name	<empty>
Telephone Options Language	English
Telephone Options Coverage Warning	Off
Telephone Options Silent Charging	Off
Telephone Book	<empty>
User Name	<empty>
Subscriptions	<empty>

3300 ICP System Features

The OpenPhones support the following 3300 ICP system features:

- Auto-answer
- Call Forward
- Call Forward - Follow Me - End Chaining
- Call Forward - Forced
- Call Forward - Override
- Call Park

- Call Pickup
- Camp-on
- Conference
- Conference Split
- Do Not Disturb
- Flash - Trunk
- Group Page
- Headset Operation
- Hold
- Language Change
- Meet Me Answer
- Messaging - Advisory
- Messaging - Callback
- Messaging - Dialed
- Override
- Record a Call
- Redial, Redial - Saved Number
- Reminder (3300 ICP system must be set to 24-hour clock)
- Speed Call - Personal
- Speed Call - System
- Swap
- Transfer.

OpenMobility Manager

You assign one of the RFPs as the primary or active OpenMobility Manager (OMM) and another as the standby or resilient OMM. The primary or active OMM performs the following tasks:

- manages media stream tasks
- manages sync-over-air functions between RFPs
- manages resiliency
- manages SNMP
- facilitates system configuration modifications.

Media Stream Management

Media stream voice packets are exchanged between the calling party and the IP RFP through which the connection to the Portable Part is established. This RFP is known as the primary RFP. In the case of a handover, where the PP establishes a new connection to another RFP, that RFP is known as the secondary RFP. The voice data is forwarded from the primary RFP to the secondary RFP. If another handover takes place, the voice data is not redirected, the secondary RFP is simply replaced. If a handover back to the primary RFP takes place, the media stream is no longer forwarded.

Media stream management consists of the following:

- call setup
- call handover
- performance management
- channel management - a total of 12 simultaneous channels, providing
 - up to 12 simultaneous channels in redirect state
 - up to 8 simultaneous calls on the air and via the Digital Signal Processor (DSP)
 - remaining 4 time slots are for control and signaling between RFPs and OpenPhones.

Sync-over-air Management

As a user moves from one RFP zone of coverage to the next, the call must be handed off to the next RFP. All RFPs need to be synchronized in order to hand over calls. The primary or active OpenMobility Manager synchronizes the RFPs.

Resiliency

With Release 2.0, both OpenMobility Manager (OMM) Resiliency and Portable Part (PP) Resiliency are supported. To perform OMM Resiliency, two OpenMobility Managers have to be provided in an OMM network; one working as the operational OMM, and the other working as the resilient or standby OMM. In the event that the RFP designated as the OMM fails, the other RFP, designated as the secondary OMM automatically assumes the role of OpenMobility Manager. PP Resiliency ensures resilient phones remain operational in the event a phone's primary 3300 ICP fails over to a secondary 3300 ICP connected to the network.



Note: For additional information about Resiliency, please refer to the 3300 ICP Resiliency document available from Mitel OnLine.

How OMM Resiliency Works

During system startup, each IP RFP retrieves either one (if non-resilient) or two (if resiliency is configured) OMM IP Addresses and tries to connect to them. The active or operational OMM will serve all connections from IP RFPs. The resilient or standby OMM will, in turn, refuse all connection attempts from IP RFPs.

During normal operations, both the active and the standby/resilient OMMs are in contact and monitor each other's operational state. They continually exchange their current resiliency states and the standby OMM receives a copy of any configuration changes on the active OMM. Provided that both OMMs are in contact with each other, their databases are synchronized automatically.

If the primary OMM fails, the OMM responsibilities are taken over by the standby OMM to maintain operation. A **No Redundancy** warning is displayed in the OMM web interface, indicating that there are no longer two functioning OMMs in the network or cluster.

Failover occurs in the following instances:

- The IP connection between OMMs fails
- An OMM software error occurs on the active OMM
- The RFP acting as the active OMM is shut down or rebooted at the Telnet console
- The OMM is rebooted in the web browser menu.

The resilient or standby OMM becomes the active OMM in the following instances:

- The established TCP link to the other OMM times out and a connection to the 3300 ICP is available
- The other OMM has a greater IP Address while no OMM is active and both OMMs are in contact with each other (normally at system startup).

If the active OMM fails, the inactive OMM recognizes this and begins to act as the active OMM, and the web service is started. All IP RFPs being maintained by the OMM will be restarted and all Portable Parts (OpenPhone 27) will be resynchronized. If the connection between the two OMMs fails, the network or cluster essentially breaks into two operational parts. The resilient or standby OMM now becomes the active OMM. The failed (previously active) OMM checks to see whether the connection to the 3300 ICP is still available. At this point, the two OMMs cannot detect one another and, therefore, cannot synchronize. When the connection between the two OMMs is reestablished, the synchronization of the OMMs forces the IP RFP with the greater IP Address to restart and become the standby OMM. Once the recently inactive IP returns to service and becomes the inactive OMM, it does not resume the role of active OMM.

Configuring OMM Resiliency

Both OMMs must be configured in the DHCP configuration section of the Mitel 3300 ICP. The DHCP server provides the OpenMobility system with a mandatory, operational OMM IP Address and an optional, resilient or standby OMM IP Address. Each OMM must be configured with their IP Addresses and DHCP Option 140 for the active OMM and DHCP Option 150 for the standby or resilient OMM.

How PP Resiliency Works

Portable Part (PP) Resiliency keeps resilient phones in an operational state, if at least the phone's primary or secondary 3300 ICP is connected to the network.

Every redirect-handoff or redirect-forced command causes rehomings. When a PP (OpenPhone 27) receives a redirect-handoff or redirect-forced command, there will be a 0-5 second delay before the link can be reestablished. It takes about 35 seconds for the OpenPhone to search for the newly active OMM and resubscribe. During this time, all existing calls will be released and no new calls can be made.



Note: Please note that while detaching/reconnecting ICPs to the network, voice streams routed through those ICPs may be affected. Voice streams are routed through the ICP during conference calls and E2T connections, therefore, during ICP disconnection or reconnection, in-progress conference calls or E2T connections will be dropped. Other calls that are established and not using services on an affected ICP will not be disrupted.

The lower right-hand corner of the OpenPhone display is shared by the OMM and the ICP. An asterisk (*) in this area of the OpenPhone display indicates that there has been a failover to the resilient OMM or ICP.

Configuring PP Resiliency

To configure PP Resiliency, the OMM administrator must enter an IP Address in the **Resilient ICP IP Address** field of the System screen of the OMM. This is the address for the resilient (failover) ICP. Every time the Resilient ICP IP Address is changed from one valid IP Address to another, the OMM will automatically be rebooted. In turn, all PPs connected to that Resilient ICP IP Address will be reset as well.

SNMP

In Release 2.0, an SNMP agent configured in each Radio Fixed Part (RFP) conveys alarm information and facilitates overall SNMP management of large, wireless networks of RFPs and PPs.

All agents are configured in a central place. RFP-dependent parameters like sysLocation and sysName are generated. The sysLocation parameter corresponds to the location configured via the web service. If this location is not configured, sysLocation is set to Location. The sysName parameter is composed of the MAC Address and RFP or OMM RFP if the OMM is running on this RFP.

The SNMP agent responds to SNMPv1 and SNMPv2 read requests for the standard MIB-II objects. You can use the publicly available IETF MIB definitions to decode SNMP messages with your network management system or MIB browser. MIB-II contains the following eleven object groups which are described in greater detail in Appendix B:

- System group
- Interfaces group
- Address Translation (AT) group
- IP group
- ICMP group
- TCP group
- UDP group

- Exterior Gateway Protocol (EGP) group
- Common Management Information Services and Protocol over TCP/IP (CMOT) group
- Transmission group
- SNMP group

For more information about MIB definitions, please navigate to the following URL:

<http://www.simpleweb.org/ietf/mibs/index.html?sel=IETF>

Configuration Management

You configure the IP-DECT Wireless Solution through the web interface provided by the OMM. This management interface allows you to configure the following:

- **System Settings** - configure the ICP used by the primary and secondary (resilient) OMMs, also configure DECT Monitor, Syslog, Regulatory Domain, and Encryption settings
- **Radio Fixed Parts** - configure the RFPs
- **Portable Parts (OpenPhones)** - program, subscribe, add, modify, and delete PPs
- **User Account** - change the OMM usernames and passwords
- **Licensing** - license the RFPs
- **Backup** - perform backups and restores.

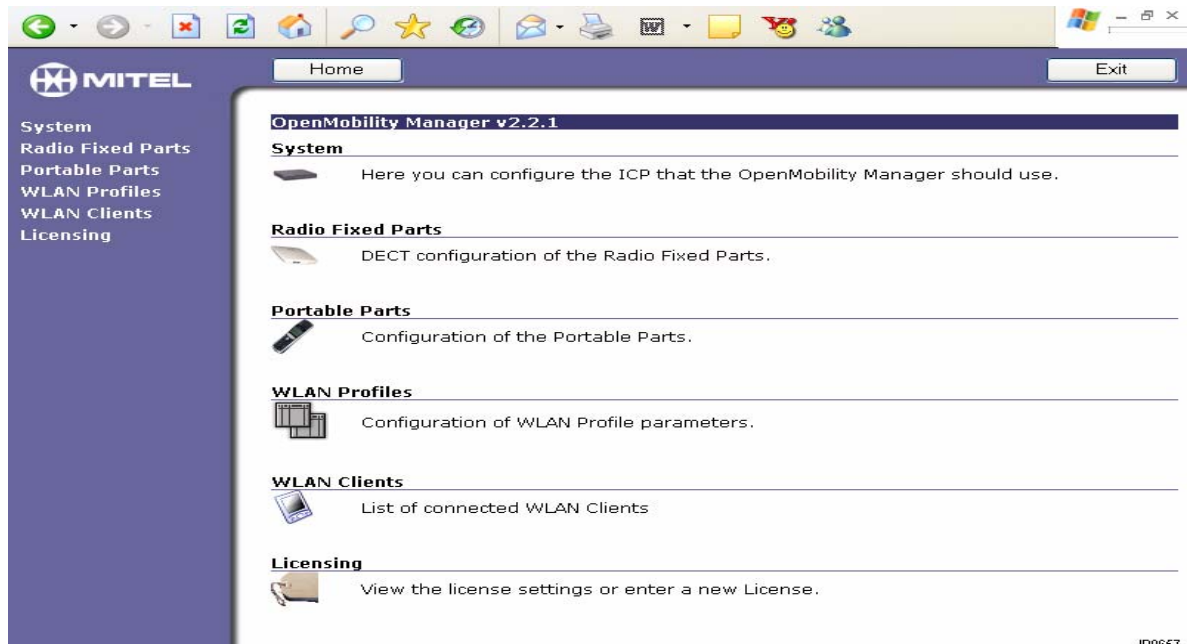


Figure 5: Main Menu of OpenMobility Manager

IP0657

3300 ICP System and IP-DECT Integration

After the RFP is powered on, it broadcasts a DHCP/BOOTP request onto the Virtual Local Area Network (VLAN). The RFP will look for a reply that has bits 140 and 224 set. The reply informs the RFP of the location of the Trivial File Transfer Protocol (TFTP) server (usually embedded in the 3300 ICP) and the file that needs to be downloaded. After the file has been downloaded, the RFP loads the data into its flash memory. The RFP then uses Dynamic Host Configuration Protocol (DHCP) to establish whether it is the designated primary or secondary OMM. If it is designated as either type of OMM, the RFP starts the necessary processes to become either the active or standby OMM. If it is not designated as an OMM, it attempts to sync with other RFPs. After this process is complete, and provided that the OMM is running and correctly licensed, the RFP LEDs turn solid green, indicating that the RFPs are available to support IP-DECT traffic. If the OMM is not correctly licensed, the RFP LEDs will flash green and amber. If any of the boot up processes fail, the RFP LEDs will flash red for two seconds on and two seconds off.

IP Phone to OpenPhone Call

The following steps describe an IP phone call to an OpenPhone that has been programmed with extension 2000.

1. The 5220 IP phone user dials extension 2000. The 3300 ICP then informs the 5220 IP phone of the IP Address for extension 2000.
2. The 5220 IP phone then broadcasts the address onto the LAN. The OMM receives the broadcast and determines that it is one of the addresses assigned to an OpenPhone.
3. The OMM responds to the broadcast by sending its own MAC Address to the 5220 IP phone. After receiving the MAC Address, the 5220 IP phone then streams voice data to the OMM.
4. The OMM determines the location of the OpenPhone and routes the voice data to the appropriate RFP using IP forwarding.
5. Next the IP media stream is connected between the 5220 IP phone and the RFP to which extension 2000 is connected.
6. The RFP converts the data from IP to DECT protocol while keeping the MiNET information intact. The RFP then transmits the data to the OpenPhone.

OpenPhone to IP Phone Call

1. The OpenPhone goes off hook and establishes a media channel to the RFP.
2. The OMM signals to the 3300 ICP that the OpenPhone has gone off hook.
3. The OpenPhone user dials extension 2000.
4. The OMM requests the IP Address of extension 2000 from the 3300 ICP.
5. After the IP Address has been received, the OMM broadcasts the IP Address onto the VLAN.
6. Extension 2000 responds by forwarding its MAC Address to the RFP that is being used by the OpenPhone and the call is then established.

OpenPhone to OpenPhone Call

A call from one OpenPhone to another that resides on the same RFP will loop back within the RFP, so the call will not pass through to the Local Area Network (LAN). Unlike signaling packets, voice packets will not impact LAN traffic. The 3300 ICP uses signaling packets to set up and control a call between two OpenPhones. These signaling packets are carried on the wired LAN between the OMM and the 3300 and will add to the traffic on the wired LAN. Voice packets to support the conversation between the two OpenPhones are not routed to the 3300 ICP, and therefore, will remain within the RFP.

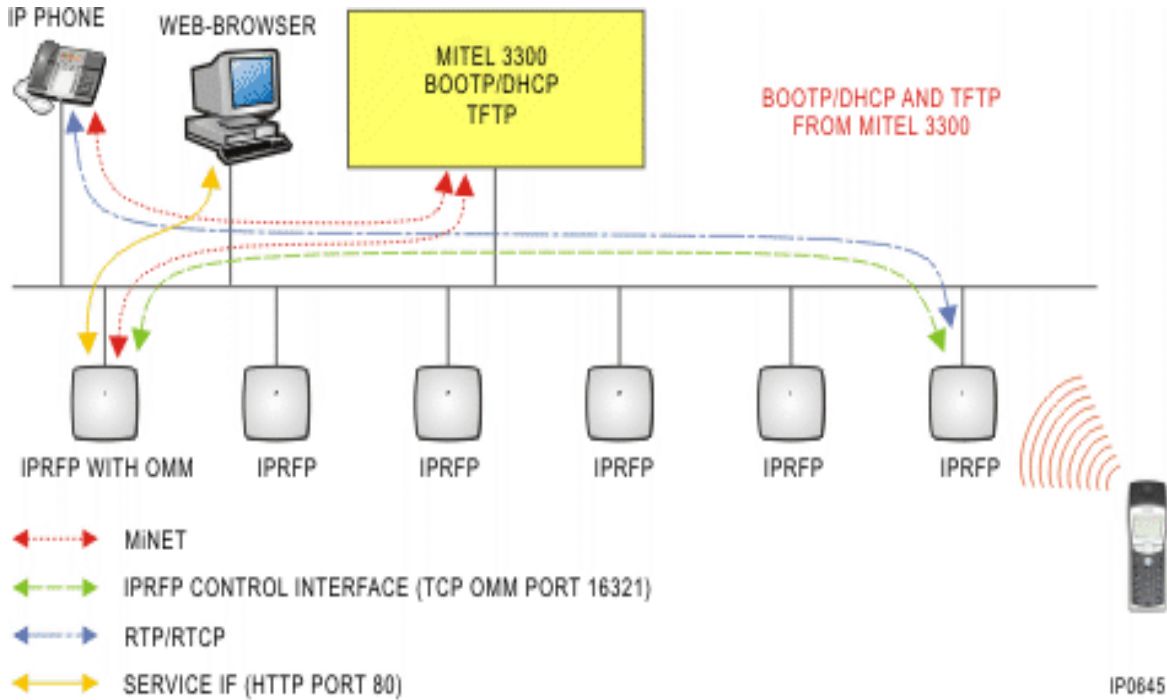
Radio Fixed Part Synchronization

As a caller moves from one RFP zone of coverage to another, the call must be transferred from one RFP to the next. RFPs must be synchronized over the airwaves to support the handover of calls. For the RFP to sync to another RFP, the signal strength cannot drop below -70 dBm. You must consider this requirement during the site survey.

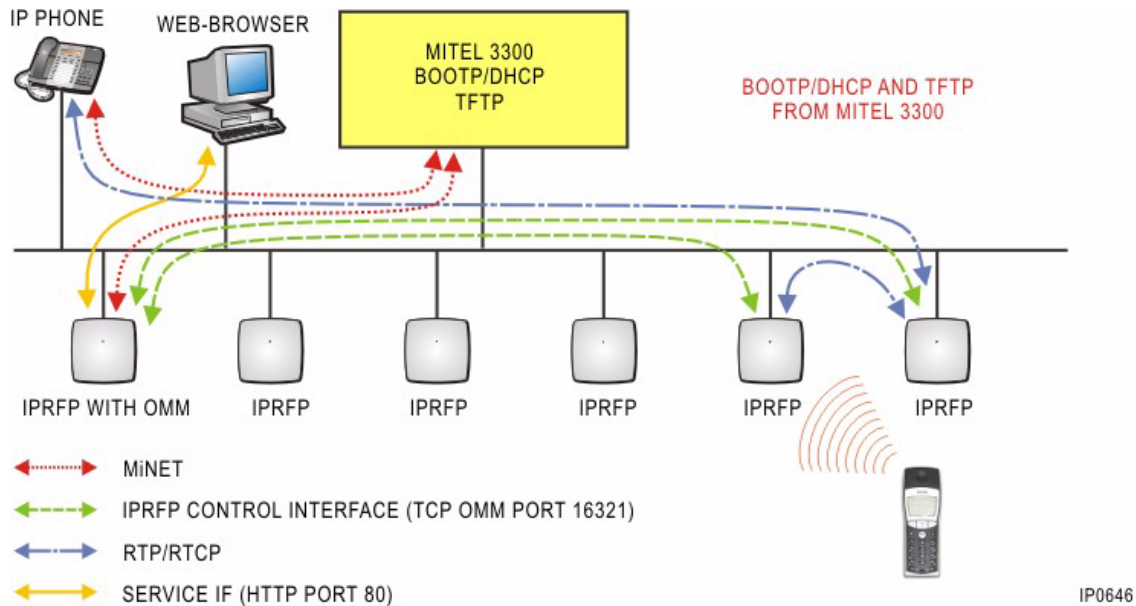
To establish a call between an IP Phone and an OpenPhone, the following media streams must be established:

- a MiNET link to and from the IP phone
- a MiNET link to and from the OMM
- a control interface between the OMM and the RFP that has a connection to the OpenPhone (known as the primary RFP)
- a Real Time Protocol (RTP) or Real Time Control Protocol (RTCP) connection between the IP Phone and the OMM; and then an RTP/RTCP connection between the IP Phone and the RFP, once IP forwarding has taken place.

Figure 6 illustrates the process of establishing media streams.

**Figure 6: Media Stream Management: Primary IP RFP**

If the OP27 user is moving, the OpenPhone detects that another RFP has a better signal strength and starts the handover process. The media stream from the IP Phone cannot move to the secondary RFP, so the primary RFP uses the LAN to direct the voice to the secondary RFP.

**Figure 7: Media Stream Management: Primary and secondary IP RFP**

As the OpenPhone user moves into the next RFP zone of coverage, the OpenPhone detects that the RFP has a better signal strength. Again, the media stream from the IP phone cannot move to the secondary RFP, so the primary RFP uses the LAN to direct the voice to the secondary RFP.

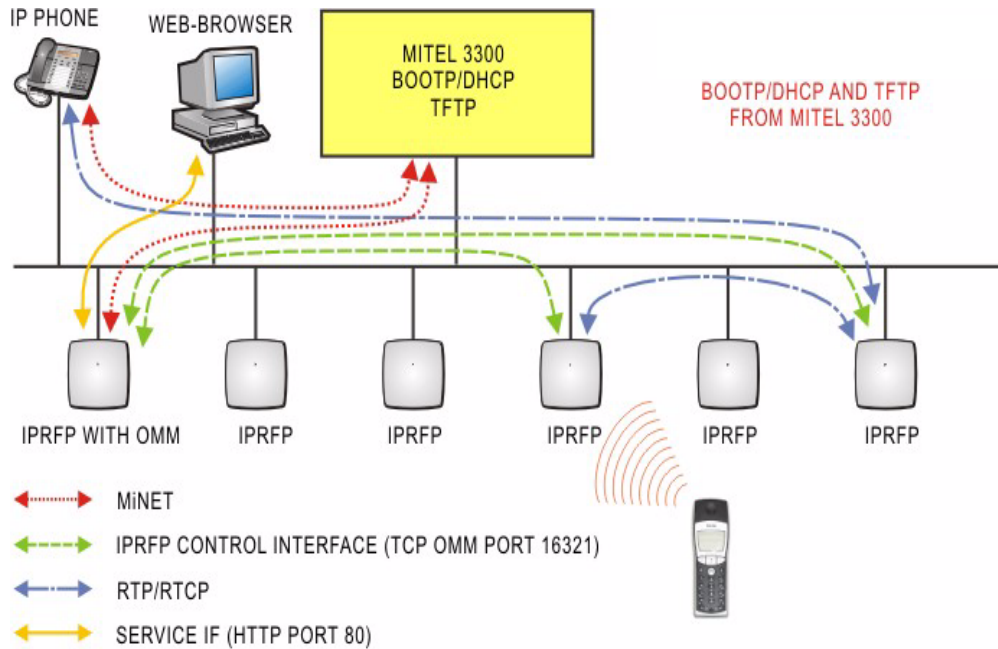


Figure 8: Media Stream Management: Primary and New Secondary IP RFP

RFP Channel Capacity

The RFP has 12 available airtime slots or channels. Eight are simultaneous voice channels with an associated DSP resource for media streaming. The maximum number of calls on an RFP is eight due to DSP resource limitation. The remaining four channels are dedicated to the handover of calls between base stations.

The IP-DECT Wireless Solution uses a 'Busy Bit' to announce to the OpenPhones that all eight voice channels are in use. Once the OpenPhone determines that another RFP is within range and can be used, the OpenPhone will begin handover to that new RFP. Once the handover is complete, the RFP will then clear the Busy Bit.

Each time the Busy Bit is announced by an RFP, a log entry is made to the system logs (see "Collecting Syslog Daemon Messages" on page 85).

If the Busy Bit is often being set in a specific zone, an extra RFP could be installed. Installing an extra RFP doubles the number of media streams available for calls.

Installation and Configuration

Overview

To install and configure the IP-DECT Wireless Solution, you must complete the following tasks:

- ☑ understand system requirements
- ☑ perform a site survey
- ☑ record site data
- ☑ install the RFPs
- ☑ configure the 3300 ICP E2T card DHCP options
- ☑ configure the DHCP scope
- ☑ configure the OMM
- ☑ configure the OpenPhones
- ☑ verify OpenPhone operation
- ☑ backup the databases.

Understanding System Requirements

Before installing the IP-DECT Wireless Solution, you must take into account the following conditions:

- RFPs must be located no more than 100 meters from a Layer 2 switch.
- To provide adequate coverage, RFPs should be positioned to ensure that signal strength is always greater than -70 dBm
- RFPs must be in the same VLAN as the 3300 ICP.
- The IP-DECT Wireless Solution must be programmed so that all Portable Parts (OpenPhones) reside on a single 3300 ICP.
- Layer 2 switch ports must be configured with native Virtual LANs in the same VLAN in which the 3300 ICP resides (VLAN tagging is not used).
- Redundant Sync-Over-Air connections should be used to prevent a single point of failure.
- OpenPhones can be programmed as resilient devices on a 3300 ICP.
- OpenPhones do not support the 3300 ICP Hot Desking feature.



Note: For more detailed information about cabling, please refer to the 3300 ICP Hardware Technical Reference Manual available from Mitel OnLine.



Note: RFPs must be located more than 20 cm away from personnel, to maintain Specific Absorption Rate (SAR) requirements for safe radio frequency (RF) levels.

Power Considerations

Each RFP requires any one of the following –48v DC power supplies:

- 802.3af compliant power supply (for example, an 802.3af compliant Layer 2 switch or an add-on PowerDsine power supply) - Power Over Ethernet (POE) can supply up to 24 RFPs from a single location.
- Power Adapter - This inline power adapter is used with the 5200 series sets. The distance between the RFP and mains supply is not crucial, but CAT-5 cabling rules apply:
 - UK variant: PN 50002080
 - International variant: PN 50002090
- Power Adapter (available from DeTeWe Corporation) - The RFP must be located within 2 meters of the mains power supply.
 - UK variant: PN 51007304
 - International variant: PN 51007304



Note: RFPs must be located more than 20 cm away from personnel, to maintain Specific Absorption Rate (SAR) requirements for safe radio frequency (RF) levels.

RFP Licensing

When you license the RFPs through the OMM configuration tool, the maximum number of RFPs that can be installed on-site is shown in the licensing menu. Note that the number of RFPs specified by the license includes the OMM RFP. There are three types of licenses:

- License A: For small installation sites with 1 or 2 RFPs.
- License B: For large installation sites with 3 to 256 RFPs.
- License C: Upgrade from A to B.

You can select one of the options listed in Table 3.

Table 3: RFP Licenses

Number of RFPs installed at site (including OMM)	Install Type	Number of MAC Addresses keyed in license	Number of keyed RFPs required to keep making calls	OMM License Type Required
1 or 2	Small site or demonstration	1 or 2 (maximum of 2 RFPs)	All	A
3 to 256	Large sites with high traffic	3 (maximum of 256 RFPs)	2	B
3 to 256	Upgrade from OMM license type A to license type B	3 (maximum of 256 RFPs)	2	C

If only one RFP is installed and it fails, the OpenPhones will lose service. If two RFPs are installed and one fails (loses connection to the LAN) the license is invalidated, and the IP-DECT Solution will go into no-way audio. Therefore, on sites where three or more RFPs are used, the best solution is to use three RFPs when licensing to provide some redundancy. If one of

the license RFPs fails or loses connection, an error will be raised on the OMM. Any OpenPhone in that RFP's zone of coverage that is able to connect to one of the other RFPs will not lose service. If the other two RFPs are still operating, then service within their zones of coverage will not be affected.

However, if the OMM RFP fails and no standby OMM is designated, all IP-DECT calls in the cluster will be dropped and no further calls can be made until the OMM is restored. If the OMM fails and a standby OMM is designated, all the calls will be dropped, but further calls can be made when the PPs have automatically resubscribed to the new OMM.

When you install the IP-DECT Solution, distribute the RFPs across different Layer 2 switches. To further increase resiliency, connect the active and standby OMMs and at least one other RFP to an uninterruptible power supply (UPS).

You need a license for each installation and a unique key to activate each license. The license security code -- the Transaction Number (TAN) -- is printed on a separate sheet of paper and supplied in its own sealed envelope. The Mitel part number printed on the paper will be visible through the window of the envelope.

Obtaining Licenses

1. Ensure that you order a type A, B, or C license suitable for the size of the installation site prior to installation.
2. Ensure that Internet access is available at the site via the customer's LAN, analog/ISDN dial-up connection, or Global Mobile Communications System (GSM) or General Packet Radio Service (GPRS) laptop connection.
3. Access Mitel OnLine by using an Internet browser to navigate to **<http://www.mitel.com>**.
4. Select Mitel OnLine from the Partners and Resellers selection menu.
5. Login to Mitel OnLine by entering your username and password.



Note: You must be a registered user to access Mitel OnLine. First-time users will be prompted to register and create a username and password which can be used on all subsequent visits.

6. Click **Technical Support**, click **ICP Password Inquiry**, and then click **IP-DECT Licences**.
7. In the User Name field, enter "mitel".
8. In the Password field, enter "berlin".
9. Click **OK**.
10. Click **generate keys**.
11. Enter your OMM serial number and TAN. See "Configuring the License Key and PARK" on page 49 for details.
12. Click **generate key**. The license type, OMM key, and PARK number are displayed. Record or print the license information.

System Capacity

The IP-DECT Solution can be expanded up to 256 RFPs, one of which must be the primary or active OMM, another of which must be the secondary or standby OMM, and up to 512 Portable Parts. All the RFPs in this configuration are used for IP-DECT conversion and data transmission.

All Portable Parts (PPs) must be programmed on a single, primary 3300 ICP. Therefore, the number of Portable Parts may be restricted by the type of 3300 ICP installed, for example, a 100-user Mitel 3300 ICP. Each Portable Part uses a device license and a user license on the 3300 ICP, so the 3300 ICP configuration guidelines must also be taken into consideration.

Table 4: System Capacities

Type	Feature	Maximum Number
DECTnetIP	OpenMobility Managers	2 (1 primary, 1 secondary)
	IP RFPs	256 (including 1 primary and 1 secondary)

Portable Part Connectivity

The Portable Part uses standard DECT over the 1.88 GHz to 1.9 GHz frequency band. The DECT signal uses Adaptive Differential Pulse Code Modulation (ADPCM) with the MiNET Protocol superimposed on its control channel giving OpenPhone users access to the 3300 ICP phone features.

Each OpenPhone is associated with a Transmission Control Protocol (TCP) connection with the OMM. For example, if 50 OpenPhones are programmed on the OMM, the OMM will have 50 virtual TCP connections on the LAN. Each time there is an ARP on the network for the OpenPhone, the OMM will respond with its own MAC Address.

The virtual TCP connections are not always connected. When you turn on an OpenPhone an IP Address is set up on the OMM and a TCP connection is established with the 3300 ICP. When you turn off the OpenPhone, the connection is closed and the IP interface is removed.

Performing the Site Survey

You must perform a site survey before you install the IP-DECT Wireless Solution. The survey determines the locations of the RFPs and identifies any areas on the site that cannot support OpenPhone service. A diagram of the building is essential for noting structural details and marking the location of the RFPs.

With Release 2.0, DECTnetIP and DECTnet2 can operate on the same system to extend network coverage to more remote and much larger locations.

Please refer to the Mitel 3300 ICP IP-DECT Wireless Solution Site Survey Instructions for Mitel Systems. These instructions are available from the Product Documentation link of Mitel OnLine at www.mitel.com.



Note: You must be a registered user to access Mitel OnLine. First-time users will be prompted to register and create a username and password which can be used on all subsequent visits.

To access Mitel OnLine:

1. Navigate to **<http://www.mitel.com>**.
2. Access Mitel OnLine from the Partners and Resellers selection menu.
3. Login to Mitel OnLine by entering your username and password.
4. To access product documentation, click **Technical Support** and then click **Product Documentation**.

Collecting and Recording Site Data

As you perform the installation, record the site data in the following table.

Table 5: Site Data

Site Data	When/Where	Value
Number of OpenPhone users	Site Survey	
Number of 3300 ICP licenses available	3300 ICP system	
Transaction Authorization Numbers for RFP licensing (see "RFP Licensing" on page 32)	Mitel Order Desk	
Number of RFPs required	Site Survey	
Number of RFP clusters	Site Survey	
Type of RFP license required	A, B, or C	
MAC Address of RFP 1 (OMM)	Recorded on RFP	
MAC Address of RFP 2	Recorded on RFP	
MAC Address of RFP 3	Recorded on RFP	
Type of DHCP server (embedded 3300 ICP or NT Server)	LAN Administrator	
If using embedded 3300 ICP DHCP server IP Address of primary OMM (RFP) IP Address of secondary OMM (RFP) IP Address of 3300 ICP IP Address of syslog daemon server Port address of syslog daemon server	LAN Administrator	
If using NT DHCP or Windows 2000 DHCP Boot Server Host Name Bootfile Name IP Address of primary OMM (RFP) IP Address of secondary OMM (RFP) IP Address of 3300 ICP IP Address of syslog daemon server Port address of syslog daemon server	LAN Administrator	

Page 1 of 2

Table 5: Site Data (continued)

Site Data	When/Where	Value
RFP IP Address (for each RFP in the system)	LAN Administrator	
RFP IP Address	LAN Administrator	
RFP IP Address	LAN Administrator	
RFP IP Address	LAN Administrator	
RFP IP Address	LAN Administrator	
IP-DECT System Serial Number	OMM	
Transaction Number (TAN)	From envelope	
PARK	Mitel OnLine	
License Key	Mitel OnLine	
Range of OpenPhone directory numbers	3300 ICP system	
OpenPhone User Names	Customer	
OpenPhone account code (AC) range	Defined during installation	
Page 2 of 2		

Configuring the 3300 ICP E2T Card DHCP Options

Normally, the E2T card of the 3300 LX Controller uses DHCP options 66 (TFTP server) and 67 (Boot filename) to retrieve its bootfile from the RTC. If an IP-DECT solution or an LX system is implemented, a conflict with options 66 and 67 will occur. The RFPs utilizing BOOTP or DHCP also use options 66 and 67 to locate the iprpf.bin file. The best solution is to set up a reserved IP Address for the E2T Card with its own DHCP option information for options 66 and 67. This avoids the conflict on an LX system.



Note: This options conflict only occurs with the 3300 LX Controller or where the E2T card is set to boot from DHCP options 66 and 67.

Configuring the DHCP Scope for Resiliency

In order to boot IP RFPs, there must be a DHCP server and a TFTP Server attached to the network, although they do not need to reside on the same host. The following RFCs are supported:

- RFC 1350, The TFTP Protocol (Revision 2), July, 1992
- RFC 2131, Dynamic Host Configuration Protocol, March, 1997.

Upon initial startup, an IP RFP starts a DHCP client to transmit a DHCP Request to determine its own IP Address, Subnet Mask, and optional values, such as Default Gateway and Mitel-specific information via DHCP. It also determines the IP Address of the TFTP server and the filename from which to download using DHCP.

The DHCP server must be configured with the following options:

- Option 66 - Boot Server Host Name (typically the IP Address of the 3300 ICP RTC)
- Option 67 - Bootfile Name (iprfp.bin)
- Option 140 - IP Address of the primary OpenMobility Manager
- Option 150 - IP Address of the secondary OpenMobility Manager (required for a resilient OMM system)
- Option 224 - The value, "OpenMobility", is required by the RFP DHCP client to determine which DHCP servers are valid.

When configuring the DHCP server, the following are optional:

- Option 141 - identifies the Syslog Daemon server
- Option 142 - determines server port of the Syslog Daemon
- Option 254 - automatically updates the booter version (from 2.x to 3.y).



Note: To fully update the Booter version, the RFPs must be rebooted twice. To verify the Booter version, log into the RFP through a Telnet session.

Once Options 140 and 150 are configured and reservations for those two options are made, the active and inactive OMMs are designated. Once the primary and secondary OMMs are designated, all other RFPs can get their IP Addresses dynamically.

Options 141 and 142 relate to the Syslog Daemon and are not required for the system to operate, but can be configured either through the OMM or at the DHCP server. For instructions on how to configure both options from the OMM, see "Configuring System Settings" on page 53.

Please note that DHCP server options can change from release to release. The following table shows the DHCP options currently used.

Table 6: DHCP Options

Number	Meaning	Additional Information
001	Subnet Mask	The DHCP Server derives the subnet mask value at runtime from other configuration parameters.
003	Router IP Address	IP Address of the default gateway (router)
050	Client IP Address	IP Address of the DHCP client
055	Parameter request list	Lists the options requested by the DHCP client
060	Vendor class identifier	Enter, "Open Mobility".
066	TFTP server for gateway/E2T	TFTP server name; Boot Server Host Name
067	Boot file name for gateway	ASCII string
128	TFTP Server (usually the controller RTC IP Address)	IP Address of the TFTP Server

Table 6: DHCP Options

Number	Meaning	Additional Information
129	RTC IP Address for controller	For Resilient systems, enter up to four IP Addresses of remote failover RTCs. Separate entries with a comma and a space, ", ".
132	VLAN ID	VLAN ID for Voice LAN (32 bits)
133	VLAN Priority	VLAN tagging priority (values are 1-7; Mitel recommends 6)
140	IP Address of active or primary OMM	Enter the IP Address of an RFP to designate it as the primary OMM. Must be 4 bytes in length.
141	Syslog Server IP Address	Enter the IP Address to identify the Syslog Daemon server.
142	Syslog Server Port IP Address	Enter the IP Address of the port to which the syslog server is listening (16 bits).
150	IP Address of standby or secondary OMM	Enter the IP Address of an RFP to designate it as the secondary OMM. Must be 4 bytes in length.
224	Magic string	The value of this string must be "OpenMobility". The DHCP client checks for this option to determine which DHCP server to use. Required by Booter version 3.x. Ignored by Booter version 2.x.
225	Public option	
226	Public option	
254	Automatic booter update	Enter "UPDATE" to automatically update booter from version 3.x to 3.y. Updating from version 2.x to 3.x requires a manual update.



Note: In order for the DHCP server to recognize a DHCP offer, either Option 224 must be activated, or the file field in the DHCP message must have a substring equal to "ip_rfp.cnt". If neither is present, the DHCP offer will be ignored. When using Booter version 3.x, Option 224 is required. When using Booter version 2.x, "ip_rfp.cnt" is required.



Note: It is possible to have both booter versions (2.x and 3.x) present in one installation at the same time.



Note: If VLAN tagging is selected (Options 132 and 133), the client suspends the current registration during startup, turns on VLAN tagging and restarts.

The IP-DECT Wireless solution can obtain IP Addresses for the RFPs from the following DHCP servers:

- a DHCP server embedded in the 3300 ICP controller (see "Configuring Embedded 3300 DHCP" on page 39)
- a DHCP server running on Windows NT Server (see "Configuring Windows NT DHCP" on page 41)

- a DHCP server running on Windows 2000 Server (see “Configuring Windows 2000 DHCP” on page 43)

Configuring Embedded 3300 DHCP

The DHCP server must be configured with the following options:

- Option 66 - Boot Server Host Name (typically the IP Address of the 3300 ICP RTC)
- Option 67 - Bootfile Name (iprftp.bin)
- Option 140 - IP Address of the primary OpenMobility Manager
- Option 150 - IP Address of the secondary OpenMobility Manager (required for a resilient system).
- Option 224 - The value, "OpenMobility", is required by the RFP DHCP client to determine which DHCP servers are valid.

When configuring the DHCP server, the following are optional:

- Option 141 - identifies the Syslog Daemon server
- Option 142 - determines server port of the Syslog Daemon
- Option 254 - automatically updates the booter version (from 3.x to 3.y).

Once Options 140 and 150 are configured and reservations for those two options are made, the active and inactive OMMs are designated. Once the primary and secondary OMMs are designated, all other RFPs can get their IP Addresses dynamically.

Option 141 and 142 relate to the Syslog Daemon and are not required for the system to operate, but can be configured either through the OMM or at the DHCP server. For instructions on how to configure both options from the OMM, see “Configuring System Settings” on page 53.



Note: To fully update the Booter version, the RFPs must be rebooted twice. To verify the Booter version, log into the RFP through a Telnet session.

To configure the embedded 3300 DHCP server:

1. Log into the 3300 ICP System Administration Tool.
2. Choose **System Configuration**, click **IP Network Configuration**, and then click **DHCP Options**.
3. In the DHCP Options form, assign the Boot Server Host Name:
 - **ID:** Enter **66**.
 - **Format:** Select **IP Address**.
 - **Value:** Enter the IP Address of the Boot Server Host Name.
 - **Scope:** Select **Global**.
4. In the DHCP Options form, assign the Bootfile Name:
 - **ID:** Enter **67**.
 - **Format:** Select **IP Address**.
 - **Value:** Enter the IP Address of the Bootfile Name.

- **Scope:** Select **Global**.
5. In the DHCP Options form, assign the primary (active) OpenMobility Manager:
 - **ID:** Enter **140**.
 - **Format:** Select **IP Address**.
 - **Value:** Enter the IP Address of the Radio Fixed Part (RFP) that you want to assign as the primary OpenMobility Manager (OMM).
 - **Scope:** Select **Global**.
 6. In the DHCP Options form, assign the secondary (standby) OpenMobility Manager:
 - **ID:** Enter **150**.
 - **Format:** Select **IP Address**.
 - **Value:** Enter the IP Address of the Radio Fixed Part (RFP) that you want to assign as the secondary (resilient) OpenMobility Manager (OMM).
 - **Scope:** Select **Global**.
 7. Enter, "OpenMobility" as the value of Option 224.
 - **ID:** Enter **OpenMobility**.
 - **Format:** Select **ASCII string**.
 - **Value:** Enter "OpenMobility" as the Vendor class identifier.
 - **Scope:** Select **Global**.
 8. Assign a server to collect the syslog daemon messages (optional). You can configure the syslog daemon of the RFPs to send messages across the network to a syslog daemon running on a network server. These log messages are useful for troubleshooting.
 - **ID:** Enter **141**.
 - **Format:** Select **IP Address**.
 - **Value:** Enter the IP Address of the server that will collect the log messages generated by the IP-DECT syslog daemon.
 - **Scope:** Select **Global**.
 9. Identify the server port of the syslog daemon (optional):
 - **ID:** Enter **142**.
 - **Format:** Select **Numeric**.
 - **Range:** Enter a 1 to 5-digit number.
 - **Value:** Enter the server port number of the syslog daemon.
 - **Scope:** Select **Global**.
 10. In the **DHCP Static IP** form, assign a static IP Address to the primary (active) OpenMobility Manager RFP (see Figure 9).
 - **Name:** Enter a name, for example "primary OMM", to identify the OpenMobility Manager RFP.
 - **Subnet:** Select the subnet of the primary OMM.
 - **IP Address:** Enter the IP Address of the primary OpenMobility Manager RFP.
 - **Protocol:** Accept default **BOOTP** (Booter version 2.x) or **DHCP** (Booter version 3.x).

Under Hardware Address:

- **Type:** Select **MAC Address**.
- **Other - Type:** Leave blank.
- **Address:** Enter the MAC Address of the primary OpenMobility Manager RFP. The MAC Address is on a label that is affixed to the base of the RFP.
- **Other - Address Length:** Leave blank.
- **Client ID:** Leave blank.

11. Repeat the previous step for the "secondary OMM" and for each RFP in the system.

Figure 9: Configuring the OMM MAC Address

Configuring Windows NT DHCP

To configure the NT DHCP Server, you must perform the following tasks:

- configure the DHCP Scope (setting Options 140 and 150). See "Configuring the DHCP Scope with Windows NT" on page 42.
- set up reservations for RFPs. See "Setting Up Reservations for RFPs with Windows NT" on page 42.
- add Booter options to reservations. See "Adding DHCP options to the Reservations with Windows NT" on page 43.

The DHCP server must be configured with the following options:

- Option 140 - IP Address of the primary OpenMobility Manager
- Option 150 - IP Address of the secondary OpenMobility Manager (required for a resilient system).
- Option 224 - The value, "OpenMobility", is required by the RFP DHCP client to determine which DHCP servers are valid.

When configuring a DHCP server, the following are optional:

- Option 141 - identifies the Syslog Daemon server
- Option 142 - determines server port of the Syslog Daemon
- Option 254 - automatically updates the booter version (from 3.x to 3.y).

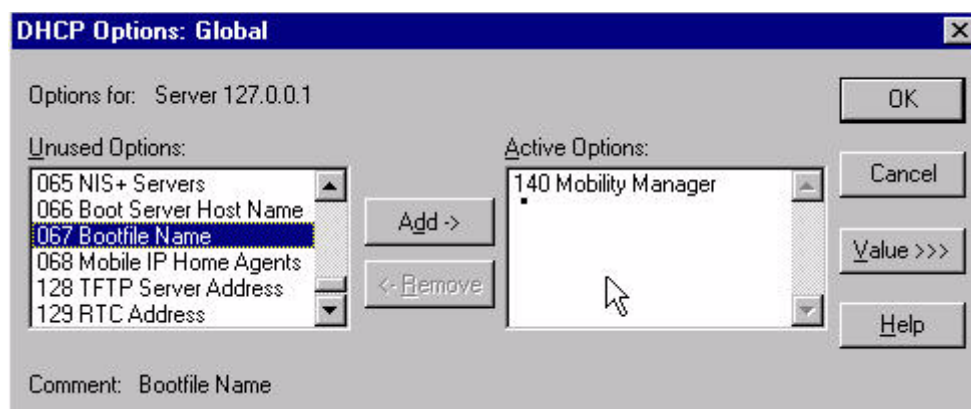


Note: To fully update the Booter version, the RFPs must be rebooted twice. To verify the Booter version, log into the RFP through a Telnet session.

Option 141 and 142 relate to the Syslog Daemon and are not required for the system to operate, but can be configured either through the OMM or at the DHCP server. For instructions on how to configure both options from the OMM, see “Configuring System Settings” on page 53.

Configuring the DHCP Scope with Windows NT

1. To configure the DHCP scope, create the following options:
 - Option 140 - IP Address of the primary OpenMobility Manager (required)
 - Option 150 - IP Address of the secondary OpenMobility Manager



IP0649

Figure 10: Configuring the DHCP Scope

2. Once you've created static IP Addresses for the active and inactive OMMs, the remaining RFPs can be configured dynamically.

Setting Up Reservations for RFPs with Windows NT

1. Highlight the DHCP scope under local machine.
2. Select **Scope** from the menu and then click **Add Reservations**.

IP0650

Figure 11: Setting Up Reservations for RFPs

3. Enter the IP Address to reserve for the RFP.
4. Enter the MAC Address in the Unique Identifier field without using the ":" delimiter; for example, 00304207ac2c. The MAC Address is on a label that is affixed to the base of the RFP.
5. Enter either "Mobility Manager" or "IP RFP" as the client name.
6. Enter the location of the RFP in the Client Comment field and click **Add**.
7. Repeat the above procedure until all RFPs have a reserved IP Address.
8. Next, add the Booter options to the Reservations. See "Adding DHCP options to the Reservations with Windows NT" on page 43 (below).

Adding DHCP options to the Reservations with Windows NT

1. Select **Scope** and then click **Active Leases**.
2. Enable **Show Reservations Only**.
3. Highlight one of the RFPs in the list.
4. Select **Properties** and display the options.
5. Select your options from the list of unused options.
6. Highlight an option on the right-hand side of the screen and click **Value**.
7. Enter the appropriate value and click **OK**.
8. Repeat the above procedure for each RFP.

Configuring Windows 2000 DHCP

To configure the DHCP Server with Windows 2000, you must perform the following tasks:

- configure the DHCP Scope. See "Configuring the DHCP Scope with Windows 2000" on page 44.
- set up reservations for RFPs. See "Setting Up Reservations for RFPs with Windows 2000" on page 45.

- add DHCP options to reservations. See “Adding DHCP Options to the Reservations with Windows 2000” on page 47.

The DHCP server must be configured with the following options:

- Option 140 - IP Address of the primary OpenMobility Manager
- Option 150 - IP Address of the secondary OpenMobility Manager (required for a resilient system).
- Option 224 - The value, "OpenMobility", is required by the RFP DHCP client to determine which DHCP servers are valid.

When configuring a DHCP server, the following are optional:

- Option 141 - identifies the Syslog Daemon server
- Option 142 - determines server port of the Syslog Daemon.
- Option 254 - automatically updates the booter version (from 3.x to 3.y).



Note: To fully update the Booter version, the RFPs must be rebooted twice. To verify the Booter version, log into the RFP through a Telnet session.

Option 141 and 142 relate to the Syslog Daemon and are not required for the system to operate, but can be configured either through the OMM or at the DHCP server. For instructions on how to configure both options from the OMM, see “Configuring System Settings” on page 53.

Configuring the DHCP Scope with Windows 2000

1. At the server level, right click and select **Set Predefined Options**.

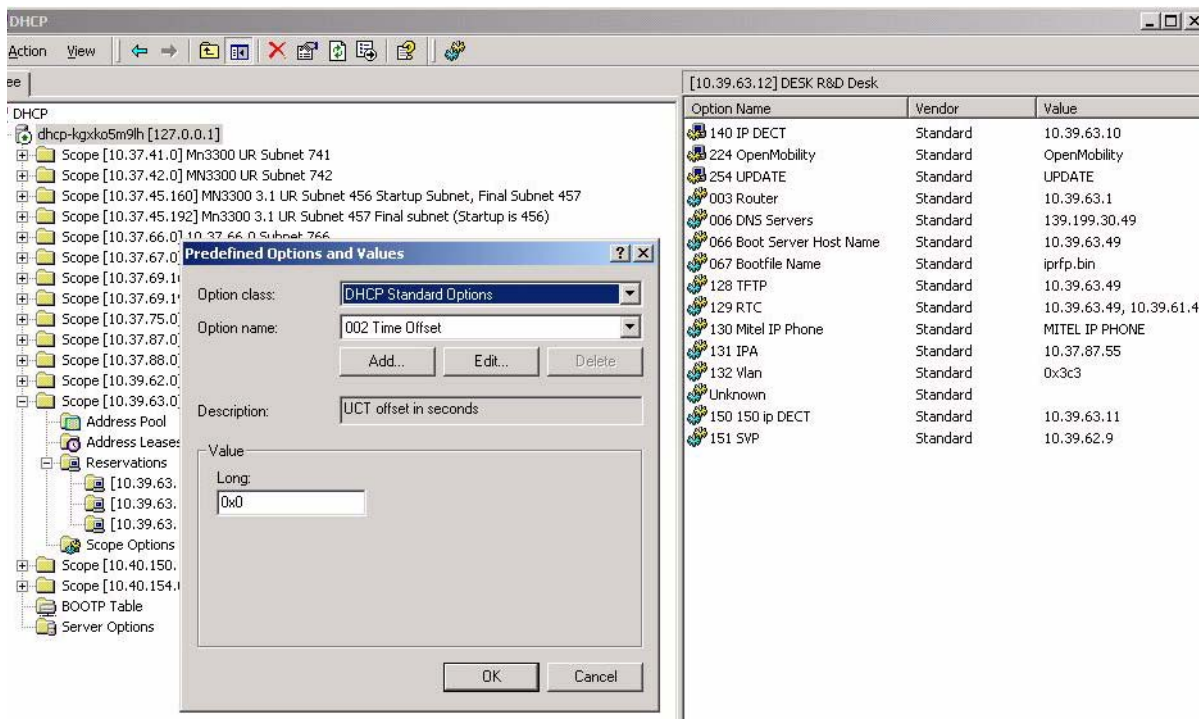


Figure 12: Setting the Predefined Options

2. Click **Add**.
3. In the name field, type a meaningful name, such as "primary OMM".
4. In the Data Type drop-down field, select **IP Address**.
5. In the Code box, type **140**, then click **OK**.

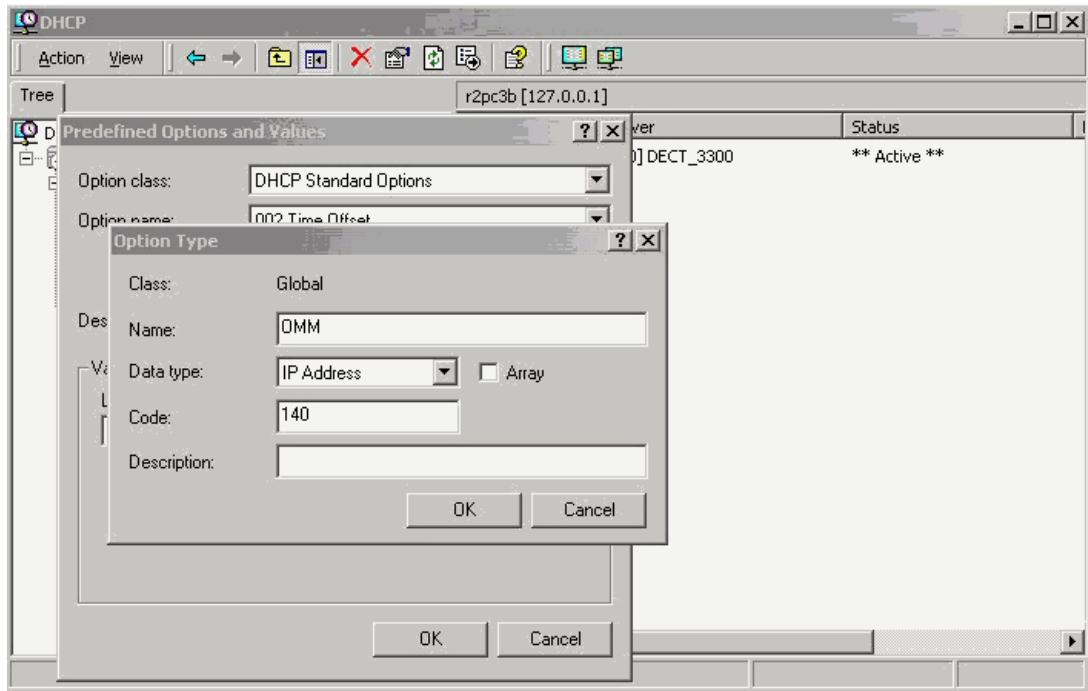


Figure 13: Defining the Option Type

6. In the value field, enter the IP Address of the OpenMobility Manager. This IP Address should be in the range of the DHCP scope and will be reserved later in this procedure.
7. Click **OK**.
8. Right-click **Scope Options**, and then select **Configure Options**.
9. Scroll down to Option 140, check the box beside it, and then click **OK**.
10. Option 141 determines the syslog daemon and Option 142 determines the Port of the syslog daemon. Both are optional at this stage as this information can later be entered into the OMM under the system page.
11. For Option 150, repeat steps 1 to 4. In the Code Box, type **150**, and then click **OK**.
12. Repeat steps 6-8. Scroll down to Option 150, check the box, and then click **OK**.
13. Next, you need to set up reservations for each RFP before connecting the RFPs to the LAN. See "Setting Up Reservations for RFPs with Windows 2000" on page 45 (below).

Setting Up Reservations for RFPs with Windows 2000

1. Right-click **Reservations**, then select **New Reservation**.

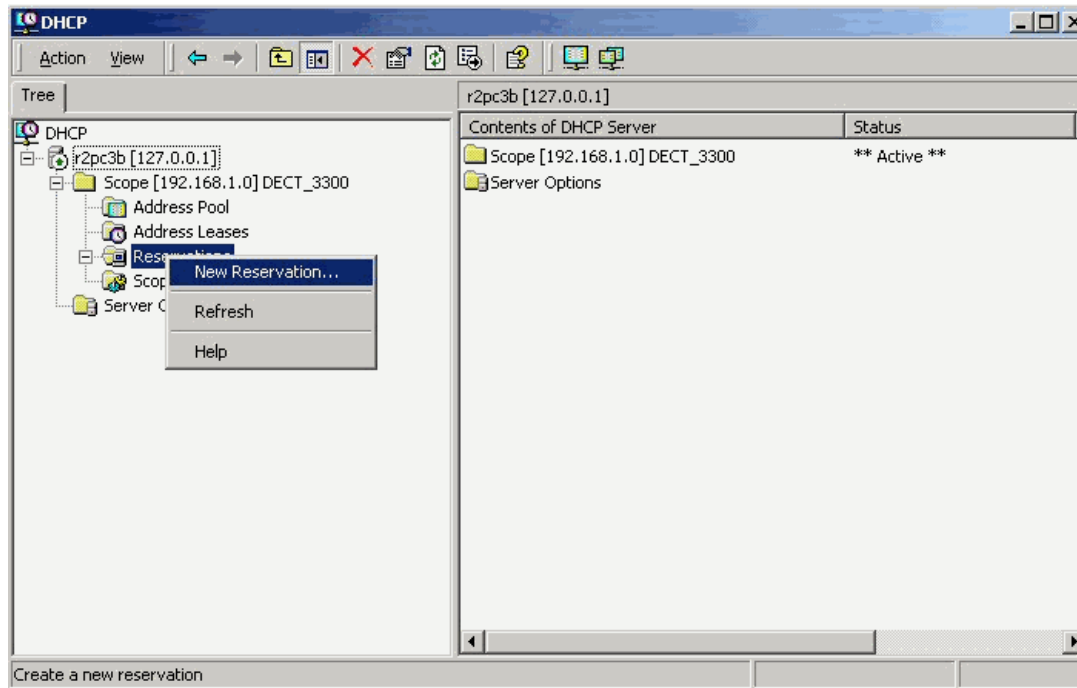


Figure 14: Initiating a New Reservation

2. In the Reservation Name, type something meaningful like "Mobility Manager" or "RFP".
3. In the IP Address field, enter the IP Address of the RFP being configured. If the RFP is the OMM, enter the IP Address that you configured against Option 140.
4. In the MAC Address field, enter the MAC Address (without delimiters) of the RFP being configured.
5. Ensure that the Supported Type is set to **Both**, and then click **Add**.

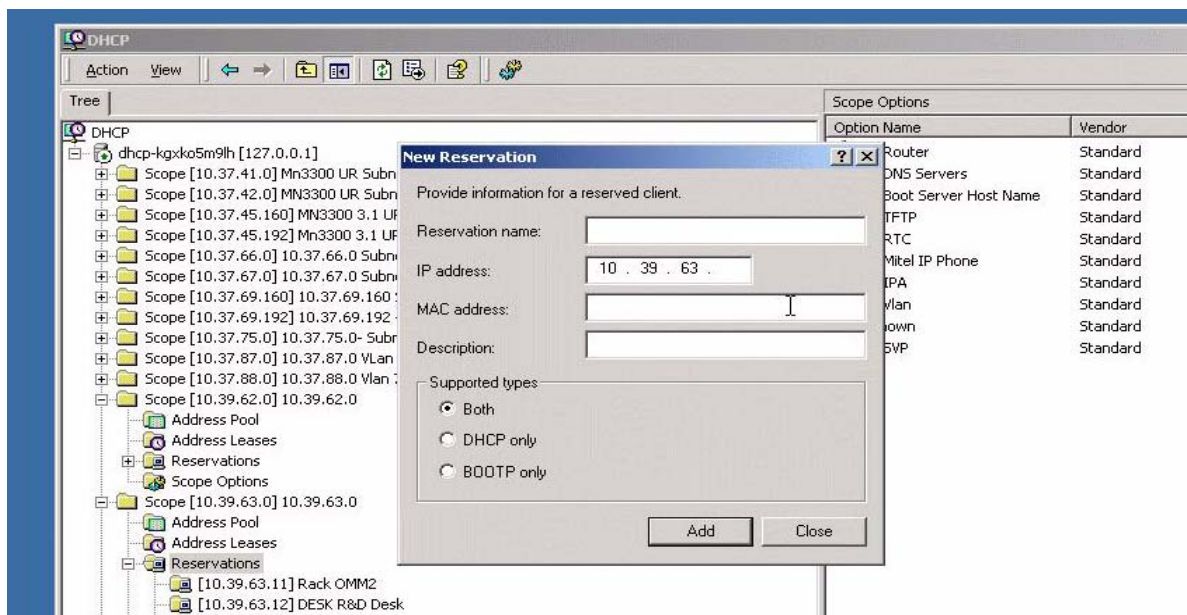


Figure 15: Adding a New Reservation

6. In the description field, identify the location of the device within the building.
7. Once you've created static IP Addresses for the active and inactive OMMs, the remaining RFPs can be configured dynamically.

Adding DHCP Options to the Reservations with Windows 2000

1. Click to open the Reservations folder. A list of all IP Addresses (Reservations) that are programmed will be displayed.
2. Right-click on the first reservation, and then select **Configure Options**.

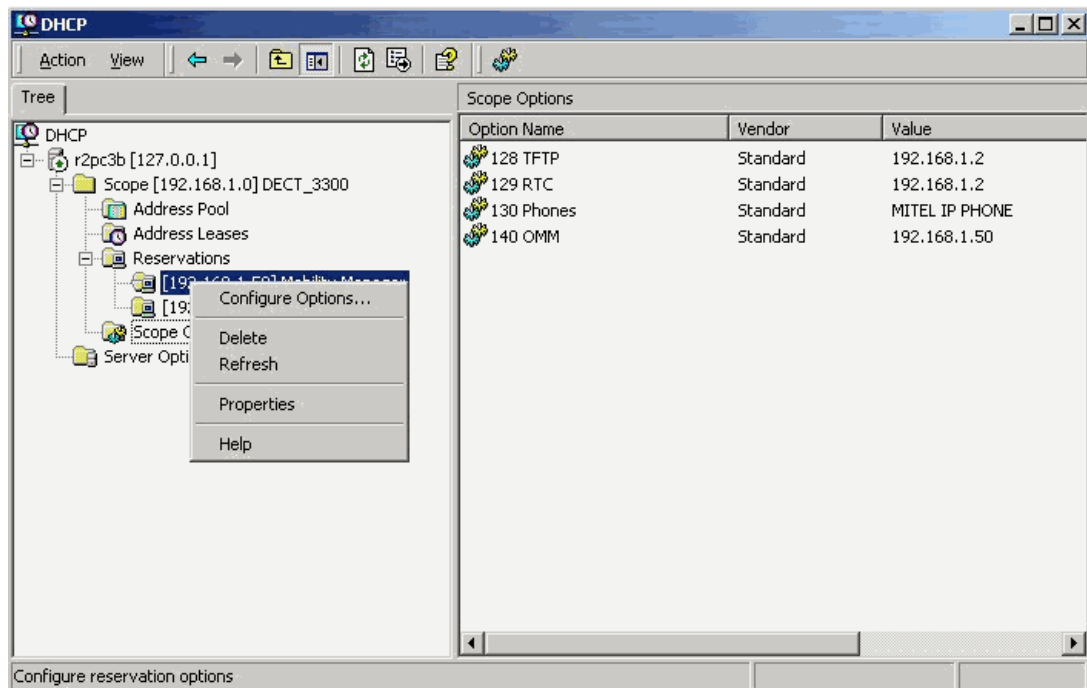


Figure 16: Adding the DHCP Options

3. Scroll down to the appropriate option and check the box beside it.
4. In the String Value field, type the appropriate value, and then click **Apply**.
5. Repeat the above procedure for each RFP.

Mounting the Radio Fixed Parts

Mount the radio fixed parts (RFPs) in the locations specified in your site plan and connect them to the LAN. Refer to the Radio Fixed Part Specification for mounting instructions and the Mitel Site Survey Instructions for details on where to locate the RFPs.

Configuring the OpenMobility Manager

Logging in

The OMM acts as a HTML server and allows you to configure the settings that are held in the OMM flash memory. You log into the OpenMobility Manager from a computer connected to the LAN. The computer must have either of the following:

- Internet Explorer 6.0 (or later), or
- Netscape Navigator 7.0 (or later).

Only one session is allowed at one time. The session is password-protected and will automatically disconnect after 5 minutes of inactivity.

1. Launch your web browser.
2. Enter the IP Address of the OMM. Enter the IP Address that you programmed for the OMM against Option 140.

The login page for the OMM is displayed.



Figure 17: OpenMobility Manager Login Page

3. Enter the default username and password:
Username: system
Password: password
4. Click **OK**.

Configuring the License Key and PARK

Before you can configure the IP-DECT Wireless Solution, you must enter a license key and a Portable Access Rights Key (PARK) into the OMM. To configure the license keys, you must

- enter the MAC Addresses of the RFPs in the OMM
- generate a serial number for the system
- obtain a license key and PARK from the license server
- enter the keys into the OMM.

To configure the license key and PARK

1. Log into the OMM.

The Licensing screen is displayed. On a new, unlicensed system, "Missing License" is displayed. Proceed to enter the license keys.

MITEL Home Exit

Licensing

1st Step
As first step you must generate a serial number key. To do this you must enter the MAC addresses of 3 IP-RFPs.
Note: These IP-RFPs may be added to the configuration with deactivated DECT part.

Serial Number	BVRUD-7B278-RXU51-1RE6U-NX5KU	New
MAC Address 1	00:30:42:07:AC:2F	✓
MAC Address 2	00:30:42:07:AC:4E	✓
MAC Address 3	00:30:42:07:AC:15	✓

2nd Step
As second step you must obtain a license from the license server. You need the serial number and the transaction ID from your delivery note.

3rd Step
As third step you must enter the license key and the PARK both generated by the license server based on your serial number key.

License Key	B79PX-QRD6E-EUWRN-84X91-3BRGA	New
PARK	1F-10-0C-F0-79	(31100147407443)
Number of Radio Fixed Parts	256	
Number of WLAN Access Points	0	

IP064

Figure 18: Licensing Screen

2. Under **1st Step**, click **New**. The New license screen is displayed.
3. Enter the MAC Addresses of the RFPs using the MAC Addresses that you identified in "Collecting and Recording Site Data" on page 35.



Note: If your system uses only two RFPs, you must leave the MAC Address of the third RFP as 00:00:00:00:00:00.

4. Click **OK**. The following screen shows an example of a system that uses three RFPs. The serial number has been generated and "Missing License" is displayed. An **X** is listed next to the MAC Address of each RFP because the RFPs are not detected by the OMM yet.

MITEL Home Exit

System
Radio Fixed Parts
Portable Parts
User Account
Licensing
Backup

Licensing

Missing Licence
Please configure a valid license key to ensure correct operation of the OpenMobility Manager.

1st Step
As first step you must generate a serial number key. To do this you must enter the MAC address of 3 IP-RFP's.

Note: These IP-RFP's will be added to the configuration with deactivated DECT part.

EXAMPLES ONLY

Serial Number	EDRRB-2B275-RX581-1RE6U-NE5AU	New
MAC-Address 1	00:30:42:07:AC:2C	✗
MAC-Address 2	00:30:42:07:AC:19	✗
MAC-Address 3	00:30:42:07:AC:54	✗

2nd Step
As second step you must obtain a license from the license server. You need the serial number and the transaction id from your delivery note.

3rd Step
As third step you must enter the license key and the PARK both generated by the license server based on your serial number key.

License Key	New
PARK	(000)
Number radio fixed parts	0

Figure 19: Licensing Screen - RFPs Not Detected

5. After the OMM detects the RFPs, the ✗ s change to ✓ s and **Not validated License** appears on the screen. Note that if you are using Internet Explorer, you must **Refresh** the screen in order to see the change in the RFP status.



Note: If any of the red crosses do not change to green check marks after a short period of time, make sure that the MAC Addresses have been entered correctly.

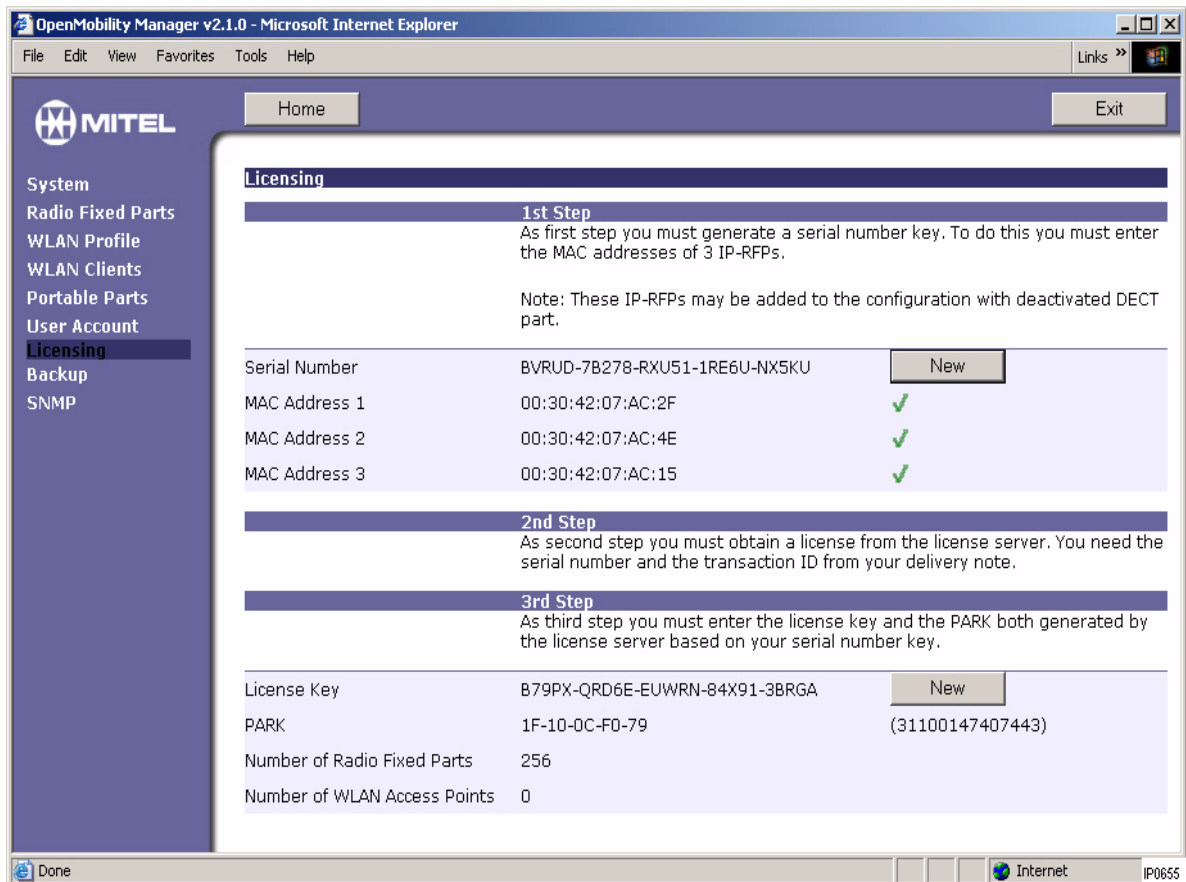


Figure 20: Licensing Screen - RFPs Detected

6. Record the serial number for your system.
7. Record the MAC Addresses of the licensed RFPs on a piece of paper. Mark these RFPs so that you will be able to recognize them easily in the future.
8. Using an Internet browser log into Mitel OnLine. Click **Technical Support**, click **ICP Password Inquiry**, and then click **IP-DECT Licences**.
9. Log in using the Mitel reseller-level username "mitel" and password "berlin" (one for all installation users).
10. From the license paper, enter the Transaction Number (TAN) and the serial number from the OMM. The license paper and TAN are shipped in a sealed envelope. Check to ensure that the seal is unbroken when you receive the envelope. If the seal has been broken, do not attempt to use the license. Contact Mitel and report that the envelope seal was broken.
11. The server will generate a License Key number and a PARK number for you. The license is logged and is traceable to deter theft.
12. The server will record the date and time when the license was used, its serial number and type, and the TAN number. The server will check the entered serial number for validity. You have three attempts to enter the serial number correctly. The TAN is compared to the list of Mitel TANs in the licensing server – if the TAN cannot be found or has already been used for another installation, an appropriate error message is displayed.

13. Under **3rd Step**, click **New**. Then, enter the license key and PARK key.

New license

License	B79PX-QRD6E-EUWRN-84X91-3BRGA
PARK	1F-10-0C-F0-79

OK Cancel

IP0656

Figure 21: Entering the License Key and PARK

14. Click **OK**. The Restart screen appears.
15. Click **Restart**.
16. After the reboot is complete, the indicators on the RFPs will turn steady green. Log into the OMM again.
17. From the Main Menu, click **Licensing**. The Licensing page displays the license key and the PARK (in hexadecimal and numerical formats) and the number of RFPs that you can install.
18. Proceed to “Configuring System Settings” on page 53.

Configuring System Settings

To configure system settings:

1. From the Main Menu of the OMM, click **System**. The System screen is displayed.

The screenshot shows the MITEL OMM System Settings interface. On the left is a sidebar menu with the following items: System, System Settings (highlighted), User Account, SNMP, Backup, Radio Fixed Parts, Portable Parts, WLAN Profiles, WLAN Clients, and Licensing. The main content area is titled 'System Settings' and has buttons for 'Home', 'Exit', 'OK', 'Cancel', and 'Restart'. It is divided into four sections:
General Settings: ICP IP Address (10.39.61.48), Resilient ICP IP Address (10.37.18.45), System Name (OMM), and Authentication Code (1234).
DECT Settings: Encryption (unchecked) and DECT Monitor (unchecked).
Syslog: A checked checkbox, IP Address (10.37.87.55), and Port (514) with a 'Default' button.
WLAN Settings: Regulatory Domain (0x20: Canada (IC)).

Figure 22: Configuring System Settings

2. Under System Settings, enter the IP Address of the primary 3300 ICP to which a PP is allowed to register.
3. Enter the IP Address of the secondary (resilient) 3300 ICP to which a PP is allowed to register.



Note: Sets will only be allowed to register with the ICPs which you have specified as primary and secondary. Redirection to all other ICPs is not supported.

4. Enter a System Name as a top-level identifier for the DECT installation.



Note: If the System Name is configured, this name will become the network name that is displayed on each OpenPhone 27 once it has been subscribed.

5. Enter an Authentication Code end users can use to authenticate when they subscribe their PP.
6. Under DECT Settings, if the DECT Monitor is to be used, check the **DECT Monitor** option to allow it to connect to the OMM. Note that this option is disabled after each reboot.



If the OMM is only supporting RFP types RFP 32, or RFP 34 then you can enable encryption by checking the **Encryption** option. If you enable encryption and an RFP 31 or RFP 33 connects to the OMM, its DECT part will not be enabled. If you want the OMM to support these RFPs then you must disable encryption. When you disable encryption, all connected RFP 31s and RFP 33s are restarted.

7. Under Syslog, if the syslog daemon is to be used, enter the **IP Address** of the server that will collect the log messages generated by the IP-DECT syslog daemon. Enter the **Port**



number of the syslog daemon server. If you entered these parameters when you configured the DHCP scope, you do not need to enter them again.

- 8. Click **OK**.
- 9. Proceed to “Configuring the RFPs” on page 54.

Configuring the RFPs

This screen lists the RFPs in order of MAC and IP Address. It also indicates whether the RFP is active and if it is synchronized with the OMM RFP. This is shown graphically. A  indicates that the RFP is in sync; an  indicates that an RFP is not in sync.

If RFP clusters are required, organize the clusters under headings. For ease of maintenance, you can enter a description (no longer than 20 characters) to identify the location of an RFP; for example, "Break Area".

RFPs that have been used to enable the License will be listed with a  (see Figure 23). You cannot delete these RFPs from the configuration. You can only delete RFPs that are listed with the  symbol.

- 1. From the Main Menu, click **Radio Fixed Parts**. The Radio Fixed Parts screen is displayed.

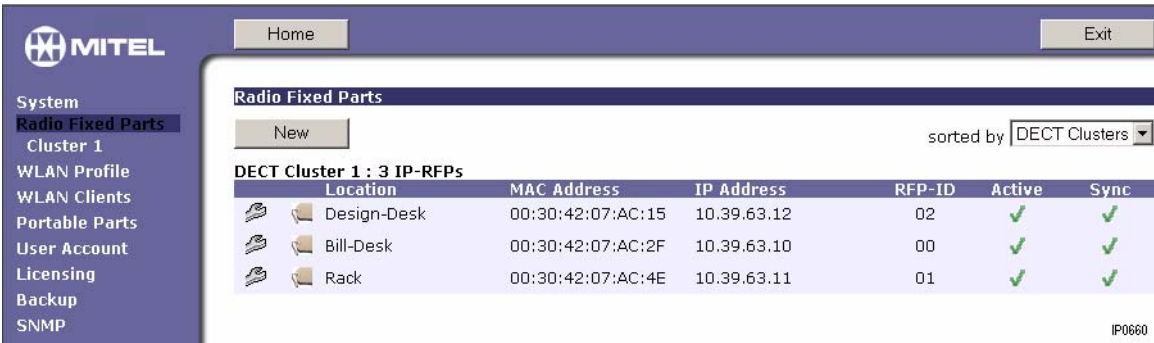




Figure 23: Configuring RFPs

- 2. Click **New**. The New Fixed Radio Part screen is displayed.

 **Tip:** Clicking the  icon also launches the New Fixed Radio Part screen.

OpenMobility Manager v2.1.0 - Microsoft Internet Explorer

New Radio Fixed Part

General Settings

MAC Address

Location

☐ **DECT Parameter**

DECT Cluster

Act as master during startup ☐

☐ **WLAN Settings**

WLAN Profile

Antenna Diversity ☒


Antenna

Channel 802.11b/g

OK Cancel

IP0659

Figure 24: Adding New RFPs

3. Under General Settings, enter the **MAC Address** of the RFP and a description of the RFP **Location** (maximum 20 characters).
 4. Check the **DECT Parameter** option for all RFPs. By default all RFPs, with the exception of the license RFPs, have the DECT Parameter option enabled. When checked, this option allows the RFP to monitor the OpenPhone 27 handsets.
 5. If this RFP is a member of a cluster, select the **DECT Cluster** number. Refer to "Clustering Radio Fixed Parts" on page 16 for a description of clusters.
 6. Ensure that **Act as Master during Startup** is not enabled.
-  **Note:** All RFPs that have been used for the License will not initialize until you have modified each one and have enabled the DECT Parameter check box.
7. Click **OK**.
 8. Continue to add new RFPs, as required. The IP RFPs are automatically numbered consecutively, starting from "00".

9. After you have added the RFPs, the Radio Fixed Parts screen will be similar to the screen shown in Figure 25. It will indicate the status of the RFPs that are used by the License and which RFPs can be deleted.

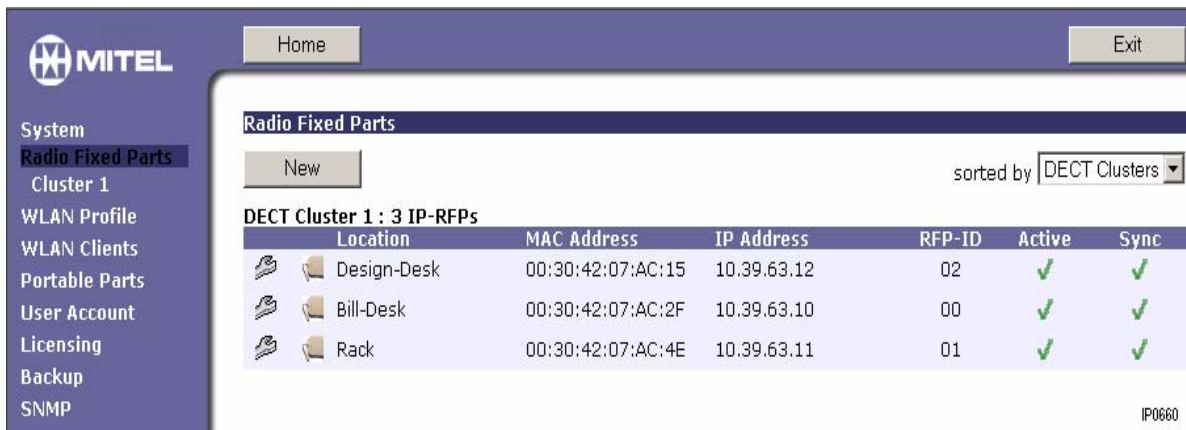


Figure 25: Displaying the License Status of RFPs

The **active** column indicates the status of the RFP:

- RFP not detected on the LAN by the OMM
- RFP detected by the OMM but has not initialized
- RFP detected and initialized

The **sync** column shows whether the RFP is in sync with the OMM:

- RFP not detected on the LAN by the OMM
- RFP attempting to sync over the air with the OMM
- RFP is in sync with the OMM.

10. Once you have completed configuring all your RFPs, click **Logout**.

Note: By default, logout be initiated automatically after 10 minutes. Logging out loads the configuration to the system as an ASCII file, which is saved on the flashcard as /die/etc/omm/omm_conf.txt. It can also be included in an OCS container with the OC1xx0 data during backup (optional).

11. Proceed to “Configuring OpenPhones (Portable Parts)” on page 59.

Verifying RFP Functionality

The following table explains the LED display of the RTF throughout the startup process.

Table 7: IP RFP LEDs

Phase	LED Colour	LED Characteristics	Meaning
PHASE 1: BOOT	RED	Steadily illuminated	Starting up
		0.25 Hz flash	Waiting for IP Link
		0.5 Hz flash	BOOTP (with Booter version 2.x) DHCP (with Booter version 3.x)
		1 Hz flash	TFTP Read Request
		2.5 Hz flash	TFTP Data Transfer
		off	Application
PHASE 2: DHCP	ORANGE	Steadily illuminated	Client searches for server and identifies OMM Operating software started by TFTP protocol; IP RFP booter starts (Linux) OS; DHCP client started
PHASE 3: DECT Activation	GREEN	0.5 Hz flash	Downloading: Waiting for IP Link
		1 Hz flash	Connecting
		2 Hz flash	Registering
		Steadily illuminated	Running, RFP is connected to OMM

Configuring SNMP

Simple Network Management Protocol (SNMP) governs the management and monitoring of network devices and their functions. The SNMP Agent supports industry-standard MIB-II definitions, and can communicate with SNMP-compatible Network Management Stations. All SNMP Agents are configured in a central place.

The RFP needs an initial OMM connection to receive its SNMP configuration. RFP-dependent parameters like **sysLocation** and **sysName** are generated.

- **sysLocation** corresponds to the location configured via the web service. If this location is not configured, **sysLocation** is set to Location.
- **sysName** is composed of the MAC Address and RFP or OMM RFP if the OMM is running on this RFP. Changing SNMP configuration forces all agents to be reconfigured.
- **sysUpTime** indicates how long an RFP has been in an operational state. This value indicates the running time of the RFP application software, not the operating system or the DECT network.

SNMP defines asynchronous messages called "traps". SNMP traps are generated to alert the Administrator when significant network or server events take place, when alarms are triggered or cleared, for instance. Traps are sent by an SNMP Agent to an SNMP Manager usually to report error conditions, but other types of messages can also be transmitted.

- **coldStart** is a trap sent by the SNMP Agent at startup and after the system is rebooted.
- **nsNotifyShutdown** is an enterprise-specific trap sent by the SNMP Agent when it stops.
- **authenticationFailure** is a trap sent by the SNMP Agent when it receives an SNMP request using an unknown community name.
- **nsNotifyRestart**, is an enterprise-specific trap generated by the SNMP Agent which replaces the non-specific coldStart/ warmStart traps after being reconfigured.

The SNMP agent responds to SNMPv1 and SNMPv2 read requests for the standard MIB-II objects. You can use the publicly available IETF MIB definitions to decode SNMP messages with your network management system or MIB browser. For more information about SNMP implementation, please see the MIB-II parameters contained in “SNMP Group (11)” on page 114.

To configure SNMP:

1. From the Main Menu of the OpenMobility Manager, click on the **SNMP** menu item. The SNMP screen is displayed.

2. Under General Settings, enter the **Read-only Community** (public, for example).
3. Enter the **System Contact**. The SNMP Agent responds with this string when requesting the MIB-II parameter **sysContact**. The **System Contact** represents the name and contact information of the person responsible for the managed node.
4. Select **Trap Handling** (optional).
5. Enter the **Trap Community**. This password is used to receive SNMP Agent traps. Use the same password you have registered with the SNMP manager. If you have not registered a password with the SNMP manager, create a new password.
6. Enter **Trap Host IP Address**. This IP Address represents the host with an SNMP manager installed and configured to receive traps.
7. Select **OK**. The SNMP Agent is reconfigured and sends a **nsNotifyRestart** trap indicating that SNMP configuration has been changed. It is not necessary to perform a system restart for the SNMP configuration changes to take effect.



Note: SNMP configuration persists after a system restart.

Configuring OpenPhones (Portable Parts)

You configure OpenPhones in the Portable Parts screen of the OMM. This screen allows you to add, modify, or delete the OpenPhones. There are three procedures for configuring the OpenPhones:

- **Configuring Authentication Codes and Portable Part Resiliency** (page 60): Use this procedure to set a System-wide Security Authentication Code and configure Portable Part Resiliency.
- **Configuring Multiple OpenPhones** (page 61): This procedure allows you to configure a large number of OpenPhones quickly because you do not need to enter the MAC Addresses for each OpenPhone into the 3300 ICP. Instead, the system automatically discovers the IPEIs and enters the appropriate MAC Address into the 3300 ICP for you.
- **Configuring Individual OpenPhones** (page 64): Use this procedure to add a new OpenPhone or GAP-compliant phone to the system.



Note: GAP-compliant phones can still be added using the conventional method.

Caution: Ensure that you have the latest version of OP27 firmware installed on the OpenPhones. See “Checking OpenPhone Firmware Versions” on page 76 and “Upgrading RFP Firmware” on page 76.

Configuring Authentication Codes and OpenPhone Resiliency

You can use the System screen, to set an Authentication Code and configure Portable Part Resiliency (OpenPhone Resiliency).

To configure Portable Part (PP) Resiliency:

1. From the Main Menu of the OMM, click on the **System** menu item. The System screen is displayed.

The screenshot shows the MITEL OMM System Settings interface. The left sidebar lists various system management options. The main content area is titled 'System Settings' and contains several configuration sections. The 'General Settings' section includes fields for ICP IP Address (10.39.61.48), Resilient ICP IP Address (10.37.18.45), System Name (OMM), and Authentication Code (1234). The 'DECT Settings' section includes checkboxes for Encryption and DECT Monitor, both of which are currently unchecked. The 'Syslog' section is checked, showing IP Address (10.37.87.55) and Port (514). The 'WLAN Settings' section includes a dropdown for Regulatory Domain (0x20: Canada (IC)). Buttons for OK, Cancel, Restart, and Default are visible throughout the interface.

Figure 26: Configuring Authentication Codes and Portable Part Resiliency

2. Under System, enter the IP Address of the 3300 ICP. The IP Address of the 3300 ICP is configured against Option 129 in the DHCP Options form of the 3300 ICP System Administration Tool.
3. Specify the following parameters:
 - **Resilient ICP IP Address**
 - **System Name**
4. You can enter an optional 4-digit system-wide security **Authentication Code** to prevent unauthorized OpenPhone subscription. Alternatively, you can omit the Authentication Code, but then the subscription process will be less secure. If you enter an Authentication Code, you will need to enter this code later into the OpenPhones when you subscribe them to the system.
5. Under DECT Parameter, if the DECT Monitor is to be used, check the **DECT Monitor** option to allow it to connect to the OMM. Note that this option is disabled after each reboot.
6. Under Syslog, if the syslog daemon is to be used, enter the **IP Address** of the server that will collect the log messages generated by the IP-DECT syslog daemon. Enter the **Port** number of the syslog daemon server. If you entered these parameters when you configured the DHCP scope, you do not need to enter them again. The PIN field is reserved for future use.
7. Click **OK**. Proceed to "Configuring OpenPhones in the OMM" on page 62.

Configuring Multiple OpenPhones (Quicker Installation)

Programming the Portable Parts

When you program the Portable Parts (OpenPhones) into the 3300 ICP, you do not need to enter the MAC Addresses.

1. Log into the 3300 ICP System Administration Tool.
2. Ensure that the required IP licenses are entered in the License and Option Selection form. Each OpenPhone will require a 3300 ICP user license and device license.
3. Ensure that Class of Service, Interconnect Restriction, and Intercept Handling is programmed for each device.
4. In the Wireless Phones IP Set Configuration form, click **Add** and enter the following information:
 - **Number of Records to add:** Enter the number of PPs that are to be programmed.
 - **Device Type:** Select **OpenPhone 26/27**.
 - **Directory Number (DN):** Enter the starting Directory Number for these phones.
 - **Wireless PIN:** Leave blank (for future use).
 - **ACD Set:** Set to **Yes** for ACD sets.
 - **Interconnect Number:** Enter the Interconnect Number.
5. Click **Save** to range program your entry.

Field Name	Value to Add	Increment by
Device Id:		-
Device Type:	OpenPhone 26/27	-
Number:		
Wireless PIN:		
ACD Set:	<input checked="" type="radio"/> No <input type="radio"/> Yes	-
Line Type:	Not Assigned	-
Interconnect Number:	1	
Language:		-
MAC Address:		-
Tenant Number:	1	



Figure 27: Programming the OpenPhone Device Type

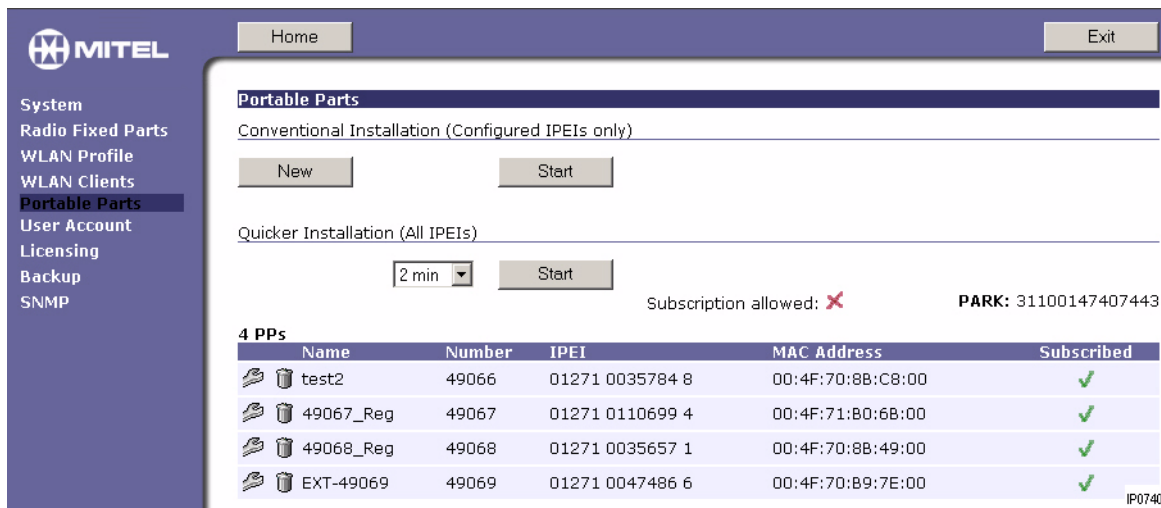
6. Optionally, in the Default Account Code Definition form, create a default account code number that will appear in all SMDR records for the phone.

7. In the Station Service Assignment form, assign a Class of Service, Class of Restriction, and Intercept Number to the DN of these phones. Assign a Default Account Code Index number if desired.
8. In the Telephone Directory Assignment form, assign a name, department, and location to all directory numbers in the system. The system propagates the assigned name to the OMM and the OpenPhone after you subscribe the OpenPhone. If you do not program a name for the OpenPhone in the Telephone Directory Assignment form, the OpenPhone will display "No User Name".
9. In the System Options Assignment form, make a note of the Set Registration Access Code. You will need this code later. In order to configure multiple OpenPhones quickly, a code must be programmed in this field.
10. Proceed to "Configuring Authentication Codes and OpenPhone Resiliency" on page 60.

Configuring OpenPhones in the OMM

You configure the OpenPhones on the Portable Parts screen of the OMM. This screen allows you to add, modify, or delete the OpenPhones.

1. In the navigation menu, click **Portable Parts**.
2. Under "Quicker Installation (All IPEIs)", set a time limit for the subscription phase and then click **Start**. After you click **Start**, you must complete the OpenPhone subscription within the selected time limit. After the time limit expires, the system will no longer allow you to subscribe handsets. The **Subscription Allowed** indicator changes from a red cross  to a green check  for the duration of the selected time limit.




Portable Parts





Conventional Installation (Configured IPEIs only)

New Start

Quicker Installation (All IPEIs)

2 min Start

Subscription allowed:  **PARK: 31100147407443**




4 PPs				
Name	Number	IPEI	MAC Address	Subscribed
test2	49066	01271 0035784 8	00:4F:70:8B:C8:00	
49067_Reg	49067	01271 0110699 4	00:4F:71:B0:6B:00	
49068_Reg	49068	01271 0035657 1	00:4F:70:8B:49:00	
EXT-49069	49069	01271 0047486 6	00:4F:70:B9:7E:00	

IP0740

Figure 28: Starting OpenPhone Subscription (Quicker Installation)

Subscribing OpenPhones to the OMM

1. Log into the OMM and click **Portable Parts** in the navigation menu.
2. Record the PArk that is displayed in the top right-hand corner of the screen.
3. On the OpenPhone:

- Press **Menu**.
- Press  to select **System**.
- Press **OK**.
- Press  to select **Subscription**.
- Press **OK**. "No Subscription" is displayed.
- Press **New**, the OpenPhone asks for the PARK number. The PARK number is optional. It only needs to be entered if there is more than one IP-DECT system in the area that may be subscribing OpenPhones. If you do not enter a PARK number, the handset will subscribe to the signal of the strongest local IP-DECT system. The advantage of entering the PARK number is that you know that the Portable Part will be subscribed to the OMM that you are programming. If the PARK number is omitted at this stage, there will be a delay while the OpenPhone searches for any other IP-DECT systems.
- If required, enter the PARK number listed in the OMM into the OpenPhone; otherwise, leave the display field blank.
- Press **Go On**. The PP will go into "Wait" state. Wait state could last just a few seconds or may last for a minute or more.
- After the Wait state, the OpenPhone prompts you for the system-wide security Access Code that you programmed in the OMM System screen. If a system-wide security Access Code has been programmed, enter it, but **DO NOT** press **Enter**. If an Access Code has not been programmed, leave the screen blank, but **DO NOT** press **Enter**.
- On the OpenPhone, press the  key and then enter the Set Registration Access Code that is programmed in the 3300 ICP System Options Assignment form, followed by the directory number of the OpenPhone that you are programming. (For example, ***3000, where *** is the Set Registration Code and 3000 is the Directory Number of the Portable Part).

Caution: If you enter a directory number that is assigned to a device type other than "OpenPhone26/27", the subscription will fail. The OpenPhone will not display "Set Locked Out" like other Mitel phones.





- Press **Enter**. The OpenPhone will now subscribe to the OMM and the registration process between the OMM and 3300 ICP will be finalized automatically. This may take up to one minute.
 - If the subscription is successful, the OpenPhone will display the directory number, user name, and time. The MAC Address for that OpenPhone will also appear in the Wireless Phones IP Set Configuration form of the 3300 ICP System Administration tool.
4. In the OMM, refresh the Portable Parts screen by pressing **F5** on the computer keyboard. The details of the programmed OpenPhone should now appear.
 5. Repeat the above procedure for each OpenPhone.

Configuring Individual OpenPhones

Programming the Portable Parts

1. In the OMM navigation menu, click **Portable Parts**.
2. Click **New**.
3. Leave the Name field blank. After you subscribe the OpenPhone, the system will automatically propagate the name assigned in the Telephone Directory Assignment form into this Name field. This field is for administration purposes only and does not appear on called sets.
4. Enter the extension number in the Number field. This number should correspond to the number that you will program in the Telephone Directory form of the 3300 ICP. This field is for administration purposes only and appears only in the OMM.

Caution: The OMM will allow an installer to add two PPs that have the same DN, but only one OP27 can be active at any one time, while the other PP will be set to ICP Pending. Rebooting or powering up one PP will automatically set the other PP to ICP Pending.

5. Enter the International Portable Equipment Identity (IPEI) of the OpenPhone. To determine the IPEI of an OpenPhone, press the following keys:
 - Short press the  key.
 - Press  to select **Local Mode**.
 - Press **OK**.
 - Press  to select **System**.
 - Press **OK**.
 - Press  to select **IPEI**.
 - Press **OK**. The IPEI appears in the display.
6. The Authentication Code field allows you to specify an optional 4-digit security Authentication Code (AC). This code ensures that OpenPhone subscription can only be performed by approved personnel (that is, only by people who know the Authentication Code). If you entered a 4-digit Authentication Code for the OpenPhone in the System screen of the OMM, the system-wide code will appear in the Authentication Code field. If the Authentication Code field is blank and a specific Authentication Code is required for the OpenPhone, enter a 4-digit code.
 - For speedier, but less secure subscription, leave the Authentication Code field blank. Then, you can just press **OK** when the OpenPhone prompts you for the Authentication Code.
 - For more secure installation, enter a 4-digit Authentication Code. You must enter this Authentication Code when you subscribe a Portable Part to the system. Using this method ensures that only authorized personnel can subscribe the handsets. Typically, you would enter the same code for all Portable Parts.

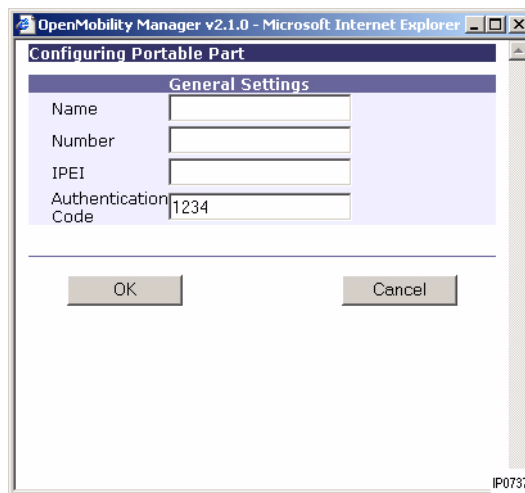


Figure 29: Configuring the OpenPhones

7. Click **OK**. After you add the OpenPhones, the entries in the Portable Parts screen will look similar to the two examples shown in Figure 30.

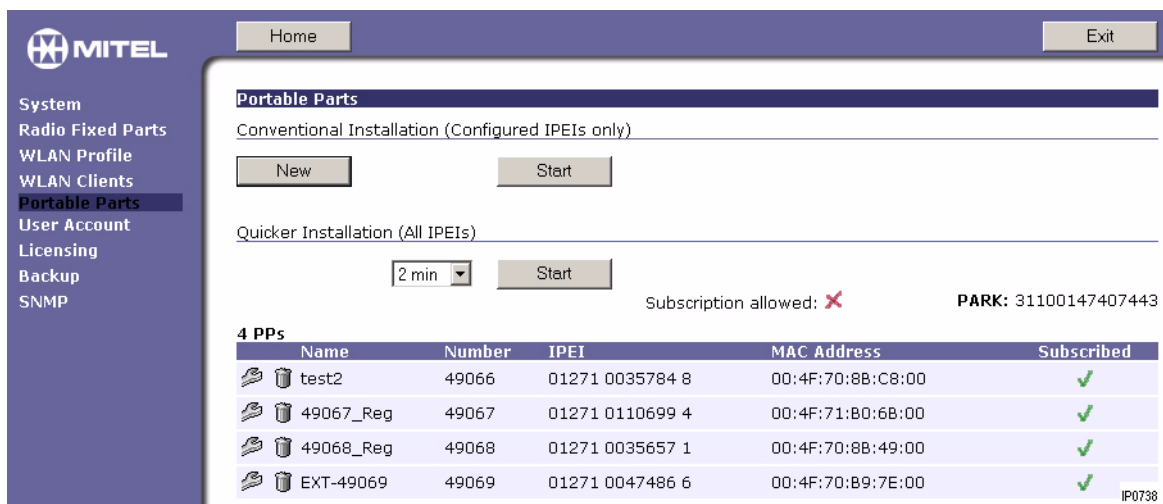


Figure 30: Portable Parts Screen

Under "Quicker Installation (All IPEIs)", the drop-down box allows you to set a time limit for the subscription phase. After you click **Start**, you must complete the OpenPhone subscription within the selected time limit. After the time limit expires, the system will no longer allow phones to be subscribed.

Each Portable Part (OpenPhone) will have the following:

- Tool icon for modification of the PP
- Trash can icon for deleting the PP
- User name (blank)
- Directory number that you have assigned
- IPEI of the OpenPhone

- MAC Address that has been generated by the OMM
 - Subscription status.
8. Proceed to “Programming the OpenPhones into the 3300 ICP” on page 66.

Programming the OpenPhones into the 3300 ICP

You program the OpenPhones into the 3300 ICP Wireless Phones IP Set Configuration form.

1. Log into the 3300 ICP System Administration Tool.
2. Ensure that the required IP licenses are entered in the License and Option Selection form. Each OpenPhone will require a 3300 ICP user license and device license.
3. Ensure that Class of Service, Interconnect Restriction, and Intercept Handling is programmed for each device.
4. In the Wireless Phones IP Set Configuration form, click **Add** and enter the following information:
 - **Device Type:** Select **OpenPhone 26/27**.
 - **Directory Number (DN):** Enter a Directory Number for this phone.
 - **Wireless PIN:** Leave blank (for future use).
 - **ACD Set:** Set to **Yes** for an ACD set.
 - **Interconnect Number:** Enter the Interconnect Number.



Note: The OMM generates a MAC Address for each portable part. The MAC Address is generated based on the IPEI and the PARK and is, therefore, unique.

Range Programming -- Web Page Dialog

This form allows you to add one or more records.

1. Enter the number of records to add:

2. Define the Add Range Programming Pattern:

Field Name	Value to Add	Increment by
Device Id:		-
Device Type:	OpenPhone 26/27	-
Directory Number:	2000	<input type="text"/>
Wireless PIN:	<input type="text"/>	<input type="text"/>
ACD Set:	<input checked="" type="radio"/> No <input type="radio"/> Yes	-
Line Type:	Not Assigned	-
Interconnect Number:	1	<input type="text"/>
Language:		-
MAC Address:	00:30:42:07:AC:2C	← EXAMPLE ONLY

Save Preview Cancel





IP0663



Figure 31: Programming the OpenPhone Device Type

5. In the Default Account Code Definition form (optional), create a default account code number that will appear in all SMDR records for the phone.
6. In the Station Service Assignment form, assign a Class of Service, Class of Restriction, and Intercept Number to the DN of the phone. Assign a Default Account Code Index number, if desired.
7. In the Telephone Directory Assignment form, assign a name, department, and location to all directory numbers in the system.
8. Proceed to "Subscribing OpenPhones to the OMM" on page 67.

Subscribing OpenPhones to the OMM









To subscribe OpenPhones to the OMM, you will need access to both the OpenPhones and the OMM.

1. Log into the OMM and click **Portable Parts**.
2. Under "Conventional Installation (Configure IPEIs only)", click **Start**. The Subscription Allowed field will change from a red cross  to a green check .
3. On the OpenPhone, press the **Menu** softkey.
4. Press  to select **System**.
5. Press **OK**.
6. Press  to select **Subscription**.

7. Press **OK**. 'No Subscription' is displayed.
8. Press **New**.
9. In the OMM screen, click **Subscribe**. The 'Configure IPEI' will be checked. Record the PARK that is displayed in the top right-hand corner of the screen.
10. Back on the OpenPhone, enter the PARK number for the OpenPhone.
11. Press **Go On**. The PP will go into wait state.
12. Enter the Authorization Code (from step 6 on page 64), or if you did not program an Authorization Code, leave the display field blank.
13. Press **OK** for "Enter Name" and "Enter Number" or let the display time out. The OpenPhone will now be subscribed to the OMM and will be able to make and receive calls.
14. Repeat the above procedure for each OpenPhone.
15. After you have configured all the OpenPhones, click the **Stop** button in the Portable Parts screen of the OMM. The Subscription Allowed field will change from a green check  to a red cross .
16. Proceed to "Configuring a Site Name and Number on an OpenPhone (Optional)" on page 68.

Configuring a Site Name and Number on an OpenPhone (Optional)

You can configure a site name and number on each OpenPhone for reference purposes only.







1. Short press the  key.
2. Press  to select **Local Mode**.
3. Press **OK**.
4. Press  to select **System**.
5. Press **OK**.
6. Press  to select **Subscription**.
7. Press **OK**.
8. Press  to select a site name (defaults to "A" followed by a check mark).
9. Press **Options**.
10. Press  to select **Edit**.
11. Press **OK**.
12. Enter the site name, for example, "Mitel", and then press **OK**. When editing the site name, press the  key to delete one character (long press of  deletes the whole word/field). Press '0' key twice to insert a space. Use the arrow keys to move the cursor left and right. Note that if the name is too long, the number will not be displayed because they share the same line on the OpenPhone display.
13. Enter the number of the OpenPhone, and then press **OK**.
14. Press **Esc** to exit back to the main display.

Configuring a Username for an OpenPhone (Optional)

This procedure changes the user name on the OpenPhone only. The name displayed on called sets will continue to be the name that is programmed in the Telephone Directory Assignment form of the 3300 ICP.

If the name that appears on the OpenPhone is different than the name that is assigned to the phone in the Telephone Directory Assignment form, you can synchronize the names by un-subscribing and then re-subscribing the OpenPhone (see “Changing the Directory Name of an OpenPhone” on page 73). You can also manually configure the OpenPhone with the correct user name.

To manually configure OpenPhone with a user name:

1. Short press the  key.
2. Press  to select **Local Mode**.
3. Press **OK**.
4. Press  to select **Telephone Option**.
5. Press **OK**.
6. Press  to select **User Name**.
7. Press **OK**.
8. Enter the user name and then press **OK**. When editing the user name, press the  key to delete one character (long press of  deletes the whole word/field). Press ‘0’ key twice to insert a space. Use the arrow keys to move the cursor left and right.
9. Press **Esc** to return to the main screen.

Verifying OpenPhone Functionality

Verify OpenPhone functionality by doing the following:

- placing calls between OpenPhones
- placing calls from a 3300 ICP IP Phone to an OpenPhone
- placing calls from OpenPhones to 3300 ICP IP Phones
- activating 3300 ICP system features on the OpenPhones (refer to the OP27 User Guide for instructions).

Backing up Databases

1. Back up the OMM database (see “Changing the Directory Name of an OpenPhone” on page 73).
2. Back up the 3300 ICP database (refer to the 3300 ICP Technician’s Handbook for instructions).

Maintenance

Health Checklist

- ☒ RFPs are functioning (see “Checking LEDs” on page 85)
- ☒ Administrator’s password is set (see “Changing the Administrator’s Password” on page 71)
- ☒ OMM database has been backed up (see “Performing Backups” on page 73)
- ☒ OpenPhone displays names correctly (see “Changing the Directory Name of an Open-Phone” on page 73)
- ☒ OpenPhone firmware is up-to-date (see “Upgrading RFP Firmware” on page 76)
- ☒ OpenPhone authorization code is set (see “Configuring OpenPhones (Portable Parts)” on page 59)

Changing the Administrator’s Password

The default settings for the Open Mobility Manager account are:

Username: system

Password: password

To change the administrator’s password to the Open Mobility account:

1. Log into the Open Mobility Manager (see “Logging in” on page 48).
2. Click **User Account**. The following screen is displayed.

Figure 32: Changing the Administrator’s User Account

3. Enter the Username of the OMM account. You can only have one user account (defaults to "system") for the OMM.
4. Enter your new password in the Password field.
5. Enter your new password again in the Password confirmation field.
6. Click **OK**. Ensure that you record the password and keep it in a secure location.

WARNING: IF YOU LOSE OR FORGET THE ADMINISTRATOR'S PASSWORD, THERE WILL BE NO WAY TO ACCESS THE OMM ACCOUNT BECAUSE THE IP-DECT SYSTEM DOES NOT HAVE A HIGHER LEVEL LOGIN ACCOUNT.

Removing an OpenPhone from the System

To delete an OpenPhone from the system:


1. Log into the OMM. See “Logging in” on page 48.
2. In the OMM navigation menu, click **Portable Parts**.
3. Click the trash can icon of the PP to delete the OpenPhone from the OMM.
4. Log into the 3300 ICP System Administration Tool and delete the OpenPhone from the Wireless Phones IP Set Configuration form.

Changing the Directory Number of an OpenPhone

To change the directory number of an OpenPhone, you must:

- delete the OpenPhone (PP) from the OMM
- change the directory number on the 3300 ICP
- re-subscribe the OpenPhone.

To change the directory number of an OpenPhone:

1. Log into the OMM. See “Logging in” on page 48.
2. In the OMM navigation menu, click **Portable Parts**.
3. Click the trash can icon of the PP to delete the OpenPhone from the OMM.
4. Log into the 3300 ICP System Administration Tool.
5. From the **Selection** menu, click **System Configuration**.
6. Click **Devices**, click **IP Telephones**, and then click **Wireless Phones IP Set Configuration**.
7. Select the directory number that you want to change.
8. Click **Change**, change the directory number, and then click **Save**.
9. Log into the OMM and click **Portable Parts** in the navigation menu.
10. Record the PARK that is displayed in the top right-hand corner of the screen.
11. Resubscribe the OpenPhone to the OMM (see “Subscribing OpenPhones to the OMM” on page 62). However, at the end of the procedure, use the Set Replacement Access Code, instead of the Set Registration Access code. On the OpenPhone, press the  key and then enter the Set Replacement Access Code that is programmed in the 3300 ICP System

Options Assignment form, followed by the directory number of the OpenPhone that you are programming. (For example, ###3000, where ### is the Set Replacement Code and 3000 is the Directory Number of the Portable Part).

Changing the Directory Name of an OpenPhone

The directory name for an OpenPhone appears in the following:

- Telephone Directory Assignment form of the 3300 ICP
- Portable Parts screen of the OMM
- The OpenPhone display.

WARNING: CHANGE DIRECTORY NAMES ONLY FROM THE TELEPHONE DIRECTORY ASSIGNMENT FORM. NAME CHANGES THAT YOU MAKE IN EITHER THE OMM OR ON THE OPENPHONE WILL NOT BE DISPLAYED ON CALLED SETS.

To change the directory name entry for an OpenPhone:

1. Log into the 3300 ICP System Administration Tool and display the Telephone Directory Assignment form.
2. Locate the directory number of the OpenPhone and change the name as required.
3. Log into the OMM. See “Logging in” on page 48.
4. In the OMM navigation menu, click **Portable Parts**.
5. Click the trash can icon of the PP to delete the OpenPhone from the OMM.
6. Configure the OpenPhone into the OMM. See “Configuring OpenPhones in the OMM” on page 62 for instructions. After the OpenPhone is registered, the name will be updated in the OMM and on the OpenPhone display. Other display phones that receive calls from the OpenPhone will see the new name.

Performing Backups

You can back up the OMM configuration settings to a local PC or to a network hard drive. The configuration is located in the flash chip of the OMM RFP. The file is checksum protected; do not attempt to manipulate it.

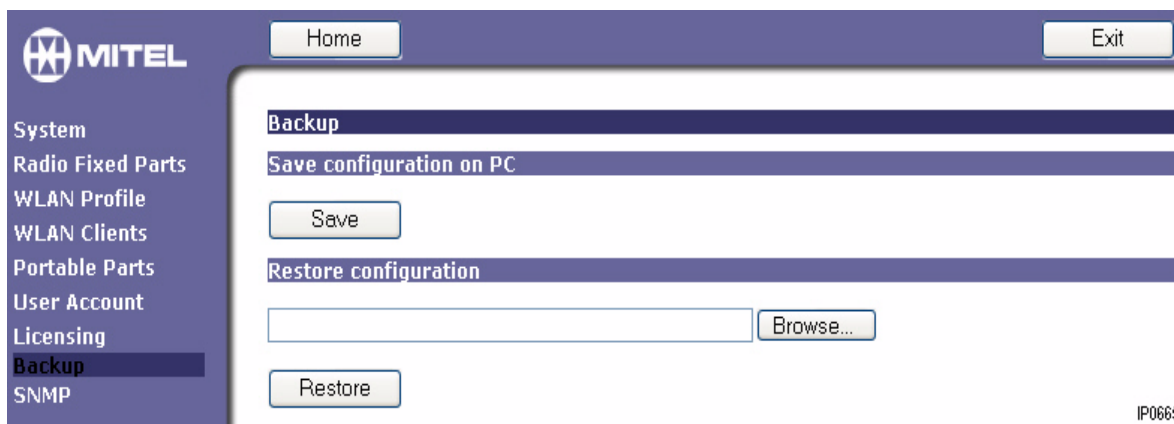
You should perform a backup in the following instances:

- after initial configuration
- after making changes
- before designating a different RFP as the OMM (the configuration from the previous RFP will be lost).

Leave a copy of the backup on-site. When you back up the configuration, do not overwrite the previous backup. Keep at least three copies.

To back up the OMM configuration:

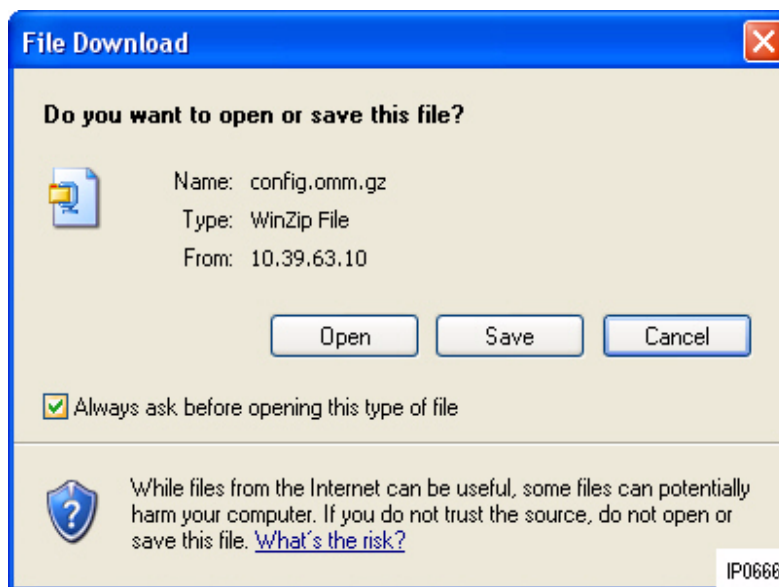
1. Log into the Open Mobility Manager (see “Logging in” on page 48).
2. Click **Backup**. The following screen is displayed.



IP0665

Figure 33: Backing Up the OMM Configuration Settings

3. Click **Save**. The following screen is displayed.



IP0666

Figure 34: Saving the Configuration File

4. Click **Save**.
5. Click **Browse** and navigate to a folder on a computer or network drive.
6. Enter the filename in the following format: <date>_confi.omm.gz
7. Click **Save**. A zip file of the configuration settings is saved to the specified folder.

Restarting the OMM

You must restart the system after the following procedures:

- restoring a backup configuration
- installing a new iprpf.bin file (see “Upgrading OpenPhone Firmware” on page 78).

Caution: During a restart, the OpenPhones are taken out of service and all active IP-DECT calls are terminated.

1. Log into the Open Mobility Manager (see “Logging in” on page 48).
2. Click **System**.
3. Click **Restart**. The following screen is displayed.

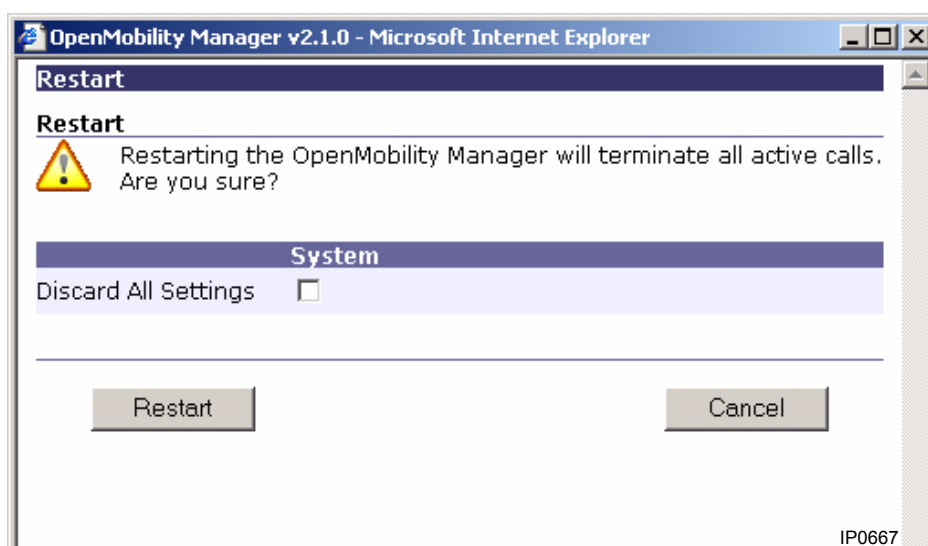


Figure 35: Restarting the OMM

Caution: If you select **Discard All Settings**, the system will revert to the default settings. If you do not have a backup of your configuration, you will have to reprogram the entire OMM configuration.

4. Click **Restart**. When the reboot is complete, the LEDs on all the RFPs should be solid green.

Resetting OMM Configuration to Defaults

You can reset the OMM configuration to the defaults by selecting **Discard All Settings** during a restore procedure. Typically, you would only use this option if you wanted to perform the following tasks:

- reinstall the system at another site

- reprogram a default OMM configuration.

Assigning a Different RFP as the OMM

Caution: If the current OMM is one of the RFPs that is used to license the system, your IP-DECT Solution license will become invalid if you remove this RFP from the system. Refer to “RFP Licensing” on page 32 and to “Replacing Failed Licensed RFPs” on page 86 for additional information.

To assign a different RFP as the OMM:

1. Back up the OMM configuration settings. See “Performing Backups” on page 73.

Caution: Assigning a different RFP as the OMM will cause the existing OMM configuration settings to be lost. Ensure that you back up the OMM configuration settings before proceeding.




2. Re-configure the DHCP scope using the IP Address of the RFP that you want to assign as the OMM. See “Configuring the DHCP Scope for Resiliency” on page 36.
3. Restore the OMM configuration settings to the newly assigned OMM RFP. See “Restoring a Database” on page 84.
4. Reboot all the RFPs. See “Restarting the OMM” on page 75.

Upgrading RFP Firmware

The RFP obtains its firmware (iprfp.bin file) from the 3300 ICP. After a new software load has been installed on the 3300 ICP, reboot each OMM in the IP-DECT system. The RFPs will then reboot with the latest software from the 3300 ICP controller.

Checking OpenPhone Firmware Versions

You can display the version information of the OpenPhone with a few keystrokes. Check the firmware version to determine whether an upgrade is required to overcome any user issues.

1. Short press the  key.
2. Press  to select **Local Mode**.
3. Press **OK**.
4. Press  to select **Telephone Option**.
5. With Telephone Option highlighted, enter the following key sequence: *1#. The display will show the software and hardware level of the OP27.





6. Press **Esc** to return to the menu.

Setting the RFP Subscription List

The RFP Subscription List provides a list of up to 20 installations/sites. You can subscribe a handset to a specific cluster by selecting the OMM IP Address of the desired cluster from the list. Automatic search is supported. If enabled, the OpenPhone supports automatic roaming. If disabled, the handset will always attempt to stay locked to the active selected cluster.

You can only delete RFPs from the subscription list when the handset is out of coverage range, or when it is not registered to the system (there will be an error beep and display will show "searching").

To access the RFP Subscription List:

1. Short press the  key.
2. Press  to select **Local Mode**.
3. Press **OK**.
4. Press  to select **System**.
5. Press **OK**.
6. Press  to select **Subscription**.
7. Press **OK**.
8. Press **Options** and select:
 - **New** - to add the IP Address of an RFP to the list
 - **Edit** - to change an entry in the list
 - **Delete** - to remove an entry from the list.

Upgrading License Requirements

Upgrading a site to a higher license level (for example, from A to C) is similar to licensing a new installation.

1. Ship the RFPs and OpenPhones to the upgrade site.
2. Check the site to identify the existing OMM RFP and the other licensed RFP (if configured). The licensed RFPs will have been marked as such during the initial installation.
3. Select the additional RFPs from the total required on-site and mark these in a manner that will enable you to recognize them easily in future as "licensed RFPs". Plan to install them in accessible positions.
4. Record the MAC Addresses of all three selected RFPs. You must include the existing RFPs MAC Addresses as license users.
5. Install the additional RFPs in accessible positions.
6. Launch the OMM application, enter your password and select **Licensing**.
7. Enter the 3 MAC Addresses of the RFP(s) that you recorded in step 4. The OMM application generates a serial number. Copy it to a piece of paper.
8. Use an Internet access point to go to the DeTeWe's license server <http://licence.de-tewe.de/mitel> and log in using the Mitel reseller-level user name "mitel" and password "berlin".
9. From the license paper, enter the Transaction Number (TAN) and the serial number from step 7. The server generates a new License Key number. The PARK number will remain the same. The server will record the date and time when the license was used, its serial number and type and the TAN number. The server will check the given serial number for validity.

You will have three attempts to enter the serial number correctly. The TAN is compared to the list of Mitel TANs in the licensing server – if the TAN cannot be found or has already been used for another installation, an appropriate error message is shown.

10. Reopen the OMM web configurator and enter the new the License Key. The IP-DECT system starts operating.

Upgrading OpenPhone Firmware

To upgrade OP27 firmware, you require a serial-to-mini USB connection cable. You can order this cable from Mitel. The upgrade is available as an executable and is run on a Windows-based PC. You download the executable from the Product Support Download page at Mitel OnLine (MOL).

1. Go to the www.mitel.com web site.
2. Log into Mitel OnLine.
3. Click **Technical Support**, and then click **Software Downloads**.
4. Click **3300 Integrated Communications Platform (ICP)**.

5. Click **OpenPhone 27**.
6. Click the latest software update.
7. Download the software update to your computer hard drive.
8. Connect the cable from the 9-pin serial port on your PC to the USB port on the side of the OpenPhone 27 (see Figure 36).

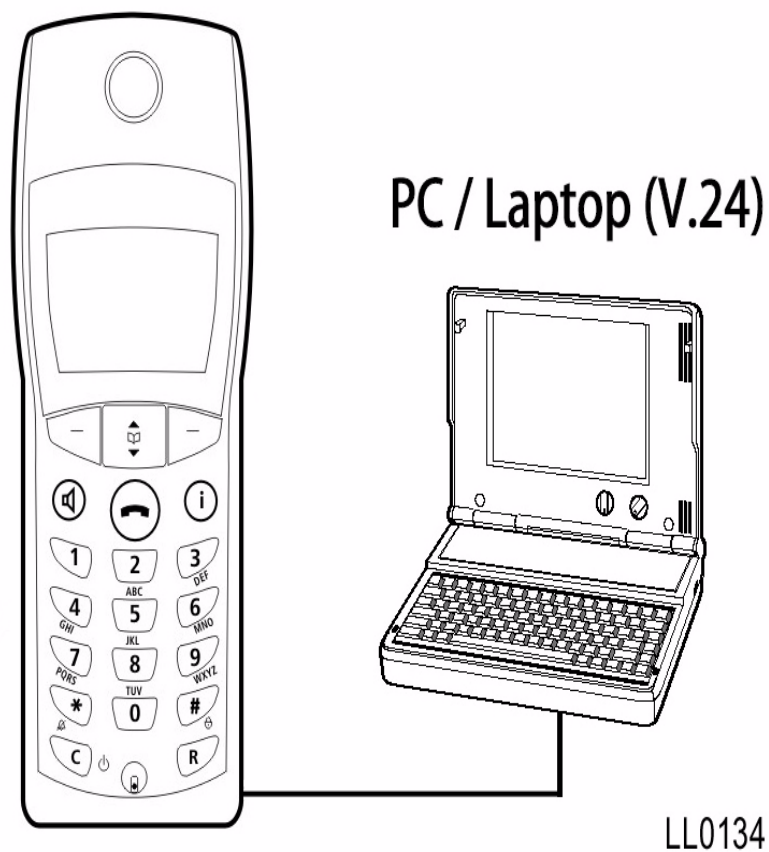


Figure 36: Upgrading the Firmware

9. Power on the OpenPhone 27.

10. Double-click the executable file. A screen similar to the following is displayed. The software version numbers are shown at the bottom of the screen.

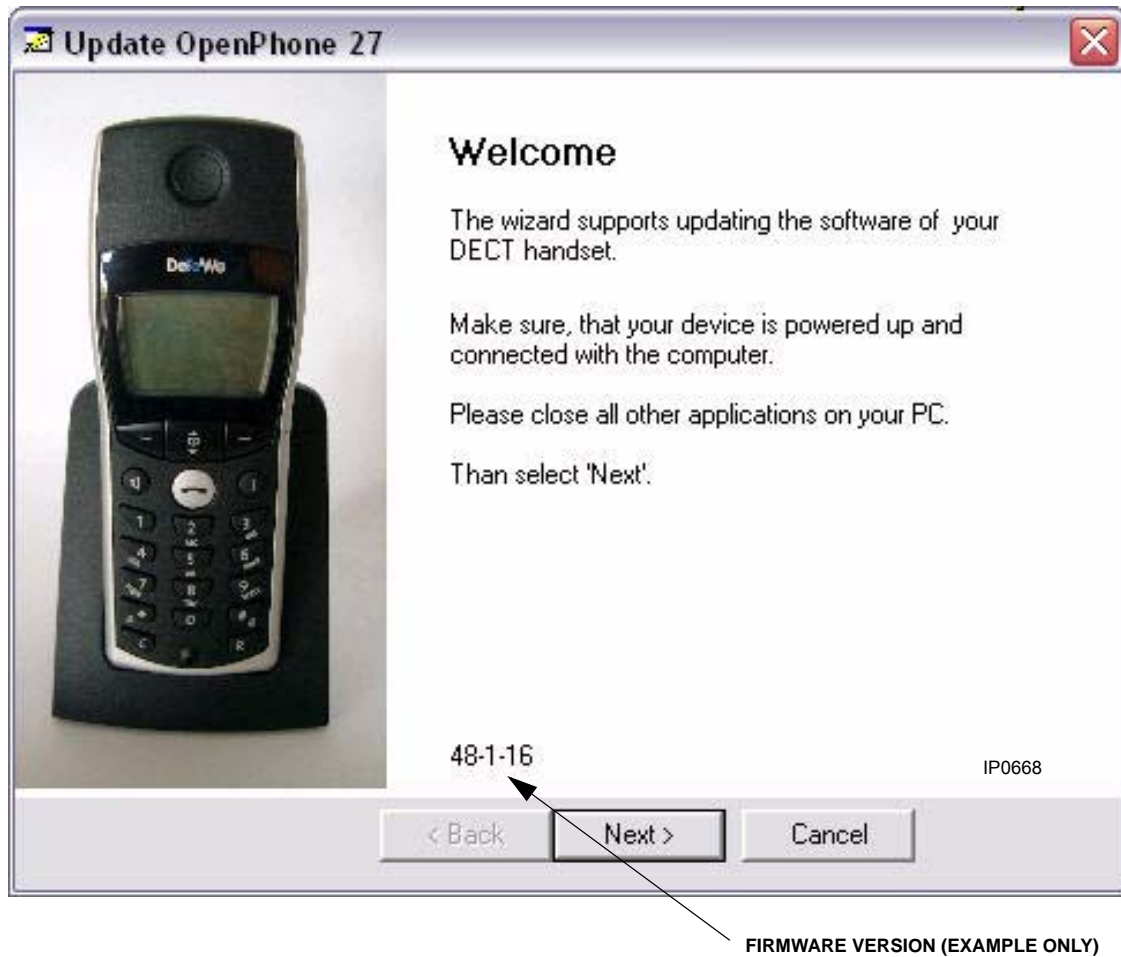
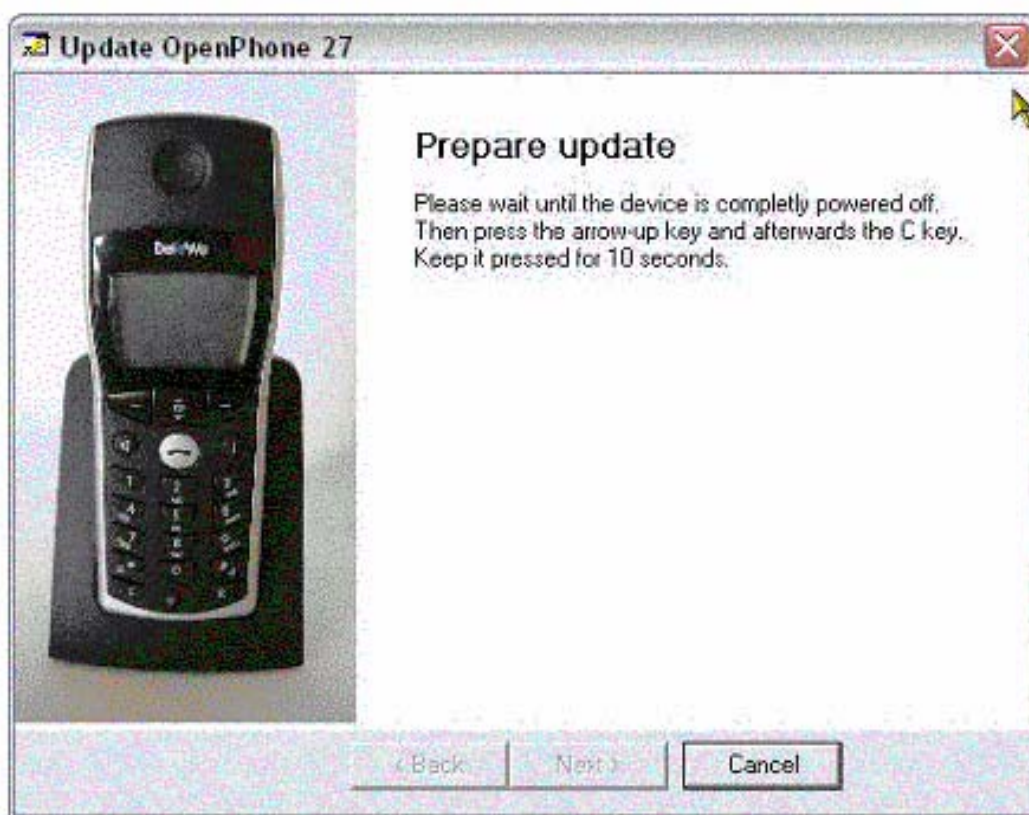






Figure 37: Launching the Executable

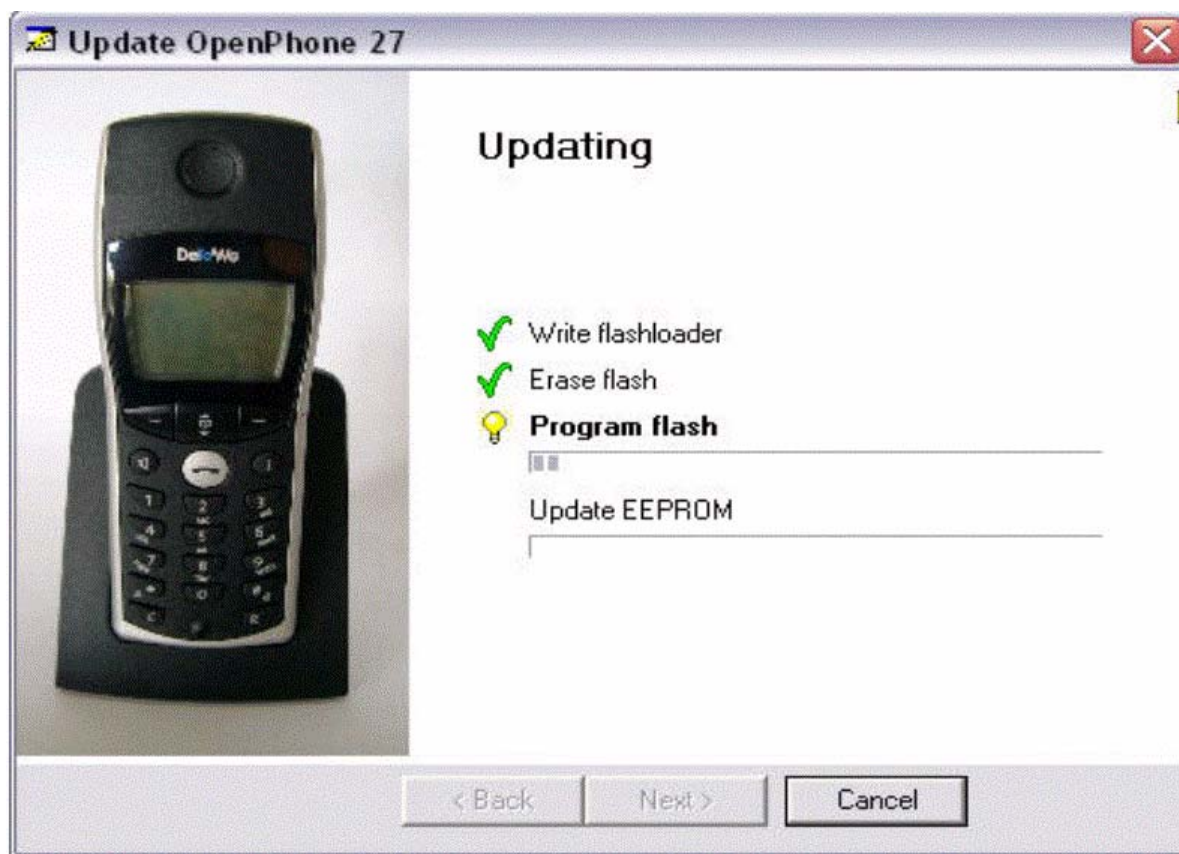
11. Click **Next** to continue. The upgrade application auto-detects which port to use, the model of OpenPhone, and the version of firmware currently on the OpenPhone. If the version of firmware is greater or the same as that built into the executable, then the update will terminate.
12. Click **Next**.



IP0669

Figure 38: Updating the OpenPhone

13. The OpenPhone 27 will switch off. Press the  (up arrow key), and then the  key; keep both keys pressed until the display changes to the Updating Screen, and then release the up arrow key while still holding down the  key. After the 'Program Flash' displays two bars, similar to those shown in Figure 39, you can then release the  key.



IP0720

Figure 39: Updating Screen

14. Wait until the following message is displayed 'Update is completed, you can exit the program'. Then, click **Exit** if you have no other PP to upgrade. If you wish to upgrade another OpenPhone, click **Next**. Connect another OpenPhone to the USB connector and repeat the procedure.

Troubleshooting

Identifying Faults

Table 8: Troubleshooting Chart

Symptom	Probable cause	Corrective Action
Handset won't power on.	Batteries are drained	Recharge batteries
Handset battery life too short	Batteries were not fully drained before charging	Replace batteries
	Dead batteries	
Can't make or receive calls	Handset not subscribed to system	Subscribe handset. Refer to "Configuring OpenPhones (Portable Parts)" on page 59.
	RFP not enabled to monitor handsets	Launch the OMM and ensure that the DECT option is enabled.
	Out of range of RFP	Move closer to an RFP. If coverage is required in the area, add another RFP
Can't dial calls from handset	Key lock enabled	Disable key lock feature. Refer to OpenPhone 27 user guide for instructions.
"Key fault indication" appears in display and there is no audio available	Licensing issue	Launch the OMM and ensure that the RFPs are licensed correctly. See "Configuring the License Key and PARK" on page 49.
Handset won't ring while in charger	Silent Charging is enabled	Disable Silent Charging. Refer to the OpenPhone 27 user guide for instructions.
Noticeable break in the voice signal in a certain area.	Inadequate RFP coverage	Must move the RFPs closer together or add another RFP.

Using the OMM Command Interface

1. Log into the system using Telnet:
 - From the **Start** menu of your computer, click **Run**.
 - In the Open field, type the following:
run telnet <IP address of OMM>
 - Click **OK**.
2. Enter the Username and Password.
3. Enter **help** for a list of all possible commands.

Table 9: OMM Commands

Command	Description
arpshow	arp table
console off	disable console on local terminal
console_on	enable console on local terminal
dmesg	print the kernel ring buffer
flash	show flash info
interface	show interface configuration
logread	show message log
mem	show memory usage
ps	show process table
ping <ipaddress>	ping
reboot	restarts the system
route	show routing table
uptime	show system uptime



Note: The RFP does not have an internal clock; hence, the date and time in the logread command will be incorrect.



Note: The reboot command will reboot the RFP and will disconnect all media paths through that RFP. Rebooting the OMM using the reboot command will reboot all RFPs.

Restoring a Database

You can correct a corrupted database by restoring a known working backup database.

1. Click **System**.
2. Click **Backup**.
3. Click **Browse**, navigate to the computer or network drive, select the file and click **OK**.
4. In the main Backup screen, click **Restore**. After the restore is complete, the LEDs on the RFPs will be solid green.
5. Reboot the system (see “Restarting the OMM” on page 75).




Checking LEDs

Table 10: RFP LED Status

LED Color	LED State	Meaning/Corrective Action
Red	Steadily illuminated	Starting up
Red	0.25 Hz flash	Waiting for IP Link
Red	0.5 Hz flash	Booter, DHCP client active
Red	1 Hz flash	TFTP Read Request
Red	2.5 Hz flash	TFTP Data Transfer, application downloading
Orange	Steadily illuminated	Identifies the OMM
Green	0.5 Hz flash	IP RFP initializing
Green	1 Hz flash	IP RFP connecting to OMM
Green	Steadily illuminated	RFP is connected to OMM
Red	Flashing (2 sec on/ 2 sec off)	One of the above processes has failed

Identifying Problem Zones

The OpenPhone 27 can operate in site survey mode that allows you to check the signal strength to the RFP. Refer to the Mitel Site Survey Instructions for more details.

1. Short press the  key.
2. Press  to select **Local Mode**.
3. Press **OK**.
4. Press  to select **Telephone Option**.
5. With **Telephone Option** highlighted, enter the following key sequence *2#.
6. This puts you into the site survey mode; to return to normal mode, carry out steps 1 to 5 again.

Collecting Syslog Daemon Messages

The syslog daemon of the IP RFP can be configured to send messages via the network to a central syslog daemon collecting the messages from all the IP RFPs.

The syslog daemon can be configured using:

- DHCP option 141 and 142.
- OMM Web interface, the configuration via DHCP is ignored in this case.
- If not configured via DHCP and Web Interface, the syslog daemon is enabled for local logging only (logread).
- There are freely available syslog daemons that can be used to collect all the messages from all IP RFPs.
- Syslog is useful for troubleshooting/monitoring the system.

An example of a syslog daemon is a software package called Kiwi. It can be downloaded from www.kiwisyslog.com.

Replacing Failed Licensed RFPs

If one of the three RFPs that has been used to license the system fails, you can replace it without having to reconfigure the OpenPhones by obtaining a new serial number of the system. To replace a failed RFP that has been used to generate the system license:

1. Record the serial numbers of the original and the new RFP.
2. Install the replacement RFP and record the MAC Address.
3. Log into the OMM (see “Logging in” on page 48).
4. Click **Licensing**.
5. Click **New**.
6. Replace the MAC Address of the faulty RFP with the MAC Address of the replacement RFP.
7. Click **OK**. A new serial number is generated.
8. Record the new serial number.
9. Contact the EMEA help desk and provide them with serial number. The help desk will provide you with a new License key.
10. Enter the License key and PARK under **3rd Step** in the Licensing screen of the OMM to enable the licensing.
11. Configure the replacement RFP (see “Configuring the RFPs” on page 54).

Appendix A: Hardware Specifications

Radio Fixed Parts

The following tables list the functionality supported by the three types of RFPs.

Table 11: DECT Functionality

DECT	RFP 31 IP RFP 33 IP
All 120 DECT channels supported for maximum use of DECT capacity	X
8 simultaneous voice channels per DECT IP base station, 4 additional channels for handover	X
Synchronization of the IP RFPs via DECT radio interface	X
GAP and CAP standards supported	X
Connection handover in line with GAP standard	X
DSAA authentication between base and handset	X
Cordless system telephones can use all features offered by the OpenCom 1000 (from Release 3.2 onwards)	X
LED signaling of current operating status	RFP 31 only
Antenna	External dipole or directional antenna on RFP 33

Table 12: VoIP Functionality

VoIP	RFP 31 IP RFP 33 IP
VoIP connection using RTP/RTCP protocol	X
G.711/G.723.1/G.729AB CODEC (additional license required) depending on voice quality and available bandwidth	X
Quality of Service supported by Diffserv/ToS Flag	X
Adaptive Jitter Compensation	X
Echo Cancellation/Suppression	X
Voice Activity Detection and Comfort Noise Generator	X

Table 13: Ethernet Functionality

Ethernet	RFP 31 IP RFP 33 IP
Connection via Ethernet 10/100 Base T	X
Power supply in line with Power over LAN standard IEEE 802.3af	X
IPv4	X
Optional SNMPv1/v2c, MIB II, read only, trap support	X
VLANs supported	none

Table 14: Technical Data

Technical Data	RFP 31 IP	RFP 33 IP
Power supply:		
Power over LAN IEEE802.3af	X	X
110 V/240 V AC adapter	X	none
Ambient temperature	-5 C to +45 C	-25 C to +55 C
Relative humidity: 0-95% uncondensed	X	X
Storage temperature: -40 C to +70 C	X	X
Current consumption	120 mA	120 mA
Power: 6W	X	X
Type of ingress protection	IP 45	IP 55
Mount	Wall-mountable	Wall- and mast-mountable
Color	Ice grey	Light grey
Weight	400g (without AC adapter)	970g
Dimensions: (W x H x D) in millimeters	151 x 101 x 85	240 x 236.5 x 65

From Release 1.5

MIPS Core with 125 MIPS

- Operating System
- IP Stack
- Applications

Two 125 MIPS DSP Cores (a total of 250 MIPS for the DSP)

- Voice packaging
- Voice Compression
- Echo Cancelling
- Jitter Buffer Handling
- Tone Generation and Detection

Ethernet Interface

- 10/100 Mbits/s IEEE 802.3 interface
- IEEE 802.3af POE (PowerDsine Certified)

Power Supply

- External Power Supply

RFP LED Status

Table 15: RFP LED Status

LED Color	LED State	Meaning
Red	On Steady	Waiting for IP Link
Red	Flash (1 sec on/ 1 sec off)	BOOTP (with Booter version 2.x) DHCP (with Booter version 3.x)
Red	Flash (0.5 sec on/ 0.5 sec off)	TFTP Read Request
Red	Flash (0.2 sec on/ 0.2 sec off)	TFTP Data Transfer
Orange	On Steady	Identifies the OMM
Green	Flashing	Connecting to OMM over air
Green	On Steady	RFP is connected to OMM
Red	Flashing (2 sec on/ 2 sec off)	One of the above processes has failed

RFP Startup Sequence

Booter (LED Solid Red)

- IP RFP has a small footprint NetBoot SW (booter) on board
- The booter implements the following:
 - BOOTP client (with Booter version 2.x)
DHCP client (with Booter version 3.x)
 - TFTP client
- Booter is updated automatically after the boot image downloads the following:
 - One initial booter
 - Two booter images
- Booter version 3.x uses DHCP instead of BOOTP. Booter version 2.x uses BOOTP instead of DHCP. The booter is used to configure the IP parameters and to locate the boot image in the network. The DHCP/BOOTP client supports the following parameters:
 - IP Address
 - Netmask
 - Gateway
 - TFTP Server IP Address
 - TFTP filename (If no filename is supplied, iprfp.bin is used)
- TFTP is used to retrieve the boot image
 - Boot image is checksum protected

- After successful download, the boot image is started



Note: ICMP is not supported. An IP RFP running the booter will not answer a ICMP request (ping).

DHCP (LED Flashing RED)

- The DHCP client is started just after successful download of the bootimage.
- The DHCP client retrieves the following data from the DHCP server (embedded 3300 ICP or NT DHCP)
 - Option 140: IP Address (U32) of the Open Mobility Manager (mandatory)
 - Option 141: IP Address (U32) of syslog daemon (optional)
 - Option 142: Port (U16) of the syslog daemon (optional)
- If the DHCP client does not get a DHCP offer with all mandatory information within 3 minutes, the system will be rebooted.
- If the DHCP client gets all mandatory information from a DHCP offer, the RFP application and the OMM will be started.

TFTP (LED Flashing RED quickly)

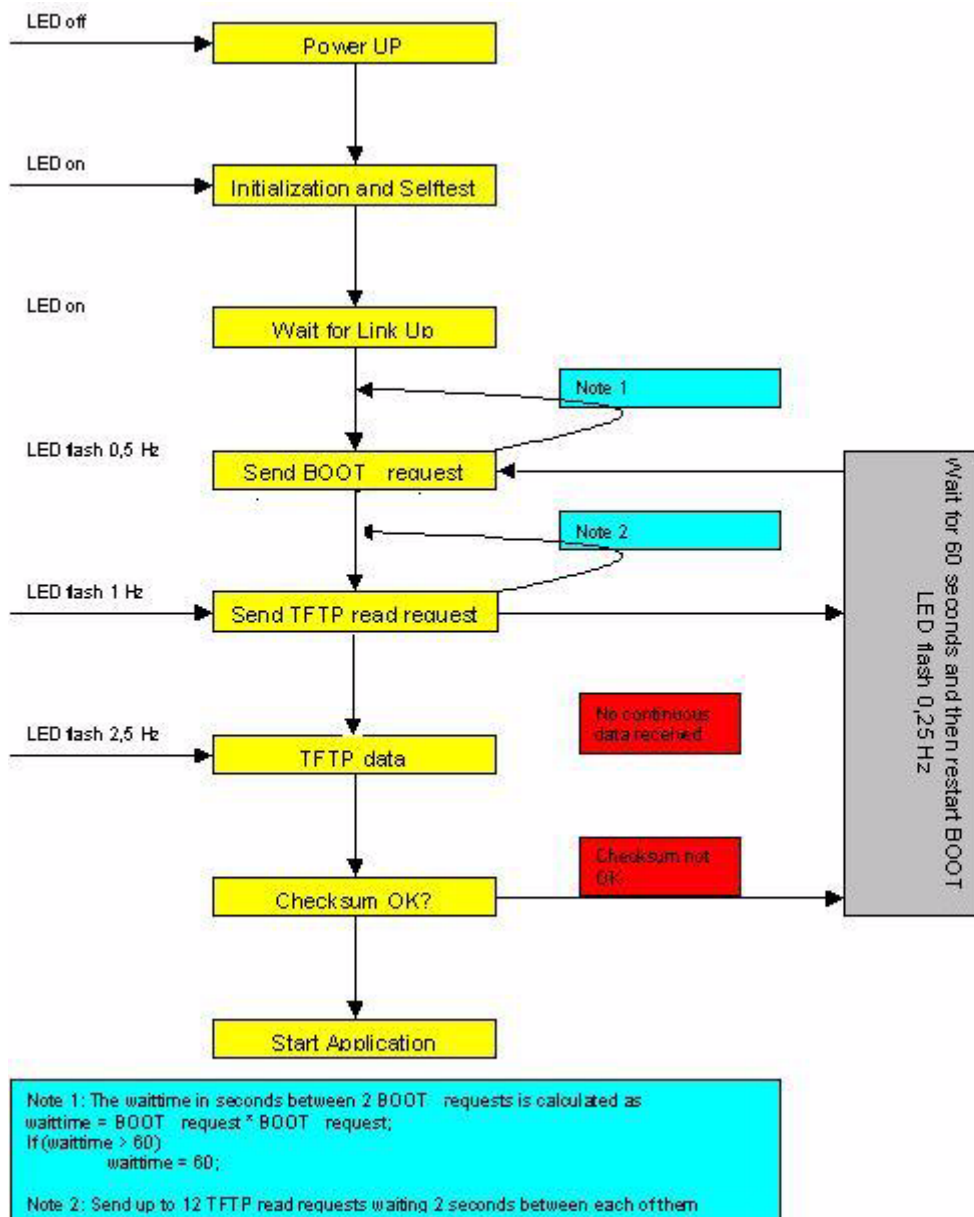
- The binary file, iprfp.bin, is downloaded from the TFTP directory within /sysro of the 3300 ICP and loaded into flash memory.

IP RFP Application (Green LED)

- Downloads BMC and DSP
- Controls DSP
- Connects to OMM
- OMM is started only on the IP RFP that has been assigned the OMM IP Address.

IP RFP Booter

Figure 40 shows the IP Boot sequence of the RFP.



IP0670

Figure 40: IP RFP Boot Sequence

Portable Parts (OpenPhones)








Only the OpenPhone 27 is supported in Mitel IP-DECT Release 2.0.

Handset Display

- 96 x 60 dots
- 1 Icon Line or Character headline

- 4 Character Lines: 3 for text, 1 for softkeys
- 16 Characters per line
- Separator line between icon line and menu text in menu mode
- Amber backlighting of LED display and keyboard -- battery backlight turns off after 10 seconds of no activity to conserve battery
- Display icons are provided for critical functions

Table 16: Display Icons







Icon	Meaning
	Off hook
	Loud speaker indication
	Ringer off
	Alarm time activated
	Field strength
	Battery condition
	Resiliency

Field Strength Display

Table 17: Field Strength

Field Strength Icon	Field Strength (dBm)
4 Bars	-57.5dBm and more
3 Bars	Between -57.5dBm and -67.5dBm
2 Bars	Between -67.5dBm and -77.5dBm
1 Bar	Between -77.5dBm and -92.0dBm

Battery Charge

Icon	Battery Charge Level
	80 to 100 %
	60 to 80 %
	40 to 60 %
	20 to 40 %
	0 to 20 %
	Frame flashes; battery is almost discharged; warning signal sounds

Power

The OP 27 is powered by 3dAAA mAH NiMH batteries:

- charge time is 6 to 7 hours
- talk time up to 20 hours (starting with a fully charged set of batteries)
- standby time up to 200 hours (starting with a fully charged set of batteries)

Appendix B: MIB-II

This appendix describes the 11 object groups published in the following RFCs:

- RFC 1156, Management Information Base for Network Management of TCP/IP-based internets, May, 1990.
- RFC 1213, Management Information Base for Network Management of TCP/IP-based internets: MIB-II, March, 1991.

The Object Identifier (OID) is displayed in brackets.

Please note that the agent does not support the following:

- MIB-II write access
- SNMPv2-MIB read/write access
- NET-SNMP-MIB read/write access
- NET-SNMP-AGENT-MIB read/write access
- SNMPv3.

System Group (1)

The vendor's authoritative identification of the network management subsystem contained in the entity. Implementation of the system group is mandatory for all systems.

sysDescr (1)

A textual description of the entity. This value should include the full name and version identification of the system's hardware type, software operating system, and networking software. It is mandatory that this only contain printable ASCII characters.

sysObjectID (2)

The vendor's authoritative identification of the network management subsystem contained in the entity.

sysUpTime (3)

The time (in hundredths of a second) since the network management portion of the system was last re-initialized.

sysContact (4)

The textual identification of the contact person for this managed node, together with information on how to contact this person.

sysName (5)

An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name.

sysLocation (6)

The physical location of this node (e.g., "telephone closet, 3rd floor").

sysServices (7)

A value which indicates the set of services that this entity potentially offers. The value is a sum. This sum initially takes the value zero. Then, for each layer, L, in the range 1 through 7, that this node performs transactions for, 2 raised to (L - 1) is added to the sum. For example, a node which performs only routing functions would have a value of 4 ($2^{(3-1)}$). In contrast, a node which is a host offering application services would have a value of 72 ($2^{(4-1)} + 2^{(7-1)}$). Note that in the context of the Internet suite of protocols, values should be calculated accordingly:

Layer	Functionality
1	Physical (i.e. repeaters)
2	Datalink/ subnetwork (i.e. bridges)
3	Internet (supports the IP)
4	End-to-end (supports the TCP)
7	Applications (supports the SMTP)

For systems including OSI protocols, layers 5 and 6 may also be counted.

Interfaces Group (2)

Implementation of the interfaces group is mandatory for all systems.

ifNumber (1)

The number of network interfaces (regardless of their current state) present on this system.

ifTable (2)

The Interfaces table contains information on the entity's interfaces. Each interface is thought of as being attached to a "subnetwork". Note that this term should not be confused with "subnet" which refers to an addressing partitioning scheme used in the Internet suite of protocols.

A list of interface entries:

ifEntry (1)

An interface entry containing objects at the subnetwork layer and below for a particular interface.

ifIndex (1)

A unique value for each interface. Its value ranges between 1 and the value of ifNumber. The value for each interface must remain constant at least from one reinitialization of the entity's network management system to the next re-initialization.

ifDescr (2)

A text string containing information about the interface. This string should include the name of the manufacturer, the product name and the version of the hardware interface. The string is intended for presentation to a human; it must not contain anything but printable ASCII characters.

ifType (3)

The type of interface, distinguished according to the physical/link/network protocol(s) immediately "below" IP in the protocol stack.

other(1)	none of the following
regular1822(2)	
hdh1822(3)	
ddn-x25(4)	
rfc877-x25(5)	
ethernet-csmacd(6)	
iso88023-csmacd(7)	
iso88024-tokenBus(8)	
iso88025-tokenRing(9)	
iso88026-man(10)	
starLan(11)	
proteon-10MBit(12)	
proteon-80MBit(13)	
hyperchannel(14)	
fddi(15)	
lapb(16)	
sdlc(17)	
t1-carrier(18)	
cept(19)	European equivalent of T-1
basicIsdn(20)	
primaryIsdn(21)	proprietary serial
propPointToPointSerial(22)	
ppp(23)	
softwareLoopback(24)	
eon(25)	CLNP over IP [12]
ethernet-3Mbit(26)	
nsip(27)	XNS over IP
slip(28)	generic SLIP
ultra(29)	ULTRA technologies
ds3(30)	T-3
sip(31)	SMDS
frame-relay(32)	

ifMtu (4)

The size of the largest IP datagram which can be sent/received on the interface, specified in octets.

ifSpeed (5)

An estimate of the interface's current bandwidth in bits per second. For interfaces which do not vary in bandwidth or for those where no accurate estimation can be made, this object should contain the nominal bandwidth.

ifPhysAddress (6)

The interface's address at the protocol layer immediately "below" IP in the protocol stack. For interfaces which do not have such an address (e.g., a serial line), this object should contain an octet string of zero length.

ifAdminStatus (7)

The desired state of the interface. The testing(3) state indicates that no operational packets can be passed.

ifOperStatus (8)

The current operational state of the interface.

up(1)	ready to pass packets
down(2)	
testing(3)	in some test mode

The testing(3) state indicates that no operational packets can be passed.

ifLastChange (9)

The value of sysUpTime at the time the interface entered its current operational state. If the current state was entered prior to the last reinitialization of the local network management subsystem, then this object contains a zero value.

ifInOctets (10)

The total number of octets received on the interface, including framing characters.

ifInUcastPkts (11)

The number of (subnet) unicast packets delivered to a higher-layer protocol.

ifInNUcastPkts(12)

The number of non-unicast (i.e., subnet broadcast or subnet multicast) packets delivered to a higher-layer protocol.

ifInDiscards (13)

The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.

ifInErrors (14)

The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

ifInUnknownProtos (15)

The number of packets received via the interface which were discarded because of an unknown or unsupported protocol.

ifOutOctets (16)

The total number of octets transmitted out of the interface, including framing characters.

ifOutUcastPkts (17)

The total number of packets that higher-level protocols requested be transmitted to a subnet-unicast address, including those that were discarded or not sent.

ifOutNUcastPkts (18)

The total number of packets that higher-level protocols requested be transmitted to a non-unicast (i.e., a subnet broadcast or subnet multicast) address, including those that were discarded or not sent.

ifOutDiscards (19)

The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.

ifOutErrors (20)

The number of outbound packets that could not be transmitted because of errors.

ifOutQLen (21)

The length of the output packet queue (in packets).

ifSpecific (22)

A reference to MIB definitions specific to the particular media being used to realize the interface. For example, if the interface is realized by an ethernet, then the value of this object refers to a document defining objects specific to ethernet. If an agent is not configured to have a value for

any of these variables, the object identifier

nullSpecific OBJECT IDENTIFIER ::= { 0 0 }

is returned. Note that "nullSpecific" is a syntactically valid object identifier, and any conformant implementation of ASN.1 and BER must be able to generate and recognize this value.

Address Translation (AT) Group (3)

Implementation of the Address Translation group is mandatory for all systems. Note, however, that this group is deprecated by MIB-II. That is, it is being included solely for compatibility with MIB-I nodes, and will most likely be excluded from MIB-III nodes.

IP Group (4)

Implementation of the IP group is mandatory for all systems.

ipForwarding (1)

The indication of whether this entity is acting as an IP gateway in respect to the forwarding of datagrams received by, but not addressed to, this entity. IP gateways forward datagrams; Hosts do not (except those Source-Routed via the host).

gateway(1)	entity forwards datagrams
host(2)	entity does NOT forward datagrams

ipDefaultTTL (2)

The default value inserted into the Time-To-Live field of the IP header of datagrams originated at this entity, whenever a TTL value is not supplied by the transport layer protocol.

ipInReceives (3)

The total number of input datagrams received from interfaces, including those received in error.

ipInHdrErrors (4)

The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, etc.

ipInAddrErrors (5)

The number of input datagrams discarded because the IP Address in their IP header's destination field was not a valid address to be received at this entity. This count includes invalid

addresses (e.g., 0.0.0.0) and addresses of unsupported Classes (e.g., Class E). For entities which are not IP Gateways and, therefore, do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.

ipForwDatagrams (6)

The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP Gateways, this counter will include only those packets which were Source-Routed via this entity, and where the Source-Route option processing was successful.

ipInUnknownProtos (7)

The number of locally-addressed datagrams received successfully, but discarded because of an unknown or unsupported protocol.

ipInDiscards (8)

The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g. for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting reassembly.

ipInDelivers (9)

The total number of input datagrams successfully delivered to IP user protocols (including ICMP).

ipOutRequests (10)

The total number of IP datagrams which local IP user protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in ipForwDatagrams.

ipOutDiscards (11)

The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). Note that this counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.

ipOutNoRoutes (12)

The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in ipForwDatagrams which meet this "no-route" criterion.

ipReasmTimeout (13)

The maximum number of seconds which received fragments are held while they are awaiting reassembly at this entity.

ipReasmReqds (14)

The number of IP fragments received which needed to be reassembled at this entity.

ipReasmOKs (15)

The number of IP datagrams successfully reassembled.

ipReasmFails (16)

The number of failures detected by the IP reassembly algorithm (for whatever reason: timed out, errors, etc). Note that this is not necessarily a count of discarded IP fragments since some algorithms (notably RFC 815) can lose track of the number of fragments by combining them as they are received.

ipFragOKs (17)

The number of IP datagrams that have been successfully fragmented at this entity.

ipFragFails (18)

The number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be, because their "Don't Fragment" flag was set, for example.

ipFragCreates (19)

The number of IP datagram fragments that have been generated as a result of fragmentation at this entity.

ipAddrTable (20)

The table of addressing information relevant to this entity's IP Addresses.

ipAddrEntry (1)

The addressing information for one of this entity's IP Addresses.

ipAdEntAddr (1)

The IP Address to which this entry's addressing information pertains.

ipAdEntIfIndex (2)

The index value which uniquely identifies the interface to which this entry is applicable. The interface identified by a particular value of this index is the same interface as identified by the same value of ifIndex.

ipAdEntNetMask (3)

The subnet mask associated with the IP Address of this entry. The value of the mask is an IP Address with all the network bits set to 1 and all the hosts bits set to 0.

ipAdEntBcastAddr (4)

The value of the least-significant bit in the IP broadcast address used for sending datagrams on the (logical) interface associated with the IP Address of this entry. For example, when the Internet standard all-ones broadcast address is used, the value will be 1.

ipAdEntReasmMaxSize (5)

The size of the largest IP datagram which this entity can reassemble from incoming IP fragmented datagrams received on this interface.

ipRouteTable (21)

The IP Route Table contains an entry for each route presently known to this entity. Note that the action to be taken in response to a request to read a non-existent entry, is specific to the network management protocol being used.

ipRouteEntry (1)

A route to a particular destination.

ipRouteDest (1)

The destination IP Address of this route. An entry with a value of 0.0.0.0 is considered a default route. Multiple such default routes can appear in the table, but access to such multiple entries is dependent on the table-access mechanisms defined by the network management protocol in use.

ipRouteIfIndex (2)

The index value which uniquely identifies the local interface through which the next hop of this route should be reached. The interface identified by a particular value of this index is the same interface as identified by the same value of ifIndex.

ipRouteMetric1 (3)

The primary routing metric for this route. The semantics of this metric are determined by the routing protocol specified in the route's ipRouteProto value. If this metric is not used, its value should be set to -1.

ipRouteMetric2 (4)

An alternate routing metric for this route. The semantics of this metric are determined by the routing- protocol specified in the route's ipRouteProto value. If this metric is not used, its value should be set to -1.

ipRouteMetric3 (5)

An alternate routing metric for this route. The semantics of this metric are determined by the routing protocol specified in the route's `ipRouteProto` value. If this metric is not used, its value should be set to -1.

ipRouteMetric4 (6)

An alternate routing metric for this route. The semantics of this metric are determined by the routing- protocol specified in the route's `ipRouteProto` value. If this metric is not used, its value should be set to -1.

ipRouteNextHop (7)

The IP Address of the next hop of this route.

ipRouteType (8)

The type of route:

other(1)	none of the following
invalid(2)	an invalidated route
	route to directly
direct(3)	connected (sub-)network
	route to a non-local
remote(4)	host/network/subnetwork

ipRouteProto (9)

The routing mechanism via which this route was learned. Inclusion of values for gateway routing protocols is not intended to imply that hosts should support those protocols.

other(1)	none of the following
	non-protocol information
local(2)	e.g., manually configured entries
netmgmt(3)	set via a network management protocol
icmp(4)	obtained via ICMP e.g., Redirect

egp(5)	the remaining values are all gateway routing protocols
ggp(6)	
hello(7)	
rip(8)	
is-is(9)	
es-is(10)	
ciscoIgrp(11)	
bbnSpflgp(12)	
oigp(13)	

ipRouteAge (10)

The number of seconds since this route was last updated or otherwise determined to be correct. Note that no semantics of "too old" can be implied except through knowledge of the routing protocol by which the route was learned.

ipRouteMask (11)

Indicate the mask to be logical-ANDed with the destination address before being compared to the value in the ipRouteDest field. For those systems that do not support arbitrary subnet masks, an agent constructs the value of the ipRouteMask by determining whether the value of the correspondent ipRouteDest field belong to a class-A, B, or C network, and then using one of: mask network 255.0.0.0 class-A 255.255.0.0 class-B 255.255.255.0 class-C If the value of the ipRouteDest is 0.0.0.0 (a default route), then the mask value is also 0.0.0.0. It should be noted that all IP routing subsystems implicitly use this mechanism.

ipRouteMetric5 (12)

An alternate routing metric for this route. The semantics of this metric are determined by the routing protocol specified in the route's ipRouteProto value. If this metric is not used, its value should be set to -1.

ipRouteInfo (13)

A reference to MIB definitions specific to the particular routing protocol which is responsible for this route, as determined by the value specified in the route's ipRouteProto value. If this information is not present, its value should be set to the OBJECT IDENTIFIER { 0 0 }, which is a syntactically valid object identifier, and any conformant implementation of ASN.1 and BER must be able to generate and recognize this value.

ipNetToMediaTable (22)

The IP Address Translation table used for mapping from IP AddressIP Addresses to physical addresses.

ipNetToMediaEntry (1)

Each entry contains one ipAddress to "physical" address equivalence.

ipNetToMediaIfIndex (1)

The interface on which this entry's equivalence is effective. The interface identified by a particular value of this index is the same interface as identified by the same value of ifIndex.

ipNetToMediaPhysAddress (2)

The media-dependent "physical" address.

ipNetToMediaNetAddress (3)

The ipAddress corresponding to the media-dependent "physical" address.

ipNetToMediaType (4)

The type of mapping.

other(1)	none of the following
invalid(2)	an invalidated mapping
dynamic(3)	
static(4)	

Setting this object to the value invalid(2) has the effect of invalidating the corresponding entry in the ipNetToMediaTable. That is, it effectively disassociates the interface identified with said entry from the mapping identified with said entry. It is an implementation-specific matter as to whether the agent removes an invalidated entry from the table. Accordingly, management stations must be prepared to receive tabular information from agents that corresponds to entries not currently in use. Proper interpretation of such entries requires examination of the relevant ipNetToMediaType object.

ipRoutingDiscards (23)

The number of routing entries which were chosen to be discarded even though they are valid. One possible reason for discarding such an entry could be to free up buffer space for other entries.

ICMP Group (5)

Implementation of the ICMP group is mandatory for all systems. The ICMP group contains the ICMP input and output statistics. Note that individual counters for ICMP message (sub-)codes have been omitted from this (version of the) MIB for simplicity.

icmplnMsgs (1)

The total number of ICMP messages which the entity received. Note that this counter includes all those counted by icmplnErrors.

icmplnErrors (2)

The number of ICMP messages which the entity received, but determined as having errors (bad ICMP checksums, bad length, etc.).

icmplnDestUnreachs (3)

The number of ICMP Destination Unreachable messages received.

icmplnTimeExcds (4)

The number of ICMP Time Exceeded messages received.

icmplnParmProbs (5)

The number of ICMP Parameter Problem messages received.

icmplnSrcQuenchs (6)

The number of ICMP Source Quench messages received.

icmplnRedirects (7)

The number of ICMP Redirect messages received.

icmplnEchos (8)

The number of ICMP Echo (request) messages received.

icmplnEchoReps (9)

The number of ICMP Echo Reply messages received.

icmplnTimestamps (10)

The number of ICMP Timestamp (request) messages received.

icmpInTimestampReps (11)

The number of ICMP Timestamp Reply messages received.

icmpInAddrMasks (12)

The number of ICMP Address Mask Request messages received.

icmpInAddrMaskReps (13)

The number of ICMP Address Mask Reply messages received.

icmpOutMsgs (14)

The total number of ICMP messages which this entity attempted to send. Note that this counter includes all those counted by icmpOutErrors.

icmpOutErrors (15)

The number of ICMP messages which this entity did not send due to problems discovered within ICMP such as a lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations, there may be no types of error which contribute to this counter's value.

icmpOutDestUnreachs (16)

The number of ICMP Destination Unreachable messages sent.

icmpOutTimeExcds (17)

The number of ICMP Time Exceeded messages sent.

icmpOutParmProbs (18)

The number of ICMP Parameter Problem messages sent.

icmpOutSrcQuenchs (19)

The number of ICMP Source Quench messages sent.

icmpOutRedirects (20)

The number of ICMP Redirect messages sent.

icmpOutEchos (21)

The number of ICMP Echo (request) messages sent.

icmpOutEchoReps (22)

The number of ICMP Echo Reply messages sent.

icmpOutTimestamps (23)

The number of ICMP Timestamp (request) messages sent.

icmpOutTimestampReps (24)

The number of ICMP Timestamp Reply messages sent.

icmpOutAddrMasks (25)

The number of ICMP Address Mask Request messages sent.

icmpOutAddrMaskReps (26)

The number of ICMP Address Mask Reply messages sent.

TCP Group (6)

Implementation of the TCP group is mandatory for all systems that implement the TCP protocol. Note that instances of object types that represent information about a particular TCP connection are transient; they persist only as long as the connection in question.

tcpRtoAlgorithm (1)

The algorithm used to determine the time out value used for retransmitting unacknowledged octets.

other(1)	none of the following
constant(2)	a constant rto
rsre(3)	MIL-STD-1778, Appendix B
vanj(4)	Van Jacobson's algorithm [15]

tcpRtoMin (2)

The minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the LBOUND quantity described in RFC 793.

tcpRtoMax (3)

The maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the UBOUND quantity described in RFC 793.

tcpMaxConn (4)

The limit on the total number of TCP connections the entity can support. In entities where the maximum number of connections is dynamic, this object should contain the value "-1".

tcpActiveOpens (5)

The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.

tcpPassiveOpens (6)

The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.

tcpAttemptFails (7)

The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.

tcpEstabResets (8)

The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.

tcpCurrEstab (9)

The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.

tcpInSegs (10)

The total number of segments received, including those received in error. This count includes segments received on currently established connections.

tcpOutSegs (11)

The total number of segments sent, including those on current connections, but excluding those containing only retransmitted octets.

tcpRetransSegs (12)

The total number of segments retransmitted - that is, the number of TCP segments transmitted containing one or more previously transmitted octets.

tcpConnTable (13)

A table containing TCP connection-specific information.

tcpConnEntry (1)

Information about a particular current TCP connection. An object of this type is transient, in that it ceases to exist when (or soon after) the connection makes the transition to the CLOSED state.

tcpConnState (1)

The state of this TCP connection.

- closed(1)
- listen(2)
- synSent(3)
- synReceived(4)
- established(5)
- finWait1(6)
- finWait2(7)
- closeWait(8)
- lastAck(9)
- closing(10)
- timeWait(11)

tcpConnLocalAddress (2)

The local IP Address for this TCP connection.

tcpConnLocalPort (3)

The local port number for this TCP connection.

tcpConnRemAddress (4)

The remote IP Address for this TCP connection.

tcpConnRemPort (5)

The remote port number for this TCP connection.

tcpInErrs (14)

The total number of segments received in error (e.g., bad TCP checksums).

tcpOutRsts (15)

The number of TCP segments sent containing the RST flag.

UDP Group (7)

Implementation of the UDP group is mandatory for all systems which implement the UDP protocol.

udpInDatagrams (1)

The total number of UDP datagrams delivered to UDP users.

udpNoPorts (2)

The total number of received UDP datagrams for which there was no application at the destination port.

udpInErrors (3)

The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.

udpOutDatagrams (4)

The total number of UDP datagrams sent from this entity.

udpTable (5)

A table containing UDP listener information.

udpEntry (1)

Information about a particular current UDP listener.

udpLocalAddress (1)

The local IP Address for this UDP listener. In the case of a UDP listener which is willing to accept datagrams for any IP interface associated with the node, the value 0.0.0.0 is used.

udpLocalPort (2)

The local port number for this UDP listener.

Exterior Gateway Protocol (EGP) Group (8)

Exterior Gateway Protocol, historical. Implementation of the EGP group is mandatory for all systems which implement the EGP.

Common Management Information Services and Protocol Over TCP/IP (CMOT) Group (9)

Common Management Information Services and Protocol over TCP/IP, deprecated.

Transmission Group (10)

Based on the transmission media underlying each interface on a system, the corresponding portion of the Transmission group is mandatory for that system. When Internet-standard definitions for managing transmission media are defined, the transmission group is used to provide a prefix for the names of those objects. Typically, such definitions reside in the experimental portion of the MIB until they are "proven", then as a part of the Internet standardization process, the definitions are accordingly elevated and a new object identifier, under the transmission group, is defined. By convention, the name assigned is:

type OBJECT IDENTIFIER ::= { transmission number }

where "type" is the symbolic value used for the media in the ifType column of the ifTable object, and "number" is the actual integer value corresponding to the symbol.

SNMP Group (11)

Implementation of the SNMP group is mandatory for all systems which support an SNMP protocol entity. Some of the objects defined below will be zero-valued in those SNMP implementations that are optimized to support only those functions specific to either a management agent or a management client.

snmpInPkts (1)

The total number of PDUs delivered to the SNMP entity from the transport service.

snmpOutPkts (2)

The total number of SNMP PDUs which were passed from the SNMP protocol entity to the transport service.

snmpInBadVersions (3)

The total number of syntactically correct SNMP PDUs which were delivered to the SNMP protocol entity and were for an unsupported SNMP version.

snmplnBadCommunityNames (4)

The total number of SNMP PDUs delivered to the SNMP protocol entity which used a SNMP community name not known to said entity.

snmplnBadCommunityUses (5)

The total number of SNMP PDUs delivered to the SNMP protocol entity which represented an SNMP operation which was not allowed by the SNMP community named in the PDU.

snmplnASNParseErrs (6)

The total number of ASN.1 parsing errors (either in encoding or syntax) encountered by the SNMP protocol entity when decoding received SNMP PDUs.

snmplnBadTypes (7)

The total number of SNMP PDUs delivered to the SNMP protocol entity which had an unknown PDU type.

snmplnTooBig (8)

The total number valid SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the "ErrorStatus" component is "tooBig."

snmplnNoSuchNames (9)

The total number valid SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the "ErrorStatus" component is "noSuchName."

snmplnBadValues (10)

The total number valid SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the "ErrorStatus" component is "badValue."

snmplnReadOnly (11)

The total number valid SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the "ErrorStatus" component is "readOnly."

snmplnGenErrs (12)

The total number valid SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the "ErrorStatus" component is "genErr."

snmplnTotalReqVars (13)

The total number of MIB objects which have been retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs.

snmpInTotalSetVars (14)

The total number of MIB objects which have been altered successfully by the SNMP protocol entity as the result of receiving valid SNMP Set-Request PDUs.

snmpInGetRequests (15)

The total number of SNMP Get-Request PDUs which have been accepted and processed by the SNMP protocol entity.

snmpInGetNexts (16)

The total number of SNMP Get-Next PDUs which have been accepted and processed by the SNMP protocol entity.

snmpInSetRequests (17)

The total number of SNMP Set-Request PDUs which have been accepted and processed by the SNMP protocol entity.

snmpInGetResponses (18)

The total number of SNMP Get-Response PDUs which have been accepted and processed by the SNMP protocol entity.

snmpInTraps (19)

The total number of SNMP Trap PDUs which have been accepted and processed by the SNMP protocol entity.

snmpOutTooBigs (20)

The total number valid SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the "ErrorStatus" component is "tooBig."

snmpOutNoSuchNames (21)

The total number valid SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the "ErrorStatus" component is "noSuchName."

snmpOutBadValues (22)

The total number valid SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the "ErrorStatus" component is "badValue."

snmpOutReadOnlys (23)

The total number valid SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the "ErrorStatus" component is "readOnly."

snmpOutGenErrs (24)

The total number valid SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the "ErrorStatus" component is "genErr."

snmpOutGetRequests (25)

The total number of SNMP Get-Request PDUs which have been generated by the SNMP protocol entity.

snmpOutGetNexts (26)

The total number of SNMP Get-Next PDUs which have been generated by the SNMP protocol entity.

snmpOutSetRequests (27)

The total number of SNMP Set-Request PDUs which have been generated by the SNMP protocol entity.

snmpOutGetResponses (28)

The total number of SNMP Get-Response PDUs which have been generated by the SNMP protocol entity.

snmpOutTraps (29)

The total number of SNMP Trap PDUs which have been generated by the SNMP protocol entity.

snmpEnableAuthTraps (30)

Indicates whether the SNMP agent process is configured to generate authentication-failure traps.

Index

Numerics

- 1.8 Ghz Media channel 13
- 3300 ICP
 - OpenPhone programming 65
 - Technician's handbook 69

A

- Active column 56
- Adaptive differential pulse code modulation 34
- Administrator's password, setting 71
- ADPCM 9
- Audience, of guide 7

B

- Backups
 - OMM database 69
 - performing 73
- Base stations
 - description 12
 - mounting 48
 - power adapter 32
 - RFP channel capacity 29
- Battery charge 94
- BOOTP 9
- Building diagram 34
- Busy bit 29

C

- Call handover 13
- Capacity, of system 34
- CAT 5 9
- CDP 9
- Charge time 94
- Checklist, for maintenance 71
- Cisco Discovery Protocol 9
- Class of service 66
- Cluster 55
- CMI 9
- Configuring
 - administrator's password 71
 - DHCP scope 36
 - licence key and PARK 49
 - license key and park 49
 - OMM 48
 - overview 31
 - reservations for RFPs 45
 - site name and number 68
 - system settings 53, 60
 - username 69

D

- Database, backing up 69
- DECT 9
 - description 12
 - parameter check box 53, 55, 59
 - restrictions 31
- DECT-monitor 53, 60
- Definitions, of terms 9
- DHCP
 - configuring scope 36
 - definition 9
 - options required on 3300 37, 39, 41, 44
 - scope 13
- Directory name, changing 73
- Discard all settings 75
- Display
 - icons on handset 93
 - of field strength 94
- Documentation web site 34
- DSP 9

E

- E2T 9
- Embedded 3300 DHCP service 37, 39, 41, 44
- Extn 9

F

- Field strength 94
- Figure
 - adding RFPs 55
 - backup screen 74
 - changing administrator's user account 71
 - configuring OMM MAC address 41
 - configuring the OpenPhones 65
 - IP-DECT wireless solution 12
 - licensing screen 49
 - Media Stream Management 28
 - OMM login page 48
 - rebooting the OMM 75
 - saving configuration file 74
 - setting up RFP reservations 43
- Flash chip 73
- FRP, power adapter 32

G

- G.711 9
- G.729a 9
- GAP 9
- General packet radio service 33
- Global mobile communications system 33
- Glossary, of terms 9
- GMI 9

GMS 9
GPRS 9
Guide
 purpose of 7
 where to find more information 7

H

Handbook 69
Handover, of calls 13
Handsets
 number supported 34
 specifications 92
Health checklist 71
HTTP 9

I

ICMP 9
ICP 9
Inactivity lockout 48
Installation overview 31
Intercept Handling 66
Interconnect Restriction 66
Internet Explorer 6.0 48
IP 9
IP phone call
 to an OpenPhone 26
IP-DECT
 description 12
 restrictions 31
IPEI 9
IPRFP 9
iprfp.bin 75

L

Launching, login page 48
LED 9
License
 server 49
 username and password 51
License key
 configuring 49
Licenses
 missing 49
 Types of licenses 32
Licensing
 replacing RFP 86
Logging in 48
Login, default passwords 48

M

MAC 9
Maintenance checklist 71

Manual
 purpose of 7
 where to find more information 7
Media stream requirements 27
MIPS 9

N

Netscape Navigator 7.0 48
NiMH batteries 94

O

OMM 10
 decription 12
 logging in 48
 platform requirements 48
 rebooting 75
Online help, for system admin tool 8
OP26, description 10
OP27
 changing name 73
OP27, description 10
Open mobility manager
 backups 69
 description 12
 logging in 48
 platform requirements 48
 rebooting 75
OpenPhone
 changing name 73
OpenPhones
 configuring on 3300 ICP 65
 number supported 34
 specifications 92
 subscription 67
 to IP phone call 26
 to OpenPhone call 27
 username configuration 69
 verifying 69

P

PARK 11
PARK, configuring 49
Password, for licensing 51
Password, OMM 71
PIN 54, 60
POE 10
Portable parts
 configuring on 3300 ICP 65
 number supported 34
 specifications 92
 subscription 67
 username configuration 69
 verifying 69

Power adapter 32
Power over ethernet 32
PowerDsine 32

R

Radio fixed part
 replacing 86
Radio fixed parts
 configuring reservations 45
 description 12
 mounting 48
 specification 7
Rebooting 75
Redundancy, for RFPs 32
Refresh 50
Reservations 47
Resiliency 31
RFP
 channel capacity 29
 deleting 54
 description 12, 13
 displaying license status 56
 licenses 32
 mounting 48
 number supported 34
 redundancy 32
 replacing failed RFP 86
 zone of coverage 13
RFPI 10
RTCP 10

S

Serial number 49
Session timeout 48
Signal strength, requirement 27
Site data, collecting and recording 35
Site diagram 34
Site name 68
Site survey
 instructions 7, 34

 performing 34
Standby time 94
Subscribing OpenPhones 67
Supply, power 32
Survey, of site 34
Synchron column 56
Synchronization, of RFPs 27
Syslog daemon server 37, 39, 42, 44
System Administration Tool 66
System settings, configuring 53, 60

T

Talk time 94
TAN 51
Technicians handbook, 3300 ICP 69
Telephone directory 14
Terms, defined 9
Tool icon 65
Training
 requirements 7
Transaction number 51
Transmission control protocol 34
Trashcan icon 65

U

Uninterruptible power supply 33
User guide, OP27 69
User name, changing 73
Username, for licensing 51

V

Verifying, handset functionality 69
VLAN 16

W

Web service 13
Windows 2000 server 39
Windows NT server 38
Wireless Phones IP Set Configuration form 66

