



Avaya Solution & Interoperability Test Lab

Application Note for Configuring the Ascom Wireless IP-DECT SIP Solution with an Avaya Aura™ Telephony Infrastructure in a Converged Voice over IP and Data Network - Issue 1.0

Abstract

These Application Notes describe a solution for supporting wireless interoperability between the Ascom wireless IP-DECT SIP solution with an Avaya Aura™ Telephony Infrastructure consisting of Avaya Aura™ Communication Manager, Avaya Aura™ SIP Enablement Services, Avaya Modular Messaging and Avaya Communication Manager Messaging in a converged Voice over IP and Data Network. Emphasis of the testing was placed on verifying good voice quality of calls with Ascom wireless IP-DECT SIP handsets registered to the Avaya telephony infrastructure.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration process necessary to provide interoperability between the Ascom wireless IP Digital Enhanced Cordless Telecommunications (IP-DECT) Solution with an Avaya Aura™ Telephony Infrastructure consisting of Avaya Aura™ Communication Manager, Avaya Aura™ SIP Enablement Services, Avaya Modular Messaging and Avaya Communication Manager Messaging.

1.1. Interoperability Compliance Testing

The compliance testing focused on verifying interoperability of the Ascom wireless IP-DECT SIP Solution comprised of the Ascom wireless IP-DECT Base Station and Ascom wireless DECT Handsets with an Avaya Aura™ Telephony Infrastructure consisting of Avaya Aura™ Communication Manager, Avaya Aura™ SIP Enablement Services, Avaya Modular Messaging and Avaya Communication Manager Messaging in a converged Voice over IP and Data Network. Additional testing verified proper operation with the Avaya 9630 IP Telephone (SIP), Avaya 9620 IP Telephone (H.323) and the Avaya 2420 Digital Telephone. Voicemail and MWI using Avaya Modular Messaging and Avaya Communication Manager Messaging 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, scalability 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.

1.2. 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 Aura™ SIP Enablement Services and the Ascom IP-DECT wireless handsets.

After the Ascom IP-DECT wireless handsets register with the Ascom IP-DECT Base Station, the Base Station registers the handsets to Avaya Aura™ SIP Enablement Services.

1.3. Support

Technical support for the Ascom Wireless IP-DECT Handset can be obtained through local Ascom suppliers.

Ascom global technical support:

Phone: +46 31 559450

Email: support@ascom.se

2. Reference Configuration

The network diagram shown in **Figure 1** illustrates the testing environment used for compliance testing. The network consists of an Avaya Aura™ Communication Manager running on an Avaya S8300 Server with an Avaya G450 Media Gateway, and Avaya S8500 server running Avaya Aura™ SIP Enablement Services, one Avaya Modular Messaging Application Server, one Avaya Modular Messaging Storage Server, one Avaya 9630 IP Telephone (SIP), one Avaya 9620 IP Telephone (H.323), one Avaya 2420 Digital Telephone, two Ascom Wireless IP-DECT Base Stations, one Ascom d62 Wireless IP-DECT Handset and one Ascom d41 Wireless IP-DECT Handset. One computer is present in the network providing network services such as DHCP, TFTP and HTTP.

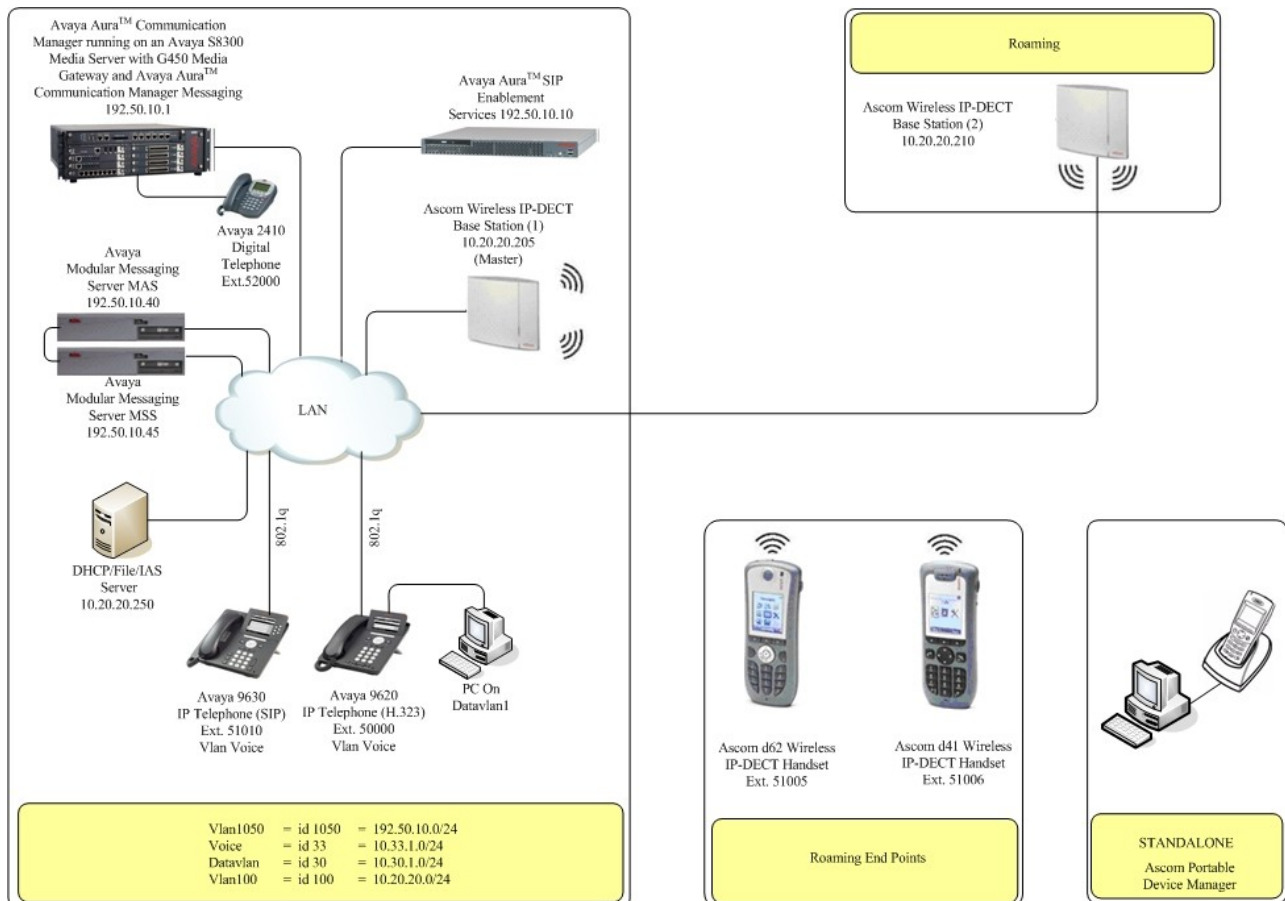


Figure 1: Sample Network Diagram

3. Equipment and Software Validated

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

Equipment	Software/Firmware
<i>Avaya PBX Products</i>	
Avaya S8300 Server running Avaya Aura™ Communication Manager	Avaya Aura™ Communication Manager 5.2
Avaya G450 Media Gateway (Corporate Site) MGP MM712 DCP Media Module	28.22.0 HW9
<i>Avaya Aura™ SIP Enablement Services</i>	
Avaya Aura™ SIP Enablement Services	5.2 SP2
<i>Avaya Messaging (Voice Mail) Products</i>	
Avaya Modular Messaging - Messaging Application Server (MAS)	5.0
Avaya Modular Messaging - Message Storage Server (MSS)	5.0
Avaya Communication Manager Messaging (CMM)	5.2.1-13.0
<i>Avaya Telephony Sets</i>	
Avaya 9600 Series IP Telephones	Avaya one-X Deskphone Edition 3.0.1
Avaya 9600 Series IP Telephones	Avaya one-X Deskphone SIP 2.4
Avaya 2410 Digital Telephone	5.0
<i>Ascom Products</i>	
Ascom Wireless IP-DECT Base Station	IPBS(3.2.2)
Ascom d62 Wireless IP-DECT Handset	2.8.22
Ascom d41 Wireless IP-DECT Handset	2.8.22
Ascom Device Manger (WinPDM)	3.3.5
<i>MS Products</i>	
DHCP / File / IAS server	Microsoft Windows 2003 Server

4. Configure Avaya Aura™ Telephony Infrastructure

This section describes the steps required for configuring Avaya Aura™ Telephony Infrastructure to support the sample network shown in **Figure 1**. The assumption is that the appropriate license and authentication files have been installed on the servers and that login and password credentials are available. It is also assumed that the standard configurations on Avaya Aura™ Communication Manager and Avaya Aura™ SIP Enabled Services have been executed to support telephony using various types of Avaya phone sets. Refer to [1], [2] and [3] for more information.

Each Ascom Wireless IP-DECT Handset configured in the sample network in **Figure 1** was administered as OPS stations (Off-PBX Stations) on Avaya Aura™ Communication Manager. For information on how to administer these types of stations refer to [1], [2], and [3].

Step	Description
1.	<p>To enable the features used for testing (Call Park, Call Park Answerback, Call Forwarding and Call Pickup) administer the configuration for Feature-Access-Codes (FAC) on Communication Manager. From the SAT (System Administration Terminal) interface on Communication Manager, use the “change feature-access-codes” command to configure the following parameters on Page 1 and Submit the changes.</p> <pre data-bbox="277 1018 1502 1766"> change feature-access-codes Page 1 of 9 FEATURE ACCESS CODE (FAC) Abbreviated Dialing List1 Access Code: *600 Abbreviated Dialing List2 Access Code: *601 Abbreviated Dialing List3 Access Code: *602 Abbreviated Dial - Prgm Group List Access Code: Announcement Access Code: *604 Answer Back Access Code: *650 Attendant Access Code: Auto Alternate Routing (AAR) Access Code: 3 Auto Route Selection (ARS) - Access Code 1: 9 Access Code 2: Automatic Callback Activation: *605 Deactivation: *606 Call Forwarding Activation Busy/DA: *607 All: *608 Deactivation: *609 Call Forwarding Enhanced Status: Act: Deactivation: Call Park Access Code: *652 Call Pickup Access Code: #6 CAS Remote Hold/Answer Hold-Unhold Access Code: CDR Account Code Access Code: Change COR Access Code: Change Coverage Access Code: Conditional Call Extend Activation: Deactivation: Contact Closure Open Code: Close Code: ESC-x=Cancel Esc-e=Submit Esc-p=Prev Pg Esc-n=Next Pg Esc-h=Help </pre>

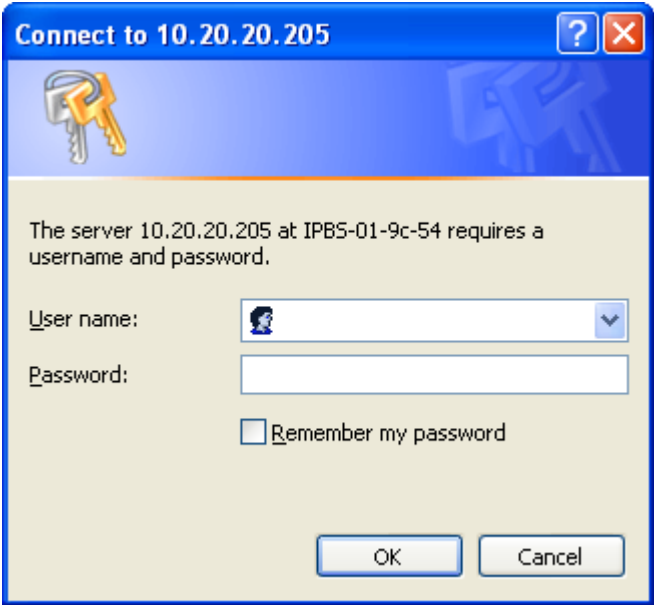
5. Configure Ascom wireless IP-DECT SIP Solution

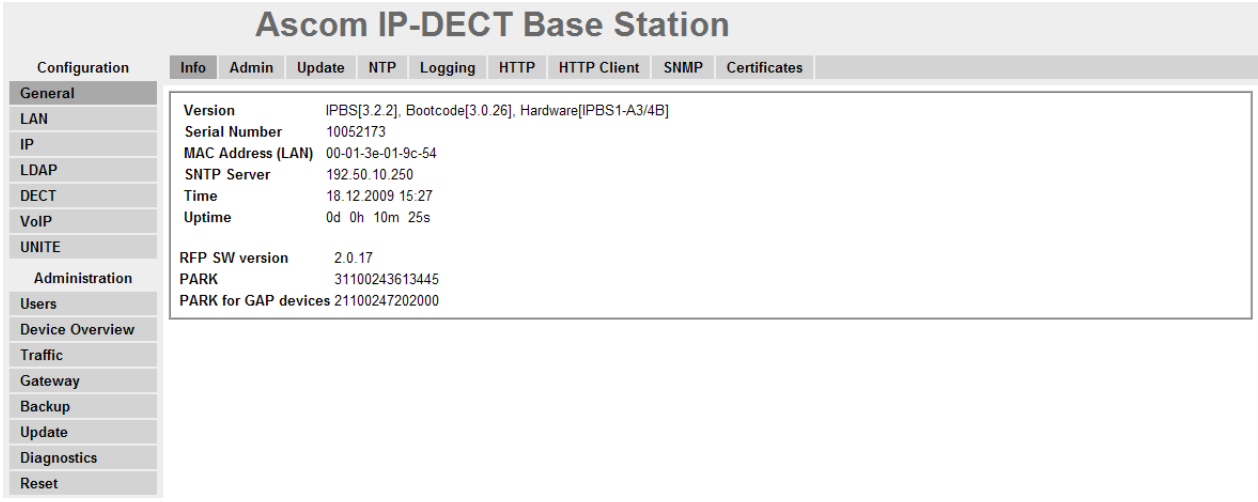
The following steps detail the initial configuration for the Ascom Wireless IP-DECT SIP Solution. Log onto the Ascom wireless IP-DECT Base Station via a web browser using the following URL format: <http://IPBS-XX-XX-XX>, where XX-XX-XX are the last 3 bytes of the MAC address of the Ascom wireless IP-DECT 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 Base Station IP address assigned by DHCP server.

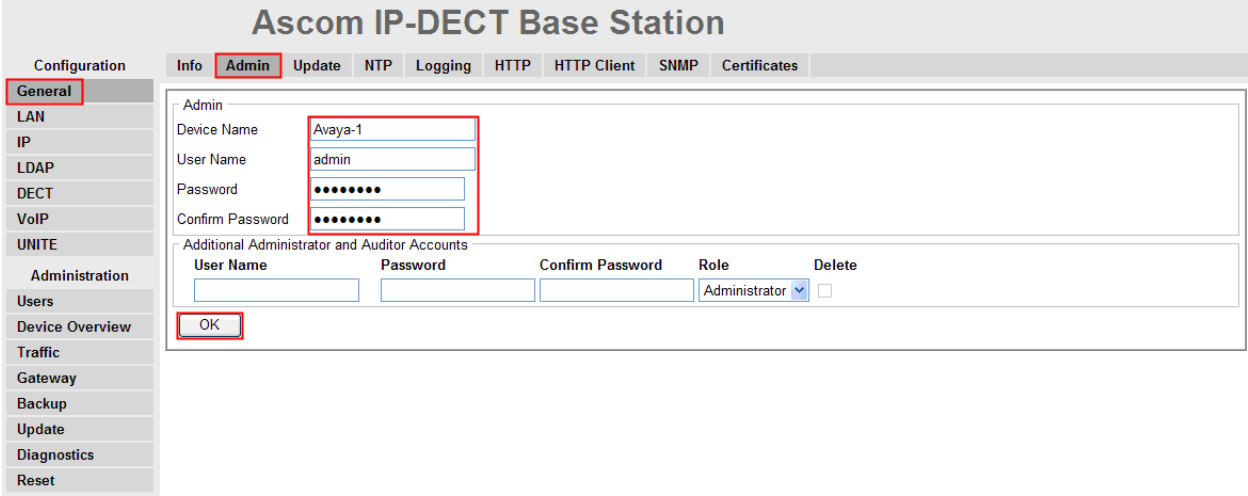
5.1. Configure IP-DECT Base Station

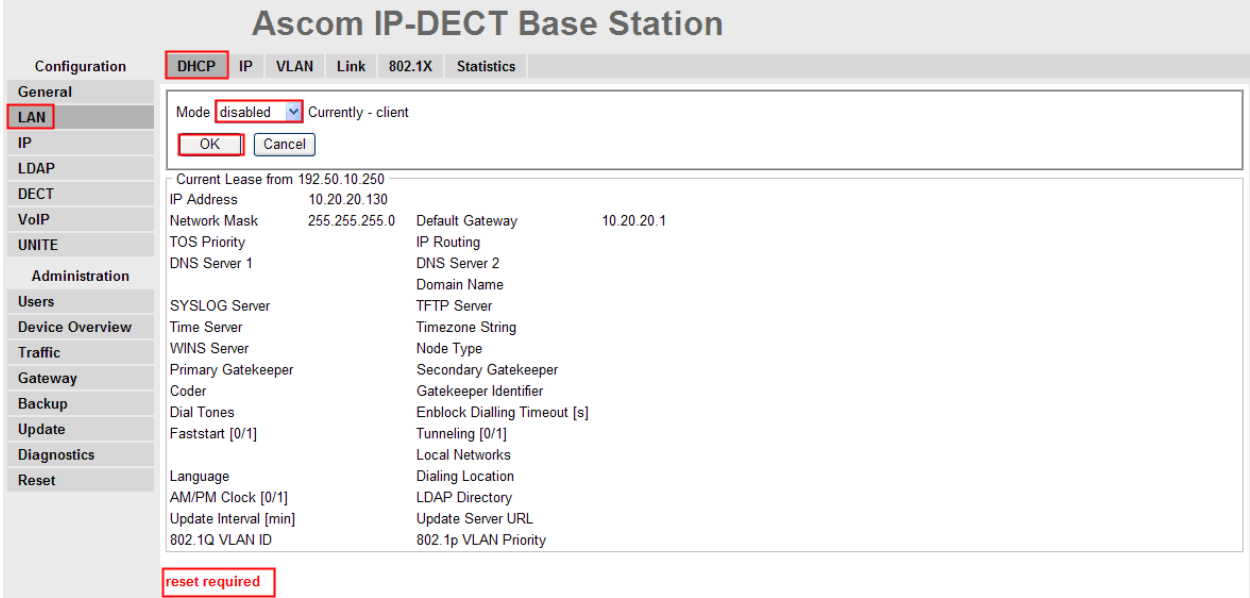
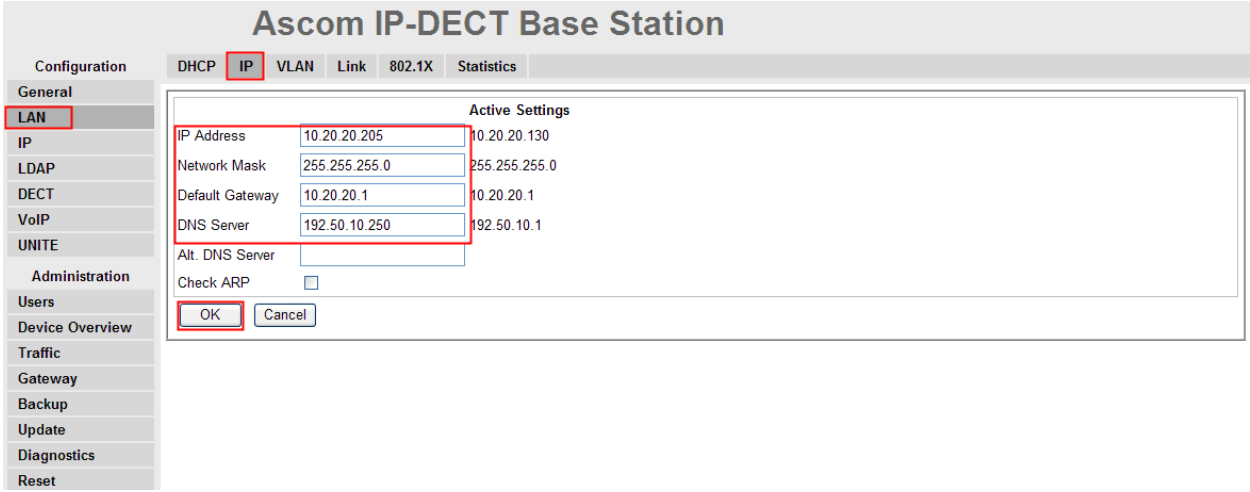
The Ascom wireless IP-DECT Base Stations can be configured in a Master/Standby Master scenario to provide redundancy or to extend the radius of coverage (roaming). The following configuration steps detail the configuration process used to configure an Ascom wireless IP-DECT Base Station in Master mode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

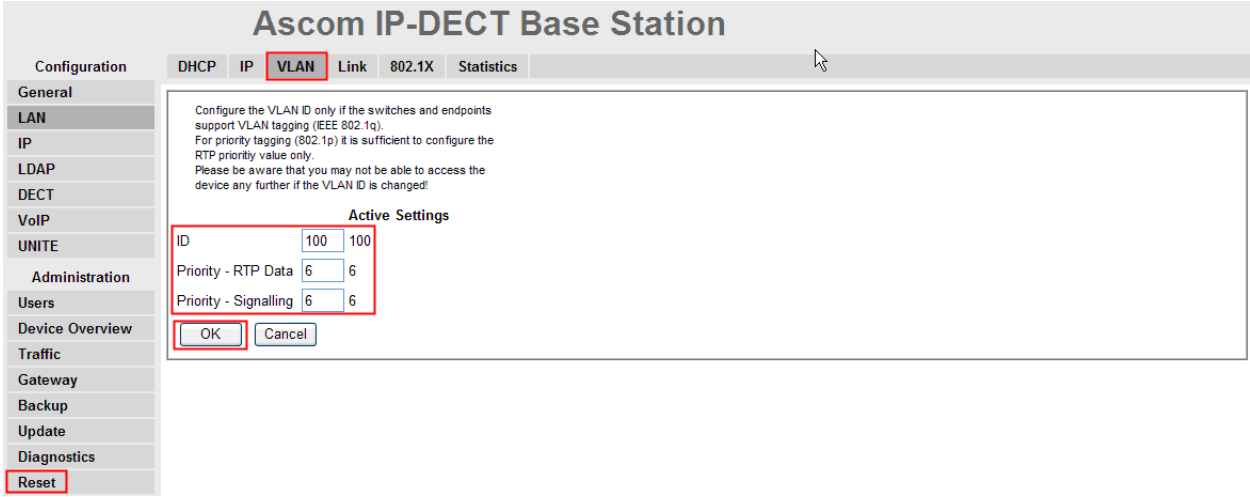
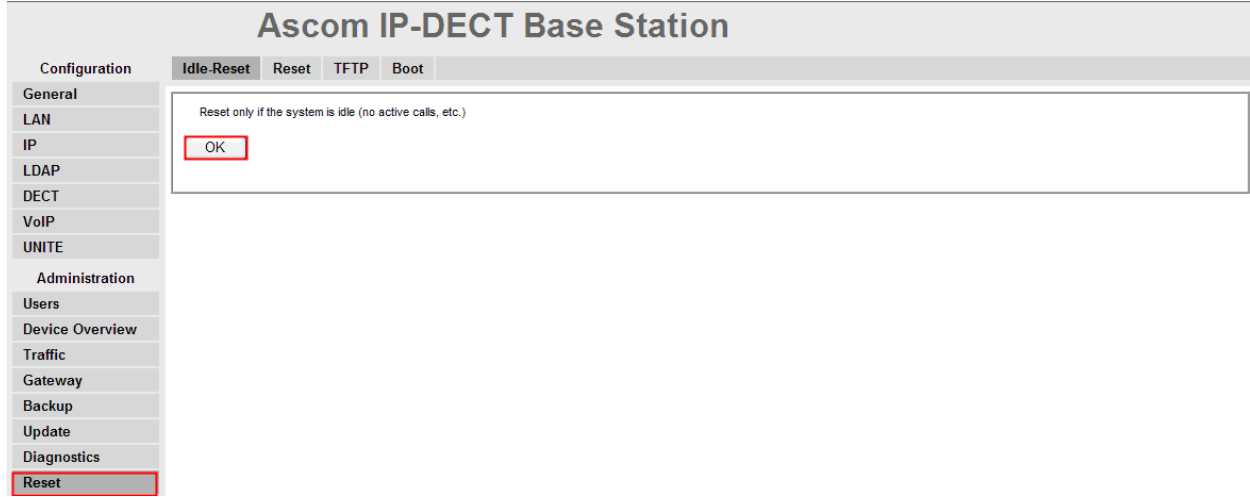
Roaming between multiple Ascom Wireless IP-DECT Base Stations as shown in Figure 1 was tested but the configuration setup will not be shown in this document. Refer to [7] for information on how to configure roaming.

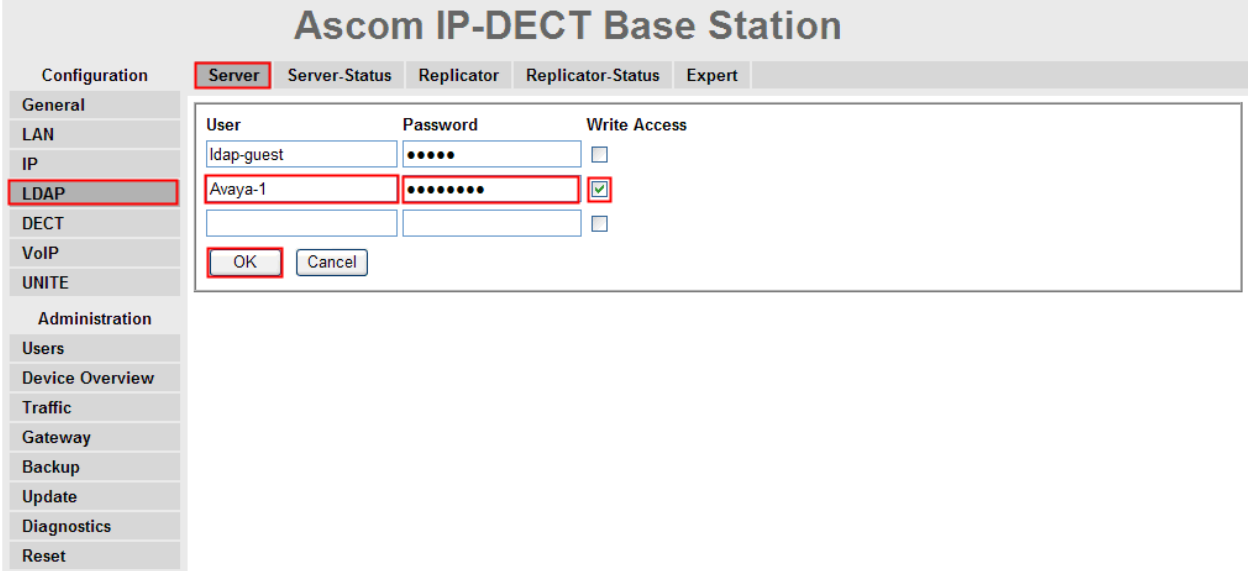
Step	Description
1.	<p>Launch a web browser and enter either the IP address, (obtained from the DHCP server) or http://IPBS-XX-XX-XX as shown in Section 5 into the URL. The user will be presented with a login screen. Refer to [7] for appropriate credentials needed to access the Ascom wireless IP-DECT Base Station. Enter the appropriate login information and then click OK.</p> <div data-bbox="578 1171 1227 1772" data-label="Image"></div>

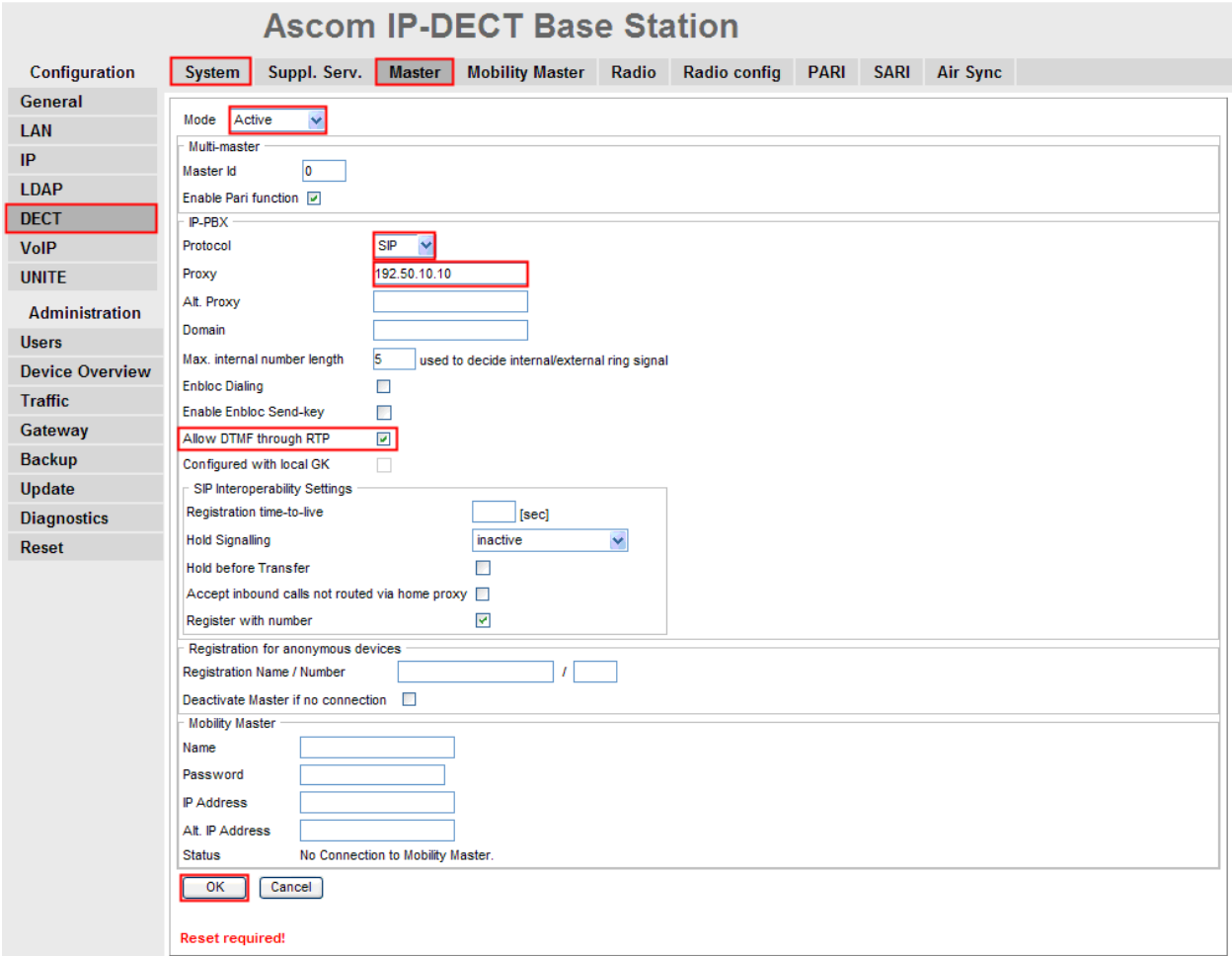
Step	Description																																																																																																																																																																										
2.	<p>The user is presented with the General Info frame where the system information for the Ascom wireless IP-DECT Base Station is displayed.</p>  <p>Ascom IP-DECT Base Station</p> <table border="1"> <thead> <tr> <th>Configuration</th> <th>Info</th> <th>Admin</th> <th>Update</th> <th>NTP</th> <th>Logging</th> <th>HTTP</th> <th>HTTP Client</th> <th>SNMP</th> <th>Certificates</th> </tr> </thead> <tbody> <tr> <td>General</td> <td>Version</td> <td colspan="8">IPBS[3.2.2], Bootcode[3.0.26], Hardware[IPBS1-A3/4B]</td> </tr> <tr> <td>LAN</td> <td>Serial Number</td> <td colspan="8">10052173</td> </tr> <tr> <td>IP</td> <td>MAC Address (LAN)</td> <td colspan="8">00-01-3e-01-9c-54</td> </tr> <tr> <td>LDAP</td> <td>SNTP Server</td> <td colspan="8">192.50.10.250</td> </tr> <tr> <td>DECT</td> <td>Time</td> <td colspan="8">18.12.2009 15:27</td> </tr> <tr> <td>VoIP</td> <td>Uptime</td> <td colspan="8">0d 0h 10m 25s</td> </tr> <tr> <td>UNITE</td> <td>RFP SW version</td> <td colspan="8">2.0.17</td> </tr> <tr> <td>Administration</td> <td>PARK</td> <td colspan="8">31100243613445</td> </tr> <tr> <td>Users</td> <td>PARK for GAP devices</td> <td colspan="8">21100247202000</td> </tr> <tr> <td>Device Overview</td> <td></td> <td colspan="8"></td> </tr> <tr> <td>Traffic</td> <td></td> <td colspan="8"></td> </tr> <tr> <td>Gateway</td> <td></td> <td colspan="8"></td> </tr> <tr> <td>Backup</td> <td></td> <td colspan="8"></td> </tr> <tr> <td>Update</td> <td></td> <td colspan="8"></td> </tr> <tr> <td>Diagnostics</td> <td></td> <td colspan="8"></td> </tr> <tr> <td>Reset</td> <td></td> <td colspan="8"></td> </tr> </tbody> </table>	Configuration	Info	Admin	Update	NTP	Logging	HTTP	HTTP Client	SNMP	Certificates	General	Version	IPBS[3.2.2], Bootcode[3.0.26], Hardware[IPBS1-A3/4B]								LAN	Serial Number	10052173								IP	MAC Address (LAN)	00-01-3e-01-9c-54								LDAP	SNTP Server	192.50.10.250								DECT	Time	18.12.2009 15:27								VoIP	Uptime	0d 0h 10m 25s								UNITE	RFP SW version	2.0.17								Administration	PARK	31100243613445								Users	PARK for GAP devices	21100247202000								Device Overview										Traffic										Gateway										Backup										Update										Diagnostics										Reset									
Configuration	Info	Admin	Update	NTP	Logging	HTTP	HTTP Client	SNMP	Certificates																																																																																																																																																																		
General	Version	IPBS[3.2.2], Bootcode[3.0.26], Hardware[IPBS1-A3/4B]																																																																																																																																																																									
LAN	Serial Number	10052173																																																																																																																																																																									
IP	MAC Address (LAN)	00-01-3e-01-9c-54																																																																																																																																																																									
LDAP	SNTP Server	192.50.10.250																																																																																																																																																																									
DECT	Time	18.12.2009 15:27																																																																																																																																																																									
VoIP	Uptime	0d 0h 10m 25s																																																																																																																																																																									
UNITE	RFP SW version	2.0.17																																																																																																																																																																									
Administration	PARK	31100243613445																																																																																																																																																																									
Users	PARK for GAP devices	21100247202000																																																																																																																																																																									
Device Overview																																																																																																																																																																											
Traffic																																																																																																																																																																											
Gateway																																																																																																																																																																											
Backup																																																																																																																																																																											
Update																																																																																																																																																																											
Diagnostics																																																																																																																																																																											
Reset																																																																																																																																																																											

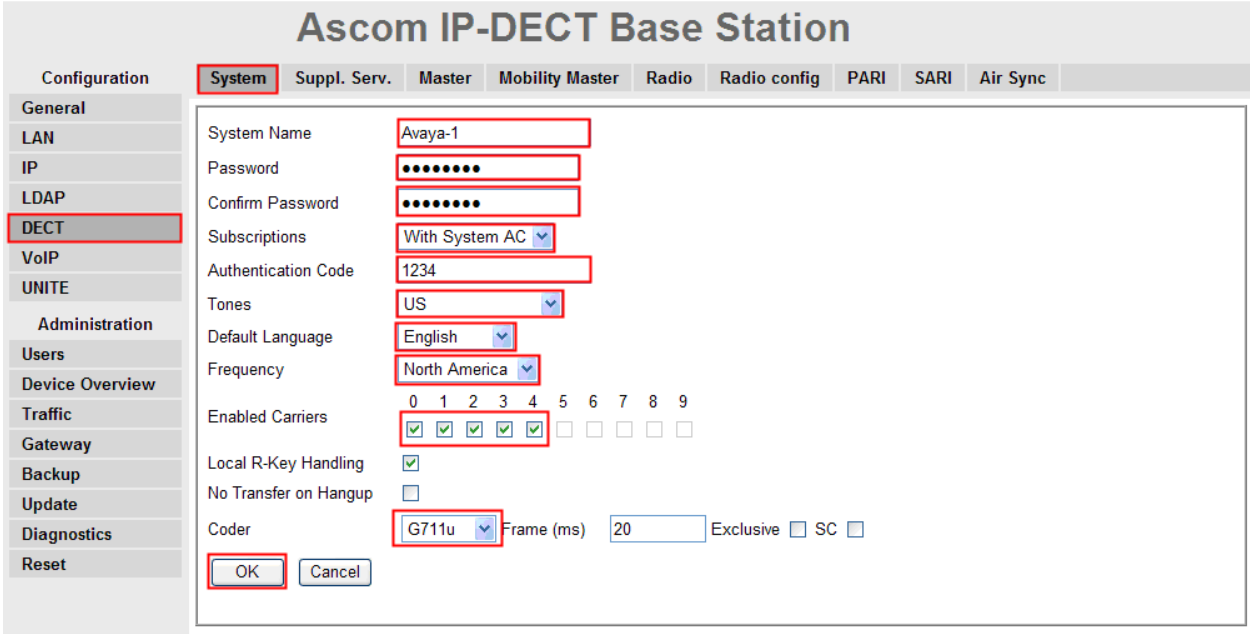
Step	Description
3.	<p>The web interface on the Ascom wireless IP-DECT Base Station consists of a series of frames selected by a two-click process, where a category and then an option are clicked. Categories are found below Configuration, which is displayed in the top left portion of the frame, and options 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-1” 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. Click OK to continue.</p> 

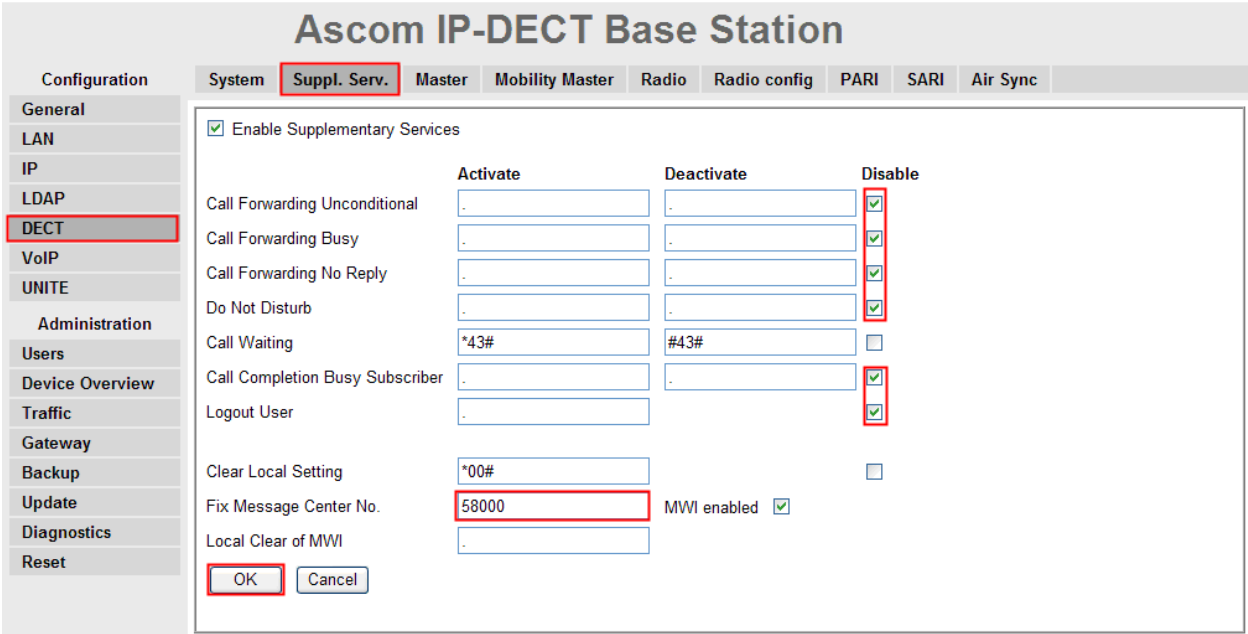
Step	Description
4.	<p>Navigate to the LAN DHCP frame by first clicking LAN and then clicking DHCP. Using the drop-down list, set Mode to “disabled” and then click OK. This will present the user with the clickable red text which reads “reset required”. Click IP tab to continue to the LAN IP frame.</p>  <p>The screenshot shows the 'Ascom IP-DECT Base Station' configuration interface. The 'DHCP' tab is selected. The 'Mode' is set to 'disabled'. A red box highlights the 'reset required' message at the bottom of the configuration area.</p>
5.	<p>Set the static IP Address, Network Mask, Default Gateway and DNS Server, and click OK. Click VLAN to continue.</p>  <p>The screenshot shows the 'Ascom IP-DECT Base Station' configuration interface. The 'IP' tab is selected. The 'Active Settings' section shows the following values: IP Address: 10.20.20.205, Network Mask: 255.255.255.0, Default Gateway: 10.20.20.1, and DNS Server: 192.50.10.250. Red boxes highlight these fields.</p>


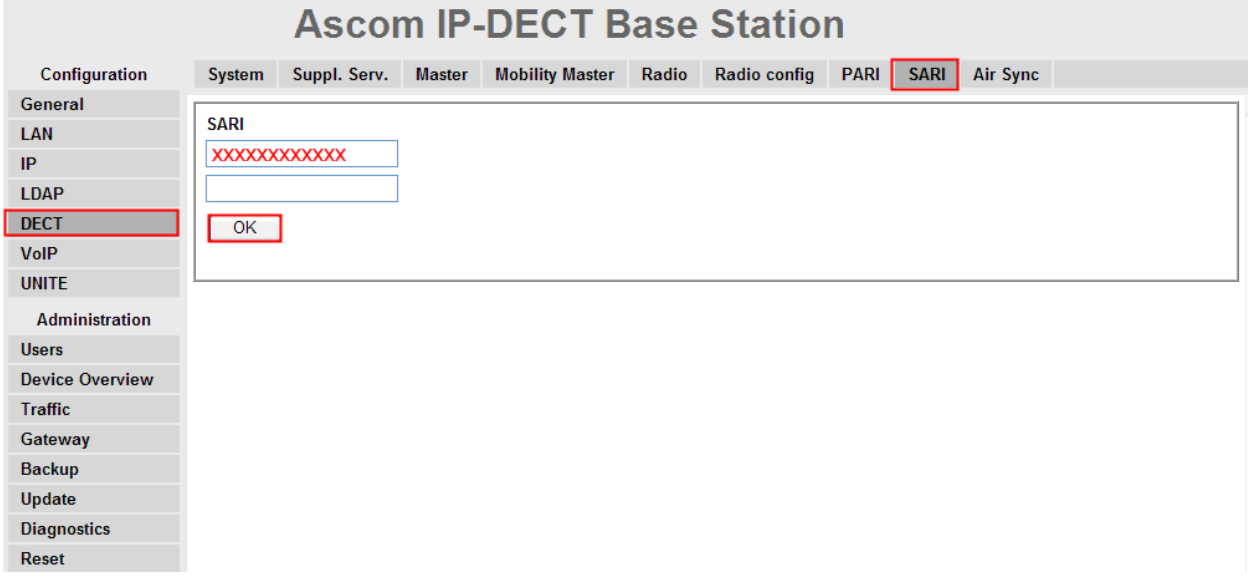
Step	Description
6.	<p>Set the ID, Priority – RTP Data and Priority – Signalling, and click OK. Click Reset to continue.</p> 
7.	<p>Click OK to initiate the system reset. Many of the other changes made to the system during the configuration process require a reboot. Repeat this process whenever a reset is required.</p> 

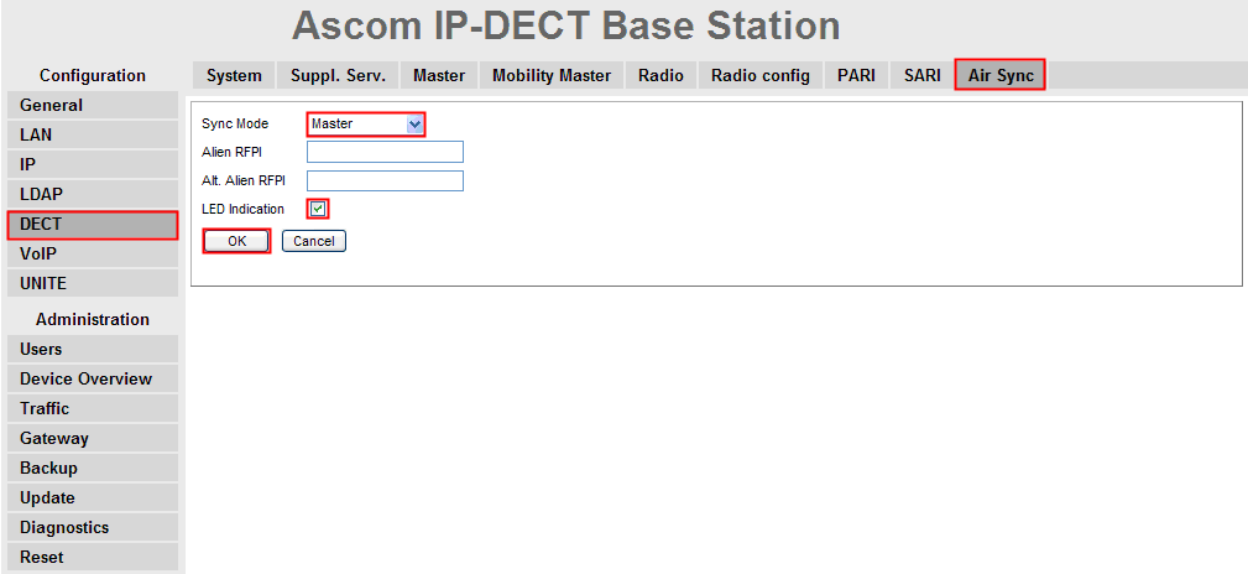
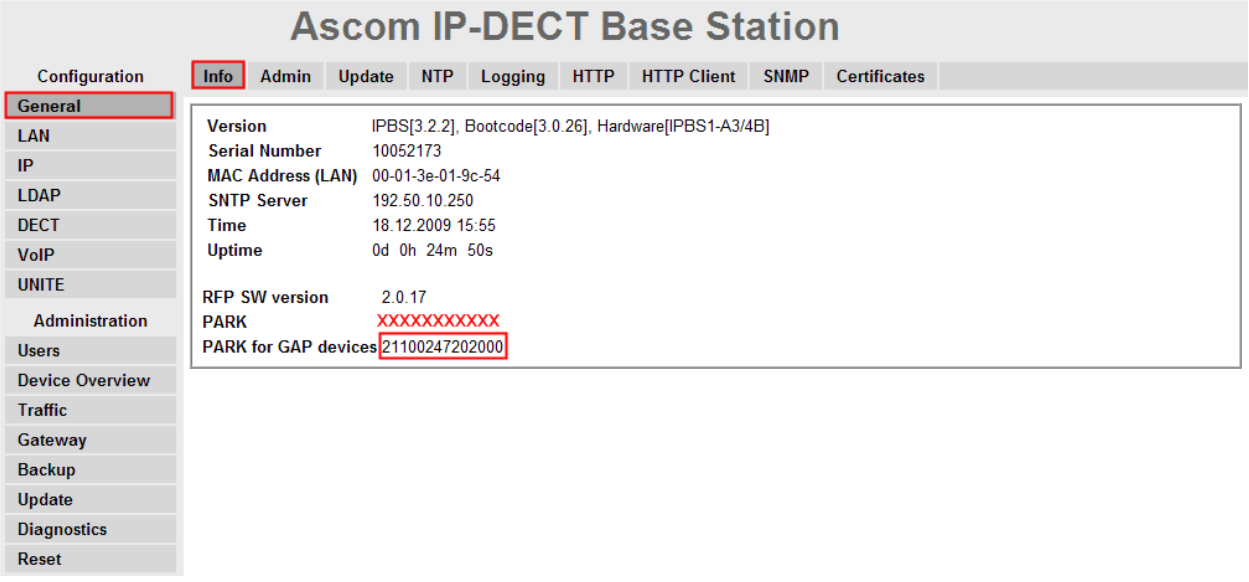
Step	Description
8.	<p>After the Ascom wireless IP-DECT Base Station (Avaya-1) has rebooted, navigate to the LDAP Server frame by clicking LDAP and then clicking Server. The “ldap-guest” account is a default system account. Configure User using the Device Name used in Step 3. Configure the Password field with the Password used in Step 3. Check the Write Access check box for the "Avaya-1" user account and then click OK to continue.</p>  <p>The screenshot shows the 'Ascom IP-DECT Base Station' configuration page. The 'LDAP' menu item is selected in the left sidebar. The 'Server' tab is active, showing a table with columns 'User', 'Password', and 'Write Access'. The 'Avaya-1' user is highlighted with a red box, and its 'Write Access' checkbox is checked. The 'OK' button is also highlighted with a red box.</p>

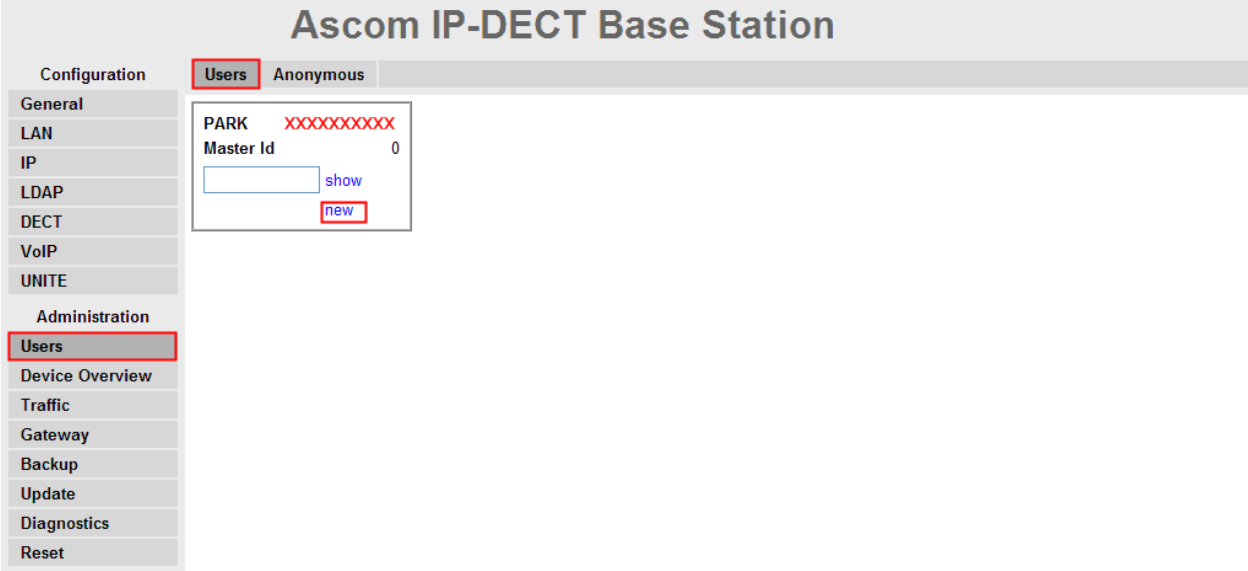
Step	Description
9.	<p>Navigate to the DECT Master frame by clicking DECT and then clicking Master. Configure the fields displayed below and then click OK. Use the drop-down list for Mode and select “Active”. Under IP-PBX, use the drop-down list for Protocol and select “SIP”. Set Proxy to the IP address of the SIP Enablement Services (see Figure 1). Check the Allow DTMF through RTP check box. Click OK. Click System to continue.</p>  <p>The screenshot shows the 'Ascom IP-DECT Base Station' configuration page. The 'System' tab is selected. The 'DECT' menu item is highlighted in the left sidebar, and the 'Master' sub-tab is active. The 'Mode' dropdown is set to 'Active'. Under 'IP-PBX', the 'Protocol' dropdown is set to 'SIP' and the 'Proxy' field contains '192.50.10.10'. The 'Allow DTMF through RTP' checkbox is checked. The 'OK' button is highlighted.</p>

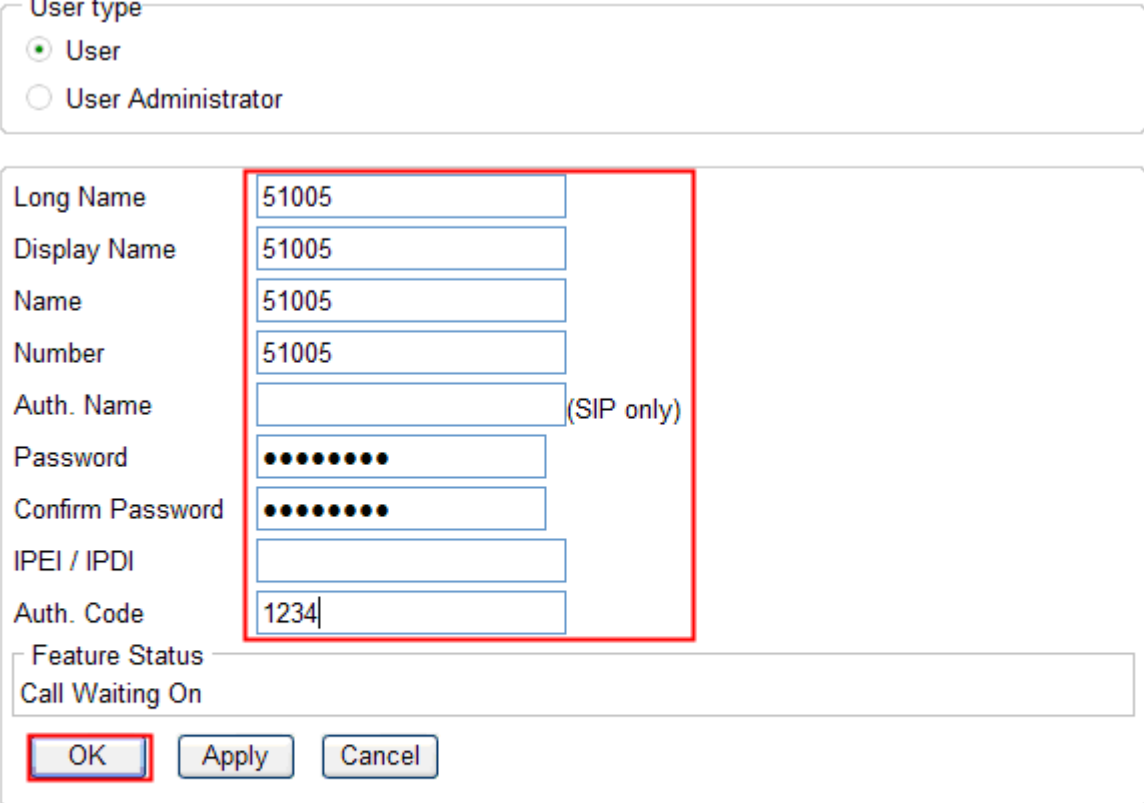
Step	Description
10.	<p>Navigate to the DECT System frame by clicking DECT and then clicking System. Configure the fields displayed below and then click OK. System Name is the Device Name used in Step 3. Password is the Password used in Step 3. The box below Password is to confirm the password and the 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 Enabled Carriers check boxes enable the DECT handsets to use different channels or frequencies when transmitting. Use the drop-down list for Coder and select “G711u”. Ensure that the codec chosen matches the codec configured on the Communication Manager.</p> <p>Note: The G.729AB codec was tested and is configured the same way.</p> 

Step	Description																																												
11.	<p>Navigate to the DECT Suppl. Serv. frame by clicking DECT and then clicking Suppl. Serv.. Check the Enable Supplementary Services check box. For the compliance testing, the Avaya PBX handled most of the features listed, so these functions were disabled on the Ascom BaseStation. Disable the following, Call Forwarding Unconditional, Call Forwarding Busy, Call Forwarding No Reply, Do not Disturb, Call Completion Busy Subscriber and Logout User. Depending on which Voicemail system is being used, enter the extension used for Avaya Modular Messaging or Avaya Communication Manager Messaging in the Fix Message Center No. field, and check the MWI enabled check box. Click OK to continue.</p>  <p>The screenshot shows the 'Ascom IP-DECT Base Station' configuration window. The 'Suppl. Serv.' tab is active. The 'Enable Supplementary Services' checkbox is checked. The following features are listed with their respective 'Activate', 'Deactivate', and 'Disable' checkboxes:</p> <table border="1"> <thead> <tr> <th>Feature</th> <th>Activate</th> <th>Deactivate</th> <th>Disable</th> </tr> </thead> <tbody> <tr> <td>Call Forwarding Unconditional</td> <td>-</td> <td>-</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>Call Forwarding Busy</td> <td>-</td> <td>-</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>Call Forwarding No Reply</td> <td>-</td> <td>-</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>Do Not Disturb</td> <td>-</td> <td>-</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>Call Waiting</td> <td>*43#</td> <td>#43#</td> <td><input type="checkbox"/></td> </tr> <tr> <td>Call Completion Busy Subscriber</td> <td>-</td> <td>-</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>Logout User</td> <td>-</td> <td>-</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>Clear Local Setting</td> <td>*00#</td> <td></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Fix Message Center No.</td> <td>58000</td> <td>MWI enabled</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>Local Clear of MWI</td> <td>-</td> <td></td> <td></td> </tr> </tbody> </table> <p>The 'OK' button is highlighted with a red box.</p>	Feature	Activate	Deactivate	Disable	Call Forwarding Unconditional	-	-	<input checked="" type="checkbox"/>	Call Forwarding Busy	-	-	<input checked="" type="checkbox"/>	Call Forwarding No Reply	-	-	<input checked="" type="checkbox"/>	Do Not Disturb	-	-	<input checked="" type="checkbox"/>	Call Waiting	*43#	#43#	<input type="checkbox"/>	Call Completion Busy Subscriber	-	-	<input checked="" type="checkbox"/>	Logout User	-	-	<input checked="" type="checkbox"/>	Clear Local Setting	*00#		<input type="checkbox"/>	Fix Message Center No.	58000	MWI enabled	<input checked="" type="checkbox"/>	Local Clear of MWI	-		
Feature	Activate	Deactivate	Disable																																										
Call Forwarding Unconditional	-	-	<input checked="" type="checkbox"/>																																										
Call Forwarding Busy	-	-	<input checked="" type="checkbox"/>																																										
Call Forwarding No Reply	-	-	<input checked="" type="checkbox"/>																																										
Do Not Disturb	-	-	<input checked="" type="checkbox"/>																																										
Call Waiting	*43#	#43#	<input type="checkbox"/>																																										
Call Completion Busy Subscriber	-	-	<input checked="" type="checkbox"/>																																										
Logout User	-	-	<input checked="" type="checkbox"/>																																										
Clear Local Setting	*00#		<input type="checkbox"/>																																										
Fix Message Center No.	58000	MWI enabled	<input checked="" type="checkbox"/>																																										
Local Clear of MWI	-																																												

Step	Description
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. Click OK to continue.</p> 
13.	<p>Navigate to the DECT SARI frame by clicking DECT and then clicking SARI. SARI is an Ascom provided activation code which is needed for the system to function. Contact Ascom to obtain a SARI. Enter the SARI value. Click OK to continue.</p> 

Step	Description
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. Click OK to continue.</p> 
15.	<p>Navigate to the General Info frame by clicking General and then clicking Info. The PARK for GAP devices is displayed. This value is needed when programming Ascom wireless DECT handsets. The PARK for GAP devices is similar to an SSID in an 802.11 wireless environment.</p> 

Step	Description
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' configuration interface. On the left is a navigation menu with 'Users' highlighted under the 'Administration' section. The main area has tabs for 'Users' and 'Anonymous'. The 'Users' tab is active, showing a 'PARK' field with 'XXXXXXXXXX', a 'Master Id' field with '0', and a 'new' button.</p>

Step	Description
17.	<p>The Edit User web page is presented. Long Name can be any descriptive name that identifies this user. Display Name is the text string that will be displayed on the LCD screen of the Ascom wireless DECT Handset. The Name & Number fields are the extension assigned to this user. The Password field is the password used to register with the SIP Enablement Services. The box below Password is to confirm the password and the value entered for the Password field must be entered here. Auth. Code is used only if Subscriptions in Step 10 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>  <p>The screenshot shows a web form for editing a user. At the top, there are two radio buttons for 'User type': 'User' (selected) and 'User Administrator'. Below this is a section with several text input fields: 'Long Name' (51005), 'Display Name' (51005), 'Name' (51005), 'Number' (51005), 'Auth. Name' (empty, with '(SIP only)' to its right), 'Password' (masked with dots), 'Confirm Password' (masked with dots), 'IPEI / IPDI' (empty), and 'Auth. Code' (1234). A red rectangular box highlights the 'Long Name' through 'Auth. Code' fields. At the bottom, there is a 'Feature Status' section with 'Call Waiting On' and three buttons: 'OK' (highlighted with a red box), 'Apply', and 'Cancel'.</p>

5.2. Configure Ascom wireless DECT Handset

Refer to [8], [9], [10] and [11] to obtain information on the procedures for subscribing and registering the Ascom wireless DECT Handsets to the Ascom wireless IP-DECT Base Station.

6. General Test Approach and Test Results

6.1. General Test Approach

All feature functionality test cases were performed manually. The general test approach entailed verifying the following:

- Registration, re-registration of Ascom wireless DECT Handsets with Avaya Aura™ SIP Enablement Services.
- Verify G.711MU and G.729AB codecs, shuffling, conferencing, Message Waiting Indicator and message retrieval from Avaya Modular Messaging Server & Avaya Communication Manager Messaging.
- Inter-office VoIP calls between Ascom wireless DECT Handsets and Avaya SIP & H.323 IP Telephones and Avaya Digital Telephones.
- Roam between multiple Ascom wireless IP-DECT Base Stations using the Ascom wireless DECT Handsets.

6.2. Test Results

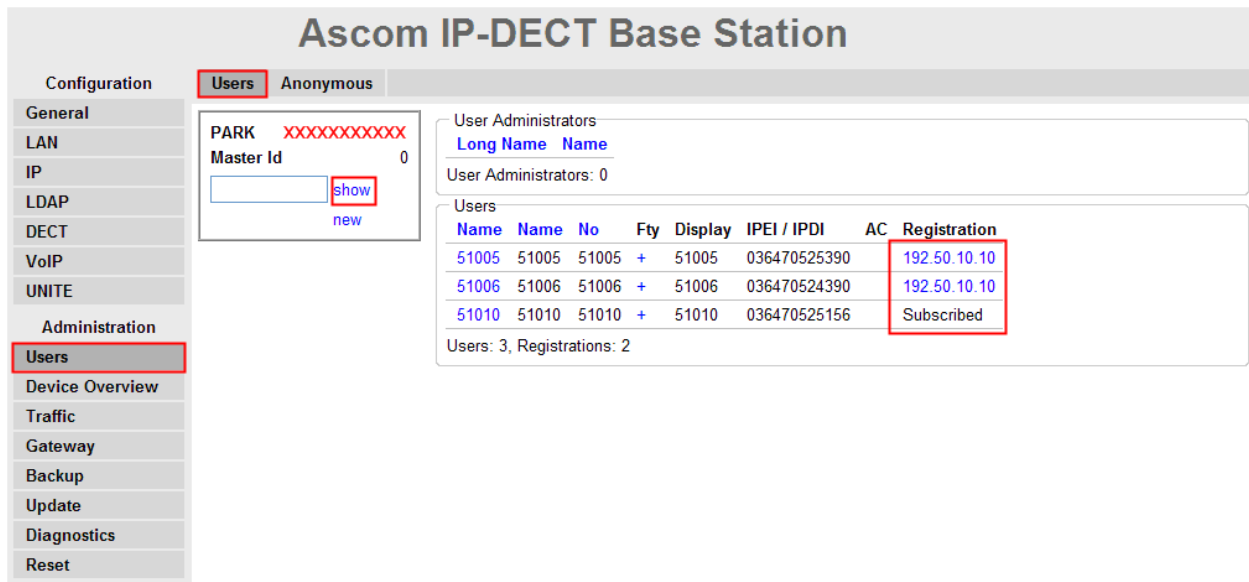
The Ascom wireless DECT Handsets passed all test cases. Ascom wireless DECT Handsets were verified to successfully register with Avaya Aura™ SIP Enablement Services. Two codecs were used for testing: G.711MU and G.729AB. Telephone calls were verified to operate correctly with the media path direct between the telephones (shuffling enabled) and with the media path centralized through Avaya Aura™ 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, call park & call pickup, bridged appearance alerting, Avaya Modular Messaging & Avaya Communication Manager Messaging voicemail and MWI.

7. Verification Steps

7.1. 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 a connection to the Ascom wireless IP-DECT Master Base Station (see **Section 5.1 Step 1**). Navigate to the **Users** frame by clicking **Users**, then clicking **Users**, and then clicking **show**. A **Registration** state of “Pending”(Not Shown) indicates an Ascom wireless DECT Handset has not registered to the Ascom wireless IP-DECT Base Station. 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 Aura™ SIP Enablement Services indicates the extension has successfully registered to both the Ascom wireless IP-DECT Base Station and Avaya Aura™ SIP Enablement Services.



The screenshot shows the 'Ascom IP-DECT Base Station' web interface. The 'Users' tab is selected, and the 'show' button is highlighted. The 'Users' table is displayed with the following data:

Name	Name	No	Fty	Display	IPEI / IPDI	AC	Registration
51005	51005	51005	+	51005	036470525390	192.50.10.10	
51006	51006	51006	+	51006	036470524390	192.50.10.10	
51010	51010	51010	+	51010	036470525156		Subscribed

Users: 3, Registrations: 2

7.2. 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.
- 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, call park & pickup, bridged appearance alerting, and voicemail Message Waiting Indicator (MWI).

8. Conclusion

These Application Notes illustrate the procedures necessary for configuring the Ascom wireless IP-DECT SIP Solution comprised of the Ascom wireless IP-DECT Base Station and Ascom wireless DECT Handsets with an Avaya Aura™ Telephony Infrastructure consisting of Avaya Aura™ Communication Manager, Avaya Aura™ SIP Enablement Services, Avaya Modular Messaging and Avaya Communication Manager Messaging in a converged Voice over IP and Data Network. All feature functionality test cases described in **Section 6.1** passed.

9. Additional References

Avaya documentation was obtained from <http://support.avaya.com>.

- [1] *Administering Avaya Aura™ Communication Manager*, May 2009 , Issue 5.0, Document Number 03-300509..
- [2] *Administering Avaya Aura™ SIP Enablement Services on the Avaya S8300 Server*, May 2009, Issue 2.0, Document 03-602508.
- [3] *Avaya Aura™ SIP Enablement Services (SES) Implementation Guide*, May 2009, Issue 6, Document 16-300140.
- [4] *Avaya one-X Deskphone Edition for 9600 Series IP Telephones Administrator Guide Release 3.0*, Document Number 16-300698.
- [5] *Avaya one-X Deskphone SIP for 9600 Series IP Telephones Administrator Guide, Release 2.0*, Document Number 16-601944.
- [6] *Modular Messaging, Release 5.0 with the Avaya MSS Messaging Application Server (MAS) Administration Guide*, January 2009.
- [7] *Avaya Aura™ Communication Manager Messaging Installation and Initial Configuration*

Ascom product documentation.

- [8] Ascom product documentation can be found at <http://www.Ascomwireless.com>

©2010 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 DevConnect Program at devconnect@avaya.com.