Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Rauland-Borg Responder® 5 with Avaya Aura® Session Manager and Avaya Aura® Communication Manager R7.0 – Issue 1.0

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 R7.0.

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.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

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 R7.0.

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 sold and supported by Rauland-Borg as 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 for example 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. During compliance testing only Avaya Desk phones were used.

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 Session Manager and Communication Manager.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

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.

2.2. Test Results

The objectives described in **Section 2.1** were verified with the following observation.

- 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 audio 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. A customer should ensure that adequate VoIP resources are available based on expected call traffic.
- Responder only supports G.711MU codec.

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 R7.0
- Avaya Aura® Session Manager R7.0
- Avaya Aura® System Manager R7.0
- Avaya Aura® Media Server R7.0
- Avaya G450 Media Gateway
- Various H.323 and SIP endpoints
- Brekeke SIP Server
- Rauland-Borg Responder® 5 Branch Regional Controller
- Rauland-Borg Responder® 5 Communication Endpoints

Calls routed to and from the Communication Manager used SIP trunks between the Brekeke SIP server and Session Manager, and in turn SIP trunks between Session Manager and Communication Manager.

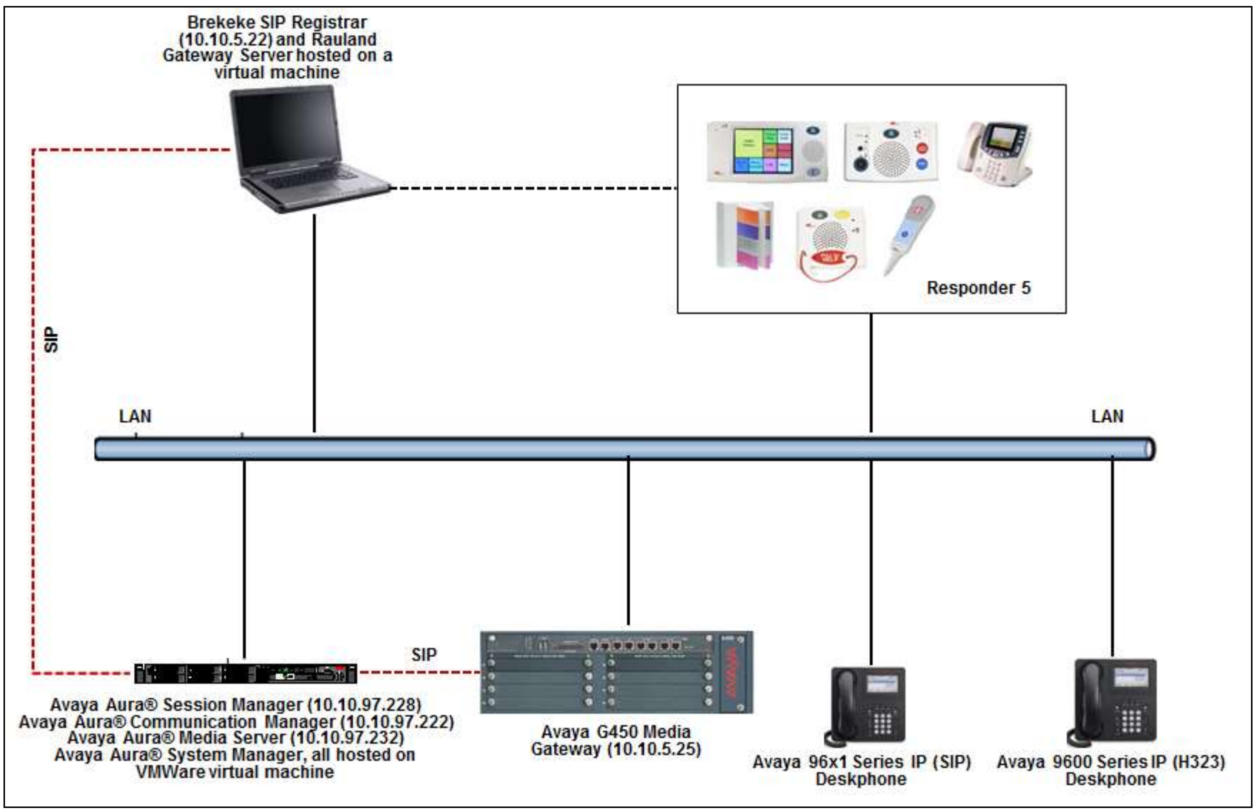


Figure 1 – Rauland-Borg Responder® 5 Compliance Test Configuration

4. Equipment and Software Validated

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

Equipment	Version
Avaya Aura® Communication Manager	7.0.0.1.0-SP1 (R017x.00.0.441.0)
Avaya Aura® Session Manager	7.0.0.0.700007
Avaya Aura® System Manager	7.0.0.0
Avaya Aura® Media Server	7.7.0.226
Avaya G450 Media Gateway	37 .19 .0 /1
Avaya IP Deskphones: 9620 (SIP) 9641 (H323)	 2.6.4 6.0.1
Rauland Nurse Call	T15 SP1
Rauland Gateway Server	T15 SP1
Rauland Apps	T15 SP1
Rauland DB	T15 SP1
Brekeke Server (Registrar)	3.3.4.4

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 5 digit 30xxx pattern. All calls routed via a 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

5.1.1. Confirm Licensing

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

```
display system-parameters customer-options                      Page   2 of
12
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 4000  10
           Maximum Concurrently Registered IP Stations: 2400  3
             Maximum Administered Remote Office Trunks: 4000  0
Maximum Concurrently Registered Remote Office Stations: 2400  0
              Maximum Concurrently Registered IP eCons: 68    0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 2400  0
                   Maximum Video Capable IP Softphones: 2400  3
                       Maximum Administered SIP Trunks: 4000  24
  Maximum Administered Ad-hoc Video Conferencing Ports: 4000  0
   Maximum Number of DS1 Boards with Echo Cancellation: 80    0
```

5.1.2. 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-VM***) and the processor Ethernet interface on Communication Manager (***procr***).

```
change node-names ip                                            Page   1 of
2
                                  IP NODE NAMES
    Name              IP Address
AVAYA-RDTT          10.10.98.71
DevvmAES            10.10.97.224
DevvmAMS            10.10.97.232
GW-G450             10.10.4.25
Loopback            10.10.97.222
SM-VM               10.10.97.228
TFTP-Server         10.10.98.72
default             0.0.0.0
procr               10.10.97.222
procr6              ::
```

5.1.3. Add SIP Signaling Group

A signaling group was added using the **add signaling group 1** command with the following settings (settings not highlighted are default):

- **Group Type**: *sip*
- **Transport Method**: *tcp*
- **IP Video:** *n*
- **Near-end Node Name**: *procr*
- **Far-end Node Name**: *SM-VM*
- **Near-end Listen Port**: *5060*
- **Far-end Listen Port**: *5060*
- **Far-end Domain**: *bvwdev.com* (Match the domain on Session Manager).
- **Direct IP-IP Audio Connections:** *n.* (Responder does not support media shuffling)
- **DTMF over IP:** *rtp-payload*

```
add signaling-group 1                                        Page   1 of   3
                                SIGNALING GROUP

 Group Number: 1             Group Type: sip
  IMS Enabled? n       Transport Method: tcp
        Q-SIP? n
     IP Video? n                                   Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
   Near-end Node Name: procr                 Far-end Node Name: SM-VM
 Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                        Far-end Network Region: 1

Far-end Domain: bvwdev.com
                                             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                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y
                                                  Alternate Route Timer(sec): 6
```

5.1.4. Add SIP Trunk Group

Using the **add trunk-group 1** command, trunk group 1 was created with the following settings (settings not highlighted are default):

- **Group Type:** *sip*
- **Group Name:** *Trunk to SM on VM*
- **TAC:** *#001*
- **Direction:** *two-way*
- **Service Type:** *tie*
- **Signaling Group:** *1*
- **Number of Members:** *24*

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

Group Number: 1                    Group Type: sip             CDR Reports: y
  Group Name: Trunk to SM on VM            COR: 1        TN: 1         TAC: #001
   Direction: two-way        Outgoing Display? y
 Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: tie                    Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 1
                                                     Number of Members: 24
```

In page 3, **Numbering Format:** *private*

```
add trunk-group 1                                                   Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                        Maintenance Tests? y



                     Numbering Format: private
                                                UUI Treatment: service-provider
```

5.1.5. Change Route Pattern

Route Pattern 1 was configured to use Trunk Group 1 for calls to Responder and Session Manager registered endpoints using the **change route-pattern 1** command with the following settings (settings not highlighted are default):

- **Pattern Name:** *To SM on VM*
- **Grp No:** *1* (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 1                                          Page   1 of   3
                    Pattern Number: 1      Pattern Name: To SM on VM
    SCCAN? n    Secure SIP? n     Used for SIP stations? n

    Grp FRL NPA Pfx Hop Toll No.  Inserted                             DCS/ IXC
    No          Mrk Lmt List Del  Digits                               QSIG
                             Dgts                                      Intw
 1: 1    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 Sub  Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
 1: y y y y y n  n            rest                               lev0-pvt  none
 2: y y y y y n  n            rest                                         none
 3: y y y y y n  n            rest                                         none
 4: y y y y y n  n            rest                                         none
 5: y y y y y n  n            rest                                         none
 6: y y y y y n  n            rest                                         none
```

5.1.6. Change AAR Analysis

Using the **change aar analysis 0** command, dialed strings of *5* digits beginning with a *30* were instructed to use the *Route Pattern 1* configured in **Section 5.1.5**. Note all Responder endpoints used a 5 digit 30xxx extension.

```
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   Num    Reqd
    2                        10   10    2          aar           n
    30                       5    5     1          aar           n
    4                        7    7     254        aar           n
    50                       5    5     1          aar           n
    54                       5    5     1          aar           n
    56                       5    5     1          aar           n
    6                        7    7     254        aar           n
    7                        7    7     254        aar           n
    8                        7    7     254        aar           n
    9                        7    7     254        aar           n
```

5.1.7. 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 end points; the Responder BRC does not support G.729. As the media gateway or media server was required to be connected to all calls, the gateways/media server were able to transcode RTP, enabling different codecs to be used for each leg of the call.

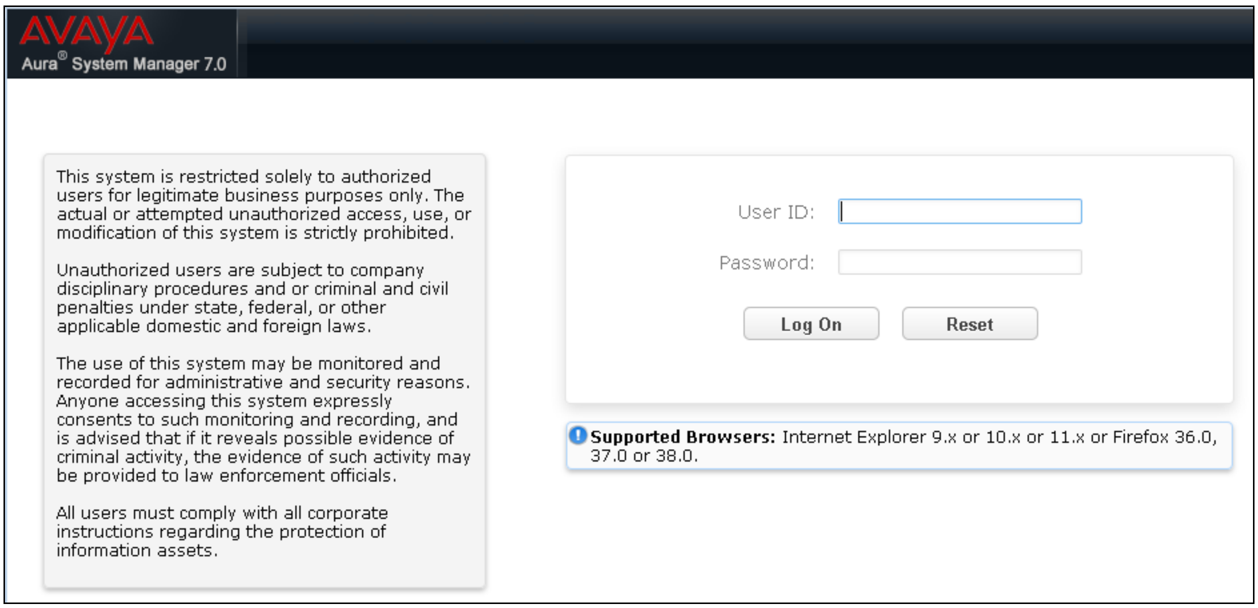
```
change ip-codec-set 1                                           Page   1 of   2

                          IP CODEC SET
    Codec Set: 1

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

6. Configure Avaya Aura® Session Manager

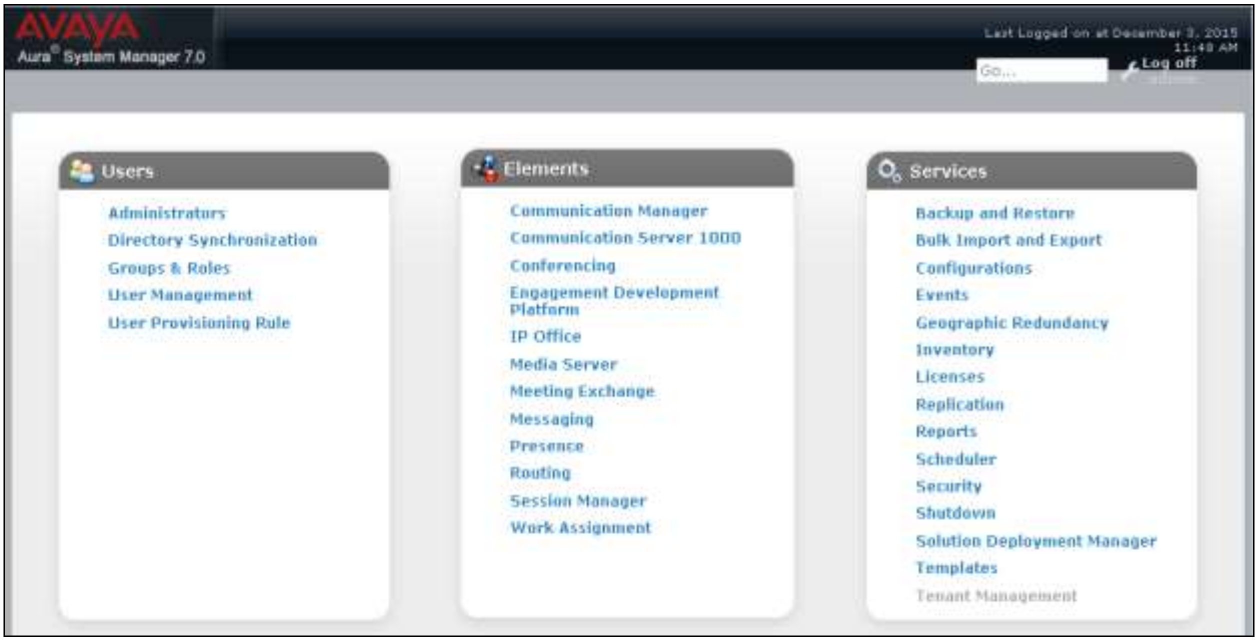
This section provides the procedures for configuring routing using Avaya Aura ® System Manager. The procedures include the following areas:

For detail configuration details of the Session Manager refer to **Section 10**.

Session Manager is administered via the Avaya Aura® 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 shown in the screen below. Click on the **Routing** link to access the Session Manager Routing Administration.



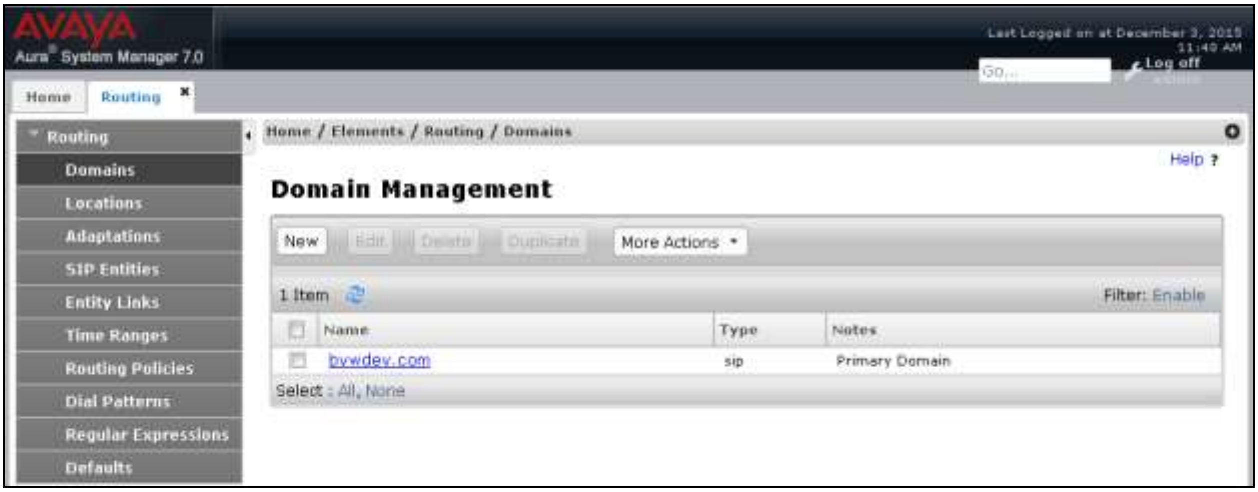
6.1. Configure Session Manager Details

Administration for the solution required the following steps:

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

6.1.1. Add a Domain

To add a domain, select **Domains** from the left hand window of the Routing screen and click on **New**. Configure a domain name and click on **Commit** (not shown) to complete adding a domain. Screen below shows a domain name of **bvwdev.com** that was added during compliance testing. Additional domains can be added in a similar fashion.



6.1.2. Add a Location

To add a location, select **Locations** from the left hand window of the Routing screen and click on **New**. Configure a location name and click on **Commit** (not shown) to complete adding a location. Screen below shows a location name of **Belleville** that was added during compliance testing. Additional locations can be added in a similar fashion.

6.1.3. Create an Adaptation Rule

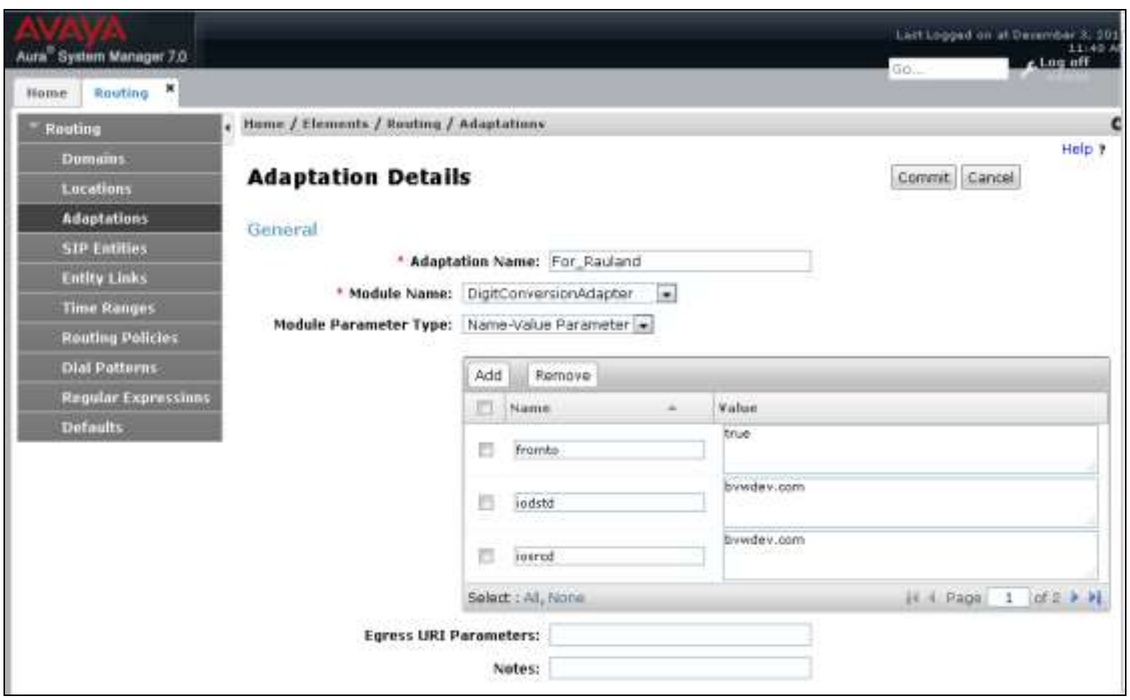
Session Manager used an Adaptation rule for two purposes. First, domains in the To and From headers were modified to reconcile differences in the ***bvwdev*** domain used on Session Manager and Communication Manager, and the IP Address of the Brekeke SIP (Rauland) registrar used as the domain on that side of the call flow. For detail configuration details of various adaptations rules refer to **Section 10**.

To add an adaptation, select **Adaptations** from the left hand window of the Routing screen. Now click on **New** (not shown) to add an Adaptation rule. Screen below shows the adaptation details used during compliance testing.

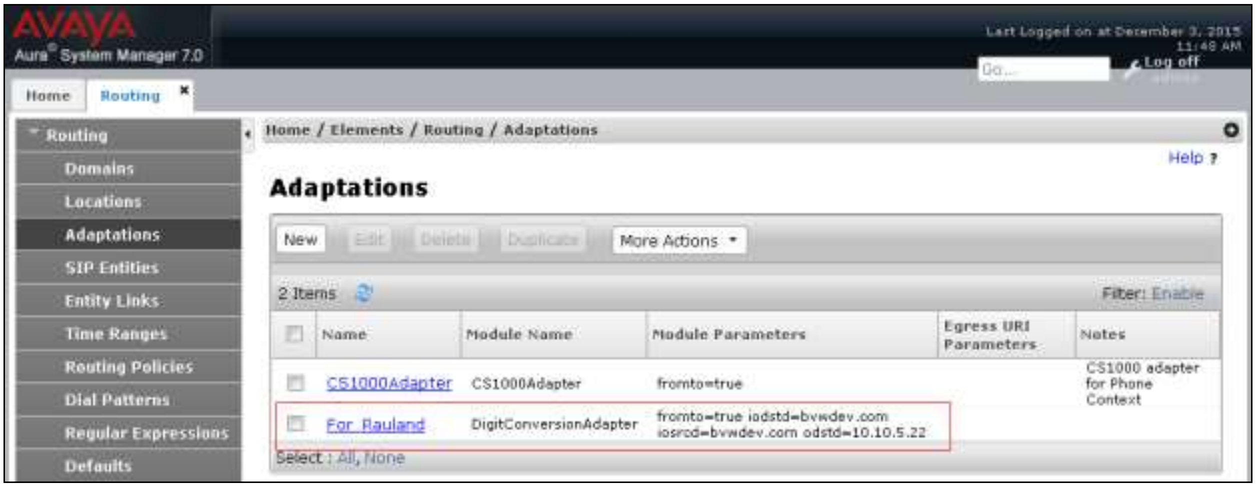
- **Adaption Name**: *For_Rauland* – Any Descriptive name.
- **Module name**: *DigitConversionAdapter* – Selected from the drop down menu.
- **Module Parameter Type**: *Name-value Parameter* – Selected from the drop down menu and values added as follows,
  fromto=true
  iodstd=bvwdev.com
  iosrcd=bvwdev.com
  odstd=10.10.5.22

This defines a rule to modify domains in SIP headers. 10.10.5.22 is the IP address of the Brekeke SIP (Rauland) registrar used during compliance testing.

Click **Commit** to save the changes, then add the adaptation rule to the SIP Entity form that will be described in **Section 6.1.4**.



Screen below shows the Adaptation rule after it was Commited.



6.1.4. Add a SIP Entity

It is assumed that user has already configured SIP entities for Session Manager and Communication Manager. This application notes only describes below the SIP entity configured for the Brekeke SIP Registrar that is being used by Responder to connect to Session Manager.

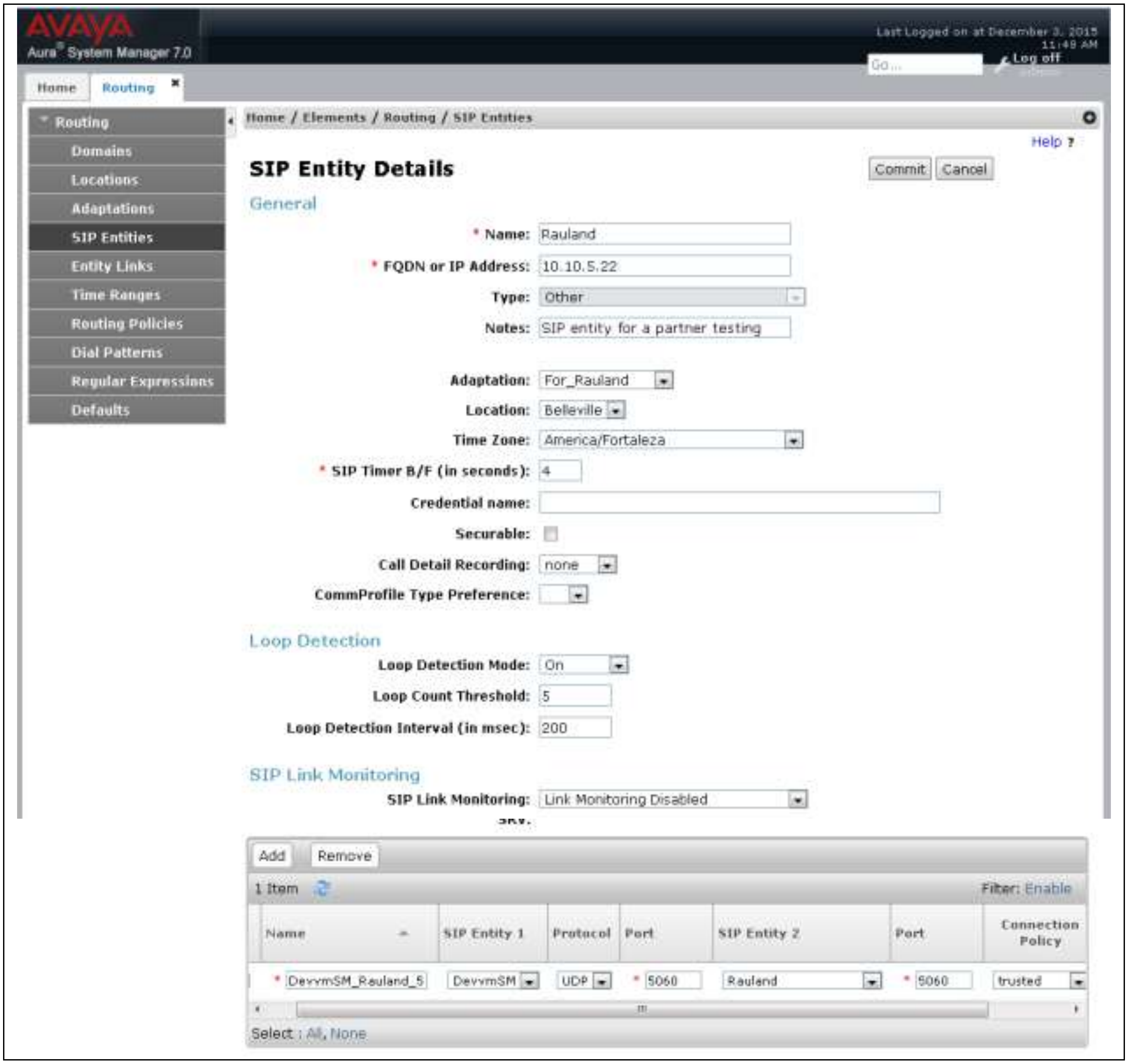
To add a SIP entity, select **SIP Entities** from the left hand window of the Routing screen and click on **New** (not shown). On the SIP Entity Details screen shown below which appears when the New button is pressed, enter the following values.

- **Name**: Enter a descriptive name for the entity (*Rauland*).
- **FQDN or IP Address:** *10.10.5.22* was the address used by the Brekeke SIP registrar during compliance testing.
- **Type:** Select *Other* from the drop down menu.
- **Notes:** Useful for quick glance identification on other screens.
- **Adaptation:** Select *For_Rauland* from the drop down menu. This adaptation rule was created in **Section 6.1.3**.
- **Location:** Select *Belleville* from the drop down menu. This was created in **Section 6.1.2**
- **SIP Link Monitoring:** Select *Link Monitoring Disabled* from the drop down menu**.** The Brekeke SIP registrar 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 **Section 6.1.5** for how the Entity Link was created.

Retain default values for other fields.

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

Note: Communication Manager SIP Entity was pre-configured and is not shown in this document as mentioned above. Communication Manager SIP Enitity was configured in similar mannar with the exeception of **Type**; it was set to *CM*. Also there was no Adaptation rule used.


AVAYA
Aura® System Manager 7.0
Last Logged on at December 3, 2015 11:49 AM
Log off
Home
Routing
Routing
Domains
Locations
Adaptations
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns
Regular Expressions
Defaults
Home / Elements / Routing / SIP Entities
Help ?
SIP Entity Details
Commit
Cancel
General
* Name: Rauland
* FQDN or IP Address: 10.10.5.22
Type: Other
Notes: SIP entity for a partner testing
Adaptation: For_Rauland
Location: Belleville
Time Zone: America/Fortaleza
* SIP Timer B/F (in seconds): 4
Credential name:
Securable:
Call Detail Recording: none
CommProfile Type Preference:
Loop Detection
Loop Detection Mode: On
Loop Count Threshold: 5
Loop Detection Interval (in msec): 200
SIP Link Monitoring
SIP Link Monitoring: Link Monitoring Disabled
Add
Remove
1 Item
Filter: Enable
Name
SIP Entity 1
Protocol
Port
SIP Entity 2
Port
Connection Policy
DevvmSM_Rauland_5
DevvmSM
UDP
5060
Rauland
5060
trusted
Select : All, None

6.1.5. Add Entity Links

It is assumed that user has already configured Entity links for Communication Manager. This application notes only describes below the Entity links configured for the Brekeke SIP registrar that is being used by Responder to connect to Session Manager.

To add an Entity Link, select **Entity Links** from the left hand window of the Routing screen and click on **New** (not shown). On the **Entity Links** screen shown below which appears when the New button is pressed, enter the following values.

- **Name**: *DevvmSM_Rauland_5060_UDP* - A Descriptive name for the Entity Link.
- **SIP Entity 1:** Select *DevvmSM* from the drop down menu **–** This is the existing Session Manager SIP Entity.
- **SIP Entity 2**: Select *Rauland* from the drop down menu – This is the newly created SIP entity in **Section 6.1.4**.
- **Protocol:** Select *UDP* from the drop down menu**.**
- **Port:** *5060* – Port 5060 is the standard listen port for the UDP SIP transport protocol.
- **Connection Policy**: Select trusted from the drop down menu.

Retain default values for other fields.

Click **Commit** to save the entries.

Note: Communication Manger SIP Entity link was pre-configured and is not shown in this document as mentioned above. Communication Manager SIP Entity was configured in similar manner with the exception of **Protocol**; it was set to *tcp*.

6.1.6. 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.

It is assumed that user has already configured routing policies for Communication Manager. This application notes only describes below the routing policy configured for the Brekeke SIP registrar that is being used by Responder to connect to Session Manager.

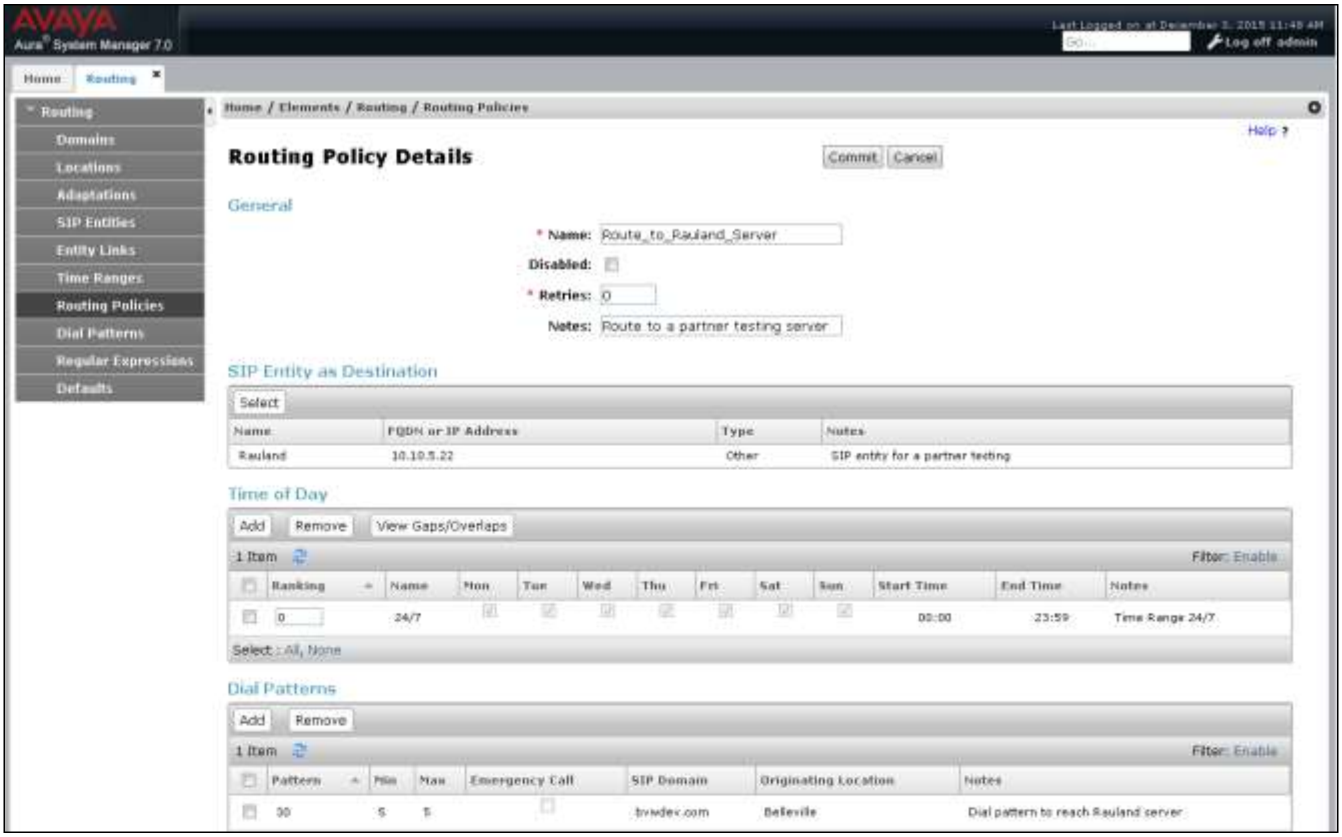
To add a routing policy, select **Routing Policies** from the left hand window of the Routing screen and click on **New** (not shown). On the **Routing Policy Details** screen shown below which appears when the New button is pressed, enter the following values.

- **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.

Retain default values for other fields.

Click **Commit** to save the entries.

Note that the **Dial Patterns** shown below was added when the **Dial Pattern** was defined in **Section 6.1.7** but is shown here for brevity.


AVAYA
Aura® System Manager 7.0
Log off admin
Home
Routing
Routing
Domains
Locations
Adaptations
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns
Regular Expressions
Defaults
Home / Elements / Routing / Routing Policies
Help ?
Routing Policy Details
Commit
Cancel
General
* Name: Route_to_Rauland_Server
Disabled:
* Retries: 0
Notes: Route to a partner testing server
SIP Entity as Destination
Select
Name
FQDN or IP Address
Type
Notes
Rauland
10.10.5.22
Other
SIP entity for a partner testing
Time of Day
Add
Remove
View Gaps/Overlaps
1 Item
Filter: Enable
Ranking
Name
Mon
Tue
Wed
Thu
Fri
Sat
Sun
Start Time
End Time
Notes
0
24/7
00:00
23:59
Time Range 24/7
Select : All, None
Dial Patterns
Add
Remove
1 Item
Filter: Enable
Pattern
Min
Max
Emergency Call
SIP Domain
Originating Location
Notes
30
5
5
bvwdev.com
Belleville
Dial pattern to reach Rauland server

6.1.7. Create a Dial Pattern

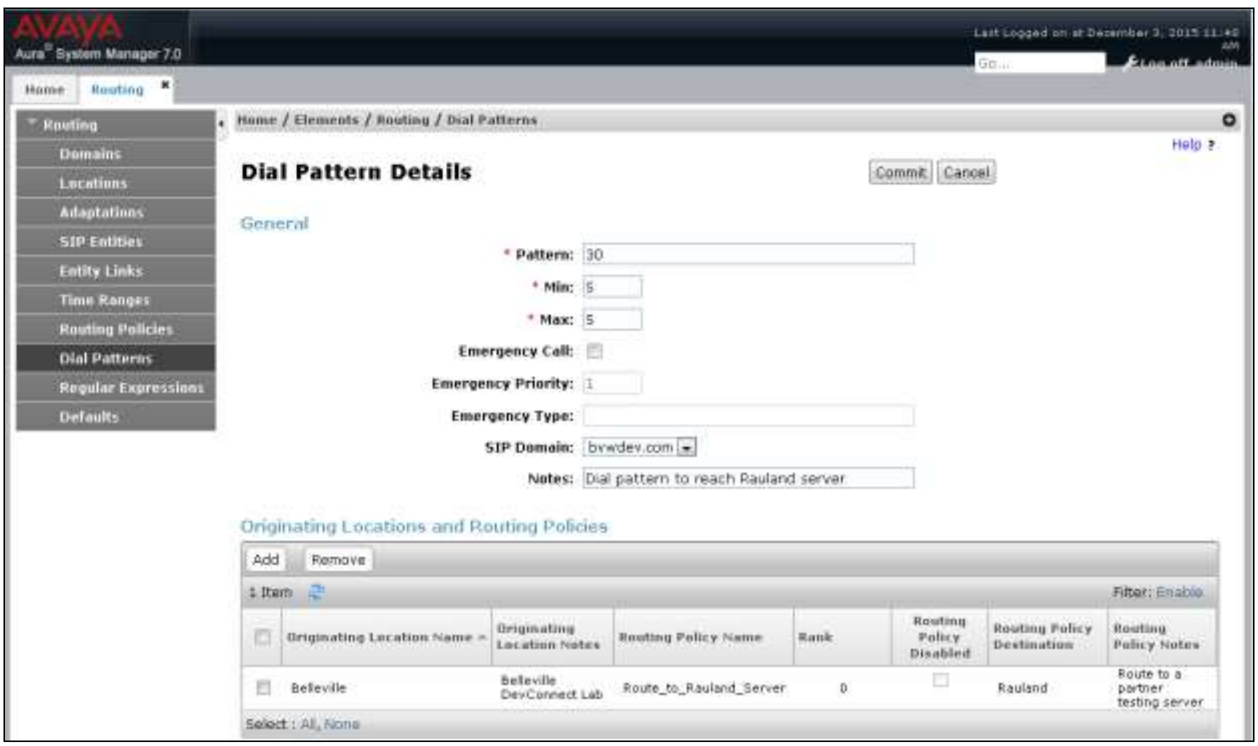
It is assumed that user has already configured dial pattern for Communication Manager. This application notes only describes below the dial pattern configured for the Brekeke SIP Registrar that is being used by Responder to connect to Session Manager.

To add a dial pattern, select **Dial Patterns** from the left hand window of the Routing screen and click on **New** (not shown). On the **Dial Pattern Details** screen shown below which appears when the New button is pressed, enter the following values.

- **Pattern:** *30* – Pilot number to reach the Rauland was defined as 30xxx during compliance testing.
- **Min and Max**: *5* – The number of digits in the dialed number to match.
- **SIP Domain**: Select *bvwdev.com* from the drop down menu – The SIP Domain was configured in **Section 6.1.1**.
- **Originating Locations and Routing Policies:** See the next page for details of this step.

Retain default values for other fields.

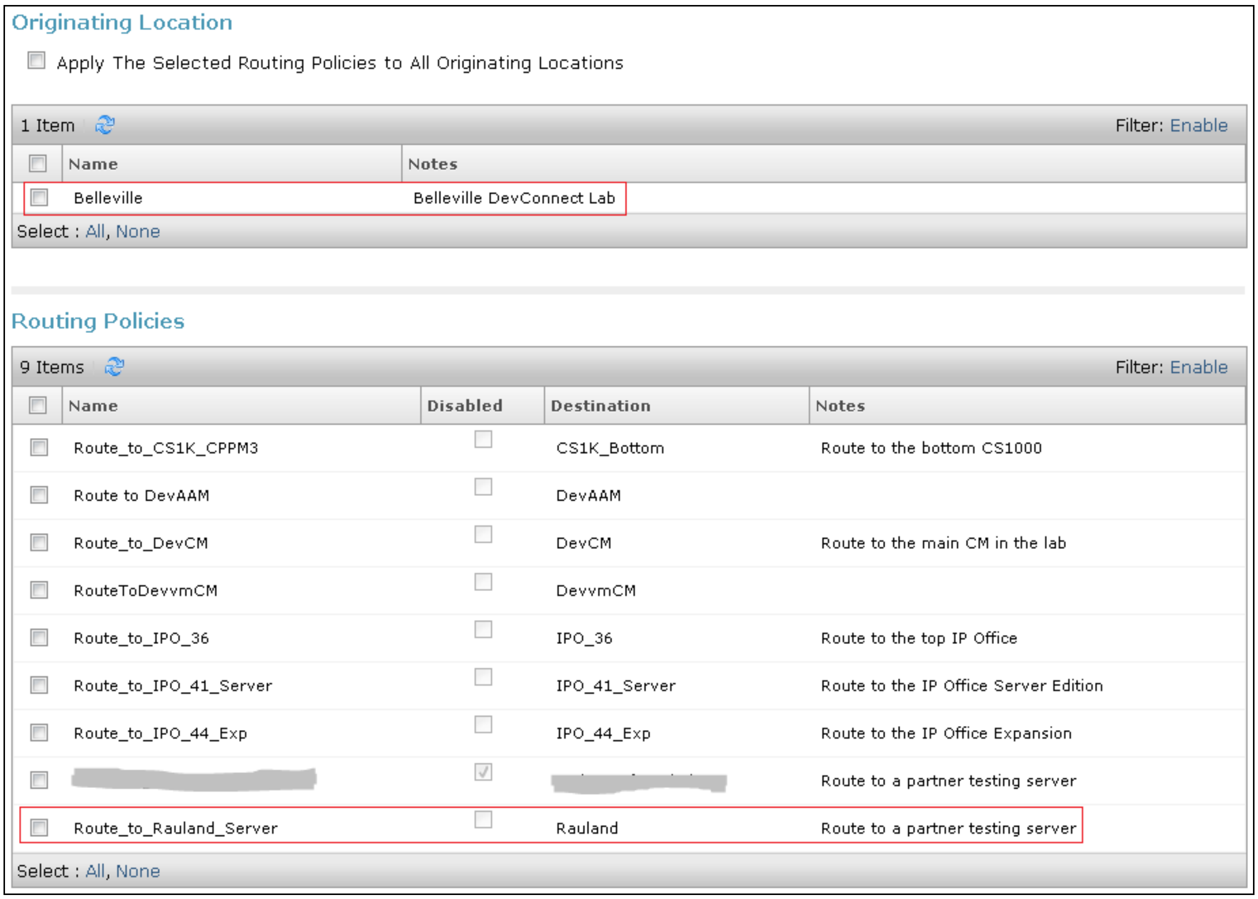
Click on the **Commit** button to save the entries after the step on the following page is completed.



When the **Add** button is clicked on the **Originating Locations and Routing Policies** section for the **Dial Pattern Details** page, the screen shown below will appear.

The **Originating Location** can be defined as any location that originates a SIP request. In the compliance test, the location **Belleville** was used and therefore this option was selected.
The *Route_To_Rauland_Server* policy defined in **Section 6.1.6** 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 registrar which serves two purposes. First, Brekeke SIP registrar 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 registrar 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

Administration for the solution required the following steps:

- Configure Endpoints
- Assign Endpoints to User
- User Login and Device Assignment
- Assign Staff to Patient Rooms

7.1.1. Configure Endpoints

Typically, hospital staff use wireless phones to enable instant communications with staff and patient rooms. In the tested confirmation, a variety of H.323 and SIP wireless devices which were previously configured on Communication 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 **Device Name/Extension**, **Type**, and a **Description**. The illustration below shows a number of devices used in the test environment, extensions *56xxx* were H.323 and SIP devices administered on Communication Manager.

Click **OK** at the bottom of the screen to complete edits on this screen.

7.1.2. Assign Endpoints to User

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 **Section 7.1.3**.

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.

Click **OK** to complete edits on this screen.

7.1.3. 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.

7.1.4. 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, *56201* is assigned to room like *501-1* by clicking on the Staff name in the left column, then clicking on the assignment space below the patient name. The staff member’s initials will appear as below when the staff member has been successfully assigned to a patient.

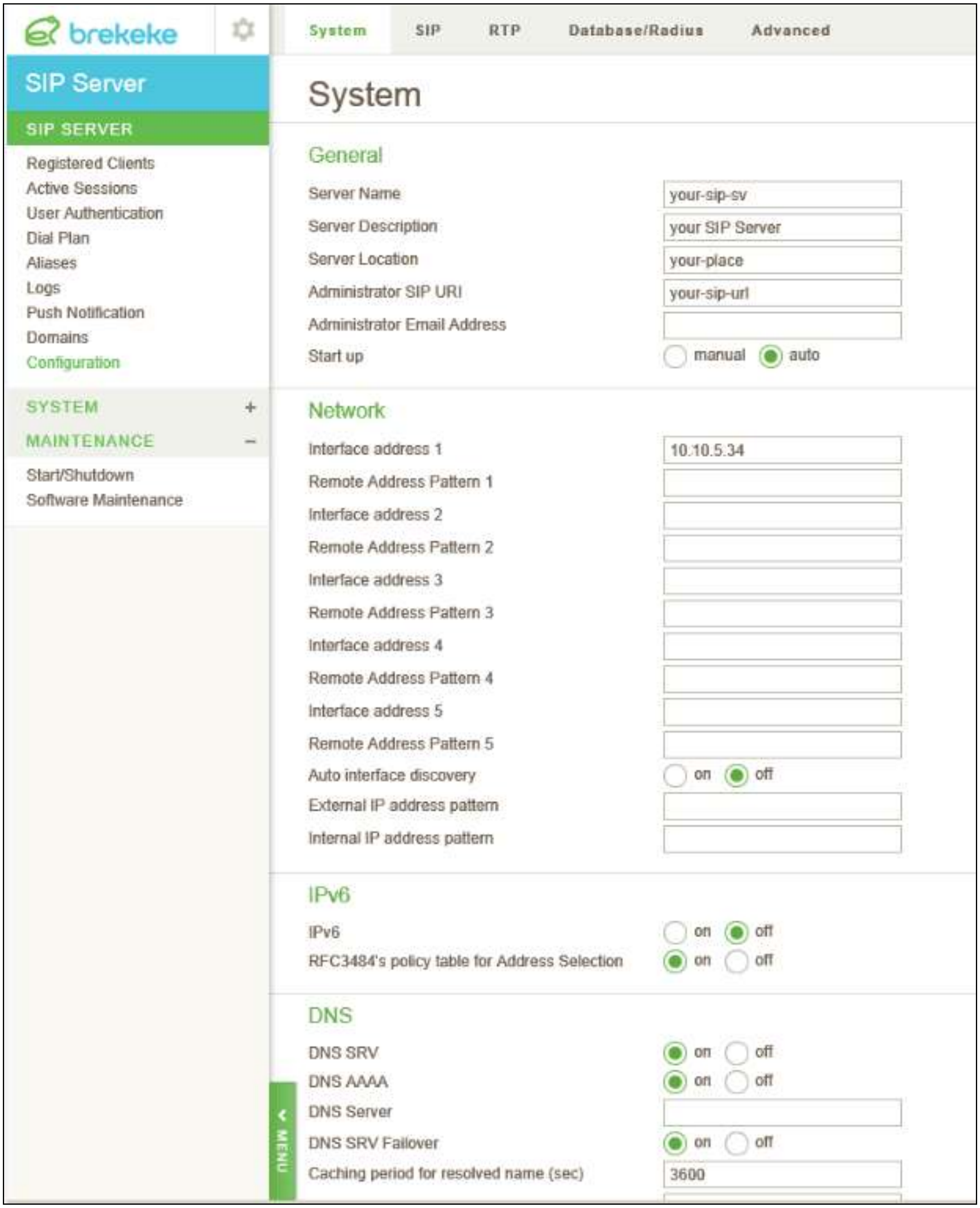
7.2. Configure Brekeke SIP Registrar

All administration is performed via web browser by navigating to the hostname or IP Address of the Brekeke server. Administration for the solution required the following steps:

- Configure SIP Server System Tab
- Configure SIP Server SIP Tab
- Configure SIP Server RTP Tab
- Configure Dial Plan Routing Rules

7.2.1. Configure SIP Server System Tab

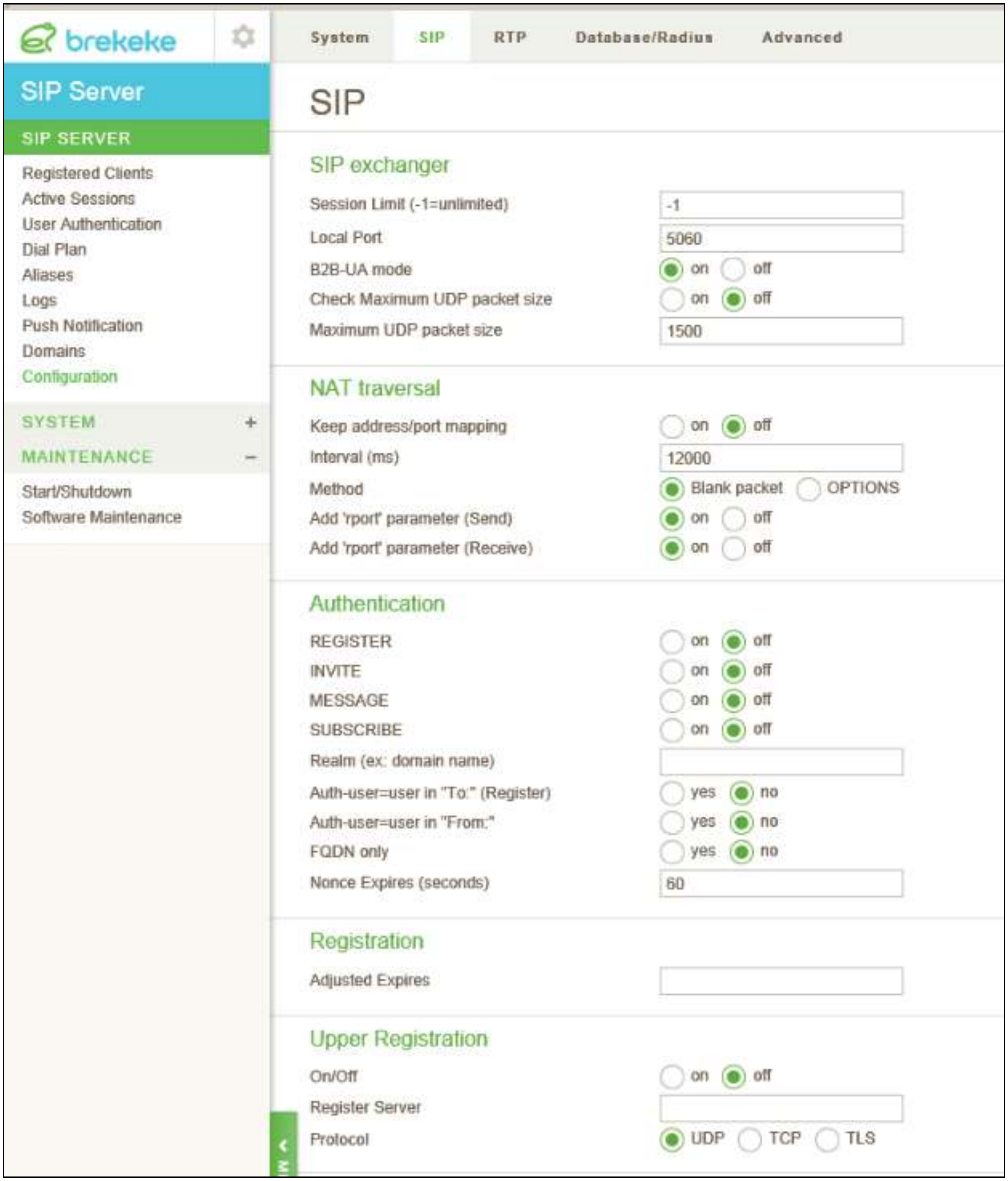
The following system properties were pre-configured for the test environment.

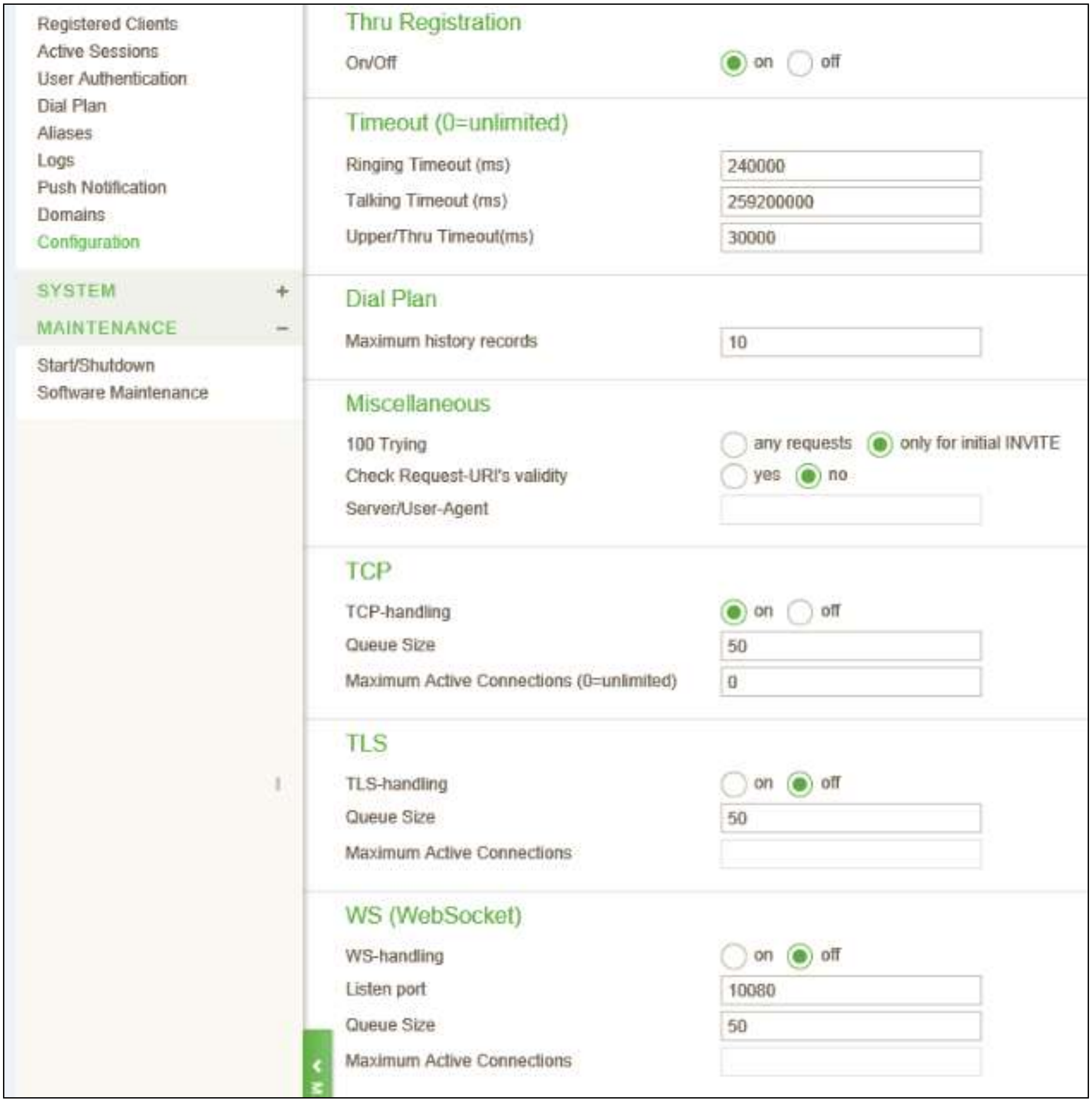


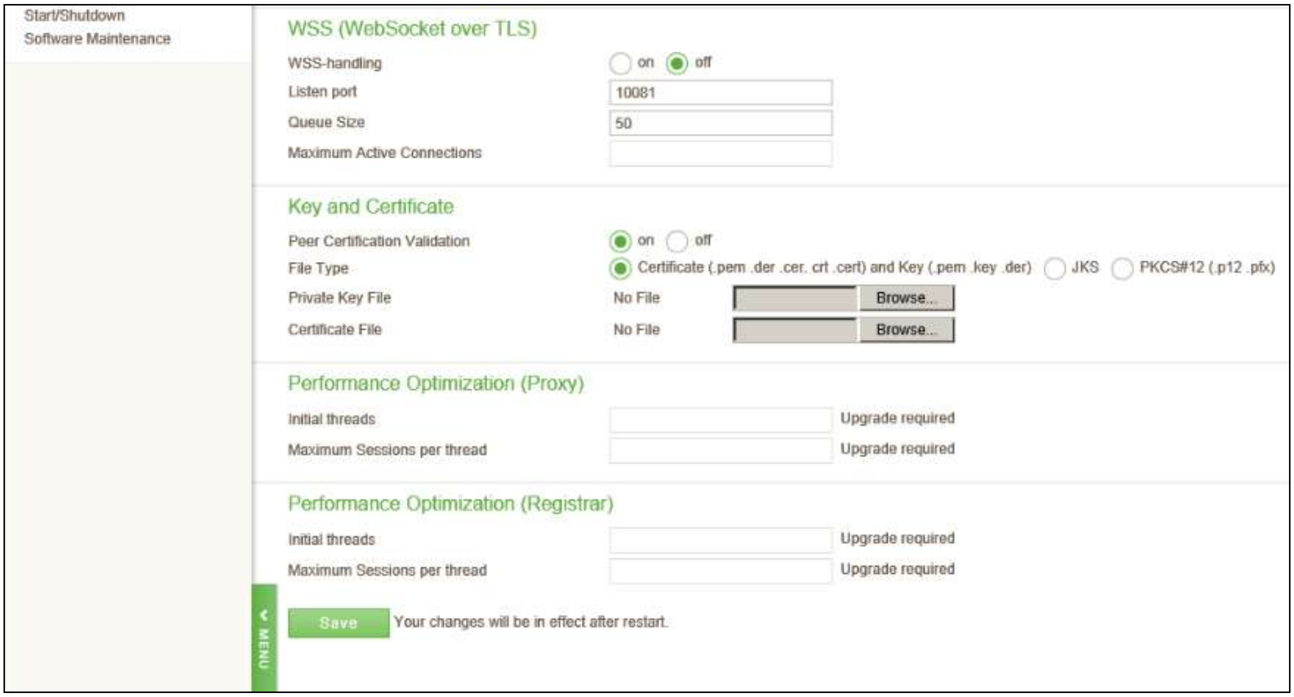

Caching period for unknown name (sec)
600
Caching period for error (sec)
10
UPnP
Enable/Disable
enable
disable
Default router IP address
Cache size
24
Cache period (sec,0=disable)
86400
Refresh Interval (sec,0=disable)
30
Java
Java VM arguments
MENU
Save
Your changes will be in effect after restart.

7.2.2. Configure SIP Server SIP Tab

The following sip properties were pre-configured for the test environment. Ensure that **B2B-UA mode** is set to *on.*

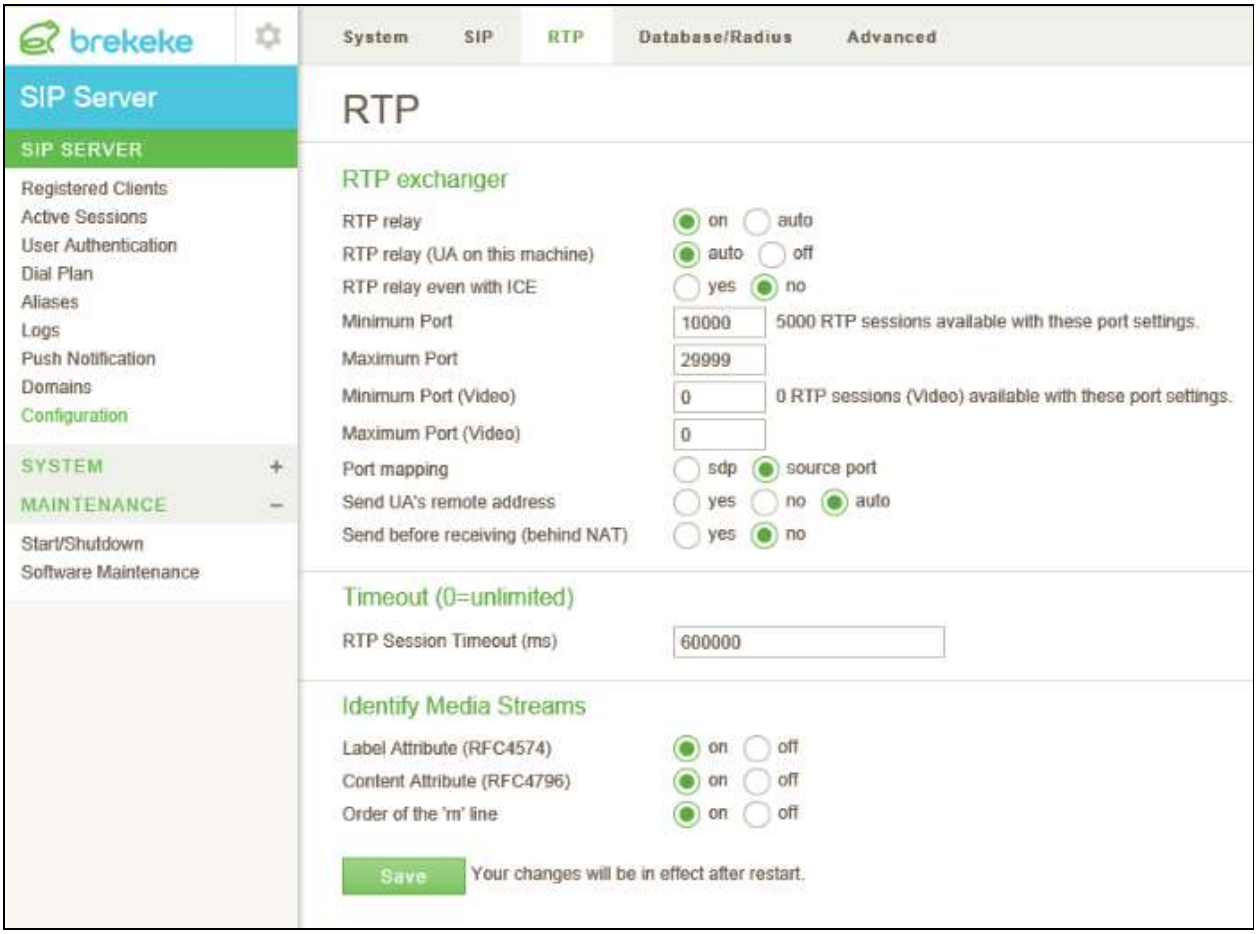



Registered Clients
Active Sessions
User Authentication
Dial Plan
Aliases
Logs
Push Notification
Domains
Configuration
SYSTEM
MAINTENANCE
Start/Shutdown
Software Maintenance
Thru Registration
On/Off
on
off
Timeout (0=unlimited)
Ringing Timeout (ms)
240000
Talking Timeout (ms)
259200000
Upper/Thru Timeout(ms)
30000
Dial Plan
Maximum history records
10
Miscellaneous
100 Trying
any requests
only for initial INVITE
Check Request-URI's validity
yes
no
Server/User-Agent
TCP
TCP-handling
on
off
Queue Size
50
Maximum Active Connections (0=unlimited)
0
TLS
TLS-handling
on
off
Queue Size
50
Maximum Active Connections
WS (WebSocket)
WS-handling
on
off
Listen port
10080
Queue Size
50
Maximum Active Connections


Start/Shutdown
Software Maintenance
WSS (WebSocket over TLS)
WSS-handling
on
off
Listen port
10081
Queue Size
50
Maximum Active Connections
Key and Certificate
Peer Certification Validation
on
off
File Type
Certificate (.pem .der .cer. crt .cert) and Key (.pem .key .der)
JKS
PKCS#12 (.p12 .pfx)
Private Key File
No File
Browse...
Certificate File
No File
Browse...
Performance Optimization (Proxy)
Initial threads
Upgrade required
Maximum Sessions per thread
Upgrade required
Performance Optimization (Registrar)
Initial threads
Upgrade required
Maximum Sessions per thread
Upgrade required
MENU
Save
Your changes will be in effect after restart.

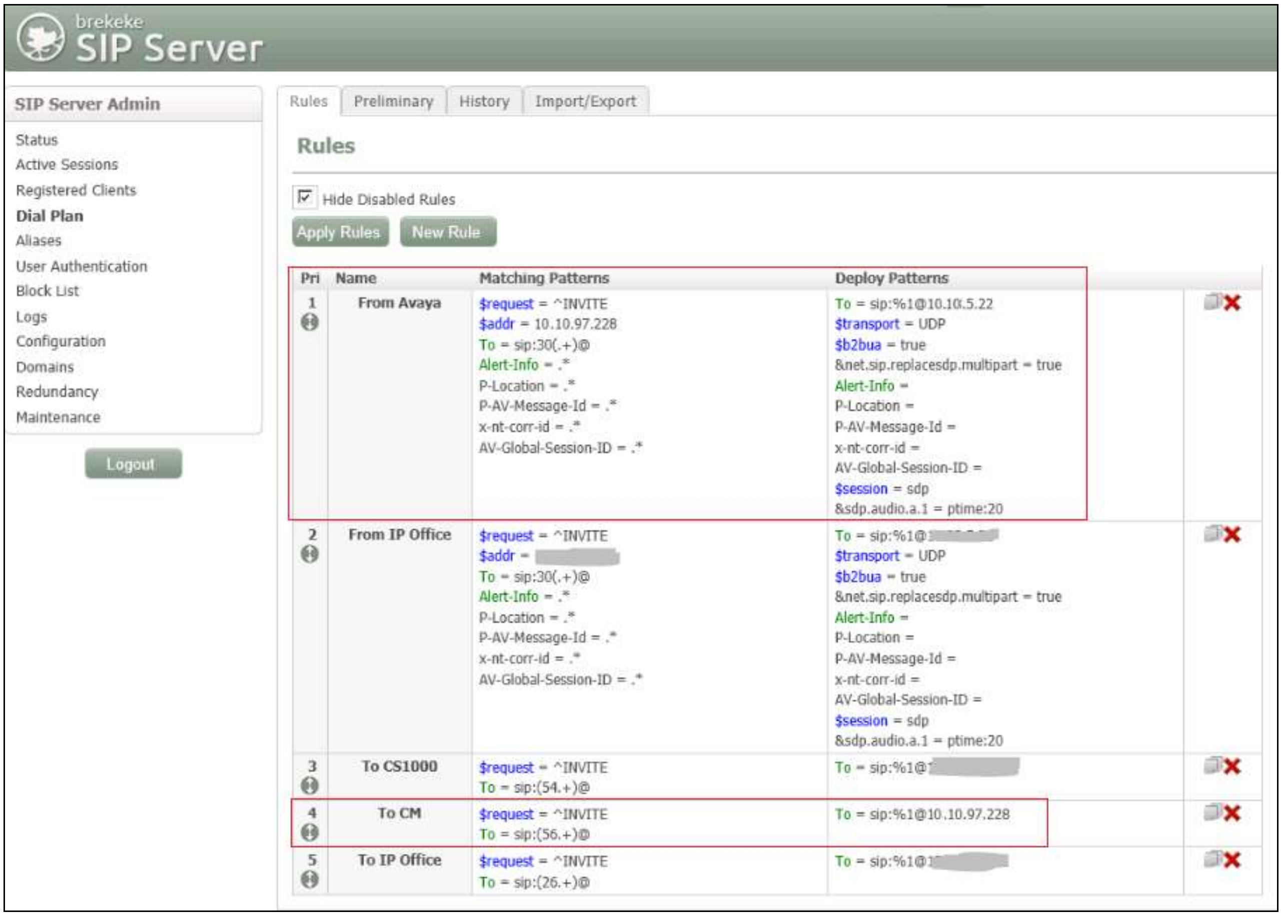
7.2.3. Configure SIP Server RTP Tab

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.



7.2.4. Configure Dial Plan Routing Rules

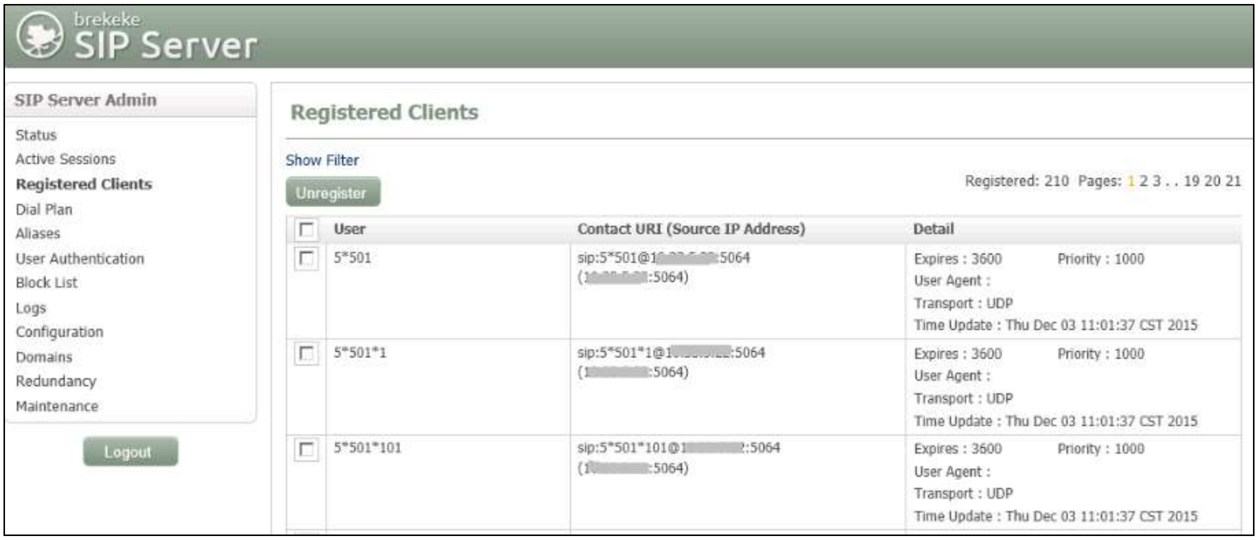
Dial Plan rules that was used is illustrated below. For calls routing from Session Manager, the **From Avaya** rule was used. For calls routing to Communication Manager, the **To CM** rule was used.



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.

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® Communication Manager via Avaya Aura® Session Manager using a Brekeke SIP Server as a SIP registrar and Proxy for the Responder 5 side of the solution.

All feature functionality test cases described in **Section 2.1** were passed with the observations pointed in **Section 2.2**.

10. Additional References

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

Avaya

1. *Implementing Avaya Aura® Session Manager* Document ID 03-603473.
2. *Administering Avaya Aura® Session Manager*, Doc ID 03-603324.
3. *Deploying Avaya Aura® System Manager*, Release 7.0.
4. *Administering Avaya Aura® System Manager for Release 7.0*, Release 7.0.
5. *Quick Start Guide to Using the Avaya Aura® Media Server with Avaya Aura® Communication Manager*.
6. *Deploying and Updating Avaya Aura® Media Server Appliance*, Release 7.7.
7. *Administering Avaya Aura® Communication Manager*, Release 7.0, 03-300509.
8. *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 7.0, 555-245-205.

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.