Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Rauland-Borg Responder® 5 to Interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager R6.0.1 – Issue 1.1

Abstract

These Application Notes describe a compliance-tested configuration consisting of the Rauland-Borg Responder® 5 solution, Avaya Aura® Session Manager and Avaya Aura® Communication Manager R6.0.1.

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® Session Manager and Avaya Aura® Communication Manager R6.0.1.

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 Session Manager 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® SIP Enablement Services and Avaya Aura® Communication Manager R5.2.1. Application Notes covering the SIP Enablement Services Interoperability Test are published separately under the title *Application Notes for Configuring Rauland-Borg Responder® 5 to Interoperate with Avaya Aura® SIP Enablement Services and Avaya Aura® Communication Manager R5.2.1.*

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 Avaya Aura® Session Manager and Avaya Aura® 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 Session Manager 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.
    - Using this method, all calls connected through the Brekeke server rather than directly between the Responder BRC and the Avaya Media Gateways.
    - The impact of this workaround is that additional processing power is used to accommodate the media processing.
    - 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.
    - 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.
    - 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 R6.0.1
- Avaya Aura® Session ManagerR6.1
- Avaya Aura® System Manager R6.1
- 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 R6.0.1 test which was performed in parallel with Communication Manager R5.2.1.

Calls routed to and from the Communication Manager R6.0.1 system used SIP trunks between the Brekeke SIP server and Session Manager, and in turn SIP trunks between Session Manager and Communication Manager. In parallel, calls destined to the other Communication Manager were routed through SIP Enablement Services and are described separately in [3].

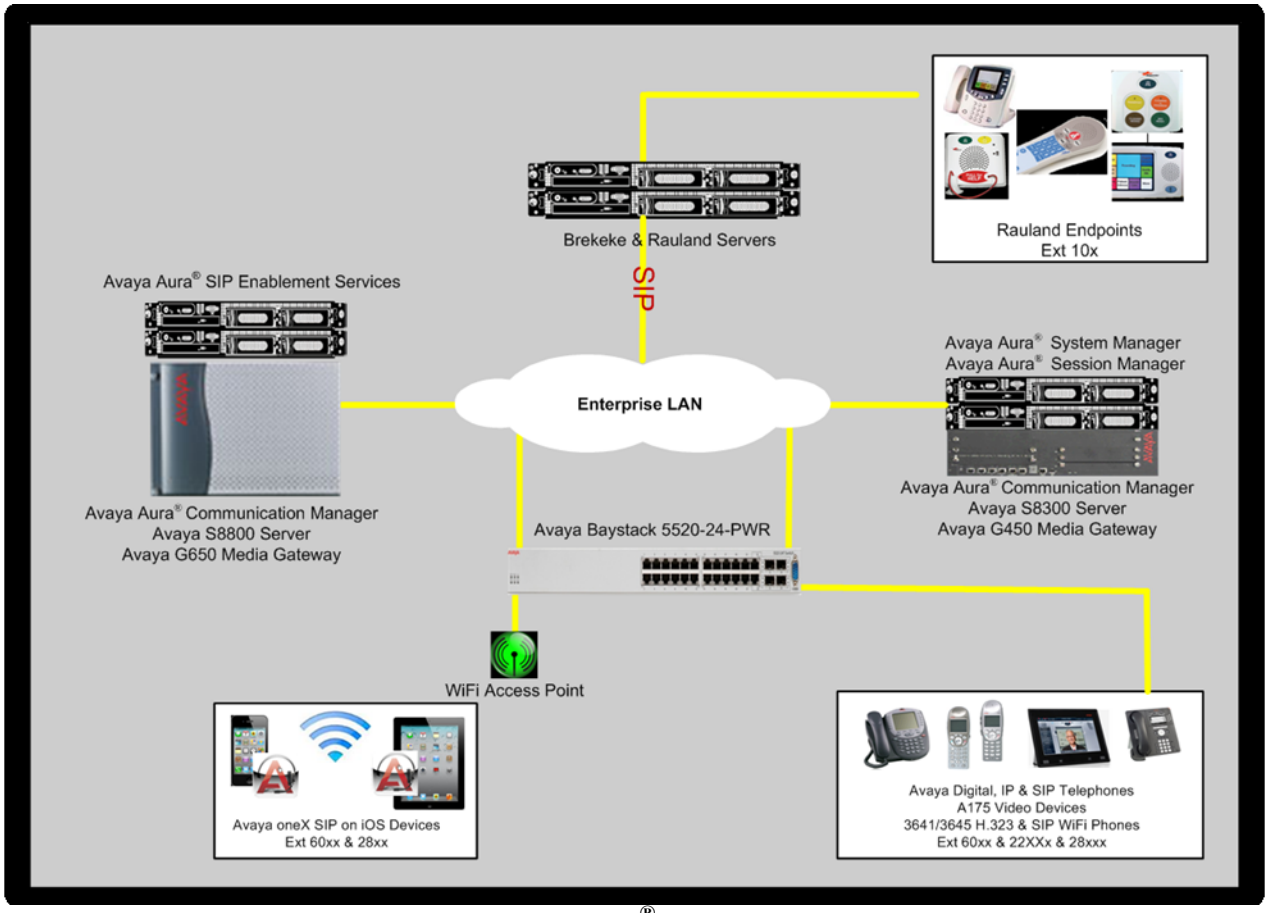


Figure 1 – Rauland-Borg Responder® 5Compliance Test Configuration

4. Equipment and Software Validated

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

Equipment	Version
Avaya S8800 Server and G450 Media Gateway	Avaya Aura® Communication Manager R6.0.1 SP6
Avaya S8800 Server	Avaya Aura® Session Manager R6.1
Avaya Phones 3641/3645 Wireless IP Phones 9600 Series IP Phones 96x1 Series IP Phones Avaya A175 Desktop Video Device	 1.056 H.323 / 2.8.26.0 SIP Avaya oneX® Deskphone 3.110b IP/2.6.4 SIP Avaya oneX® Deskphone 3.110b IP/2.6.4 SIP A175-IPT-SIP-R1_1_0-122211
Apple iPad 2 Apple iPhone 4	Avaya oneX® Mobile SIP for iOS 1.0.1-9
Responder 5 endpoints and media gateway (BRC)	R5
Dell Laptop with Windows 2003 Server	Responder® 5 Applications
Windows 2008R2 Server	Brekeke SIP Server R2.4.7.3

Following are illustrations of Avaya endpoints used in the compliance test.

Avaya 3641 & 3645 WiFi SIP/IP Phones

Avaya oneX® Mobile SIP on Apple iPhone and iPad2

Avaya 96x1 Series SIP/IP Phones

Avaya 9600 Series SIP/IP Phones

Avaya Desktop Video Device (A175)

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 Session Manager registered endpoints to be able to reach the Responder endpoints.

5.1. Configure Communication Manager Details

Calls were routed to Rauland endpoints using a 4 digit 75xx pattern. All calls routed via SIP trunk between Communication Manager and Session Manager 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

Step	Description

Step	Description
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.

```
display system-parameters customer-options                      Page   2 of  10
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                             USED
                     Maximum Administered H.323 Trunks: 1000  0
           Maximum Concurrently Registered IP Stations: 18000 3
             Maximum Administered Remote Office Trunks: 0     0
Maximum Concurrently Registered Remote Office Stations: 0     0
              Maximum Concurrently Registered IP eCons: 0     0
  Max Concur Registered Unauthenticated H.323 Stations: 0     0
                  Maximum Video Capable H.323 Stations: 100   3
                   Maximum Video Capable IP Softphones: 100   2
Maximum Administered SIP Trunks: 800   20
  Maximum Administered Ad-hoc Video Conferencing Ports: 0     0
   Maximum Number of DS1 Boards with Echo Cancellation: 0     0
                             Maximum TN2501 VAL Boards: 10    0
                     Maximum Media Gateway VAL Sources: 0     0
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   0
   Maximum Number of Expanded Meet-me Conference Ports: 0     0
```

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 Session Manager (***SM***) and the processor Ethernet interface on Communication Manager (***procr***).

```
change node-names ip                                            Page   1 of   2
                                   IP NODE NAMES
    Name              IP Address
procr10.64.10.67
SM 10.64.21.31
```

Step	Description
3.	**Add SIP Signaling Group** A signaling group was added using the **add signaling group 30** command with the following settings (settings not highlighted are default): **Group Type**:***sip*** **Transport Method**:***tcp*** **Near-endNode Name**:***procr*** **Far-end Node Name**:***SM*** **Near-endListen Port**:***5060*** **Far-endListen Port**:***5060*** **Far-end Domain**:***avaya.com*** (Match the domain on Session Manager). **Direct IP-IP Audio Connections:*n*.**(Responder does not support media shuffling).

```
add signaling-group 30 Page   1 of   1
                                SIGNALING GROUP

Group Number: 30             Group Type: sip
                         Transport Method: tcp
  IMS Enabled? n




   Near-end Node Name: procr                 Far-end Node Name: SM
 Near-end Listen Port: 5060                Far-end Listen Port: 5060
Far-end Network Region: 1
Far-end Domain: avaya.com

                                            Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
DTMF over IP: rtp-payloadDirect IP-IP Audio Connections? n
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? n                       Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 6
```

Step	Description
4.	**Add SIP Trunk Group** Using the **add trunk-group 30**command, trunk group 30 was created with the following settings (settings not highlighted are default): **Group Type:** ***sip*** **Group Name:** ***to SM/Rauland*** **TAC:** ****030*** **Direction:** ***two-way*** **Service Type:** ***tie*** **Signaling Group:** ***30*** **Number of Members:** ***10*** **Numbering Format:** ***public***

```
add trunk-group 30                    Page   1 of  21
                                TRUNK GROUP

Group Number: 202                 Group Type: sip          CDR Reports: n
Group Name: to SM/Rauland           COR: 1        TN: 1        TAC: *030
Direction: two-way        Outgoing Display? y
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: tieAuth Code? n

Signaling Group: 30
                                                      Number of Members: 10


add trunk-group 202                           Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                         Maintenance Tests? y



Numbering Format: public
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n


 Show ANSWERED BY on Display? y
```

Step	Description
5.	**Change Route Pattern** Route Pattern 30 was configured to use Trunk Group 30 for calls to Responder and Session Manager registered endpoints using the **change route-pattern 30** command with the following settings (settings not highlighted are default): **Pattern Name: *SM*** **Grp No: *30*** (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).

```
change route-pattern 202        Page   1 of   3
                    Pattern Number: 202 Pattern Name: SM
                              SCCAN? n     Secure SIP? n
Grp FRL NPA Pfx Hop Toll No.  Inserted                              DCS/ IXC
No MrkLmt List Del  Digits                              QSIG
DgtsIntw
 1: 30   0                                                            n   user
 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 M 4 W     Request                                 Dgts Format
Subaddress
 1: y yyyy n  n            rest                                          none
 2: y yyyy n  n            rest                                          none
 3: y yyyy n  n            rest                                          none
 4: y yyyy n  n            rest                                          none
 5: y yyyy n  n            rest                                          none
 6: y yyyy n  n            rest                                          none
```

6.	**Change AAR Analysis** Using the **change aar analysis 0** command, dialed strings of ***4*** digits beginning with a ***75*** were instructed to use the ***Route Pattern 30*** configured in the previous step. Note all Responder endpoints used a 3 digit 5xx extension, a 7 was appended in Communication Manager in order to avoid conflicts with other uses of dial patterns starting with 5.

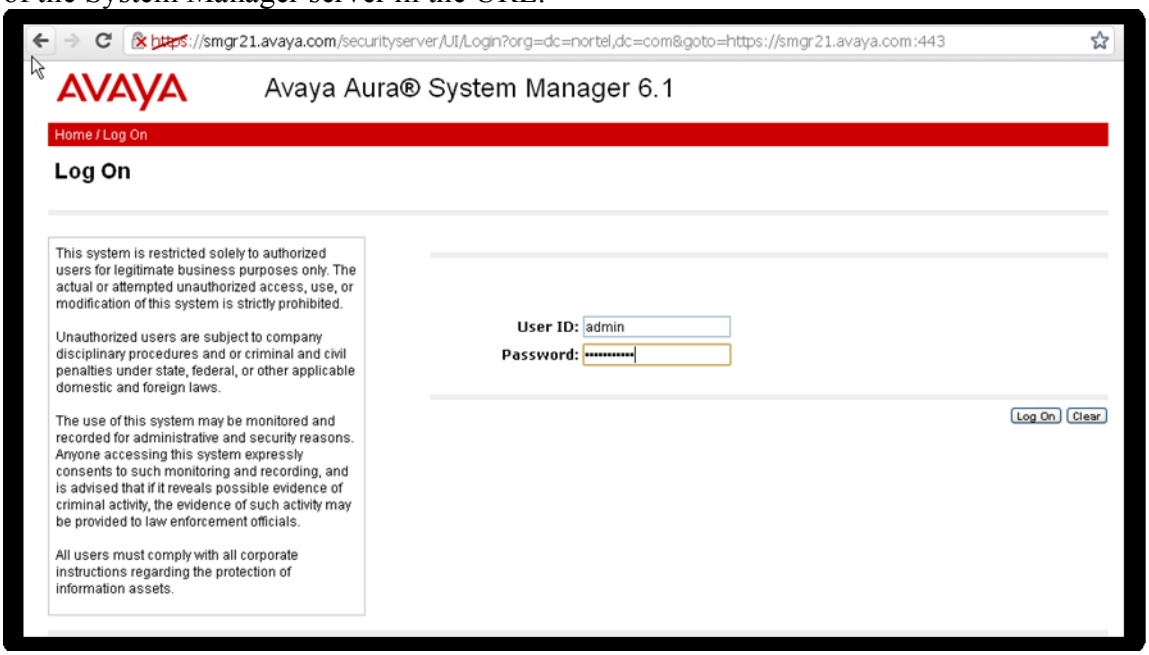
```
change aar analysis 0                                          Page   1 of   2
                            AAR DIGIT ANALYSIS TABLE
                                  Location:  all           Percent Full:    2

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   NumReqd
6014430 aar          n
754430aar          n
```

Step	Description
7.	**Confirm IP codecs** Use the **change ip-codec-set n** command to add or change 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.

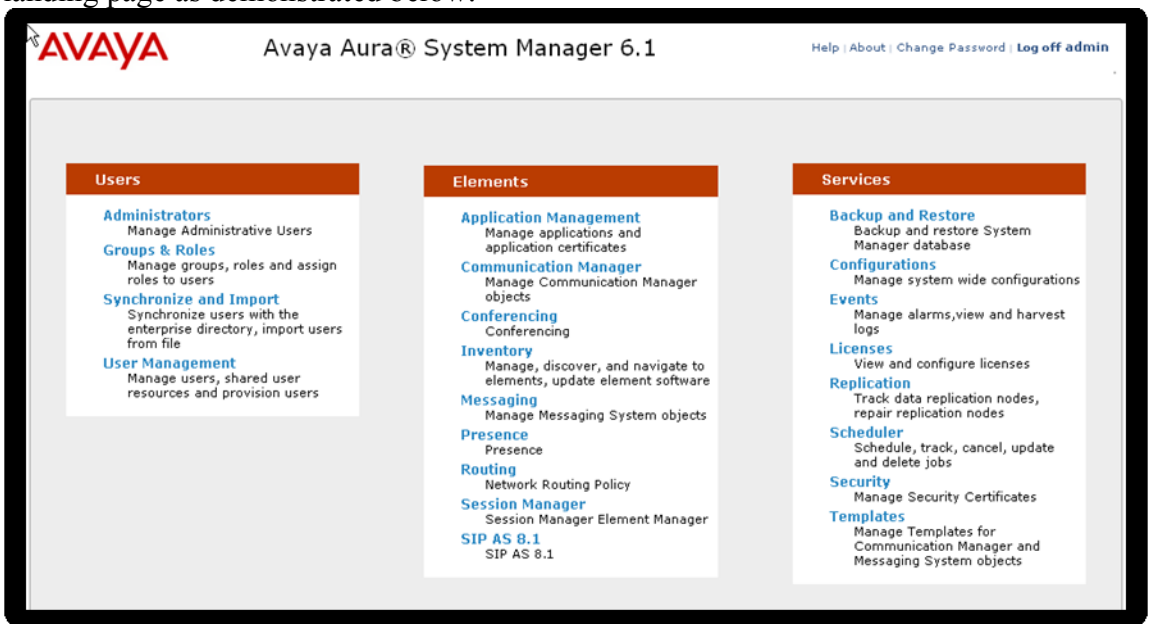
```
change ip-codec-set 1                                          Page   1 of   2

                           IP Codec Set

    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
1: G.711MU           n          2        20
 2: G.729             n          2        20
```

6. Configure Avaya Aura® Session Manager

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



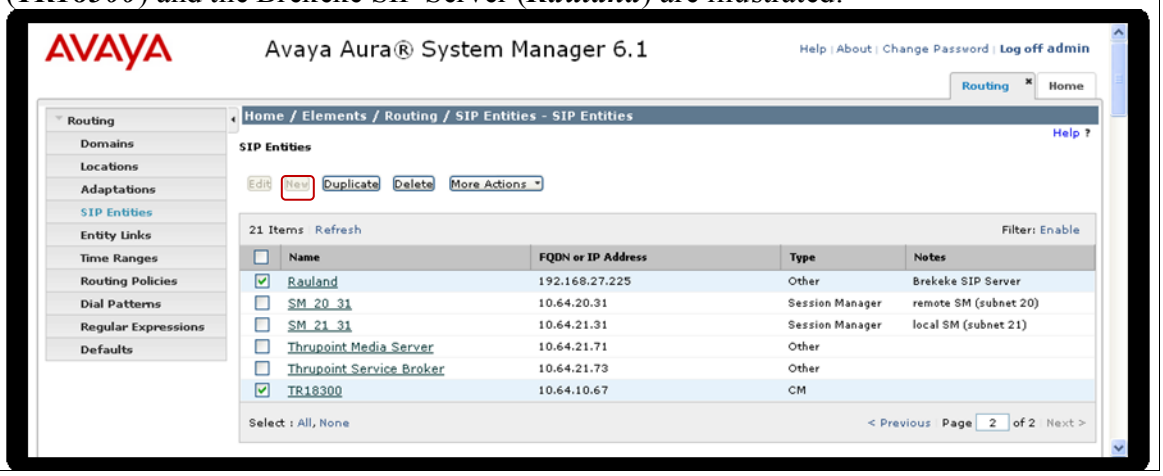
All navigation is performed by clicking links in the navigation links on the System Manager landing page as demonstrated below.



6.1. Configure Session Manager Details

Administration for the solution required the following steps:

- Add a SIP Entity
- Add a SIP Entity Link
- Create an Adaptation Rule
- Create a Routing Policy
- Create a Dial Pattern

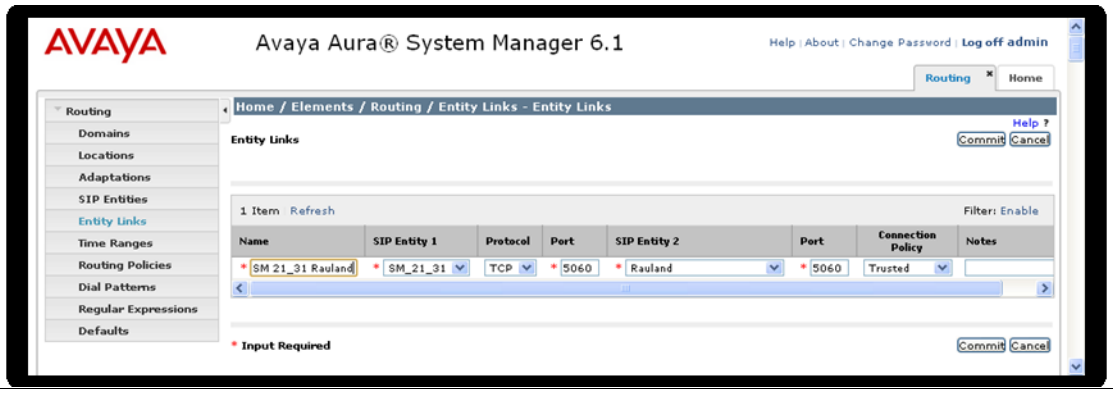
1.	**Add a SIP Entity** Navigate to **Routing > SIP Entities** and click **New** to add a new SIP Entity for the Brekeke SIP Server. In the illustration below, the entities for Communication Manager (***TR18300***) and the Brekeke SIP Server (***Rauland***) are illustrated: 

Add a SIP Entity(Continued)

On the SIP Entity Details screen which appears when the New button is pressed above, enter the following:

- **Name**: Enter a descriptive name for the entity (***Rauland***).
- **FQDN or IP Address:*192.168.27.225*** was the address used by the Brekeke SIP server in the test configuration.
- **Type: *Other***
- **Notes:** useful for quick glance identification on other screens.
- **Adaptation:** This was modified in a subsequent step with the adaptation called ***Rauland*** created in **Step 3** below but is described in this step for brevity.
- **SIP Link Monitoring:** This was set to ***Link Monitoring Disabled*.** The Brekeke SIP Server does not use link monitoring.
- **Entity Links:** This was added in a subsequent edit to the Entity record using the **Add** button but is described here for brevity purposes**.** See **Step 2** for how the Entity Link was created.

Click **Commit** to complete the entries on this screen.

2.	**Add a SIP Entity Link** Navigate to **Routing > Entity Links** and click **New** to add a new Entity Link to the Brekeke SIP Server (not shown). Enter the following to create the Entity Link: • **Name**: ***SM21_31 Rauland***- A Descriptive name for the Entity Link. • **SIP Entity 1: *SM_21_31* -** Select the existing Session Manager SIP Entity. • **SIP Entity 2**:***Rauland*** – Select the newly created SIP entity. • **Protocol: *TCP.*** Brekeke SIP Server does not currently support TLS, use TCP for the transport protocol. • **Port:*5060*** – Port 5060 is the standard listen port for the TCP SIP transport protocol. Click **Commit** to save the entries. 

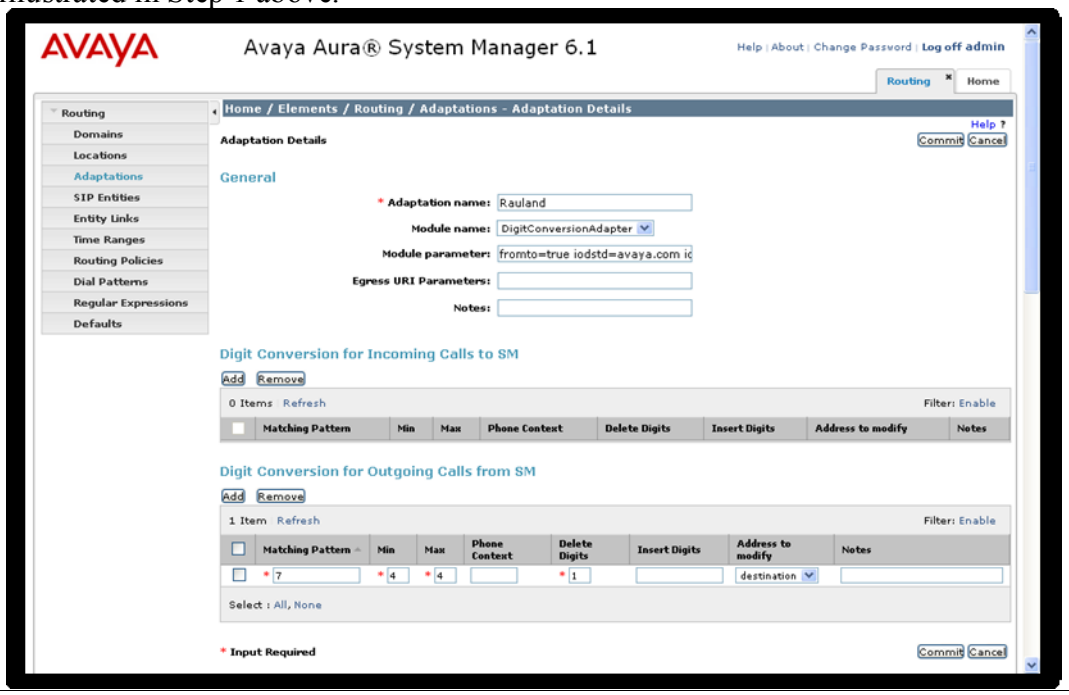
3. **Create an Adaptation Rule**

Session Manager used an Adaptation rule for two purposes. First, domains in the To and From headers were modified to reconcile differences in the ***Avaya*** domain used on Session Manager and Communication Manager, and the IP Address of the Brekeke SIP Server used as the domain on that side of the call flow.

Navigate to **Routing > Adaptations** and click **New** (not shown) to add an Adaptation rule. For this rule, the following entries were made:

- **Adaption Name**: ***Rauland*** – Any Descriptive name.
- **Module name**:***DigitConversionAdapter*** – Selected from the list.
- **Module Parameter**:***fromto=true iodstd=avaya.com iosrcd=avaya.com osrcd=10.64.21.31 odstd=192.168.27.225***–this defines a rule to modify domains in SIP headers. See product documentation [2] for more information on the use of Adaptation Rules.
- **Digit Conversion for Outgoing Calls from SM**: This defined a rule to remove 1 digit from the destination address for four digit dialed numbers starting with 7. Communication Manager users, in order to avoid conflicting dial plans used a 7xxx dial plan to dial Responder endpoints. This rule removed the 7 and sent 5xx to the Brekeke SIP server in order to match dial plans on that side of the solution.

Click **Commit** to save the changes, then add the adaptation rule to the SIP Entity form as illustrated in Step 1 above.



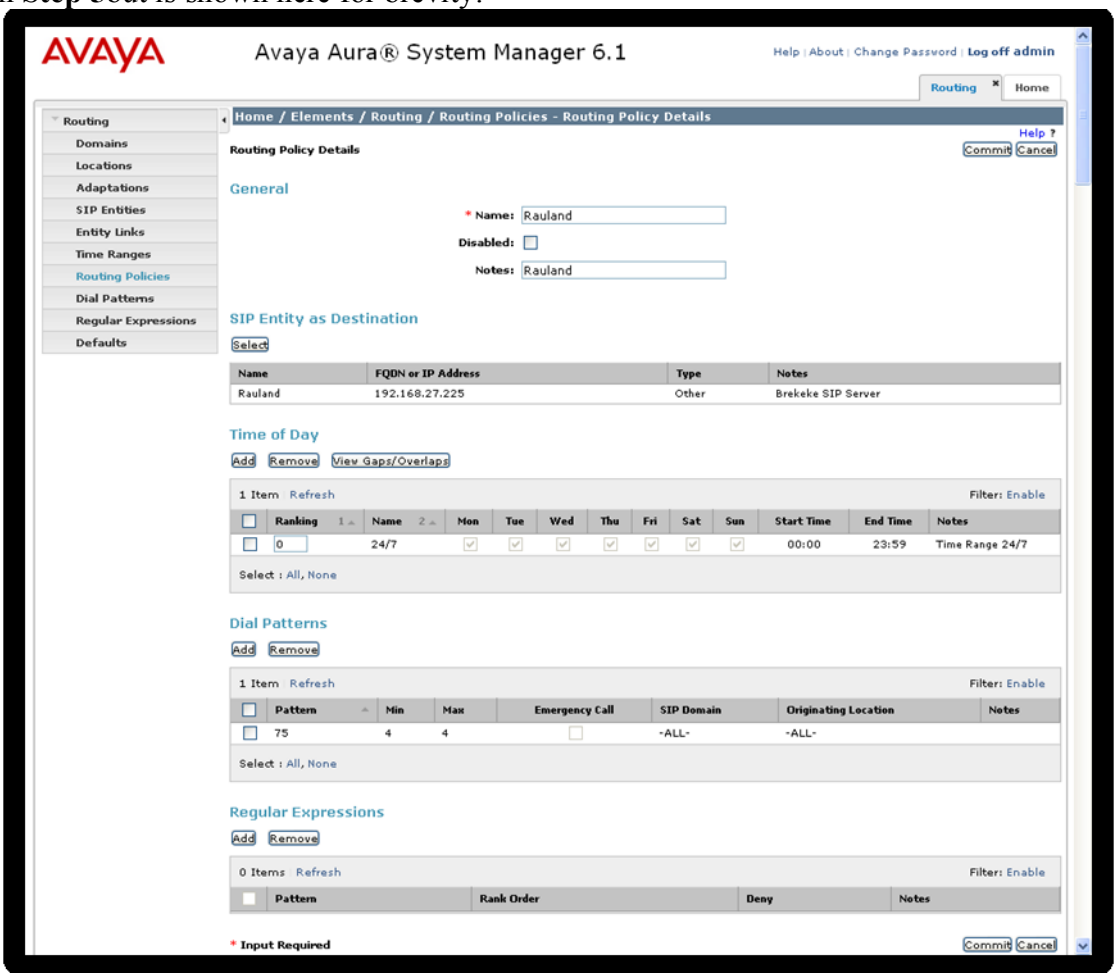
4. **Create a Routing Policy**

Routing Policies require definition of a Routing Policy, and definition of Dial Patterns. A new Routing Policy is created first, leaving the Dial Pattern undefined, then a Dial Pattern is defined, then the Dial Pattern is applied to the Routing Policy.

Navigate to **Routing > Routing Policies** and click the **New** button (not shown). On the **Routing Policy Details** page, provide a **Name** and **Notes** as desired for the policy. Click the **Select** button to select the **SIP Entity as Destination** (not shown). The ***Rauland*** SIP Entity was selected as the Destination.

Click **Commit** to save the entries.

Note that the **Dial Patterns** shown below was added when the **Dial Pattern** was defined in **Step 5**but is shown here for brevity.



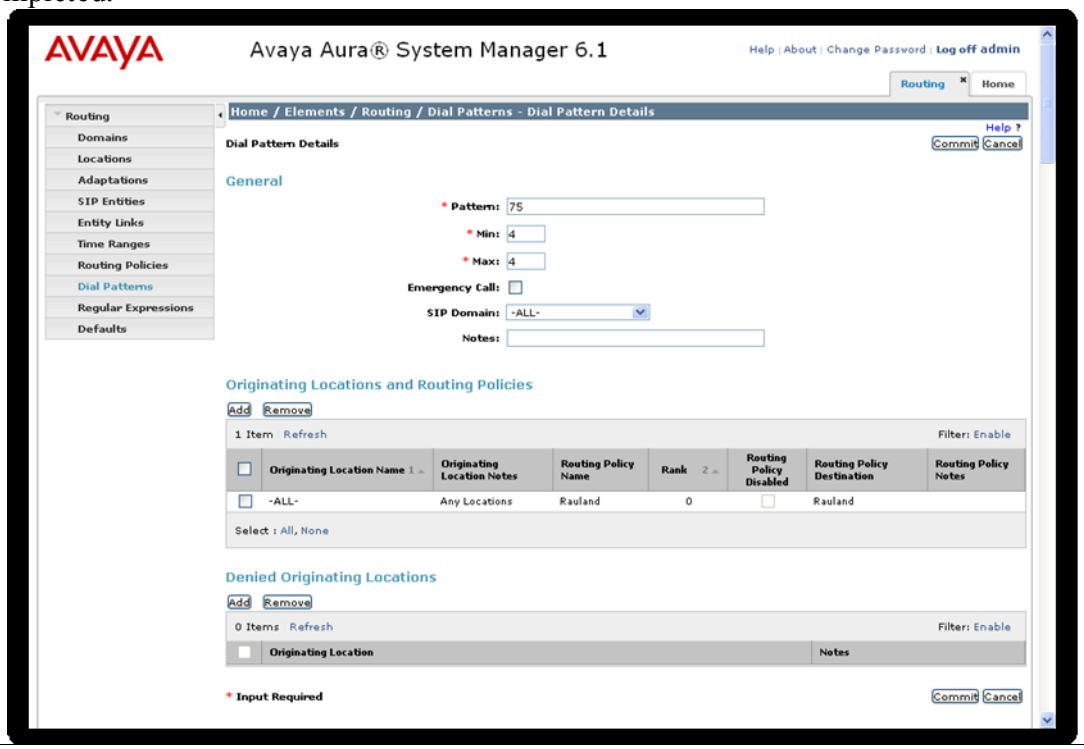
5. **Create a Dial Pattern**

To create a Dial Pattern, navigate to **Routing > Dial Patterns** and select **New** (not shown).

Enter the following:

- **Pattern:** ***75*** – the leading digits to match on the To header for SIP messages.
- **Min and Max**:***4***– The number of digits in the dialed number to match.
- **SIP Domain**:***All*** – The SIP Domain can be used to implement domain based routing rules, this option was not used in the compliance test.
- **Originating Locations and Routing Policies:** See the next page for details of this step.

Click on the **Commit** button to save the entries after the step on the following page is completed.

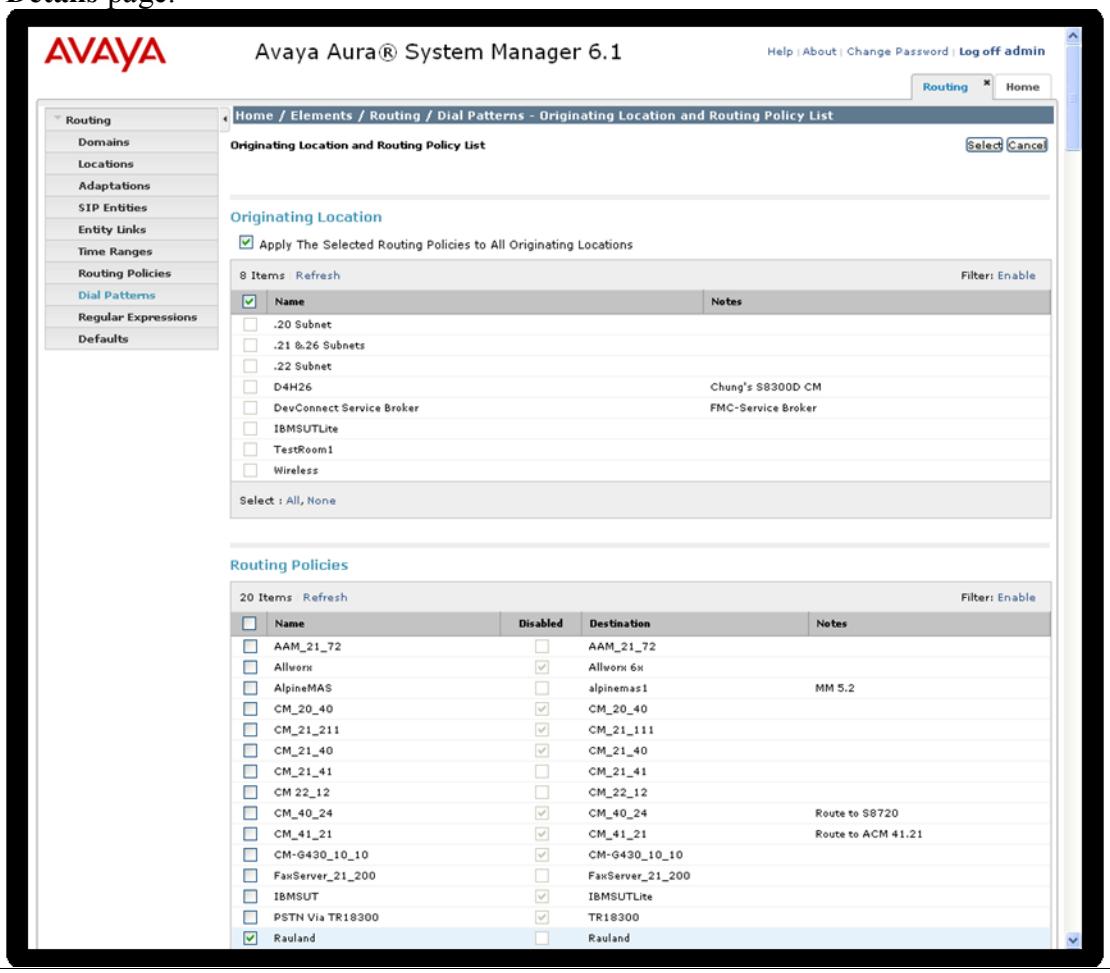


Create a Dial Pattern (Continued)

When the **Add** button is clicked on the **Originating Locations and Routing Policies** section for the **Dial Pattern Detail** page, the following will appear.

The **Originating Location** can be defined as any location that originates a SIP request. In the compliance test, location based routing was not used so the **Apply The Selected Routing Policies to All Originating Locations** option was selected.

The ***Rauland*** policy defined is Step 4 was selected in the **Routing Policies** section. Click the **Save** button (not shown) to save these changes and return to the **Dial Pattern Details** page.



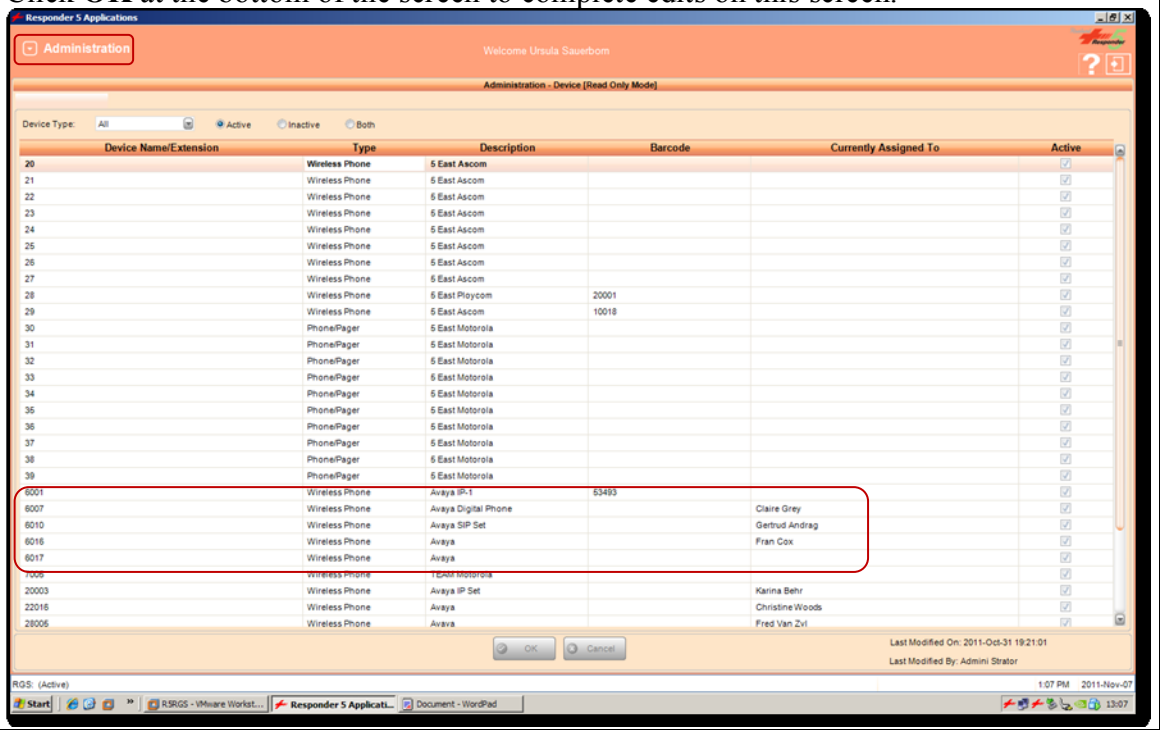
7. Configure Responder® 5

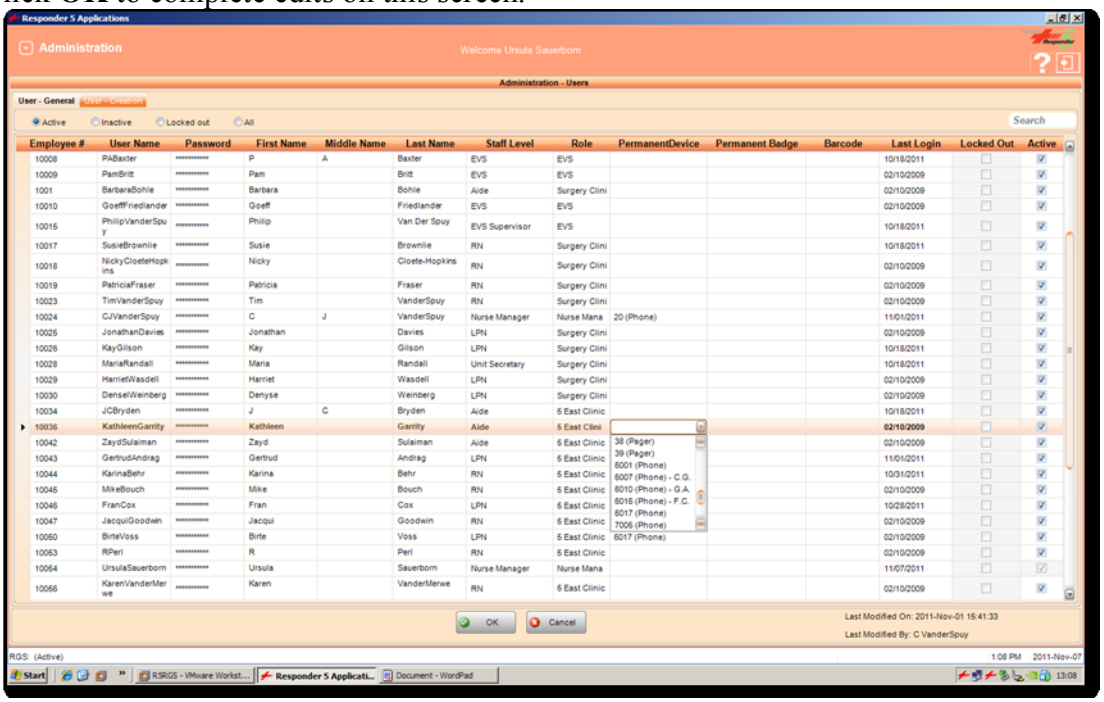
The Responder solution is typically implemented by Rauland engineers or their resale partners. When integrated with a third party SIP PBX, it is always deployed with a Brekeke SIP server which serves two purposes. First, Brekeke SIP server is commonly deployed with a variety of SIP capable PBX solutions 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.

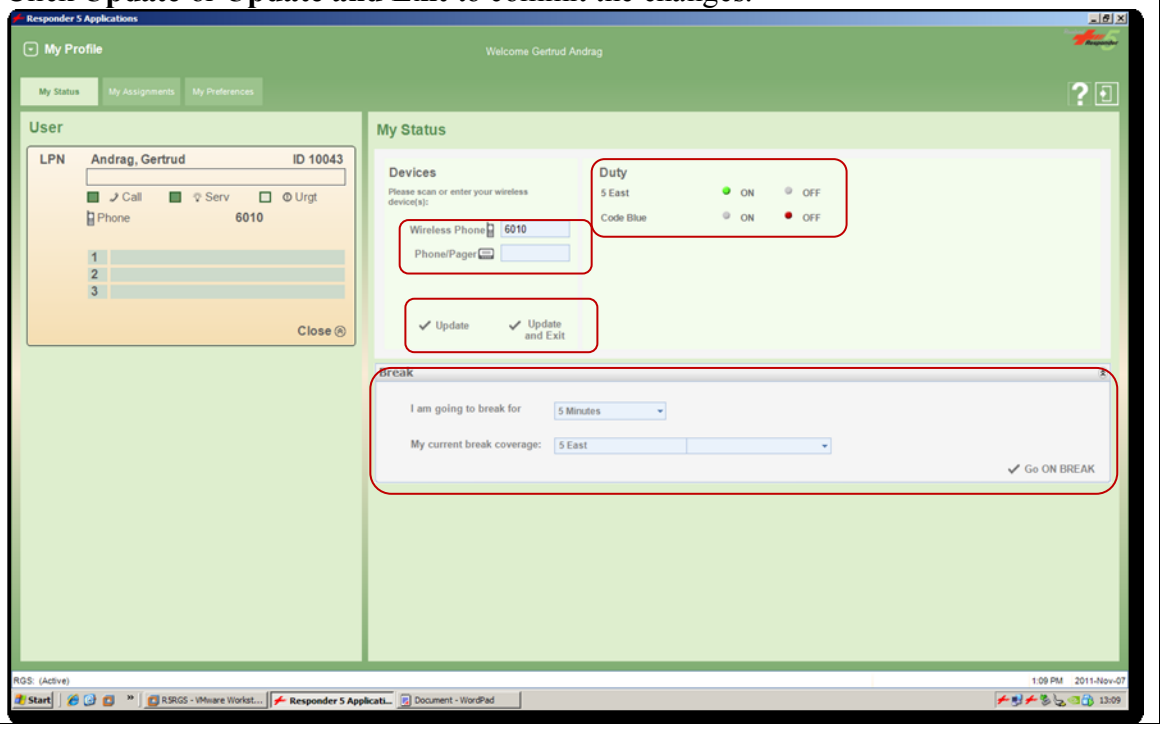
The Responder equipment will be provisioned completely by Rauland engineers based on site requirements, and will be configured to use the Brekeke SIP server for all calls destined to endpoints outside of the Responder endpoints.

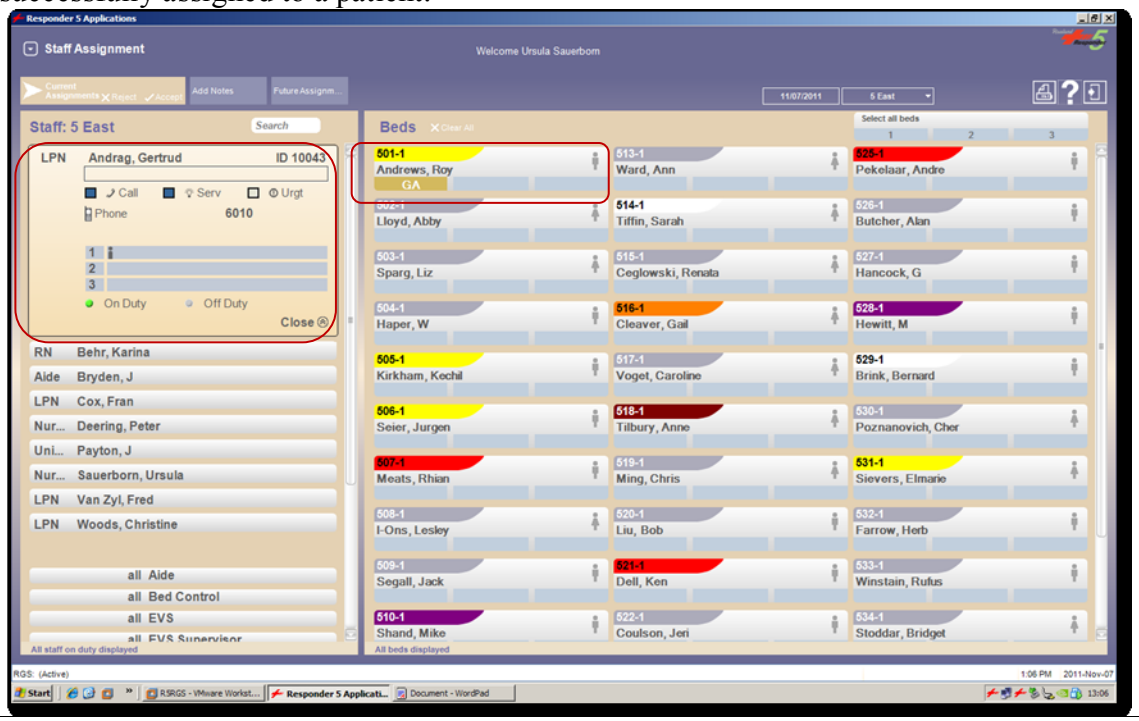
The focus of this section will be on administration of the Responder applications, and configuration of the Brekeke SIP Server to properly route SIP calls and RTP.

7.1. Responder 5Configuration Details

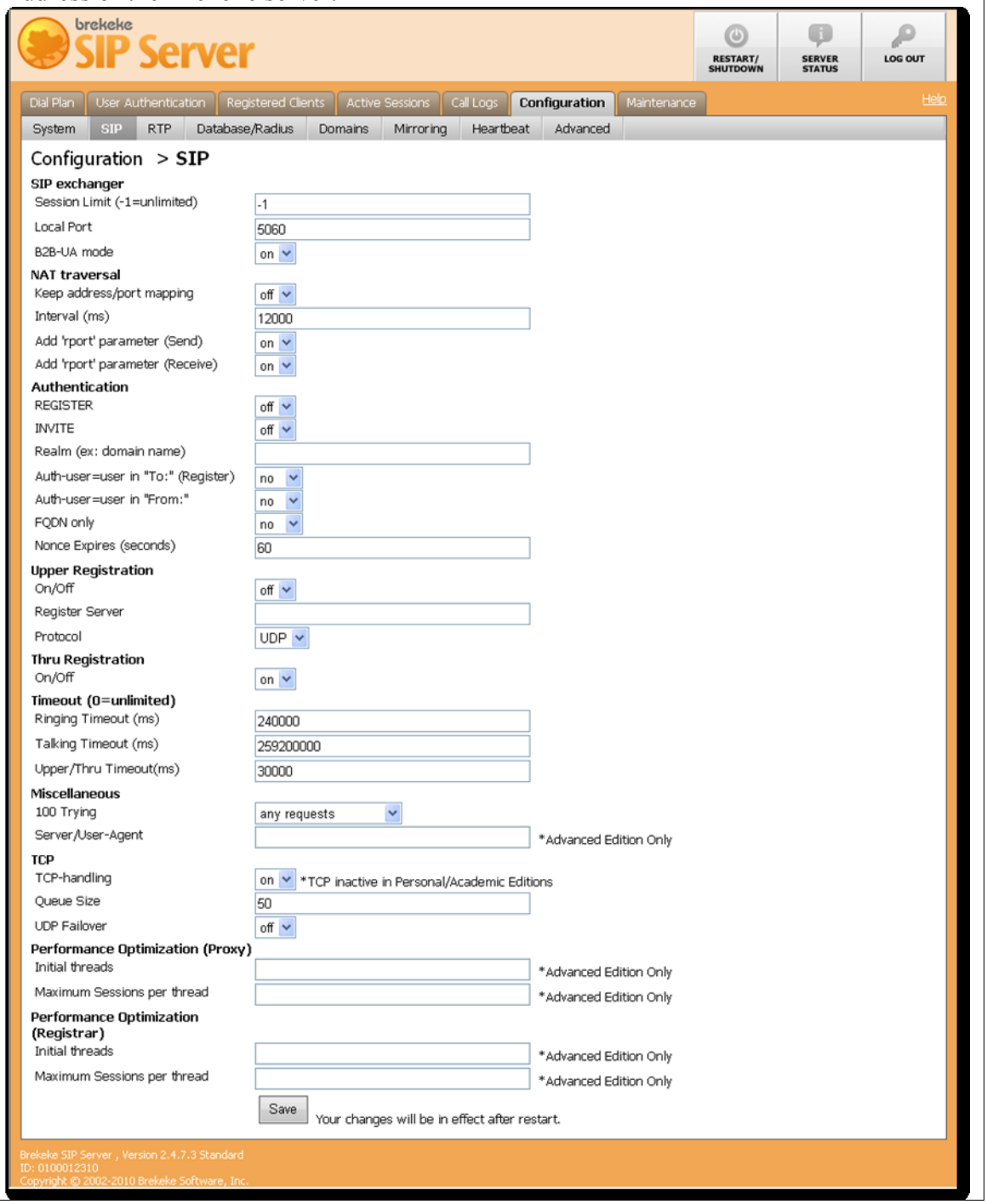
Step	Description
1.	**Configure Endpoints** Typically, hospital staff uses wireless phones to enable instant communications with staff and patient rooms. In the tested confirmation, a variety of IP and SIP wireless devices which were previously configured on Communication Manager and Session Manager 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 ***6xx*** were IP and SIP devices administered on Communication Manager and Session Manager. Click **OK** at the bottom of the screen to complete edits on this screen. 

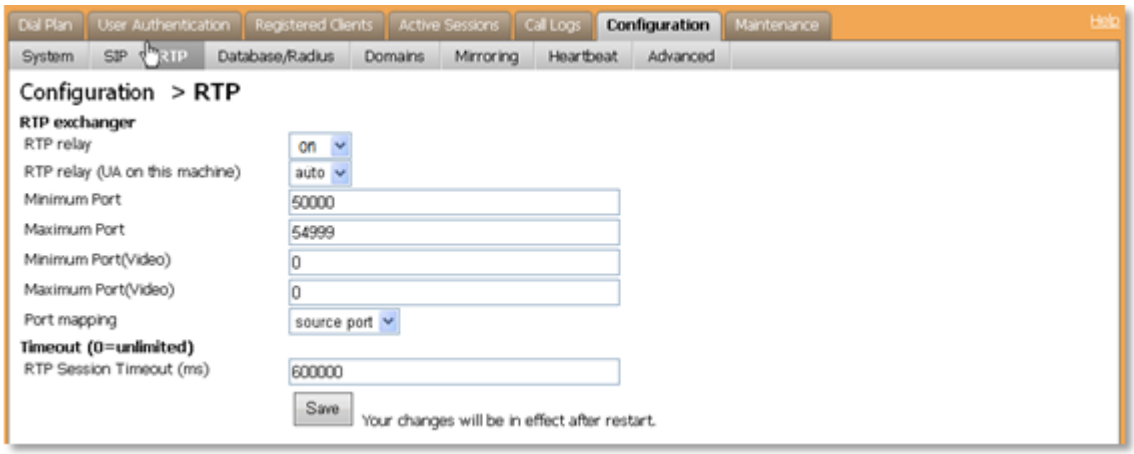
Step	Description
2.	**Assign Endpoints to Users** Select **Administration – Devices** in the upper left drop down list (not shown) to add or modify users and to assign devices to the users. This task is only necessary for statically assigned device assignments. Users who share devices are able to enter the device they are using for a shift when they login as described in **Step 3**. Users can be created or modified on the **User – Creation** 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 **User – General** tab as shown below. In the illustration below, devices were selected from a list of phones (from the list in **Step 1** above) in the **PermanentDevice** column for each user. Click **OK** to complete edits on this screen. 

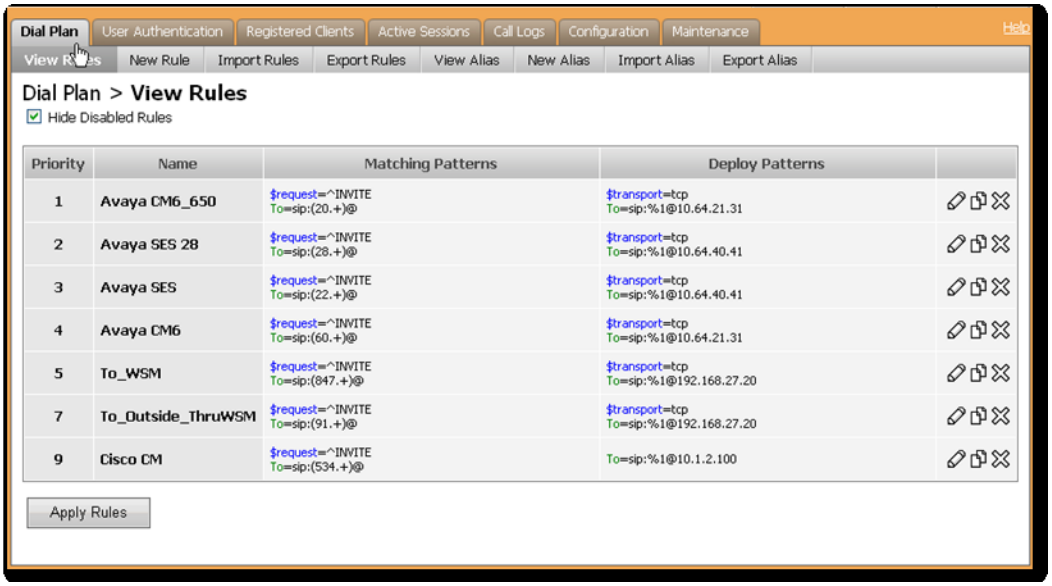
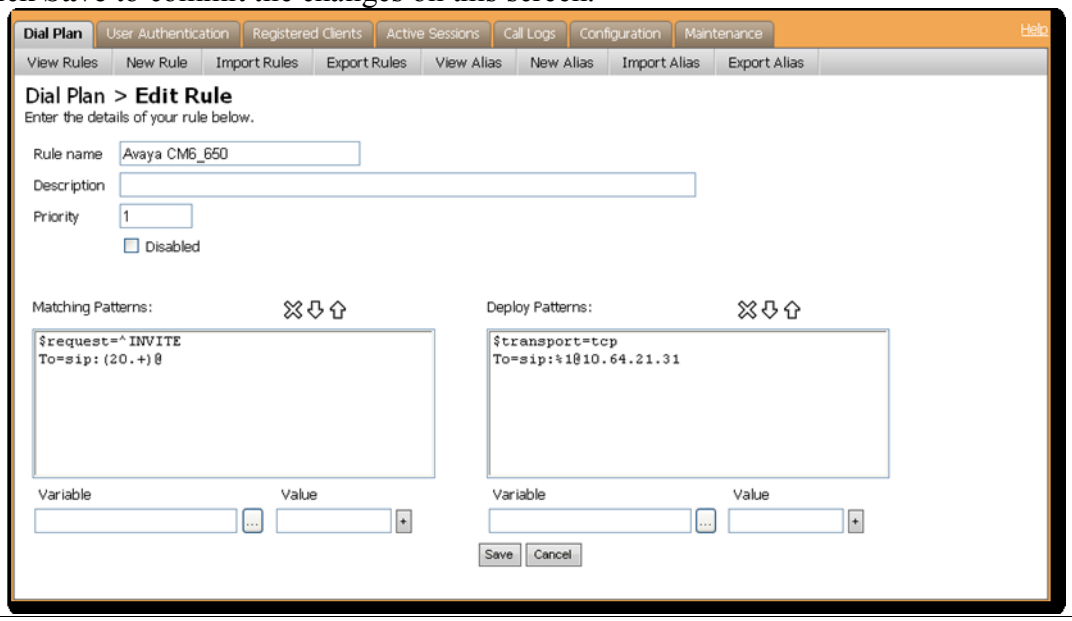
Step	Description
3.	**User Login and Device Assignment** At the beginning of a shift, or return to duty from breaks, users will scan their Hospital ID badge bar code with a scanner connected to the PC which will automatically log them in to the **My Profile** screen. From this screen, a **Wireless Phone** and/or **Pager** number can be entered, duty status update, 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. 

Step	Description
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. 

Step	Description
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.



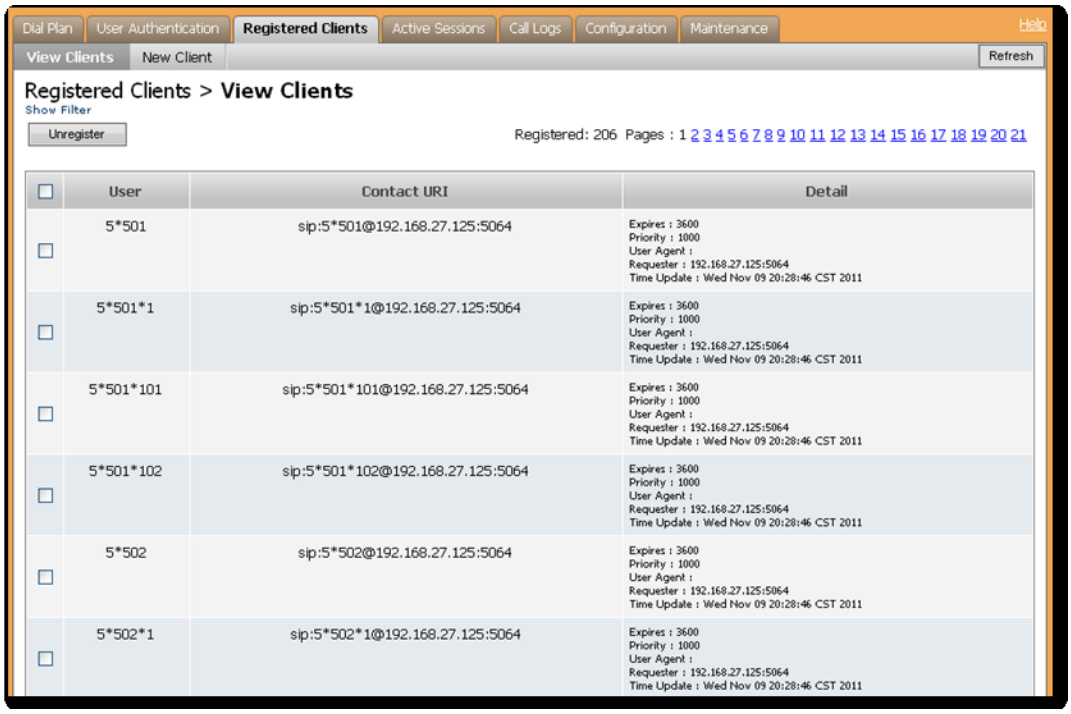
Step	Description
6.	**Configure RTP Relay settings** The tested configuration required that all media (RTP) send to and from Rauland endpoints be connected through the Brekeke SIP Server. This was required in order to overcome an incompatibility between Rauland and Avaya media servers as described in **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. 

Step	Description
7.	**Configure Dial Plan Routing rules** Several **Dial Plan** rules were used as illustrated below. For calls routing to Session Manager, the **Avaya CM6** rule was used. The other rules were used to route calls to the SIP Enablement Services 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 patters starting with **60** were routed to Session Manager at **10.64.21.31**. 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® Session Manager 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

[1] *Administering Avaya Aura™ Communication Manager*, Doc # 03-300509, Release 6.0, Issue 6.0, June 2010.

[2] *Administering Avaya Aura® Session Manager, Doc # 03-603324, Release 6.1, November 2010.*

[3] *Application Notes for Configuring Rauland-Borg Responder® 5 to Interoperate with Avaya Aura® SIP Enablement Services and Avaya Aura® Communication Manager R5.2.1.*

Rauland-Borg

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

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.