



Avaya Solution & Interoperability Test Lab

Application Note for Configuring the Ascom wireless IP-DECT SIP Solution with Avaya Communication Manager, Avaya SIP Enablement Services and Avaya Modular Messaging - Issue 1.0

Abstract

These Application Notes describe a solution for supporting wireless interoperability between the Ascom wireless IP-DECT SIP solution with Avaya Communication Manager, Avaya SIP Enablement Services and Avaya Modular Messaging. Emphasis of the testing was placed on verifying good voice quality on calls from and to Ascom wireless IP-DECT SIP handsets registered to the Avaya telephony infrastructure. Information in these Application Notes has been obtained through compliance testing and additional technical discussions. Testing was conducted via the *DeveloperConnection* Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes detail the steps for creating a SIP VoIP-enabled wireless network using Digital Enhanced Cordless Telecommunications (DECT) with connectivity that enables interoperability between the Ascom wireless IP-DECT SIP solution with Avaya Communication Manager, Avaya SIP Enablement Services and Avaya Modular Messaging. The specific calling features that were verified to operate correctly include transfer (attended and unattended), hold/return from hold, multiple call appearances, caller ID operation, call forwarding (unconditional, on busy/no answer and clear), pickup groups, call pickup, bridged appearances, and voicemail Message Waiting Indicator (MWI).

1.1. Ascom IP DECT Base Station

The Ascom IP-DECT system is a modular solution for large and small deployments with full handover capabilities with one PBX. The Ascom IP-DECT Base Station works as a conduit between the Avaya SIP Enablement Services system and the Ascom IP-DECT wireless handsets. After the Ascom IP-DECT wireless handsets Sync up with the Ascom IP-DECT Base Station the Base station registers the handsets to the Avaya SIP Enablement Services.

1.2. Network Diagram

The network diagram shown in **Figure 1** illustrates the testing environment used for compliance testing. The network consists of an Avaya Communication Manager running on an Avaya S8300 Server with an Avaya G700 Media Gateway, Avaya SIP Enablement Server, Avaya Modular Messaging Server, Avaya Modular Messaging Server, one Avaya 9630 one-X Deskphone Edition IP Telephone, one Avaya 9620 one-X Deskphone Edition IP Telephone, one Avaya 2420 Digital Telephone one Ascom wireless IP-DECT Base Station, one Ascom wireless 9d24, one Ascom wireless OfficeT DECT Handset and one OfficeM DECT Handset. One computer is present in the network providing network services such as DHCP, TFTP, HTTP and RADIUS.

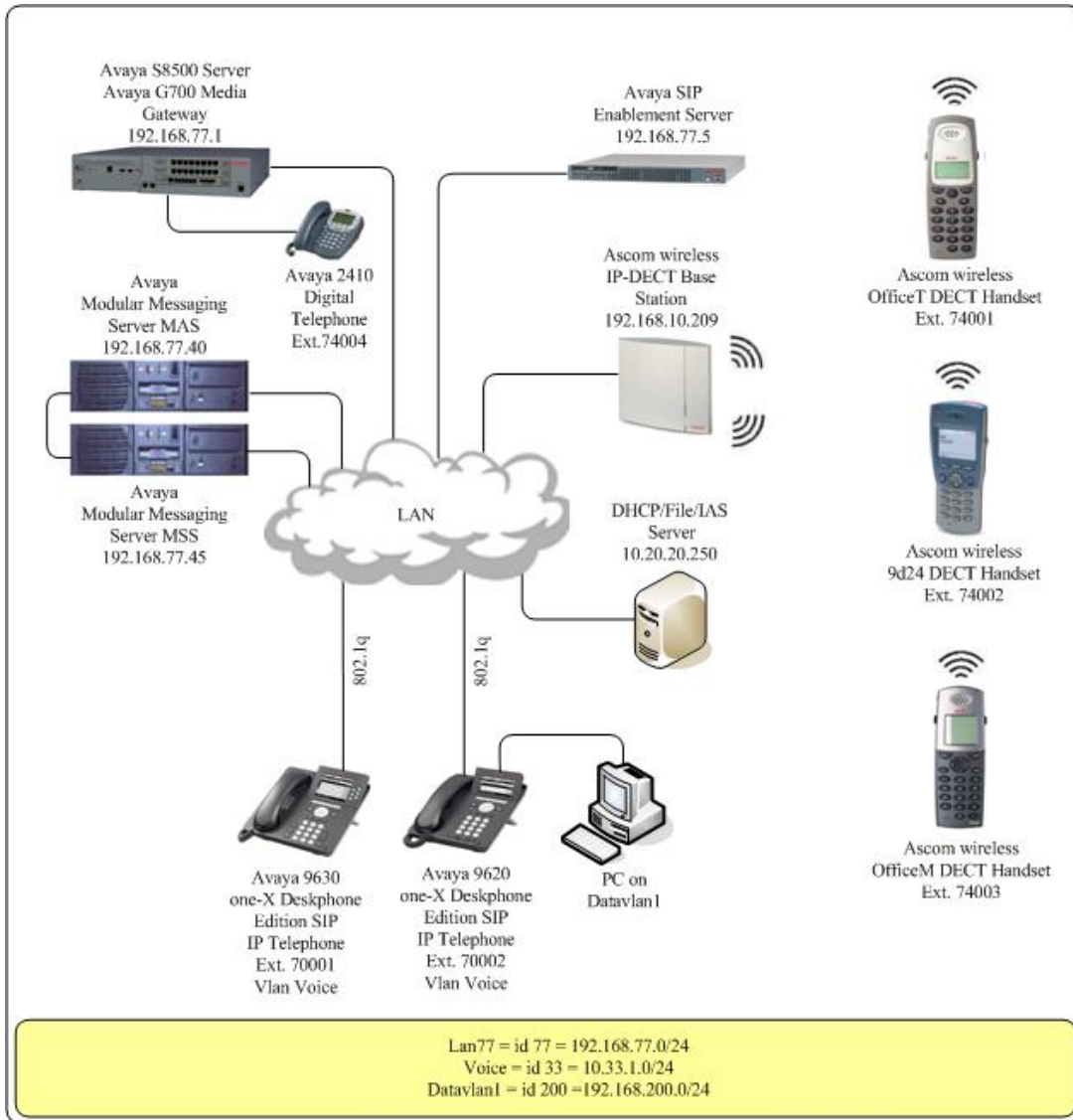


Figure 1: Sample Network Diagram

2. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment	Software
Avaya S8300 Server with Avaya Communication Manager	4.0 (04.0-00.1.731.2)
<ul style="list-style-type: none">• Avaya G700 Media Gateway• (MM712 DCP Media Module 8)	26.31.0 HW05 / FW08
Avaya Modular Messaging	3.0 and 3.1
Avaya SIP Enablement Services	4.0 (SES04.0-04.0.032.0)
Avaya 2420 Digital Telephone	N/A
Avaya 9630 IP Telephone (SIP)	1.5
Avaya 9620 IP Telephone (SIP)	1.5
Ascom wireless IP-DECT Base Station	2.0.12
Ascom wireless 9d24 DECT Handset	3.26
Ascom wireless OfficeT DECT Handset	1.06
Ascom wireless OfficeM DECT Handset	1.08

Avaya Communication Manager, Avaya SIP Enablement Services and Avaya Modular Messaging Configuration

All of the telephones configured in the sample network in **Figure 1** were administered as stations in Avaya Communication Manager. SIP stations were administered as Off-PBX stations in Avaya Communication Manager. For information on how to administer these types of stations refer to **Section 9 [1]**.

SIP stations were administered as users on the Avaya SIP Enablement Services. Media server extensions were associated with these SIP users to link the SIP users to the Avaya Communication Manager stations. For information on how to administer SIP stations on Avaya SIP Enablement Services refer to **Section 9 [2]**.

Voicemail services were provided by Avaya Modular Messaging. For information on how to administer Avaya Modular Messaging refer to **Section 9 [7]**.

Certain Avaya Communication Manager features were tested with the Ascom wireless DECT Handsets. The configuration related to these specific features tested is included in the following section.

2.1. Configure Avaya Communication Manager Features

Step	Description
1.	<p>To enable the features used for testing (Call Park, Call Answer, Call Forwarding and Call Pickup), administer the configuration for Feature Access Codes (FAC) and Feature Name Extensions (FNE) on Avaya Communication Manager. In order for the FACs and FNEs to be routed through the system properly the digits used for Auto Route Selection (ARS), Auto Alternate Routing (AAR) and FACs need to be administered in the dial plan. From the System Administration Terminal (SAT) interface on Avaya Communication Manager use the “change dialplan analysis” command and configure the values displayed in bold below and submit the change. The values specified for the “Dialed String” field must match the ones configured in Step 2 for Auto Alternate Routing (AAR) Access Code and Auto Route Selection (ARS) - Access Code.</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <pre> change dialplan analysis Page 1 of 12 DIAL PLAN ANALYSIS TABLE Percent Full: 3 Dialed Total Call Dialed Total Call Dialed Total Call String Length Type String Length Type String Length Type 1 3 dac 5 5 aar 7 5 ext 75000 5 ext 8 1 fac 9 1 fac * 3 fac 60 2 fac 61 2 fac # 3 fac </pre> </div>

Step	Description
2.	<p>The features implemented for SIP stations need to be paired with the features implemented for non-SIP stations, therefore, these values need to be specified even when using only SIP stations. From the SAT interface on Avaya Communication Manager use the “change feature-access-codes” command to configure the following values and submit the changes.</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <pre> Change feature-access-codes Page 1 of 7 FEATURE ACCESS CODE (FAC) Abbreviated Dialing List1 Access Code: Abbreviated Dialing List2 Access Code: Abbreviated Dialing List3 Access Code: Abbreviated Dial - Prgm Group List Access Code: Announcement Access Code: Attendant Access Code: Answer Back Access Code: #11 Auto Alternate Routing (AAR) Access Code: 60 Auto Route Selection (ARS) - Access Code: 61 Call Forwarding Activation Busy/DA: #15 All: #16 Deactivation: #17 Automatic Callback Activation: Deactivation: Call Forwarding Enhanced Status: Act: Deactivation: Call Park Access Code: #10 Call Pickup Access Code: #12 CAS Remote Hold/Answer Hold-Unhold Access Code: CDR Account Code Access Code: Change COR Access Code: Change Coverage Access Code: Contact Closure Open Code: Close Code: </pre> </div>

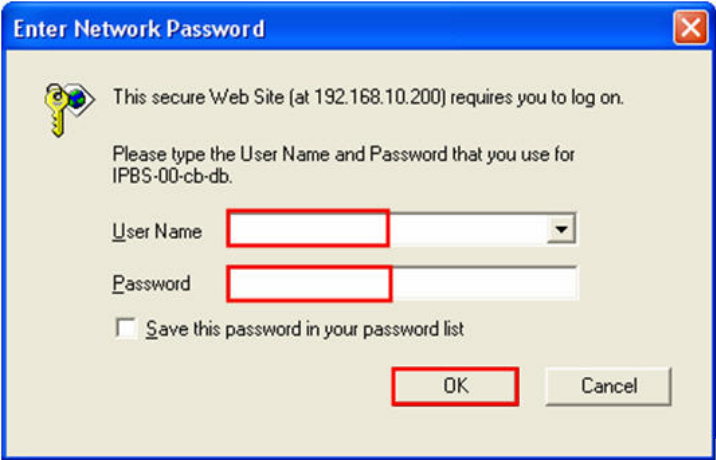
Step	Description
3.	<p>From the SAT interface use the “change off-pbx-stations feature-name extensions” command to configure the following values and submit the changes. Note that the extensions used for FNEs match those used for FACs by pre-pending the FAC code with “710”. Having this uniformity between FACs and FNEs is recommended.</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <pre> change off-pbx-telephone feature-name-extensions Page 1 of 2 EXTENSIONS TO CALL WHICH ACTIVATE FEATURES BY NAME Active Appearance Select: Automatic Call Back: Automatic Call-Back Cancel: Call Forward All: 71016 Call Forward Busy/No Answer: 71015 Call Forward Cancel: 71017 Call Park: 71010 Call Park Answer Back: 71011 Call Pick-Up: 71012 Calling Number Block: Calling Number Unblock: Conference on Answer: Directed Call Pick-Up: Drop Last Added Party: Exclusion (Toggle On/Off): Extended Group Call Pickup: Held Appearance Select: </pre> </div>

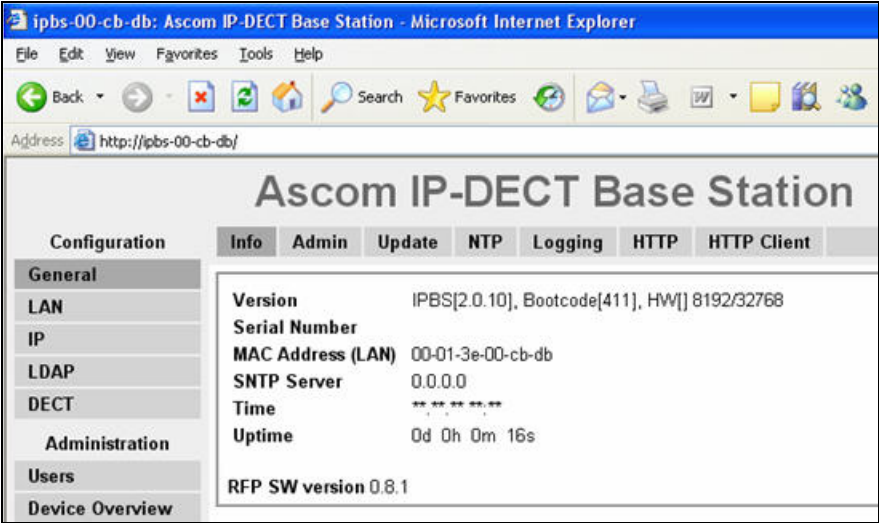
3. Ascom wireless IP-DECT SIP Solution Configuration

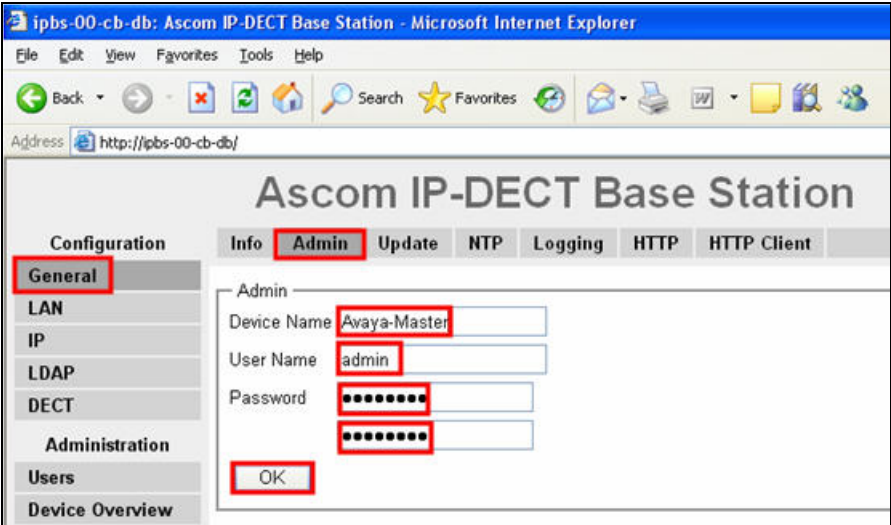
The following steps detail the initial configuration for the Ascom wireless IP-DECT SIP Solution. In the sample network the DHCP server was configured to register DHCP client information to a DNS server. This allows the Ascom wireless IP-DECT Base Station to be reachable via a DNS name using the following format: <http://IPBS-XX-XX-XX>, where XX-XX-XX are the last 3 bytes of the MAC address of the Ascom wireless IP-DECT Base Station. For example, an Ascom wireless IP-DECT Base Station with a MAC address of 00-01-3E-00-CB-DB could be accessed using <http://IPBS-00-CB-DB> or via the IP address assigned by DHCP.

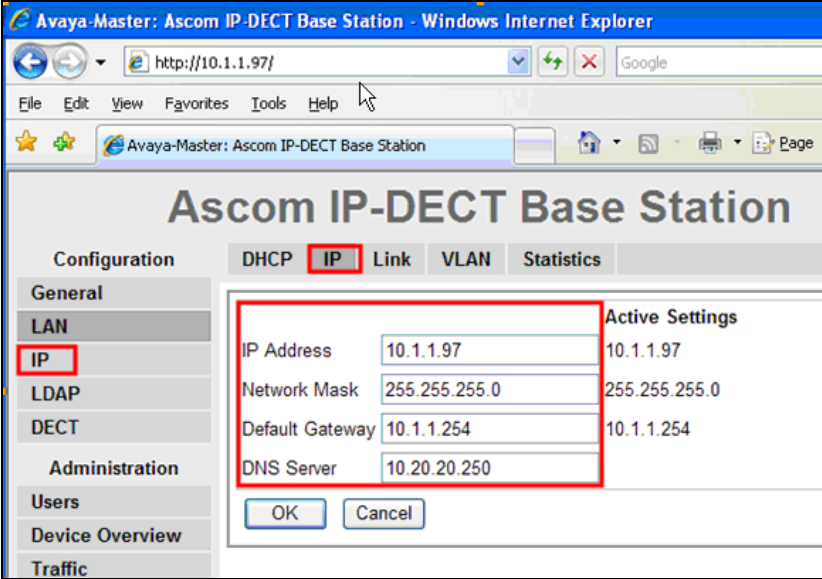
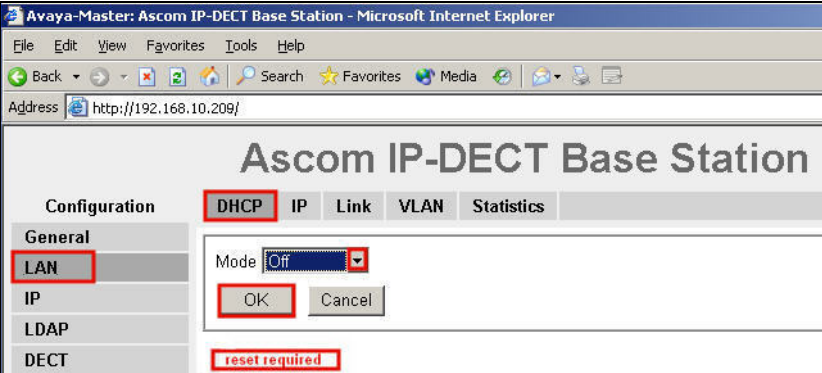
3.1. Configure IP-DECT Base Station

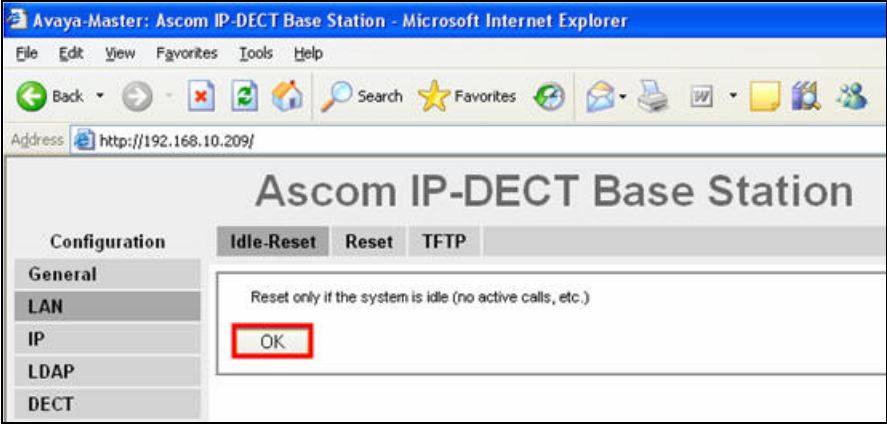
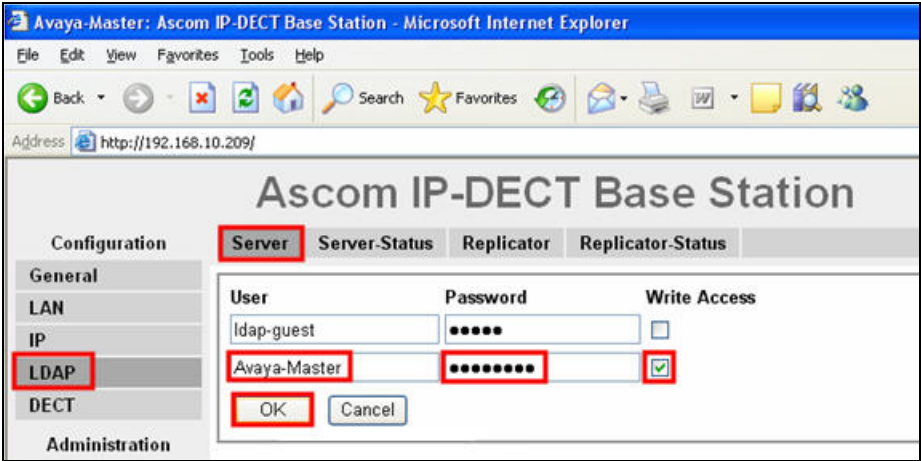
The Ascom wireless IP-DECT Base Stations can be configured in a Master/Standby Master scenario to provide redundancy or to extend the radius of coverage. The following configuration steps detail the configuration process used to configure an Ascom wireless IP-DECT Base Station in Master mode only.

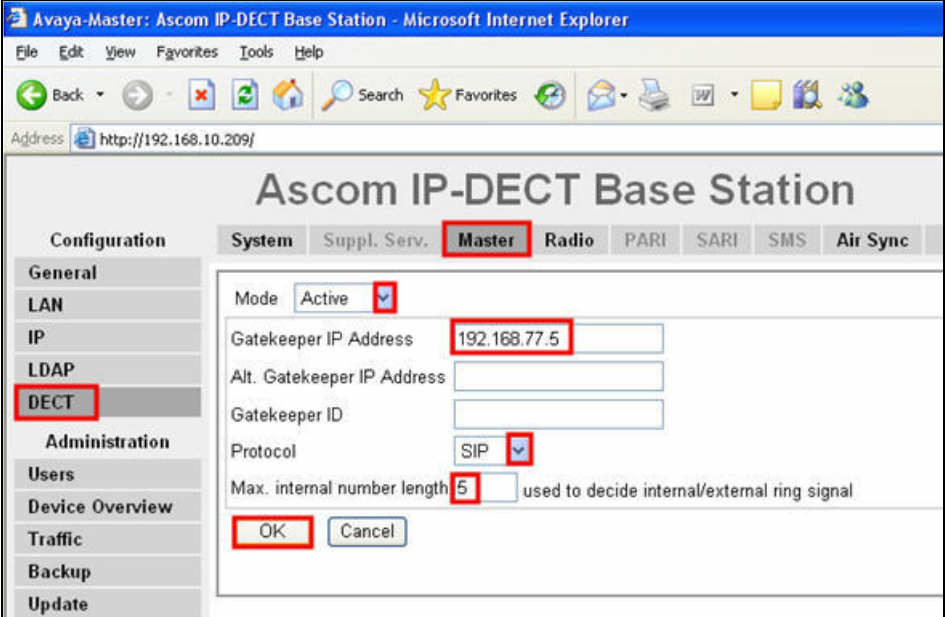
Step	Description
1.	<p>Launch a web browser and place either the IP address or the DNS name of the Ascom wireless IP-DECT Base Station into the URL. The user will be presented with a login screen. Refer to Section 9 [3] for appropriate credentials needed to access the Ascom wireless IP-DECT Base Station. Enter the appropriate login information and then click OK.</p> <div data-bbox="500 1100 1211 1556"></div>

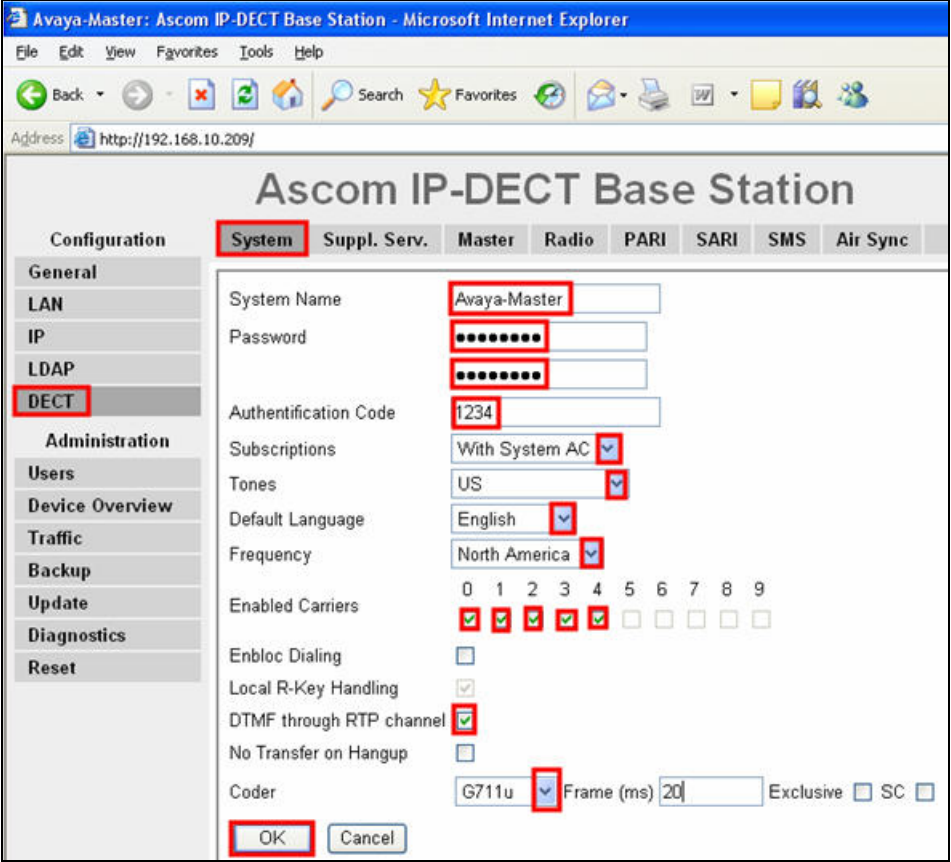
Step	Description
2.	<p>The user is presented with the General Info frame where the system information for the Ascum wireless IP-DECT Base Station is displayed.</p> 

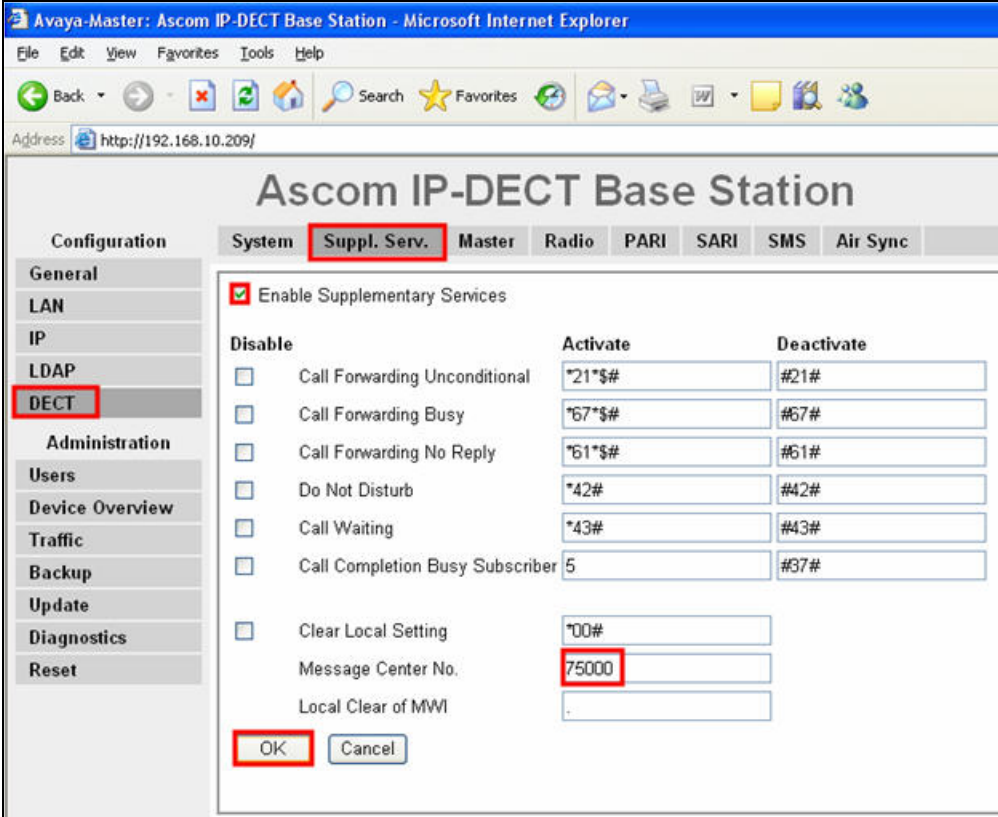
Step	Description
3.	<p>To navigate the web interface on the Ascom wireless IP-DECT Base Station the user will navigate through a series of frames which lead to forms and web pages for configuration or to display information. The user flow is a two-click process where a category and then an option are clicked. Categories are found below Configuration, which is displayed in the top left portion of the frame, and options are found to the right.</p> <p>Navigate to the General Admin frame by clicking General and then clicking Admin. Configure the fields displayed below and then click OK. The Device Name can be any descriptive name that identifies this Ascom wireless IP-DECT Base Station. In the sample network the name “Avaya-Master” was chosen. The User Name and Password fields were populated using the default credentials. The box below Password is to confirm the password and the value entered for the Password field must be entered here.</p> 

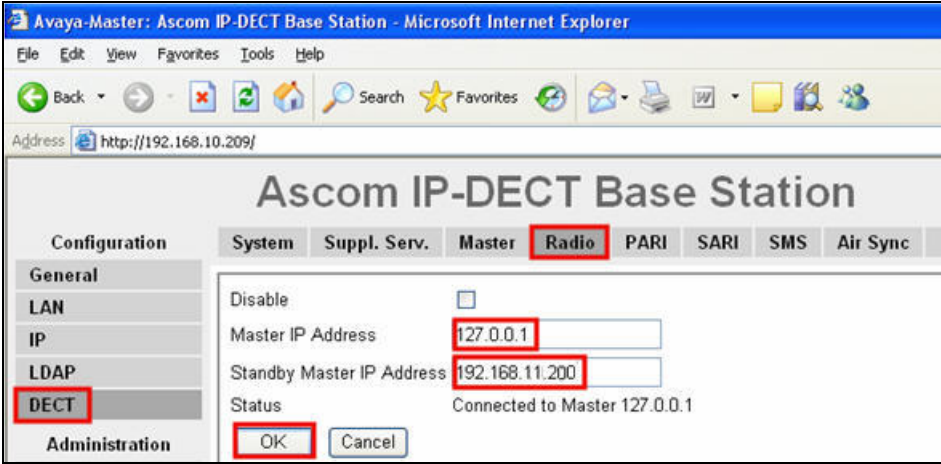
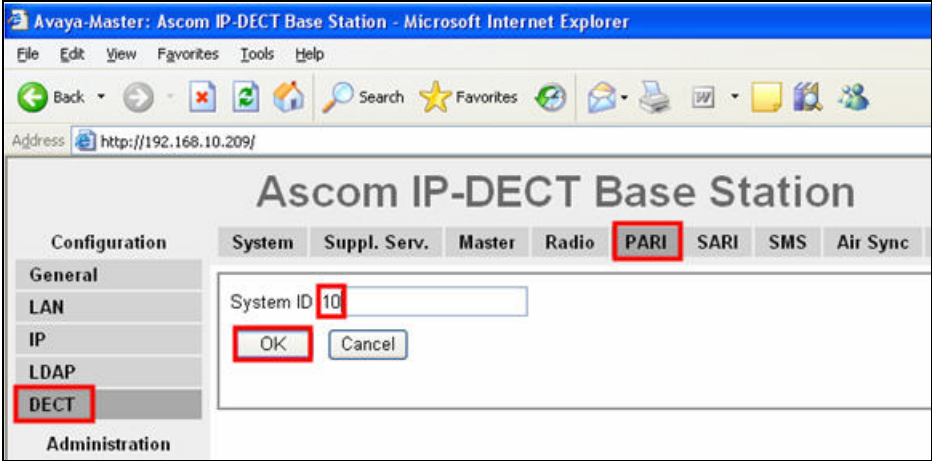
Step	Description
4.	<p>Navigate to the LAN IP frame by first clicking LAN and then clicking IP. Set the static IP Address, Network Mask, and Default Gateway.</p> 
5.	<p>Navigate to the LAN DHCP frame by first clicking LAN and then clicking DHCP. Using the drop-down list, set Mode to “Off” and then click OK. This will present the user with the clickable red text which reads “reset required”. Click reset required.</p> 

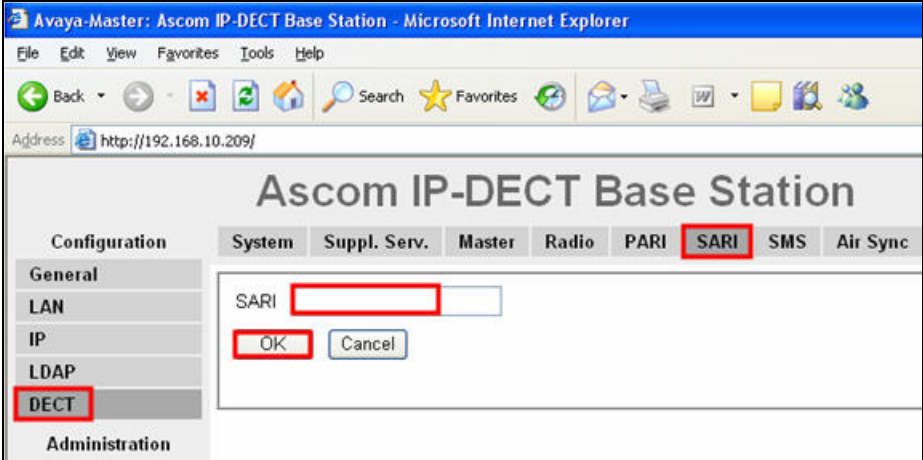
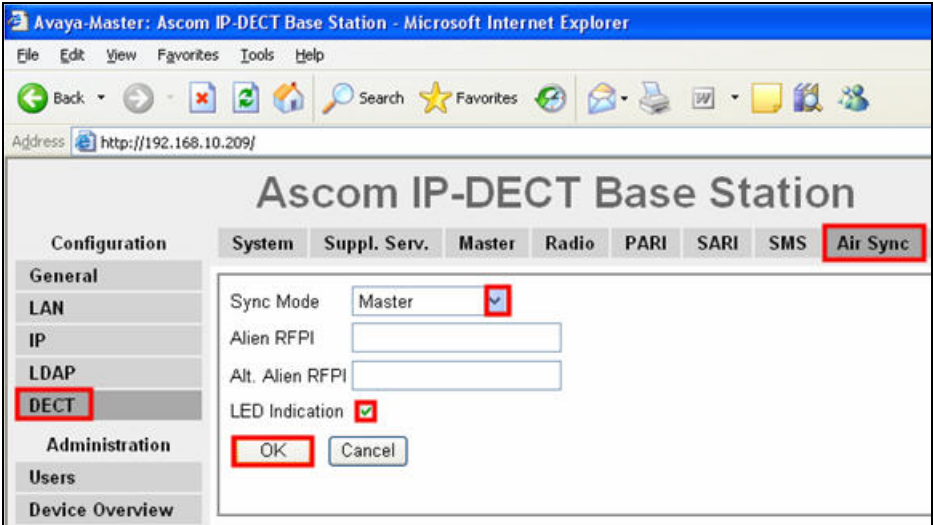
Step	Description
6.	<p>The user is presented with the reset confirmation dialogue. Click OK to initiate the system reset. Many of the other changes made to the system during the configuration process require a reboot. Repeat this process whenever a reset is required.</p> 
7.	<p>After the Ascom wireless IP-DECT Base Station (Avaya-Master) has rebooted, navigate to the LDAP Server frame by clicking LDAP and then clicking Server. The “ldap-guest” account is a default system account. Configure User using the Device Name used in Step 3. Configure the Password field with the Password used in Step 3. Check the Write Access check box for the "Avaya-Master" user account and then click OK.</p> 

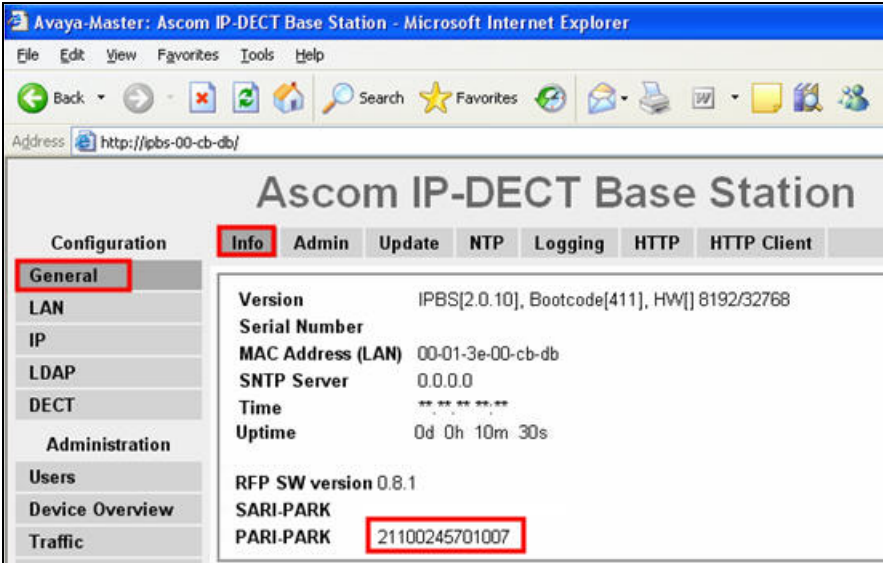
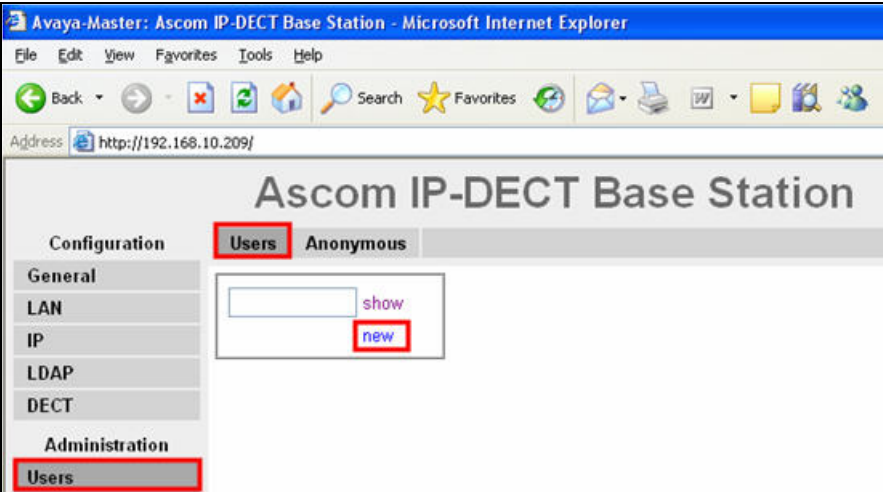
Step	Description
8.	<p>Navigate to the DECT Master frame by clicking DECT and then clicking Master. Configure the fields displayed below and then click OK. Use the drop-down list for Mode and select “Active”. Gatekeeper IP Address was set to the IP address of the Avaya SIP Enablement Services (see Figure 1). Use the drop-down list for Protocol and select “SIP”. In the sample network, five digit extensions were used and Max. internal number length was set to “5”.</p> 

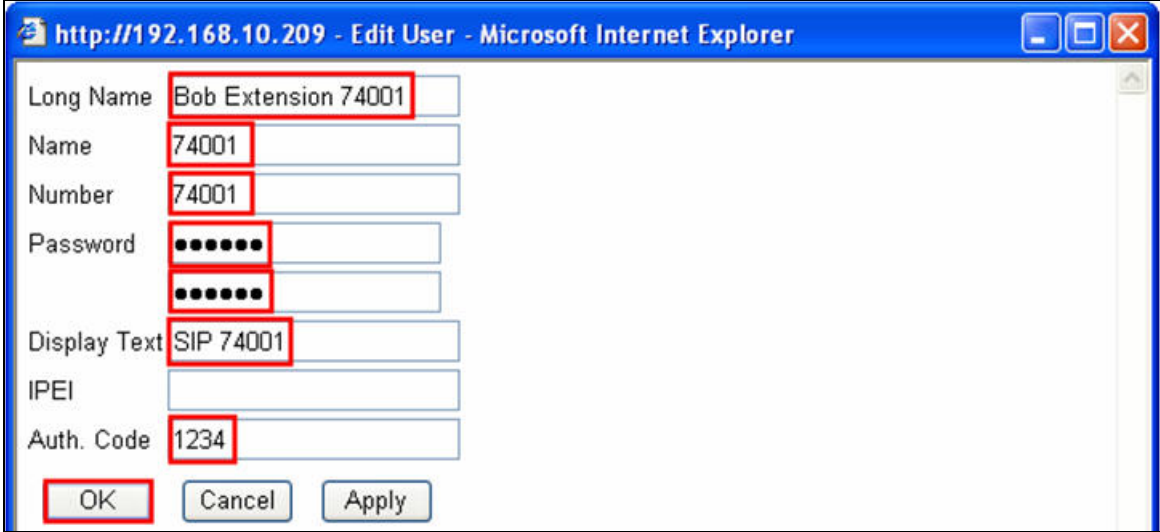
Step	Description
9.	<p>Navigate to the DECT System frame by clicking DECT and then clicking System. Configure the fields displayed below and then click OK. System Name is the Device Name used in Step 3. Password is the “Password” used in Step 3. The box below Password is to confirm the password and the value configured for Password field must be entered here. The Authentication Code is a numerical code that every DECT handset will need to use to subscribe to this system. Using the drop-down list, Subscriptions can be set to “With User AC”, “With System AC”, or “Disable”. In the sample configuration “With System AC” was used. This enables the system to use the Authentication Code when challenging DECT handsets during registration. Use the drop-down list for Tones and select “US”. Use the drop-down list for Default Language and select “English”. Use the drop-down list for Frequency and select “North America”. Check the 0,1,2,3 and 4 check boxes. The Enable Carrier check boxes enable the DECT handsets to use different channels or frequencies when transmitting. Check the DTMF through RTP channel check box. Use the drop-down list for Coder and select “G711u”.</p> 

Step	Description
10.	<p>Navigate to the DECT Suppl. Serv. frame by clicking DECT and then clicking Suppl. Serv.. Check the Enable Supplementary Services check box. Enter the extension used for Avaya Modular Messaging in the Message Center No. field. Click OK.</p> 

Step	Description
11.	<p>Navigate to the DECT Radio frame by clicking DECT and then clicking Radio. Configure the fields displayed below and then click OK. Master IP Address can be either the loopback IP address (127.0.0.1) or the IP address assigned to the Ascom wireless IP-DECT Master Base Station. Standby Master IP Address is the IP address of the Ascom wireless IP-DECT Standby Master Base Station.</p> 
12.	<p>Navigate to the DECT PARI frame by clicking DECT and then clicking PARI. PARI is a user-defined system value and must range from 1-35. Enter any number from 1-35 and then click OK.</p> 

Step	Description
13.	<p>Navigate to the DECT SARI frame by clicking DECT and then clicking SARI. SARI is an Ascom wireless provided activation code which is needed for the system to function. Contact Ascom wireless to obtain a SARI. Enter the SARI value and then click OK.</p> 
14.	<p>Navigate to the DECT Air Sync frame by clicking DECT and then clicking Air Sync. Use the drop-down list for Sync Mode and select “Master”. Check the LED Indication check box and then click OK.</p> 

Step	Description
15.	<p>Navigate to the General Info frame by clicking General and then clicking Info. The PARI-PARK is displayed. This value is needed when programming Ascom wireless DECT handsets. The PARI-PARK is similar to an SSID in an 802.11 wireless environment.</p>  <p>The screenshot shows the 'Ascom IP-DECT Base Station' web interface in Microsoft Internet Explorer. The address bar shows 'http://ipbs-00-cb-db/'. The 'Configuration' menu is open, and 'General' is selected. The 'Info' tab is active, displaying system information: Version (IPBS[2.0.10], Bootcode[411], HW[] 8192/32768), Serial Number, MAC Address (LAN) 00-01-3e-00-cb-db, SNTP Server 0.0.0.0, Time, Uptime (0d 0h 10m 30s), RFP SW version 0.8.1, SARI-PARK, and PARI-PARK (21100245701007). The PARI-PARK value is highlighted with a red box.</p>
16.	<p>Navigate to the Users frame by clicking Users and then clicking Users. Click new to provision a new user account.</p>  <p>The screenshot shows the 'Ascom IP-DECT Base Station' web interface in Microsoft Internet Explorer. The address bar shows 'http://192.168.10.209/'. The 'Configuration' menu is open, and 'Users' is selected. The 'Users' page is displayed, showing a search box with a 'show' button and a 'new' button. The 'new' button is highlighted with a red box.</p>

Step	Description
17.	<p>The user is presented with the Edit User web page. Long Name and Name can be any descriptive name that identifies this user. The Number field is the extension assigned to this user. The Password field is the password used to register with the Avaya SIP Enablement Services. The box below Password is to confirm the password and the value entered for the Password field must be entered here. Display Text is the text string that will be displayed on the LCD screen of the Ascom wireless DECT Handset. Auth. Code is used only if Subscriptions in Step 8 is set to “With User AC”. Once all the user information has been configured, click OK. Repeat this process for each user being added to the system.</p> 

4. Ascom wireless DECT Handset Configuration

Refer to **Section 9** [3], [4], [5] and [6] to obtain information on the procedures for subscribing and registering the Ascom wireless DECT Handsets to the Ascom wireless IP-DECT Base Station.

5. Interoperability Compliance Testing

The compliance testing focused on verifying interoperability of the Ascom wireless IP-DECT SIP solution which is comprised of the Ascom wireless IP-DECT Base Station and Ascom wireless DECT Handsets with Avaya Communication Manager, Avaya SIP Enablement Services and Avaya Modular Messaging. Additional testing verified proper operation with the Avaya 9630 IP Telephone, Avaya 9620 IP Telephone and the Avaya 2420 Digital Telephone. Voicemail using Avaya Modular Messaging with MWI was tested and verified to operate correctly.

Avaya’s formal testing and Declaration of Conformity is provided only on the headsets/handsets that carry the Avaya brand or logo. Avaya may conduct testing of non-Avaya headsets/handsets to determine interoperability with Avaya telephones. However, Avaya does not conduct the

testing of non-Avaya headsets/handsets for: Acoustic Pressure, Safety, Hearing Aid Compliance, EMC regulations, or any other tests to ensure conformity with safety, audio quality, long-term reliability or any regulation requirements. As a result, Avaya makes no representations whether a particular non-Avaya headset will work with Avaya's telephones or with a different generation of the same Avaya telephone.

Since there is no industry standard for handset interfaces, different manufacturers utilize different handset/headset interfaces with their telephones. Therefore, any claim made by a headset vendor that its product is compatible with Avaya telephones does not equate to a guarantee that the headset will provide adequate safety protection or audio quality.

5.1. General Test Approach

The general test approach was to register the Ascom wireless DECT Handsets with Avaya SIP Enablement Services through the Ascom wireless IP-DECT cordless network and that voice mail left on Avaya Modular Messaging could be retrieved and that MWI worked. Calls were made between both wired and wireless telephones and specific calling features were exercised.

5.2. Test Results

The Ascom wireless DECT Handsets passed all test cases. Ascom wireless DECT Handsets were verified to successfully register with Avaya SIP Enablement Services. Two codecs were used for testing: G.711MU and G.729AB. Telephone calls were verified to operate correctly with the media path direct between the telephones (shuffling enabled) and with the media path centralized through Avaya Communication Manager (shuffling disabled). Calls were maintained for durations over one minute without degradation to voice quality. The telephony features verified to operate correctly included transfer (attended and unattended), hold/return from hold, multiple call appearances, caller ID operation, call forwarding (unconditional, on busy/no answer and clear), pickup groups, call pickup, bridged appearances, and verifying Avaya Modular Messaging voicemail and MWI.

6. Verification Steps

6.1. Ascom wireless DECT Handset Registration Verification

The following steps can be used to ascertain the registration state of the Ascom wireless DECT Handsets that the Ascom wireless IP-DECT Base Station is configured to support.

From a web browser open up a connection to the Ascom wireless IP-DECT Master Base Station, refer to **Section 3 Step 1**. Navigate to the **Users** frame by clicking **Users** then clicking **Users** and then clicking **show**. A **Registration** state of "Pending" indicates an Ascom wireless DECT Handset has not registered to the Ascom wireless IP-DECT Base Station and requested that particular extension. A **Registration** state of "Subscribed" indicates that an Ascom wireless DECT Handset has connected to the Ascom wireless IP-DECT Base Station and requested the use of that particular extension. A **Registration** state that displays the IP Address of the Avaya SIP Enablement Services indicates the extension has successfully registered to both the Ascom wireless IP-DECT Base Station and Avaya SIP Enablement Services.

Avaya-Master: Ascom IP-DECT Base Station - Microsoft Internet Explorer

Address: http://192.168.10.209/

Ascom IP-DECT Base Station

Configuration: **Users** Anonymous

General

LAN

IP

LDAP

DECT

Administration

Users

Long Name	Name	No	Display	IPEI	AC	Registration
Bob 74001	74001	74001	SIP 74001	002020391142	1234	192.168.77.5
Jim 74002	74002	74002	SIP 74002	002020413082	1234	192.168.77.5
OfficeM	74004	74004	OfficeM		1234	Pending
OfficeT	74003	74003	OfficeT	005930783661	1234	Subscribed

Users: 4, Registrations: 2

Avaya-Master: Ascom IP-DECT Base Station - Microsoft Internet Explorer

Address: http://192.168.10.209/

Ascom IP-DECT Base Station

Configuration: **Users** Anonymous

General

LAN

IP

LDAP

DECT

Administration

Users

Long Name	Name	No	Display	IPEI	AC	Registration
Bob 74001	74001	74001	SIP 74001	002020391142	1234	192.168.77.5
Jim 74002	74002	74002	SIP 74002	002020413082	1234	192.168.77.5
OfficeM	74004	74004	OfficeM	030020412082	1234	192.168.77.5
OfficeT	74003	74003	OfficeT	005930783661	1234	192.168.77.5

Users: 4, Registrations: 4

6.2. Ascom wireless DECT Handset Function Verification

The following steps can be used to verify proper operation of the Ascom wireless DECT Handsets.

- Place calls from the Ascom wireless DECT Handsets and verify two-way audio.
- Place a call to the Ascom wireless DECT Handsets, allow the call to be directed to voicemail, leave a voicemail message and verify the MWI message is received.
- Using each Ascom wireless DECT Handset that received a voicemail, connect to the voicemail system to retrieve the voicemail and verify the MWI clears.
- Place calls to the Ascom wireless DECT Handsets and exercise calling features such as transfer and hold.

7. Support

Technical support for the Ascom wireless IP-DECT Base Station and Handsets can be obtained through the following:

- **Phone:** 1-877-71ASCOM or 1-877-712-7266
- **Email:** techsupport@ascomwireless.com

8. Conclusion

These Application Notes demonstrate how to build a sample SIP VoIP-enabled wireless network using the Ascom wireless IP-DECT Base Station with the Ascom wireless DECT Handsets. These Application Notes also demonstrate how to provide interoperability between Avaya Communication Manager, Avaya SIP Enablement Services and Avaya Modular Messaging with the Ascom wireless IP-DECT Base station and Handsets.

9. Additional References

The documents referenced below were used for additional support and configuration information. The Avaya documentation was obtained from <http://support.avaya.com>. The Ascom wireless documentation was obtained from <http://www.Ascomwireless.com> (access to Ascom wireless documentation may require a support account).

- [1] *Administrator Guide for Avaya Communication Manager*, February 2007, Issue 3.1, Document Number 03-300509
- [2] *Installing and Administering SIP Enablement Services*, March 2007, Issue 2.1, Document Number 03-600768
- [3] *Installation and Operation Manual IP-DECT Base Station*, January 2007 Ver. C, Document Number TD 92372GB
- [4] *User Manual 9d24 MkII Cordless Handset USA*, February 2007 Ver. C, Document Number TD 92411GB
- [5] *User Manual OfficeM Cordless Telephone*, May 2006 Ver. C, Document Number TD 92288GB
- [6] *User Manual Cordless Telephone OfficeT*, May 2006 Ver. C, Document Number TD 92282GB
- [7] *Messaging Application Server (MAS) Administration Guide Release 3.1 with the Avaya*, February 2007

©2007 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Developer*Connection* Program at devconnect@avaya.com.