Application Notes for Configuring Rauland-Borg Responder® 5 to Interoperate with Avaya Aura® SIP Enablement Services and Avaya Aura® Communication Manager R5.2.1 – Issue 1.1

Abstract

These Application Notes describe a compliance-tested configuration consisting of the Rauland-Borg Responder® 5 solution, Avaya Aura® SIP Enablement Services and Avaya Aura® Communication Manager R5.2.1.

The Rauland-Borg Responder® 5 solution is a complete nurse call system with associated Staff Management applications, ensuring calls for assistance from patient rooms are immediately routed to the proper staff for response.

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 a compliance-tested configuration consisting of the Rauland-Borg Responder® 5 solution, Avaya Aura® SIP Enablement Services and Avaya Aura® Communication Manager R5.2.1.

The Responder solution is a complete nurse call system with associated Staff Management applications, ensuring calls for assistance from patient rooms are immediately routed to the proper staff for response. It should be noted that the solution involves the use of a third party Brekeke SIP Server, which is a standard element of any solution involving SIP PBX integrations.

Calls from a patient room could be initiated by a patient (pain, assistance needed, etc.), or hospital staff (room cleaning, linens, etc.) with the push of a button. Staff using Avaya phones can be incorporated into the system so that calls to talk to a nurse would route through SIP Enablement Services to Communication Manager, and to be able to call the patient room in return. This adds the benefit of staff having access to other resources in the hospital using Avaya endpoints.

Hospital staff members who are responsible for direct communication with patient rooms generally roam using wireless phones. The Compliance Test used a variety of wireless devices, including 3600 series SIP and IP wireless sets, Avaya oneX® Mobile SIP for Apple iOS devices (iPhone and iPad), and Avaya Desktop Video Devices (A175) as well as several stationary desksets.

The solution was tested in parallel with Avaya Aura® Session Manager and Avaya Aura® Communication Manager R6.0.1. Application Notes covering the Session Manager Interoperability Test are published separately under the title Application Notes for Configuring Rauland-Borg Responder® 5 to Interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager R6.0.1.
2. General Test Approach and Test Results

The compliance test focused on the ability for Rauland Responder® 5 endpoints to initiate and receive calls to and from SIP Enablement Services and Communication Manager.

2.1. Interoperability Compliance Testing

The compliance test validated the ability of Responder to route calls to and from patient rooms to Avaya endpoints. Additionally, testing validated the ability for the Responder solution to recover from common outages such as network outages and server reboots.

Responder endpoints are designed for purpose with limited functionality. Responder endpoints are not designed for multi-line functions like Hold, Conference and Transfer. These functions were successfully carried out on Avaya devices registered to SIP Enablement Services and Communication Manager while connected to calls with Responder endpoints.

2.2. Test Results

The objectives described in Section 2.1 were verified.

Two observations were made in the course of this testing.

One-way audio was observed in certain conditions:

- The Responder Branch Regional Controller media processing unit (BRC) sends audio (RTP) on a different port than it listens on (asymmetric). For example, if a session is established with the Session Description Protocol (SDP) indicating the Responder BRC will be listening on port 5004 for RTP packets, it will send the RTP to the Avaya Media Gateway from a different port (50957 for example).
- The Avaya G450 Media Gateway, and TN2602 (Crossfire) Media Resource boards implement security in the Digital Signal Processing (DSP) firmware which blocks audio sent asymmetrically. Note that TN2302 Media Processing boards do not implement this security and thus no conflicts were observed when using this board for media processing.
- Since NAT or Firewall implementations expect RTP to be sent and received on the same port (5004 in the above example), packets sent from the BRC are not passed through to other endpoints. This could impact not only the Avaya Media Resources, but also any intervening NAT or Firewall traversal devices between the two solutions.

Two workarounds were tested to resolve this conflict.

- VoIP DSP firmware on the G450 Media Gateway, and TN2602 IP Media Resource boards was modified. This is not recommended for two reasons:
  - The VoIP firmware settings are used for security reasons, thus alternative network security would need to be implemented to block denial of service type attacks on the boards.
  - The settings are not well publicized due to the security implications, thus implementations relying on this workaround method could be delayed.
• The second workaround involved using the Brekeke SIP Server as a Media Relay.
  o Using this method, all calls connected through the Brekeke server rather than
directly between the Responder BRC and the Avaya Media Gateways.
  o The impact of this workaround is that additional processing power is used to
accommodate the media processing.
  o Rauland engineers should be consulted to ensure adequate hardware resources are
planned based on expected call traffic.

The second observation is that the Responder Branch Regional Controller (BRC) media
processing unit does not support media shuffling.

• Attempts by the Avaya Media Gateway, or Media Resource/Processing boards to offer
direct connections between IP endpoints and the BRC failed.
  o The impact of this was that additional DSP resources were required on the Avaya
Media Gateways and Media Resource/Processing boards to accommodate
connections to Responder endpoints.
  o Avaya engineers should be consulted to ensure adequate VoIP resources are
planned based on expected call traffic.

2.3. Support
Information, documentation and technical support for Rauland-Borg products can be obtained at:
  – Phone: 1-847-590-7130
  – Web: http://www.rauland.com/
3. Reference Configuration

Figure 1 illustrates the compliance test configuration consisting of:

- Avaya Aura® Communication Manager R5.2.1
- Avaya Aura® SIP Enablement Services R5.2.1
- Various IP, SIP and Digital endpoints. Note that most endpoints were wireless.
- Brekeke SIP Server
- Responder® 5 Branch Regional Controller
- Responder® 5 Communication Endpoints

Note that while the test configuration illustrates two Communication Manager platforms, these Application Notes focus on the Communication Manager R5.2.1 test which was performed in parallel with Communication Manager R6.0.1.

Calls routed to and from the Communication Manager 5.2.1 system used SIP trunks between the Brekeke SIP server and SIP Enablement Services, and in turn SIP trunks between SIP Enablement Services and Communication Manager. In parallel, calls destined to the other Communication Manager were routed through Session Manager and are described separately in [3].
Figure 1 – Rauland-Borg Responder® 5Compliance Test Configuration
4. Equipment and Software Validated

The following equipment and version were used in the reference configuration described above:

<table>
<thead>
<tr>
<th>Equipment</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avaya S8800 Server and G650 Media Gateway</td>
<td>Avaya Aura® Communication Manager R5.2.1 SP9</td>
</tr>
<tr>
<td>Avaya S8800 Server</td>
<td>Avaya Aura® SIP Enablement Services R5.2.1 SP4</td>
</tr>
<tr>
<td>Avaya Phones</td>
<td>1.056 H.323 / 2.8.26.0 SIP</td>
</tr>
<tr>
<td>3641/3645 Wireless IP Phones</td>
<td>Avaya oneX® Deskphone 3.110b IP/2.6.4 SIP</td>
</tr>
<tr>
<td>9600 Series IP Phones</td>
<td>Avaya oneX® Deskphone 3.110b IP/2.6.4 SIP</td>
</tr>
<tr>
<td>96x1 Series IP Phones</td>
<td>Avaya A175-IPT-SIP-R1_1_0-122211</td>
</tr>
<tr>
<td>Avaya A175 Desktop Video Device</td>
<td>Avaya oneX® Mobile SIP for iOS 1.0.1-9</td>
</tr>
<tr>
<td>Apple iPad 2</td>
<td>R5</td>
</tr>
<tr>
<td>Apple iPhone 4</td>
<td>Responder® 5 Applications</td>
</tr>
<tr>
<td>Responder 5 endpoints and media gateways</td>
<td>Responder® 5 Applications</td>
</tr>
<tr>
<td>Dell Laptop with Windows 2003 Server</td>
<td>Brekeke SIP Server R2.4.7.3</td>
</tr>
<tr>
<td>Windows 2008R2 Server</td>
<td></td>
</tr>
</tbody>
</table>

Following are illustrations of Avaya endpoints used in the compliance test.
5. Configure Avaya Aura® Communication Manager

Configuration of Communication Manager required standard station administration which will not be covered in these Application Notes. In addition, routing was configured to enable calls originating from Communication Manager and SIP Enablement Services registered endpoints to be able to reach the Responder endpoints.

5.1. Configure Communication Manager Details

Calls were routed to Rauland endpoints using a 3 digit 5xx pattern. All calls routed via SIP trunk between Communication Manager and SIP Enablement Services using TCP transport. Existing SIP Trunks were in place in the environment, the steps below outline modifications made to accommodate the Responder solution. Therefore, some details required for SIP trunks may be omitted.

Administration for the solution required the following steps:

- Confirm Licensing
- Add node-names
- Add SIP Signaling Group
- Add SIP Trunk Group
- Change Route Pattern
- Change AAR Analysis
- Confirm IP codecs

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>


### Step 1: Confirm Licensing

Using the `display system-parameters customer-options` command, confirm that the system has capacity for additional SIP Trunks. If additional licenses are required, contact an authorized Avaya Sales or Reseller representative.

<table>
<thead>
<tr>
<th>display system-parameters customer-options</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP PORT CAPACITIES</td>
</tr>
<tr>
<td>Maximum Administered H.323 Trunks: 1000 0</td>
</tr>
<tr>
<td>Maximum Concurrently Registered IP Stations: 18000 3</td>
</tr>
<tr>
<td>Maximum Administered Remote Office Trunks: 0 0</td>
</tr>
<tr>
<td>Maximum Concurrently Registered Remote Office Stations: 0 0</td>
</tr>
<tr>
<td>Max Concur Registered Unauthenticated H.323 Stations: 0 0</td>
</tr>
<tr>
<td>Maximum Video Capable H.323 Stations: 100 3</td>
</tr>
<tr>
<td>Maximum Video Capable IP Softphones: 100 2</td>
</tr>
<tr>
<td><strong>Maximum Administered SIP Trunks</strong>: 800 20</td>
</tr>
<tr>
<td>Maximum Administered Ad-hoc Video Conferencing Ports: 0 0</td>
</tr>
<tr>
<td>Maximum Number of DS1 Boards with Echo Cancellation: 0 0</td>
</tr>
<tr>
<td>Maximum TN2501 VAL Boards: 10 0</td>
</tr>
<tr>
<td>Maximum Media Gateway VAL Sources: 0 0</td>
</tr>
<tr>
<td>Maximum TN2602 Boards with 80 VoIP Channels: 128 0</td>
</tr>
<tr>
<td>Maximum TN2602 Boards with 320 VoIP Channels: 128 0</td>
</tr>
<tr>
<td>Maximum Number of Expanded Meet-me Conference Ports: 0 0</td>
</tr>
</tbody>
</table>

### Step 2: Add node-names

Communication Manager uses the node-names ip table as a host lookup table. Host names used in subsequent steps will refer to these. Using the `change node-names ip` command, entries were added for SIP Enablement Services (SES) and the local CLAN address (CLAN).

<table>
<thead>
<tr>
<th>change node-names ip</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP NODE NAMES</td>
</tr>
<tr>
<td>Name</td>
</tr>
<tr>
<td>CLAN</td>
</tr>
<tr>
<td>SES</td>
</tr>
<tr>
<td>Step</td>
</tr>
<tr>
<td>------</td>
</tr>
</tbody>
</table>
| 3.   | **Add SIP Signaling Group**  
A signaling group was added using the `add signaling group 202` command with the following settings (settings not highlighted are default):  

*Group Type:* `sip`  
*Transport Method:* `tcp`  
*Near-end Node Name:* `CLAN`  
*Far-end Node Name:* `SES`  
*Near-end Listen Port:* `5060`  
*Far-end Listen Port:* `5060`  
*Far-end Domain:* `blank` (enable all domains).  
**Direct IP-IP Audio Connections:** `n`. (Responder does not support media shuffling). |

```
add signaling-group 202  
GROUP 202  
SIGNALING GROUP  
Group Number: 202  
Group Type: sip  
Transport Method: tcp  
Near-end Node Name: CLAN  
Far-end Node Name: SES  
Near-end Listen Port: 5060  
Far-end Listen Port: 5060  
Far-end Network Region: 1  
Far-end Domain:  
Bypass If IP Threshold Exceeded? n  
Incoming Dialog Loopbacks: eliminate  
RFC 3389 Comfort Noise? n  
DTMF over IP: rtp-payload  
Direct IP-IP Audio Connections? n  
Session Establishment Timer(min): 3  
Enable Layer 3 Test? n  
IP Audio Hairpinning? n  
H.323 Station Outgoing Direct Media? n  
Direct IP-IP Early Media? n  
Alternate Route Timer(sec): 6 |
```
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 4.   | **Add SIP Trunk Group**  
Using the `add trunk-group 202` command, trunk group 202 was created with the following settings (settings not highlighted are default):  

**Group Type:** sip  
**Group Name:** to SES/Rauland  
**TAC:** 117  
**Direction:** two-way  
**Service Type:** tie  
**Signaling Group:** 202  
**Number of Members:** 10  
**Numbering Format:** public |

```
add trunk-group 202  
Page 1 of 21  
TRUNK GROUP  
Group Number: 202  
Group Type: sip  
CDR Reports: n  
Group Name: to SES/Rauland  
COR: 1  
TN: 1  
TAC: 117  
Direction: two-way  
Outgoing Display? y  
Queue Length: 0  
Dial Access? n  
Night Service:  
Service Type: tie  
Auth Code? n  
Signaling Group: 202  
Number of Members: 10  
Numbering Format: public  
UUI Treatment: service-provider  
Replace Restricted Numbers? n  
Replace Unavailable Numbers? n  
Show ANSWERED BY on Display? y
```
### Step 5. Change Route Pattern

Route Pattern 202 was configured to use Trunk Group 202 for calls to Responder endpoints using the **change route-pattern 202** command with the following settings (settings not highlighted are default):

- **Pattern Name:** Rauland
- **Grp No:** 202 (This specifies the Trunk Group to use)
- **FRL:** 0 (This can be used as a security setting to restrict access to trunks based on Class Of Restriction, 0 is least restrictive).

```plaintext
change route-pattern 202
Pattern Number: 202
Pattern Name: Rauland
Grp No 202
FRL 0

Grp FRL NPA Pfx Hop Toll No. Inserted DCS/IXC
No MrkLmt List Del Digits

DgtsIntw
1: 202 0
2: n user
3: n user
4: n user
5: n user
6: n user

BCC VALUE TSC CA-TSC ITC BCIE Service/Feature PARM No. Numbering LAR
0 1 2 3 W Request Dgts Format

Subaddress
1: yyyy n n rest none
2: yyyy n n rest none
3: yyyy n n rest none
4: yyyy n n rest none
5: yyyy n n rest none
6: yyyy n n rest none
```

### Step 6. Change AAR Analysis

Using the **change aar analysis 0** command, dialed strings of 3 digits beginning with a 5 were instructed to use the **Route Pattern 202** configured in the previous step.

```plaintext
change aar analysis 0
AAR DIGIT ANALYSIS TABLE
Location: all
Percent Full: 2

<table>
<thead>
<tr>
<th>Dialed String</th>
<th>Total Min</th>
<th>Route Pattern</th>
<th>Call Type</th>
<th>Node ANI</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>2</td>
<td>3 202 aar</td>
<td>n</td>
<td></td>
</tr>
</tbody>
</table>
```

<table>
<thead>
<tr>
<th>Dialed String</th>
<th>Total Min</th>
<th>Route Pattern</th>
<th>Call Type</th>
<th>Node ANI</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>2</td>
<td>3 202 aar</td>
<td>n</td>
<td></td>
</tr>
</tbody>
</table>
7. **Confirm IP codecs**

Use the `change ip-codec-set n` command to add or modify RTP codecs. In the test environment, codec set 1 was used for all endpoints and trunks. **G.711MU** was used for all calls with responder endpoints, the Responder BRC does not support G.729. As the media gateway was required to be connected to all calls, the gateways were able to transcode RTP enabling different codecs to be used for each leg of the call.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.</td>
<td>Confirm IP codecs</td>
</tr>
</tbody>
</table>

Use the `change ip-codec-set n` command to add or modify RTP codecs. In the test environment, codec set 1 was used for all endpoints and trunks. **G.711MU** was used for all calls with responder endpoints, the Responder BRC does not support G.729. As the media gateway was required to be connected to all calls, the gateways were able to transcode RTP enabling different codecs to be used for each leg of the call.

### change ip-codec-set 1

<table>
<thead>
<tr>
<th>Codec Set: 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio Codec</td>
</tr>
<tr>
<td>1: G.711MU</td>
</tr>
<tr>
<td>2: G.729</td>
</tr>
</tbody>
</table>
6. Configure Avaya Aura® SIP Enablement Services

SIP Enablement Services is administered via web interface. In a browser, navigate to https://<hostname>/admin and login with appropriate credentials. Use the hostname or IP Address of the SIP Enablement Services server in the URL.

All navigation is performed by clicking links in the navigation panel on the left side of the screen.

1. **Configure the SIP Trunk to Communication Manager**

Navigate to Communication Manager Servers > List > Edit to modify the SIP Trunk settings. In the tested configuration, **TCP** protocol was used on the SIP Trunks. Click the Update button at the bottom of the screen to commit the change.
2. **Add a Trusted Host**

Navigate to **Trusted Hosts > Add** to add a new entry for the Brekeke SIP Server. In the illustration below showing the settings for the previously configured Trusted Host, the **IP Address** of 192.168.27.199 was the Brekeke SIP Server, and the **Perform Origination Processing** option was selected. Click **Update** to commit the changes.
3. **Add Host Address Map**

SIP Enablement Services uses the **Host Address Map** to define routing policies to route to Trusted Hosts. Navigate to **Hosts > List** and select the **Map** link to edit the **Host Address Map** table.

The following illustrates the previously added entries. Use the **Add Another Contact** link to add contact information.

The **Edit Host Contact** shows the settings used when the contact was previously created. The entry `sip:$(user)@192.168.27.199:5060;transport=udp` instructs SIP Enablement Services to forward SIP messages to the `192.168.27.199` domain using **udp** port **5060**.
Add Host Address Map (continued)

From the List Host Address Map screen shown above, click Add Another Map link to specify dialed number patterns which will use this routing policy. The two patterns shown below were added to instruct SIP Enablement Services to use this policy for 2 digit number 29, and three digit 5xx extensions on the Responder system.
4. **Add Communication Manager Server Address Map**

SIP Enablement Services uses the **Communication Manager Server Address Map** to define routing policies to route to Communication Manager. Navigate to **Communication Manager Servers** > **List** and select the **Map** link to edit the **Communication Manager Server Address Map** table.

The following illustrates the previously added entries. Use the **Add Another Contact** link to add contact information.

The **Edit Communication Manager Contact** link shows the settings used when the contact was previously created. The entry

```
sip:$(user)@10.64.40.24:5060;transport=tcp
```

instructs SIP Enablement Services to forward SIP messages to Communication Manager using **tcp** port **5060**.
5. **Add Host Address Map (continued)**

From the **List Communication Manager Server Address Map** screen shown above, click the **Add Another Map** link to specify dialed number patterns which will use this routing policy. The pattern shown below was added to instruct SIP Enablement Services to use this policy for 5 digit numbers 2xxxx on Communication Manager.
7. Configure Responder® 5

The Responder solution is typically implemented by Rauland engineers or their resale partners. When integrated with a third party SIP PBX, it is always deployed with a Brekeke SIP server which serves two purposes. First, Brekeke SIP server is commonly deployed with a variety of SIP capable PBX solutions giving the Responder equipment a common and predictable SIP interface that is adaptable to many environments. Second, the Brekeke SIP Server is capable of providing registrar services without requiring provisioning for each Responder endpoint, thus significantly reducing the implementation and ongoing administration of the solution.

The Responder equipment will be provisioned completely by Rauland engineers based on site requirements, and will be configured to use the Brekeke SIP server for all calls destined to endpoints outside of the Responder endpoints.

The focus of this section will be on administration of the Responder applications, and configuration of the Brekeke SIP Server to properly route SIP calls and RTP.
### 7.1. Responder 5 Configuration Details

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1.   | **Configure Endpoints**  
Typically, hospital staff uses wireless phones to enable instant communications with staff and patient rooms. In the tested confirmation, a variety of IP and SIP wireless devices which were previously configured on Communication Manager and SIP Enablement Services, were administered in the Responder applications to associate the endpoints with the hospital staff.  
The Responder applications are accessed from the Windows PC used by a staff administrator and/or at nurse stations throughout the hospital. These PCs are used by staff to clock in and manage patient room assignments. The applications are launched from **Start> All Programs> Responder 5 Applications**.  
In the top left corner is a drop down list that navigates to the various applications. Each requires an appropriate login (not shown). Select **Administration – Devices** in the upper left drop down list (not shown) to add or modify phones. Enter the appropriate **DeviceName/Extension**, **Type**, and a **Description**. The illustration below shows a number of devices used in the test environment, extensions 22xxx and 28xxx were IP and SIP devices administered on Communication Manager and SIP Enablement Services respectively.  
**Click OK** at the bottom of the screen to complete edits on this screen. |
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td><strong>Assign Endpoints to Users</strong>&lt;br&gt;Select <em>Administration – Devices</em> in the upper left drop down list (not shown) to add or modify users and to assign devices to the users. This task is only necessary for statically assigned device assignments. Users who share devices are able to enter the device they are using for a shift when they login as described in <strong>Step 3</strong>. Users can be created or modified on the <em>User – Creation</em> tab (user creation is beyond the scope of these application notes, see Responder documentation for details of this task). Devices (phones) are created on the <em>User – General</em> tab as shown below. In the illustration below, devices were selected from a list of phones (from the list in <strong>Step 1</strong> above) in the <em>PermanentDevice</em> column for each user. Click <strong>OK</strong> to complete edits on this screen.</td>
</tr>
</tbody>
</table>
### Step 3: User Login and Device Assignment

At the beginning of a shift, or return to duty from breaks, users will scan their Hospital ID badge bar code with a scanner connected to the PC which will automatically log them in to the **My Profile** screen.

From this screen, a **Wireless Phone** and/or **Pager** number can be entered, duty status updated, and break status entered. The **My Assignments** and **My Preferences** tabs are available for staff to review the patient rooms they are assigned to and modify user preferences. The details of these tasks are beyond the scope of these Application Notes.

Click **Update** or **Update and Exit** to commit the changes.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td><strong>User Login and Device Assignment</strong></td>
</tr>
</tbody>
</table>

- **At the beginning of a shift, or return to duty from breaks,** users will scan their Hospital ID badge bar code with a scanner connected to the PC which will automatically log them in to the **My Profile** screen.

- From this screen, a **Wireless Phone** and/or **Pager** number can be entered, duty status updated, and break status entered. The **My Assignments** and **My Preferences** tabs are available for staff to review the patient rooms they are assigned to and modify user preferences. The details of these tasks are beyond the scope of these Application Notes.

- Click **Update** or **Update and Exit** to commit the changes.
4. **Assign Staff to Patient Rooms**  
This task is typically performed by shift supervisors. Staff can be assigned to patient rooms on the **Staff Assignment** screen which is accessed from the drop down menu at the upper left of the Responder 5 Applications. In the illustration below, **GA (Gertrud Andrag)** is assigned to room **501-1** by clicking on the Staff name in the left column, then clicking on the assignment space below the patient name. The staff members initials (**GA** in this case) will appear as below when the staff member has been successfully assigned to a patient.

![Staff Assignment Screen](image-url)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.</td>
<td><strong>Assign Staff to Patient Rooms</strong>&lt;br&gt;This task is typically performed by shift supervisors. Staff can be assigned to patient rooms on the <strong>Staff Assignment</strong> screen which is accessed from the drop down menu at the upper left of the Responder 5 Applications. In the illustration below, <strong>GA (Gertrud Andrag)</strong> is assigned to room <strong>501-1</strong> by clicking on the Staff name in the left column, then clicking on the assignment space below the patient name. The staff members initials (<strong>GA</strong> in this case) will appear as below when the staff member has been successfully assigned to a patient.</td>
</tr>
</tbody>
</table>
### Step 5

**Configure Brekeke SIP Server SIP Properties**

The following SIP settings were pre-configured for the test environment.

All administration is performed via web browser by navigating to the hostname or IP Address of the Brekeke server.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td><strong>Configure Brekeke SIP Server SIP Properties</strong>&lt;br&gt;The following SIP settings were pre-configured for the test environment.&lt;br&gt;&lt;br&gt;All administration is performed via web browser by navigating to the hostname or IP Address of the Brekeke server.</td>
</tr>
<tr>
<td>Step</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| 6.   | **Configure RTP Relay settings**  
The tested configuration required that all media (RTP) send to and from Rauland endpoints be connected through the Brekeke SIP Server. This was required in order to overcome an incompatibility between Rauland and Avaya media servers as described in Section 2.  

On the Configuration > RTP screen, set RTP Relay to **on**, RTP relay (UA on this machine) to **auto**, Port mapping to **source port** and click **Save** to complete entries. Note, the **Minimum** and **Maximum Port** range settings should be sufficient to handle the maximum number of concurrent RTP sessions between systems. |
Configure Dial Plan Routing rules

Several Dial Plan rules were used as illustrated below. For calls routing to SIP Enablement Services, Avaya SES and Avaya SES 28 rules were used. The other rules were used to route calls to the Session Manager system covered in the alternate Application Notes previously mentioned.

All rules were identical except for the values for the Matching Patterns and Deploy Patterns. In the screenshot below, calls to number patterns starting with 28 were routed to SIP Enablement Services at 10.64.40.41. For the system covered in these application notes, the patterns 22 and 28 were defined and routed to SIP Enablement Services.

Click Save to commit the changes on this screen.
8. Verification Steps

Calls were placed to and from Responder endpoints, and two-way audio was confirmed. The nature of these devices is simple, one-way communications with Hospital staff, complex calls like transfer and conference are not supported on the patient room devices, but Avaya endpoints were tested to confirm conference and transfer functionality.

On the Brekeke SIP Server, the **Registered Clients > View Clients** screen will confirm if Responder endpoints are successfully registered as shown below.
9. Conclusion
These Application Notes describe the procedures required to configure Rauland-Borg Responder® 5 to interoperate with endpoints registered to Avaya Aura® SIP Enablement Services and Avaya Aura® Communication Manager using a Brekeke SIP Server as a SIP registrar and Proxy for the Responder 5 side of the solution.

Caution is advised to pay particular attention to the observations noted in Section 2 above when planning to implement this solution.

10. Additional References
Product documentation for Avaya products may be found at http://support.avaya.com.

Avaya

Rauland-Borg
Product information for Rauland-Borg products can be found at http://www.rauland.com/.