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.
    - 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 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].

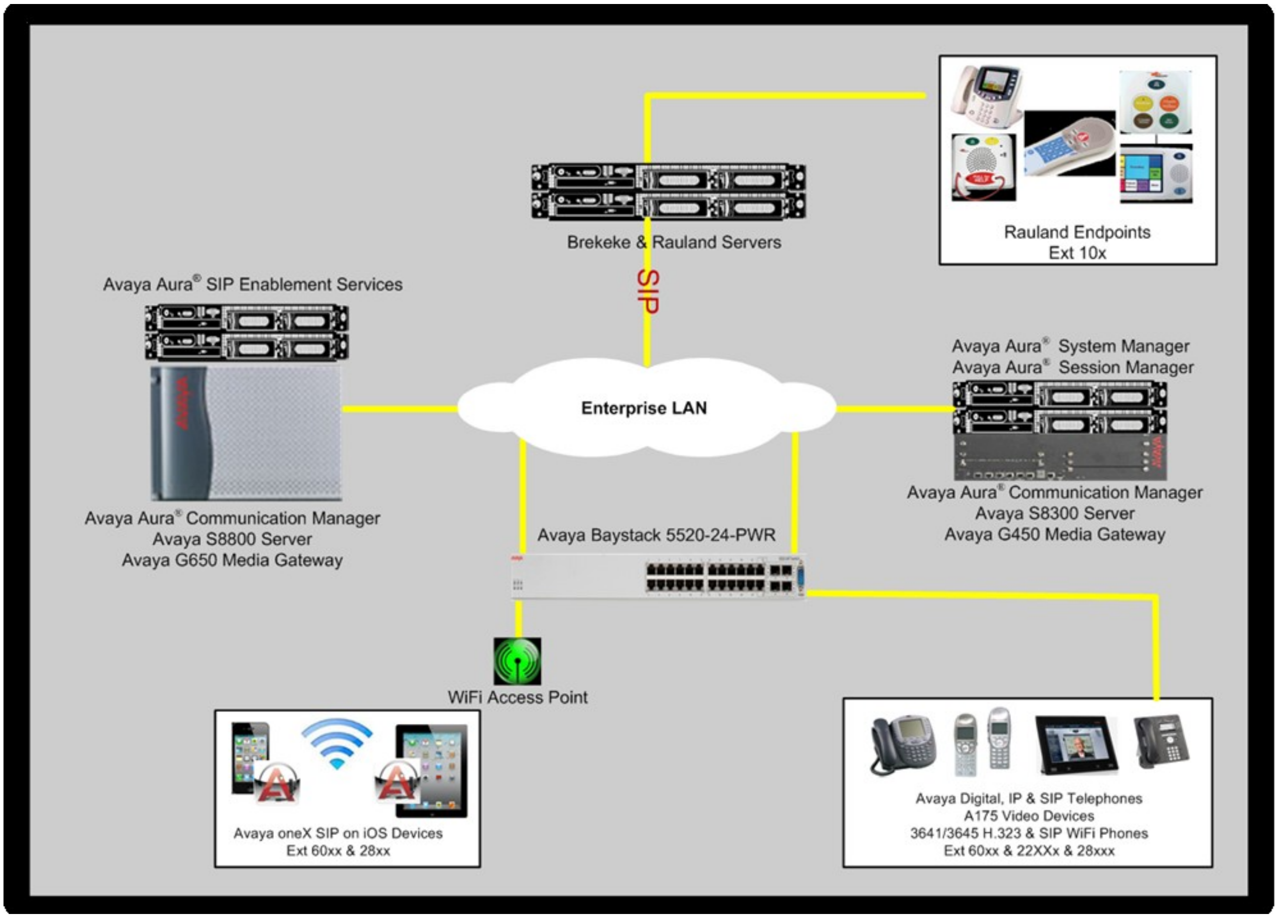

Rauland Endpoints
Ext 10x
Brekeke & Rauland Servers
SIP
Avaya Aura® SIP Enablement Services
Avaya Aura® System Manager
Avaya Aura® Session Manager
Enterprise LAN
Avaya Aura® Communication Manager
Avaya S8800 Server
Avaya G650 Media Gateway
Avaya Aura® Communication Manager
Avaya S8300 Server
Avaya G450 Media Gateway
Avaya Baystack 5520-24-PWR
WiFi Access Point
Avaya oneX SIP on iOS Devices
Ext 60xx & 28xx
Avaya Digital, IP & SIP Telephones
A175 Video Devices
3641/3645 H.323 & SIP WiFi Phones
Ext 60xx & 22XXx & 28xxx

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 G650 Media Gateway	Avaya Aura® Communication Manager R5.2.1 SP9
Avaya S8800 Server	Avaya Aura® SIP Enablement Services R5.2.1 SP4
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 gateways	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 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

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**

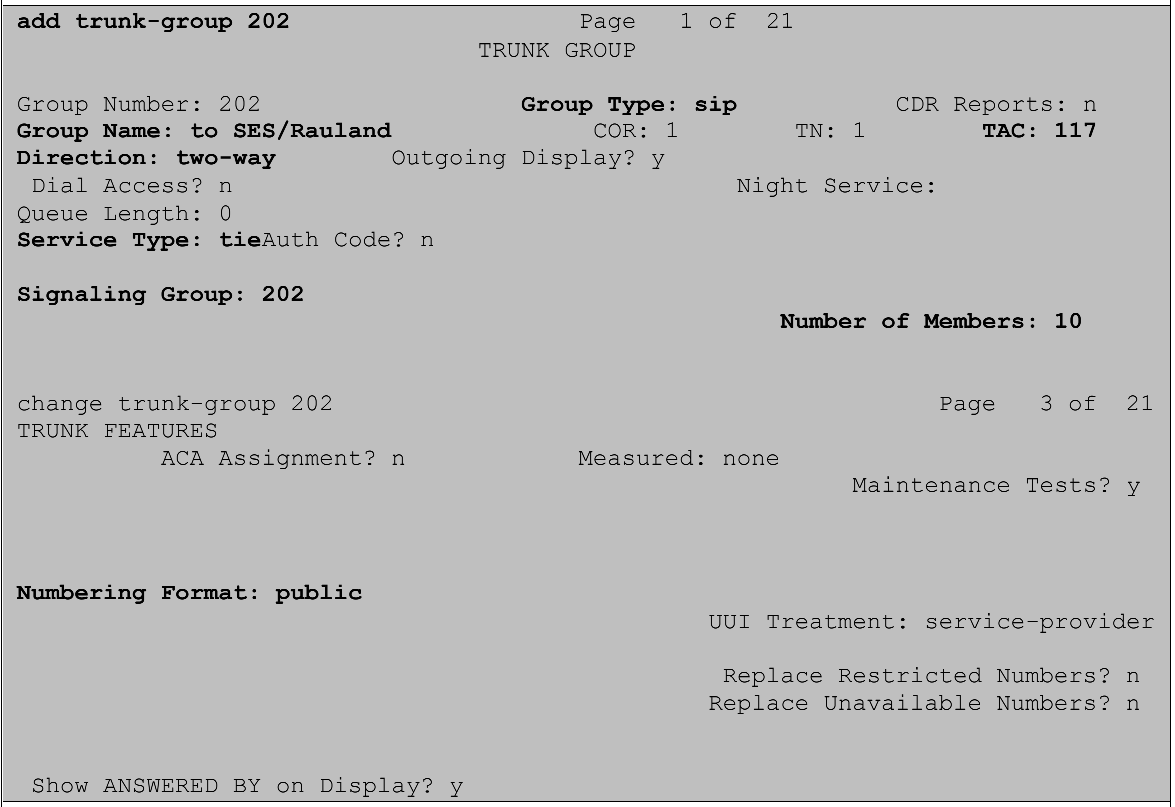
Communication Manager uses the node-names ip table as a host lookup table. Host names used in subsequent steps will refer to these. Using the **change node-names ip** command, entries were added for SIP Enablement Services (***SES***) and the local CLAN address (***CLAN***).

```
change node-names ip                                              Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
CLAN                10.64.40.24
SES10.64.40.41
```

Step	Description
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-endNode Name**:***CLAN*** **Far-end Node Name**:***SES*** **Near-endListen Port**:***5060*** **Far-endListen Port**:***5060*** **Far-end Domain**:***blank*** (enable all domains). **Direct IP-IP Audio Connections:*n.***(Responder does not support media shuffling).

```
add signaling-group 202Page   1 of   1
                                SIGNALING GROUP

Group Number: 202             Group Type: sip
                         Transport Method: tcp
  IMS Enabled? n





   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-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 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
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: tieAuth Code? n

Signaling Group: 202
                                                     Number of Members: 10


change 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 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).

```
change route-pattern 202        Page   1 of   3
                    Pattern Number: 202 Pattern Name: Rauland
                             SCCAN? n     Secure SIP? n
Grp FRL NPA Pfx Hop Toll No.  Inserted                           DCS/ IXC
No MrkLmt List Del  Digits                              QSIG
DgtsIntw
 1: 202  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
```

Step	Description
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.

```
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
    2                     2    2     202       aar         n
5                     3    3     202       aar         n
```

Step	Description
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.

```
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
```

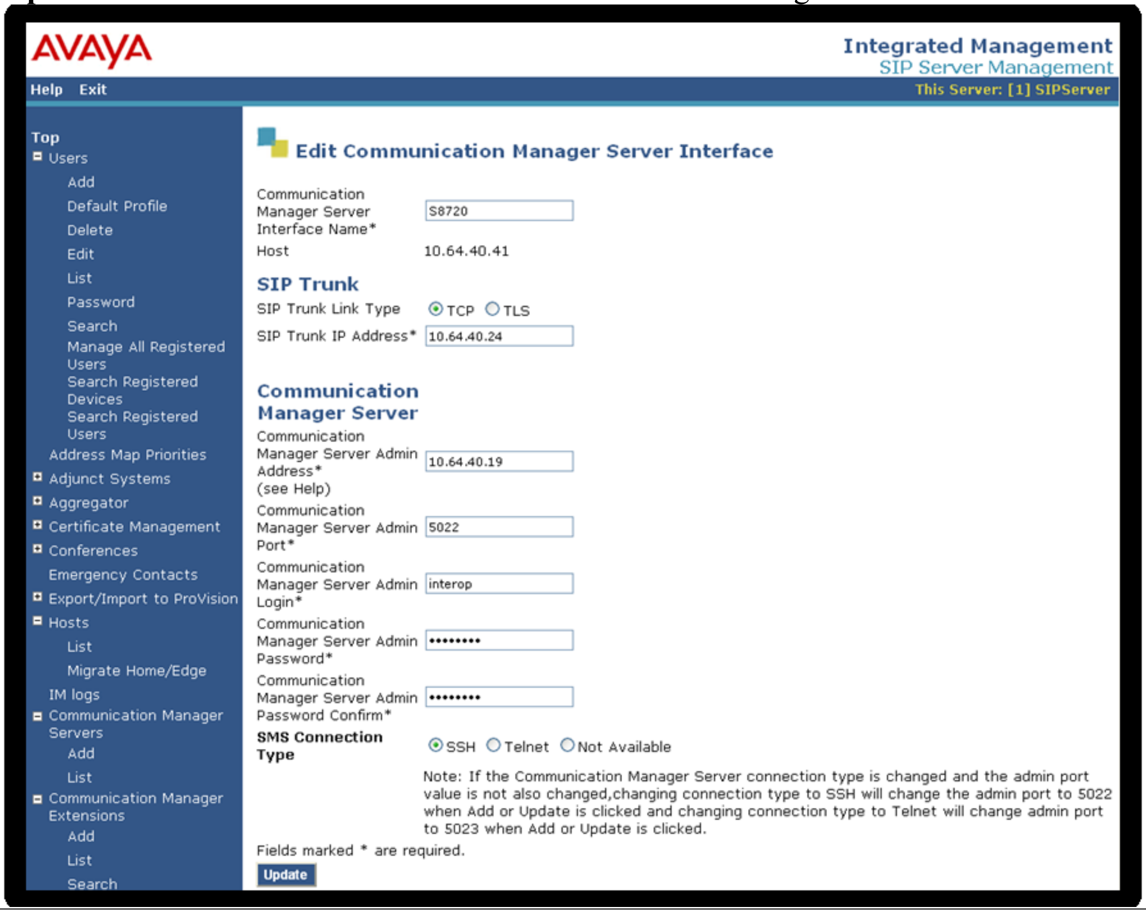
6. Configure Avaya Aura® SIP Enablement Services

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.



Edit Communication Manager Server Interface

Communication Manager Server Interface Name*: S8720

Host: 10.64.40.41

SIP Trunk

SIP Trunk Link Type: ● TCP ○ TLS

SIP Trunk IP Address*: 10.64.40.24

Communication Manager Server

Communication Manager Server Admin Address* (see Help): 10.64.40.19

Communication Manager Server Admin Port*: 5022

Communication Manager Server Admin Login*: interop

Communication Manager Server Admin Password*: ••••••••

Communication Manager Server Admin Password Confirm*: ••••••••

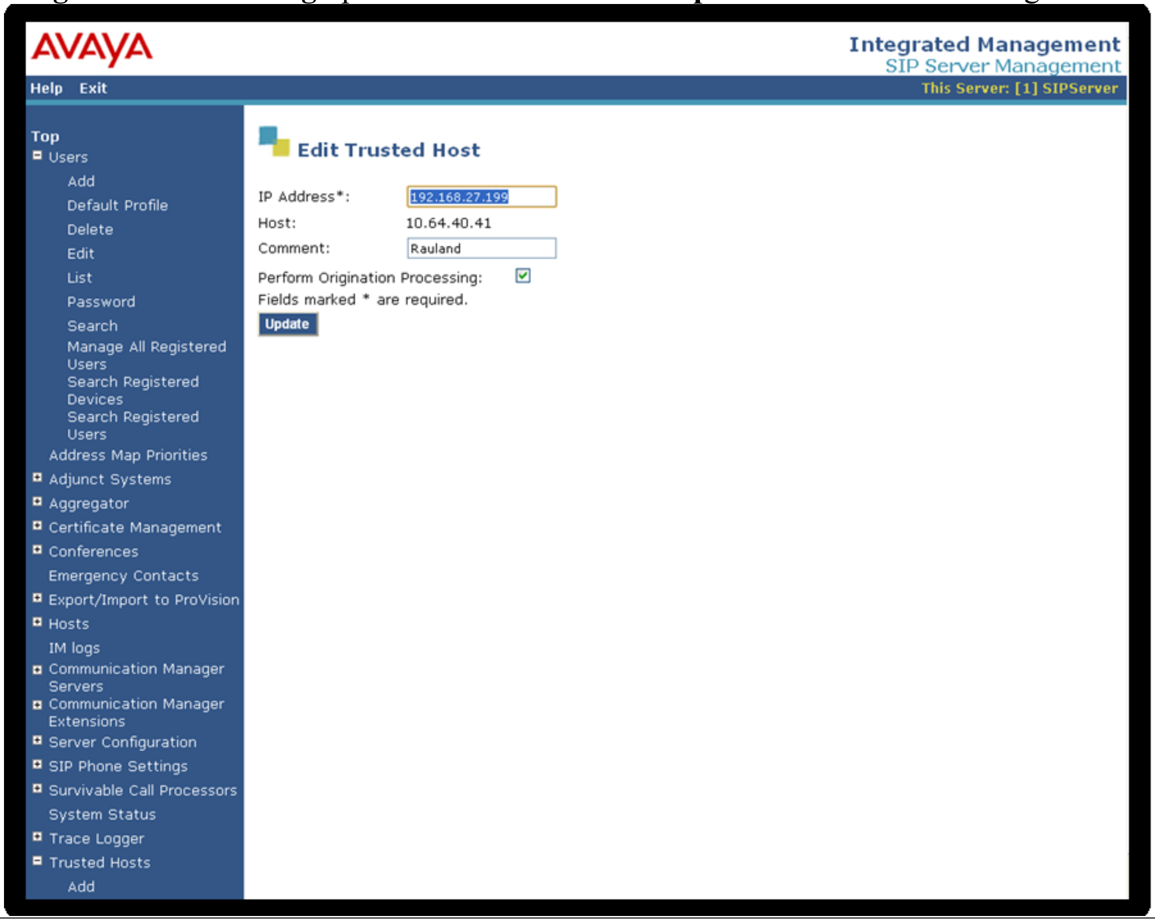
SMS Connection Type: ● SSH ○ Telnet ○ Not Available

Note: If the Communication Manager Server connection type is changed and the admin port value is not also changed,changing connection type to SSH will change the admin port to 5022 when Add or Update is clicked and changing connection type to Telnet will change admin port to 5023 when Add or Update is clicked.

Fields marked * are required.

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.



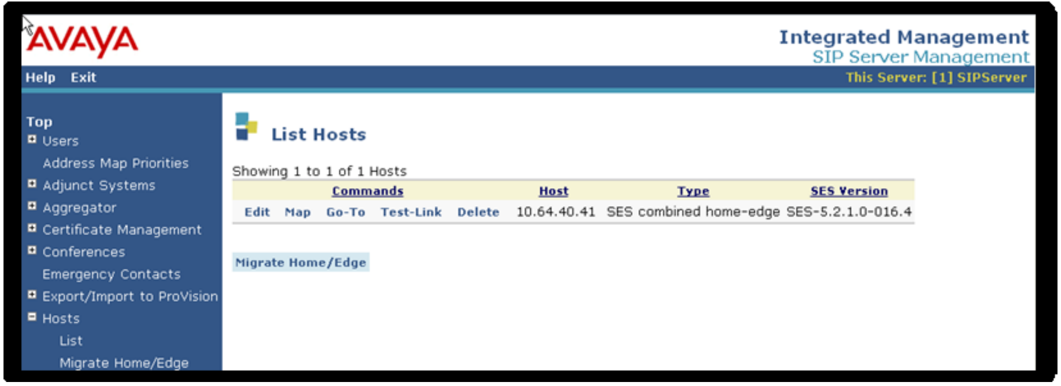
Edit Trusted Host

IP Address*: 192.168.27.199
Host: 10.64.40.41
Comment: Rauland
Perform Origination Processing: ☑
Fields marked * are required.

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.

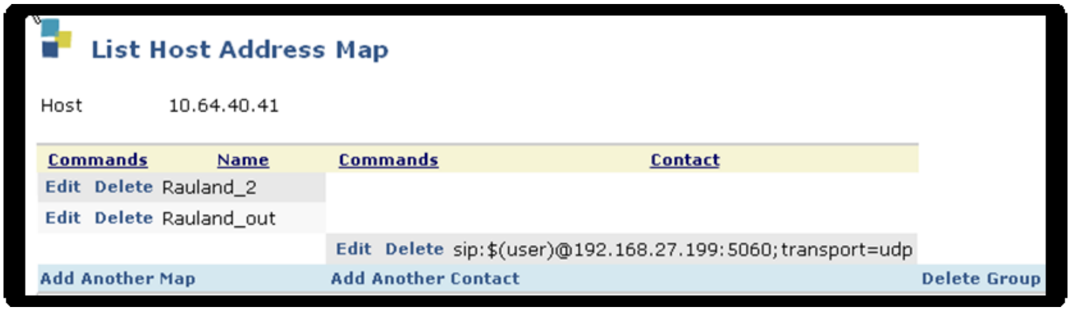


List Hosts

Showing 1 to 1 of 1 Hosts

Commands	Host	Type	SES Version
Edit Map Go-To Test-Link Delete	10.64.40.41	SES combined home-edge	SES-5.2.1.0-016.4

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

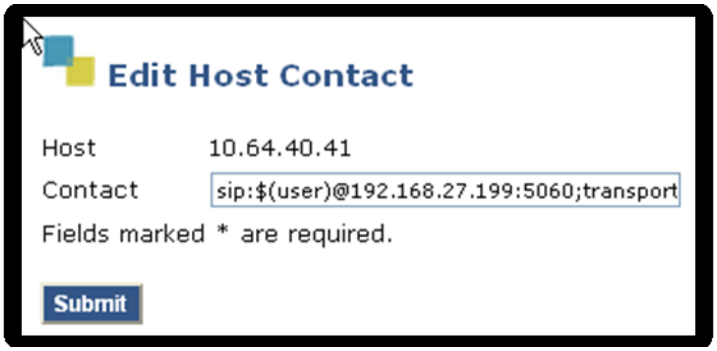


List Host Address Map

Host 10.64.40.41

Commands	Name	Commands	Contact
Edit Delete	Rauland_2		
Edit Delete	Rauland_out		
		Edit Delete	sip:$(user)@192.168.27.199:5060;transport=udp

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**.



Edit Host Contact

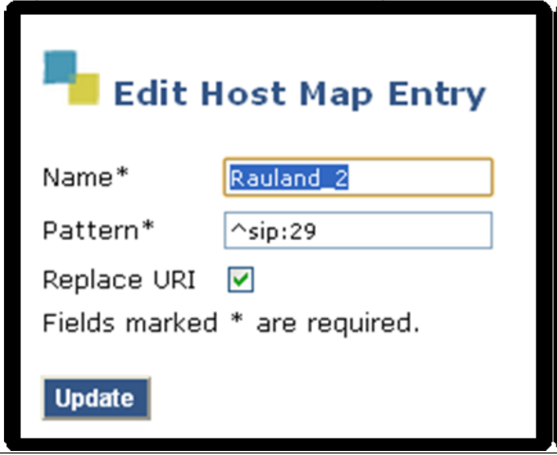
Host 10.64.40.41

Contact sip:$(user)@192.168.27.199:5060;transport

Fields marked * are required.

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.



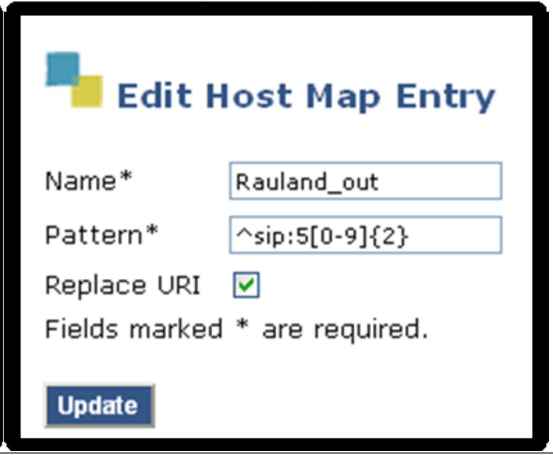
Edit Host Map Entry

Name* Rauland_2

Pattern* ^sip:29

Replace URI ☑

Fields marked * are required.



Edit Host Map Entry

Name* Rauland_out

Pattern* ^sip:5[0-9]{2}

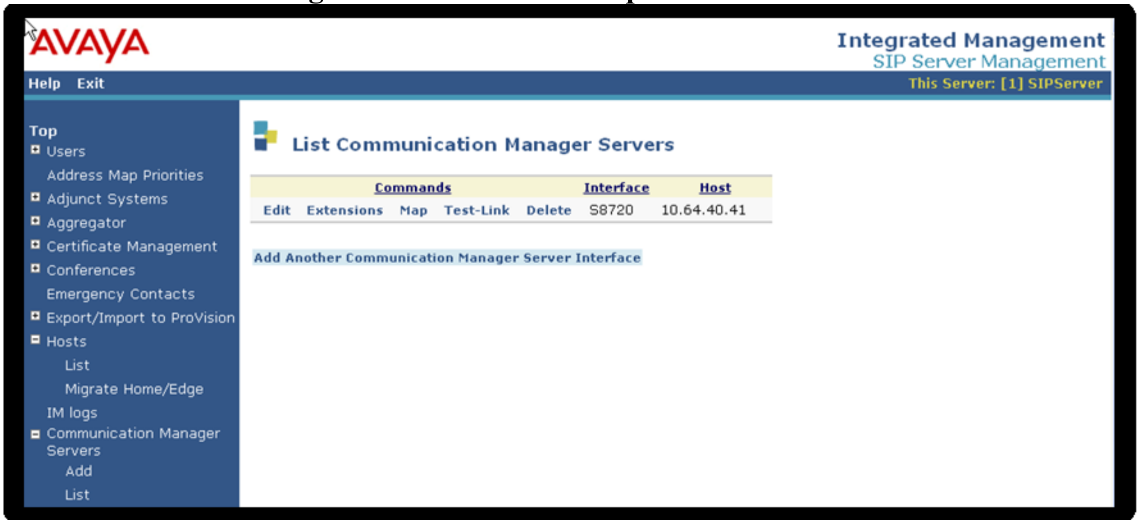
Replace URI ☑

Fields marked * are required.

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.

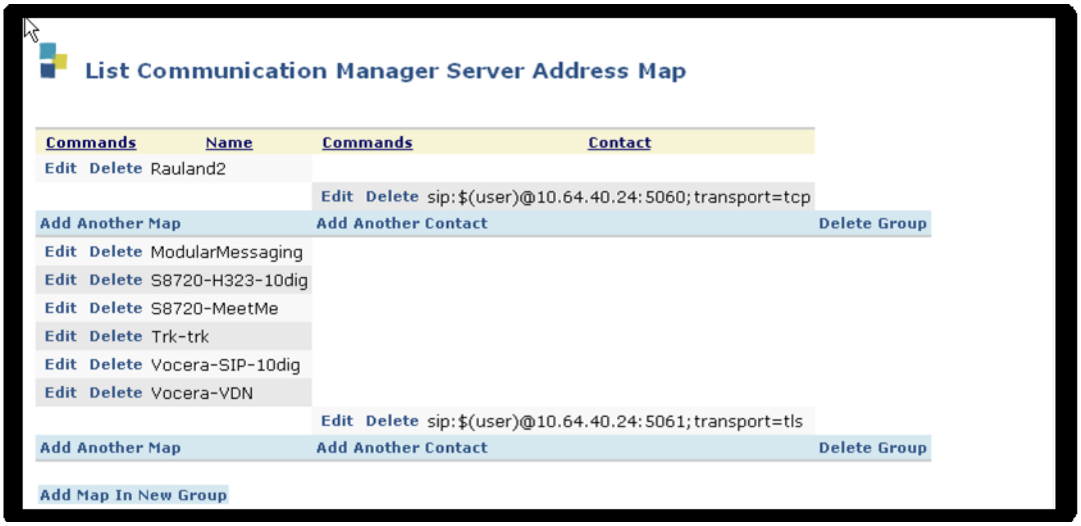


List Communication Manager Servers

Commands	Interface	Host
Edit Extensions Map Test-Link Delete	S8720	10.64.40.41

Add Another Communication Manager Server Interface

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

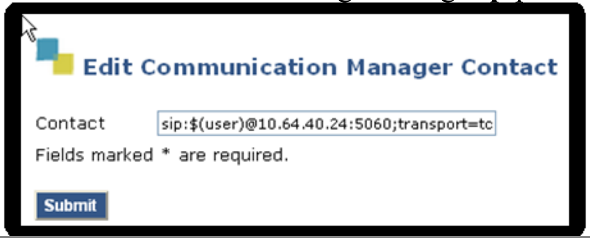


List Communication Manager Server Address Map

Commands	Name	Commands	Contact
Edit Delete	Rauland2		
		Edit Delete	sip:$(user)@10.64.40.24:5060;transport=tcp
Add Another Map		Add Another Contact	Delete Group
Edit Delete	ModularMessaging		
Edit Delete	S8720-H323-10dig		
Edit Delete	S8720-MeetMe		
Edit Delete	Trk-trk		
Edit Delete	Vocera-SIP-10dig		
Edit Delete	Vocera-VDN		
		Edit Delete	sip:$(user)@10.64.40.24:5061;transport=tls
Add Another Map		Add Another Contact	Delete Group

Add Map In New Group

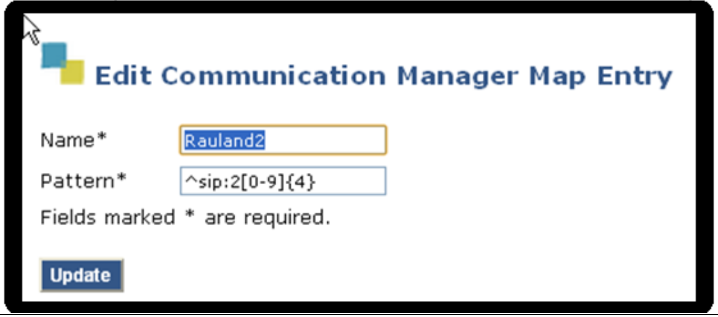
The **Edit Communication Manager Contact** link shows the settings used when the contact was previously created. The entry sip:$(user)@10.64.40.24:5060;transport=tcp instructs SIP Enablement Services to forward SIP messages to Communication Manager using **tcp** port **5060**.



Edit Communication Manager Contact

Contact sip:$(user)@10.64.40.24:5060;transport=tc

Fields marked * are required.

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.  Edit Communication Manager Map Entry Name* Rauland2 Pattern* ^sip:2[0-9]{4} Fields marked * are required.

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

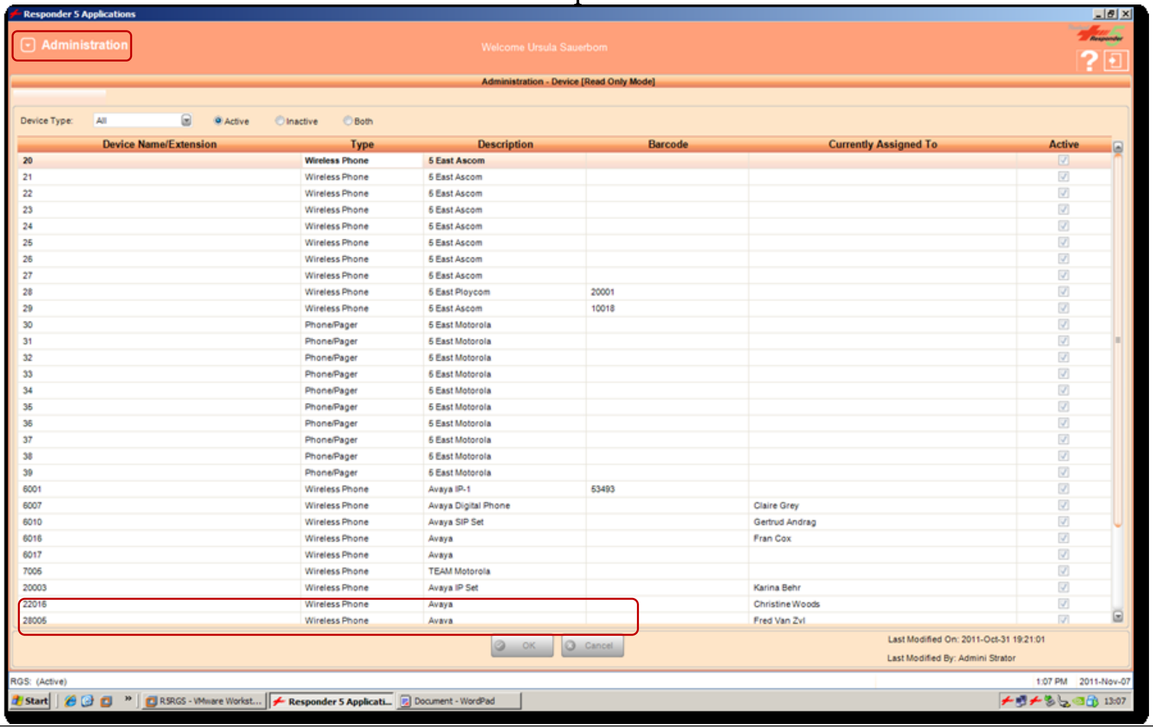
<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>1.</td><td>

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.



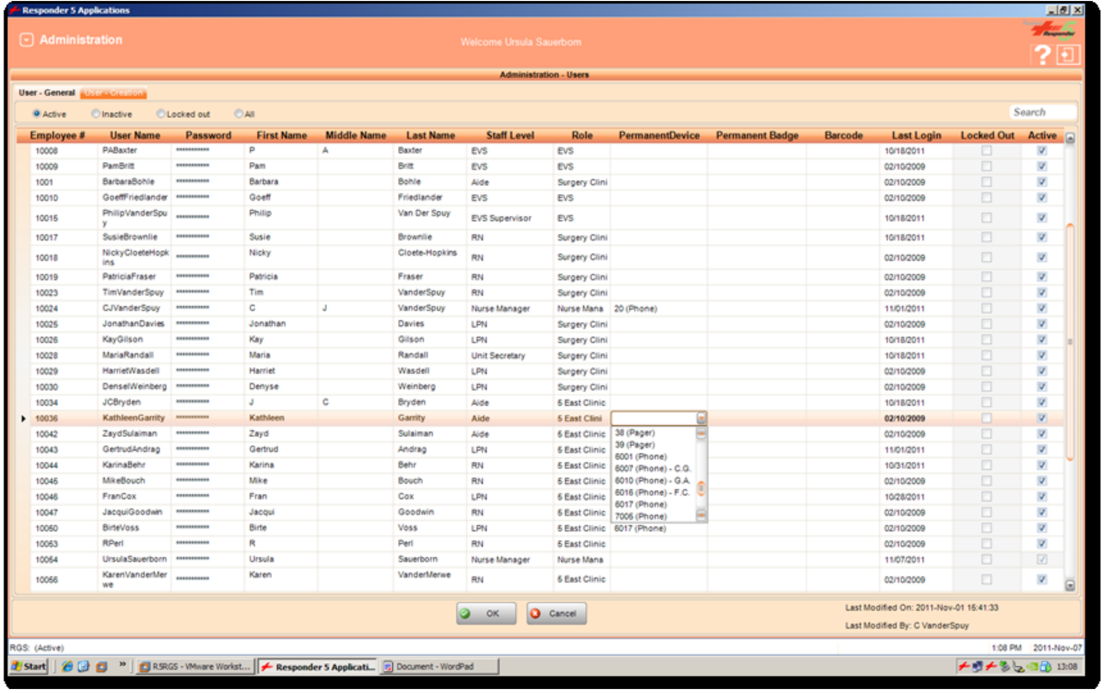
Device Type: All ● Active ○ Inactive ○ Both

<table>
<tr><th>Device Name/Extension</th><th>Type</th><th>Description</th><th>Barcode</th><th>Currently Assigned To</th><th>Active</th></tr>
<tr><td>20</td><td>Wireless Phone</td><td>5 East Ascom</td><td></td><td></td><td>☑</td></tr>
<tr><td>21</td><td>Wireless Phone</td><td>5 East Ascom</td><td></td><td></td><td>☑</td></tr>
<tr><td>22</td><td>Wireless Phone</td><td>5 East Ascom</td><td></td><td></td><td>☑</td></tr>
<tr><td>23</td><td>Wireless Phone</td><td>5 East Ascom</td><td></td><td></td><td>☑</td></tr>
<tr><td>24</td><td>Wireless Phone</td><td>5 East Ascom</td><td></td><td></td><td>☑</td></tr>
<tr><td>25</td><td>Wireless Phone</td><td>5 East Ascom</td><td></td><td></td><td>☑</td></tr>
<tr><td>26</td><td>Wireless Phone</td><td>5 East Ascom</td><td></td><td></td><td>☑</td></tr>
<tr><td>27</td><td>Wireless Phone</td><td>5 East Ascom</td><td></td><td></td><td>☑</td></tr>
<tr><td>28</td><td>Wireless Phone</td><td>5 East Ploycom</td><td>20001</td><td></td><td>☑</td></tr>
<tr><td>29</td><td>Wireless Phone</td><td>5 East Ascom</td><td>10018</td><td></td><td>☑</td></tr>
<tr><td>30</td><td>Phone/Pager</td><td>5 East Motorola</td><td></td><td></td><td>☑</td></tr>
<tr><td>31</td><td>Phone/Pager</td><td>5 East Motorola</td><td></td><td></td><td>☑</td></tr>
<tr><td>32</td><td>Phone/Pager</td><td>5 East Motorola</td><td></td><td></td><td>☑</td></tr>
<tr><td>33</td><td>Phone/Pager</td><td>5 East Motorola</td><td></td><td></td><td>☑</td></tr>
<tr><td>34</td><td>Phone/Pager</td><td>5 East Motorola</td><td></td><td></td><td>☑</td></tr>
<tr><td>35</td><td>Phone/Pager</td><td>5 East Motorola</td><td></td><td></td><td>☑</td></tr>
<tr><td>36</td><td>Phone/Pager</td><td>5 East Motorola</td><td></td><td></td><td>☑</td></tr>
<tr><td>37</td><td>Phone/Pager</td><td>5 East Motorola</td><td></td><td></td><td>☑</td></tr>
<tr><td>38</td><td>Phone/Pager</td><td>5 East Motorola</td><td></td><td></td><td>☑</td></tr>
<tr><td>39</td><td>Phone/Pager</td><td>5 East Motorola</td><td></td><td></td><td>☑</td></tr>
<tr><td>6001</td><td>Wireless Phone</td><td>Avaya IP-1</td><td>53493</td><td></td><td>☑</td></tr>
<tr><td>6007</td><td>Wireless Phone</td><td>Avaya Digital Phone</td><td></td><td>Claire Grey</td><td>☑</td></tr>
<tr><td>6010</td><td>Wireless Phone</td><td>Avaya SIP Set</td><td></td><td>Gertrud Andrag</td><td>☑</td></tr>
<tr><td>6016</td><td>Wireless Phone</td><td>Avaya</td><td></td><td>Fran Cox</td><td>☑</td></tr>
<tr><td>6017</td><td>Wireless Phone</td><td>Avaya</td><td></td><td></td><td>☑</td></tr>
<tr><td>7006</td><td>Wireless Phone</td><td>TEAM Motorola</td><td></td><td></td><td>☑</td></tr>
<tr><td>20003</td><td>Wireless Phone</td><td>Avaya IP Set</td><td></td><td>Karina Behr</td><td>☑</td></tr>
<tr><td>22016</td><td>Wireless Phone</td><td>Avaya</td><td></td><td>Christine Woods</td><td>☑</td></tr>
<tr><td>28006</td><td>Wireless Phone</td><td>Avaya</td><td></td><td>Fred Van Zvl</td><td>☑</td></tr>
</table>

Last Modified On: 2011-Oct-31 19:21:01
Last Modified By: Admini Strator

RGS: (Active) 1:07 PM 2011-Nov-07

</td></tr>
</table>

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. 

Administration - Users

User - General | User - Creation

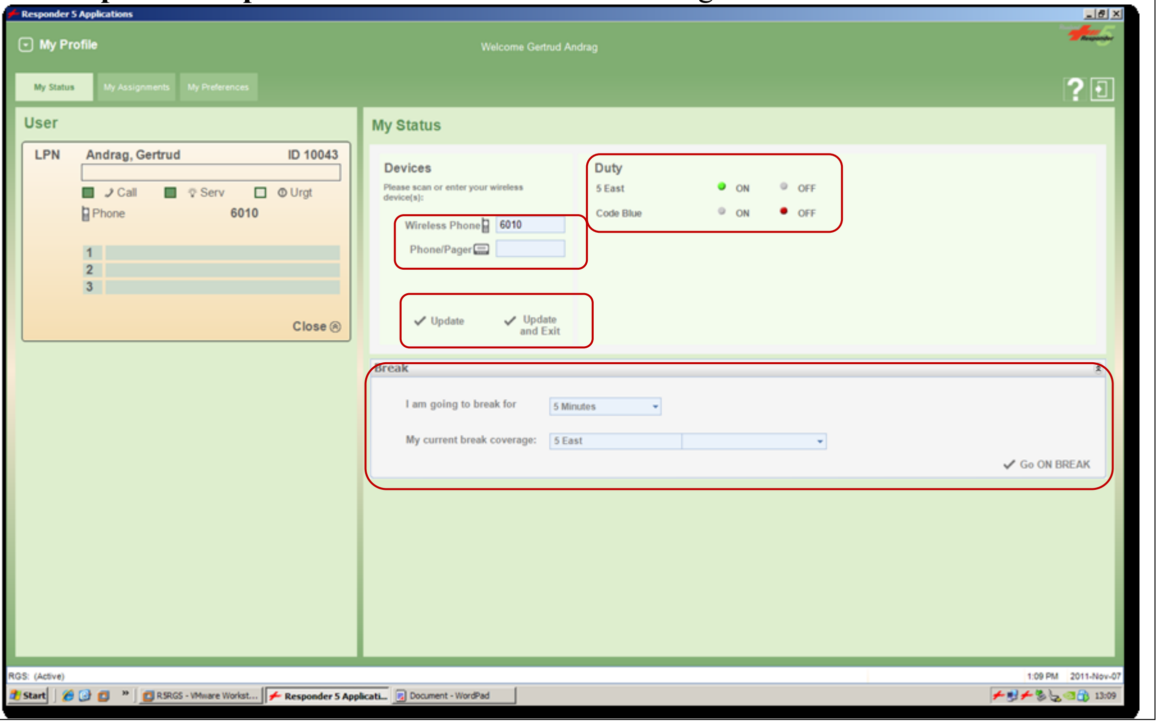
● Active ○ Inactive ○ Locked out ○ All

Search

Employee #	User Name	Password	First Name	Middle Name	Last Name	Staff Level	Role	PermanentDevice	Permanent Badge	Barcode	Last Login	Locked Out	Active
10008	PABaxter	************	P	A	Baxter	EVS	EVS				10/18/2011	☐	☑
10009	PamBritt	************	Pam		Britt	EVS	EVS				02/10/2009	☐	☑
1001	BarbaraBohle	************	Barbara		Bohle	Aide	Surgery Clini				02/10/2009	☐	☑
10010	GoeffFriedlander	************	Goeff		Friedlander	EVS	EVS				02/10/2009	☐	☑
10015	PhilipVanderSpuy	************	Philip		Van Der Spuy	EVS Supervisor	EVS				10/18/2011	☐	☑
10017	SusieBrownlie	************	Susie		Brownlie	RN	Surgery Clini				10/18/2011	☐	☑
10018	NickyCloeteHopkins	************	Nicky		Cloete-Hopkins	RN	Surgery Clini				02/10/2009	☐	☑
10019	PatriciaFraser	************	Patricia		Fraser	RN	Surgery Clini				02/10/2009	☐	☑
10023	TimVanderSpuy	************	Tim		VanderSpuy	RN	Surgery Clini				02/10/2009	☐	☑
10024	CJVanderSpuy	************	C	J	VanderSpuy	Nurse Manager	Nurse Mana	20 (Phone)			11/01/2011	☐	☑
10025	JonathanDavies	************	Jonathan		Davies	LPN	Surgery Clini				02/10/2009	☐	☑
10026	KayGilson	************	Kay		Gilson	LPN	Surgery Clini				10/18/2011	☐	☑
10028	MariaRandall	************	Maria		Randall	Unit Secretary	Surgery Clini				10/18/2011	☐	☑
10029	HarrietWasdell	************	Harriet		Wasdell	LPN	Surgery Clini				02/10/2009	☐	☑
10030	DenselWeinberg	************	Denyse		Weinberg	LPN	Surgery Clini				02/10/2009	☐	☑
10034	JCBryden	************	J	C	Bryden	Aide	5 East Clinic				10/18/2011	☐	☑
10036	KathleenGarrity	************	Kathleen		Garrity	Aide	5 East Clini				02/10/2009	☐	☑
10042	ZaydSulaiman	************	Zayd		Sulaiman	Aide	5 East Clinic	38 (Pager)			02/10/2009	☐	☑
10043	GertrudAndrag	************	Gertrud		Andrag	LPN	5 East Clinic	39 (Pager)			11/01/2011	☐	☑
10044	KarinaBehr	************	Karina		Behr	RN	5 East Clinic	6001 (Phone)			10/31/2011	☐	☑
10045	MikeBouch	************	Mike		Bouch	RN	5 East Clinic	6007 (Phone) - C.G.			02/10/2009	☐	☑
10046	FranCox	************	Fran		Cox	LPN	5 East Clinic	6010 (Phone) - G.A. 6016 (Phone) - F.C.			10/28/2011	☐	☑
10047	JacquiGoodwin	************	Jacqui		Goodwin	RN	5 East Clinic	6017 (Phone) 7006 (Phone)			02/10/2009	☐	☑
10050	BirteVoss	************	Birte		Voss	LPN	5 East Clinic	6017 (Phone)			02/10/2009	☐	☑
10053	RPerl	************	R		Perl	RN	5 East Clinic				02/10/2009	☐	☑
10054	UrsulaSauerborn	************	Ursula		Sauerborn	Nurse Manager	Nurse Mana				11/07/2011	☐	☑
10056	KarenVanderMerwe	************	Karen		VanderMerwe	RN	5 East Clinic				02/10/2009	☐	☑

Last Modified On: 2011-Nov-01 15:41:33
Last Modified By: C VanderSpuy

RGS: (Active) 1:08 PM 2011-Nov-07

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 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. 

Responder 5 Applications

My Profile

Welcome Gertrud Andrag

User

LPN Andrag, Gertrud ID 10043

Phone 6010

My Status

Devices

Please scan or enter your wireless device(s):

Wireless Phone: 6010

Phone/Pager:

Duty

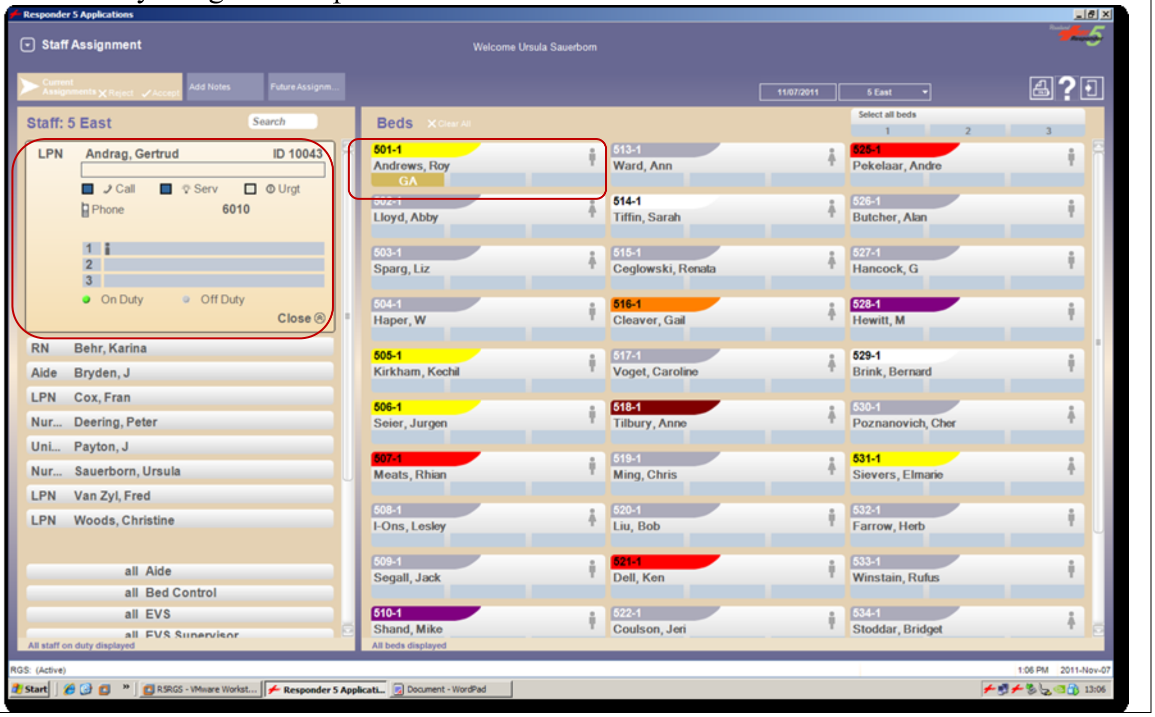
5 East	● ON	○ OFF
Code Blue	○ ON	● OFF

Break

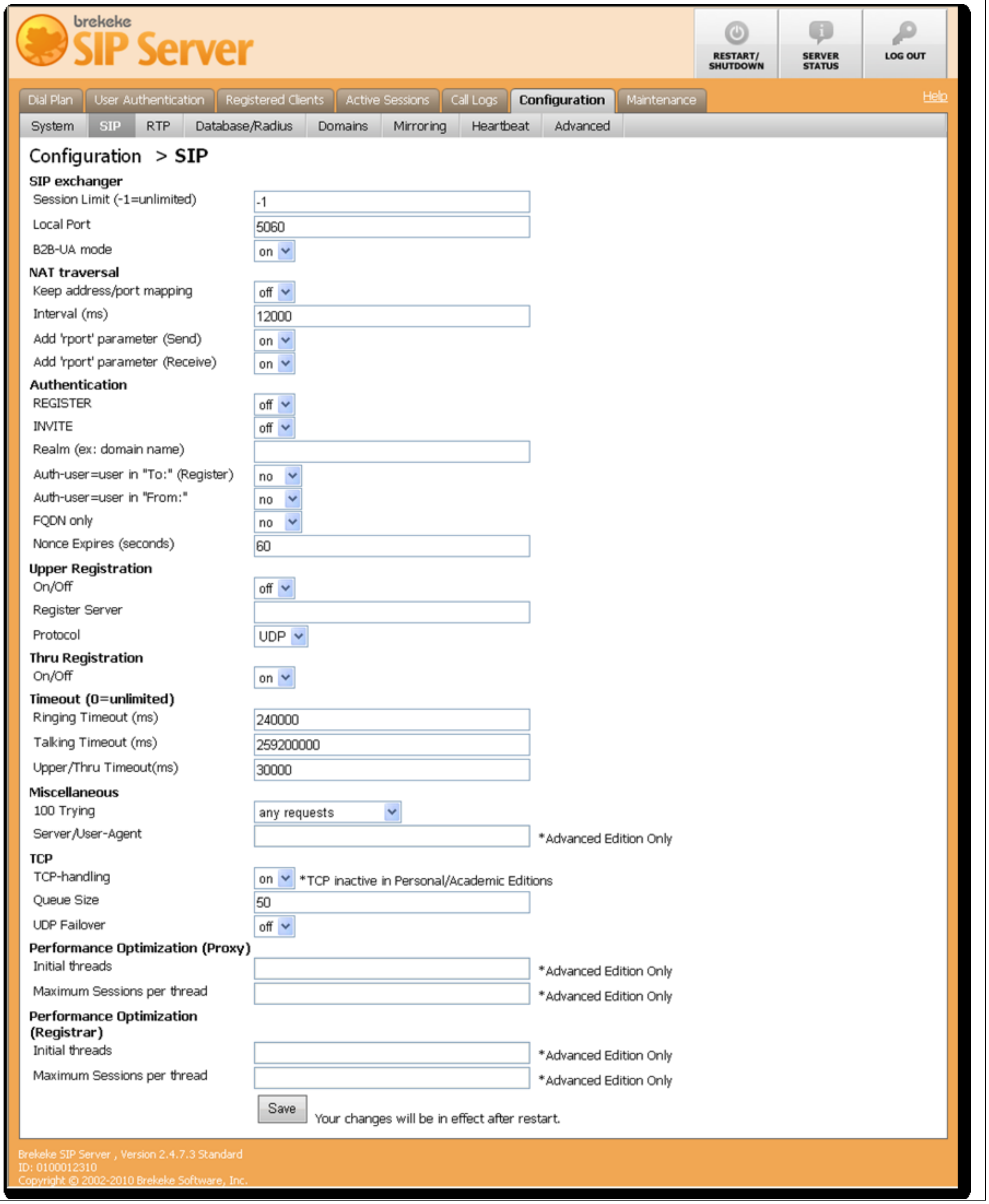
I am going to break for: 5 Minutes

My current break coverage: 5 East

RGS: (Active) 1:09 PM 2011-Nov-07

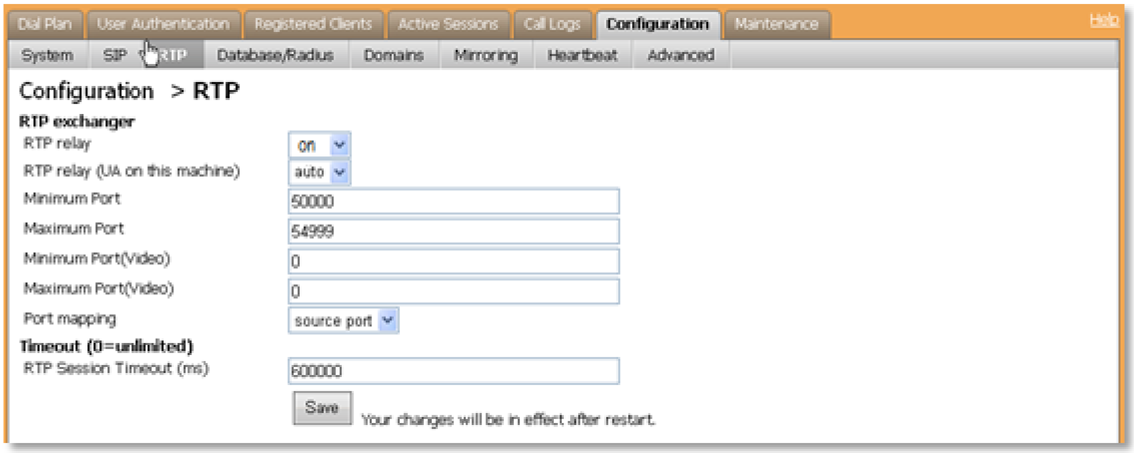
Step	Description
4.	**Assign Staff to Patient Rooms** This task is typically performed by shift supervisors. Staff can be assigned to patient rooms on the **Staff Assignment** screen which is accessed from the drop down menu at the upper left of the Responder 5 Applications. In the illustration below, ***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. 

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>5.</td><td><b>Configure Brekeke SIP Server SIP Properties</b>
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.


brekeke SIP Server
RESTART/ SHUTDOWN
SERVER STATUS
LOG OUT
Dial Plan
User Authentication
Registered Clients
Active Sessions
Call Logs
Configuration
Maintenance
Help
System
SIP
RTP
Database/Radius
Domains
Mirroring
Heartbeat
Advanced

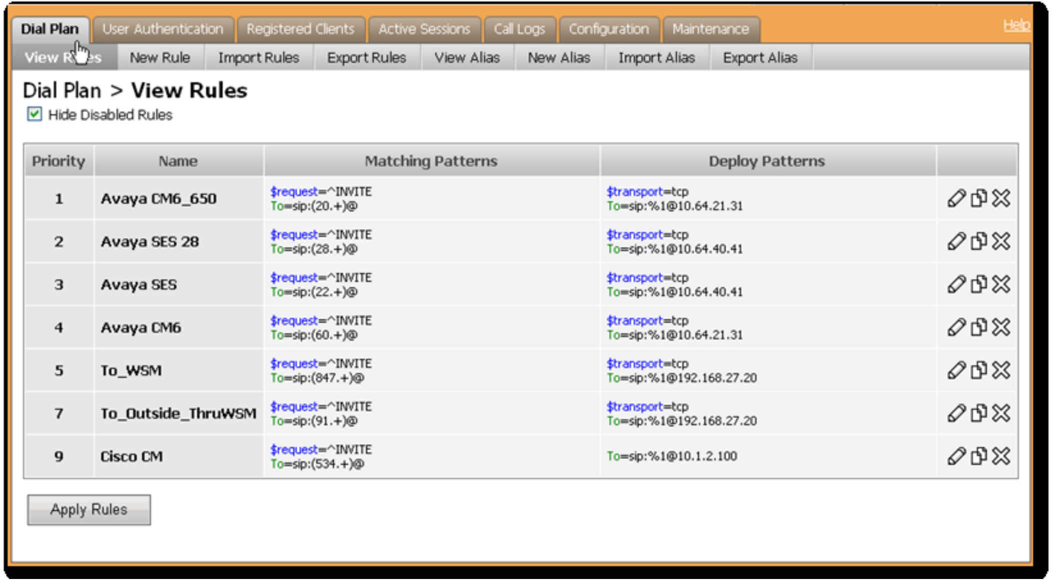
Configuration &gt; SIP
<b>SIP exchanger</b>
Session Limit (-1=unlimited): -1
Local Port: 5060
B2B-UA mode: on
<b>NAT traversal</b>
Keep address/port mapping: off
Interval (ms): 12000
Add 'rport' parameter (Send): on
Add 'rport' parameter (Receive): on
<b>Authentication</b>
REGISTER: off
INVITE: off
Realm (ex: domain name):
Auth-user=user in "To:" (Register): no
Auth-user=user in "From:": no
FQDN only: no
Nonce Expires (seconds): 60
<b>Upper Registration</b>
On/Off: off
Register Server:
Protocol: UDP
<b>Thru Registration</b>
On/Off: on
<b>Timeout (0=unlimited)</b>
Ringing Timeout (ms): 240000
Talking Timeout (ms): 259200000
Upper/Thru Timeout(ms): 30000
<b>Miscellaneous</b>
100 Trying: any requests
Server/User-Agent: *Advanced Edition Only
<b>TCP</b>
TCP-handling: on *TCP inactive in Personal/Academic Editions
Queue Size: 50
UDP Failover: off
<b>Performance Optimization (Proxy)</b>
Initial threads: *Advanced Edition Only
Maximum Sessions per thread: *Advanced Edition Only
<b>Performance Optimization (Registrar)</b>
Initial threads: *Advanced Edition Only
Maximum Sessions per thread: *Advanced Edition Only
Save Your changes will be in effect after restart.
Brekeke SIP Server , Version 2.4.7.3 Standard
ID: 0100012310
Copyright © 2002-2010 Brekeke Software, Inc.</td></tr>
</table>

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.  Configuration > RTP **RTP exchanger** RTP relay: on RTP relay (UA on this machine): auto Minimum Port: 50000 Maximum Port: 54999 Minimum Port(Video): 0 Maximum Port(Video): 0 Port mapping: source port **Timeout (0=unlimited)** RTP Session Timeout (ms): 600000 Save Your changes will be in effect after restart.

Step	Description

7. **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.



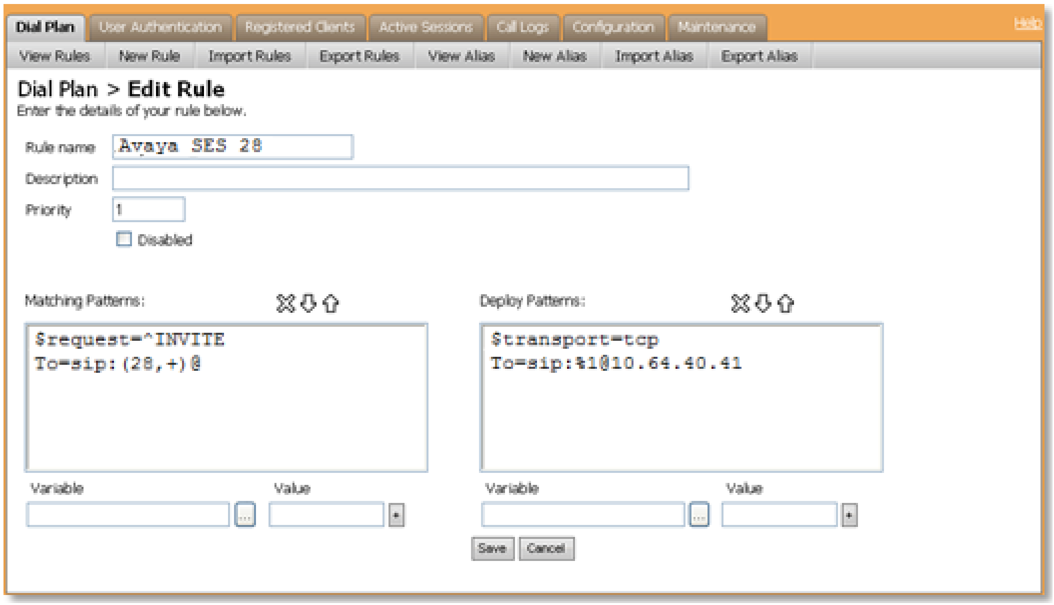
Dial Plan > **View Rules**

☑ Hide Disabled Rules

Priority	Name	Matching Patterns	Deploy Patterns	
1	Avaya CM6_650	$request=^INVITE To=sip:(20.+)@	$transport=tcp To=sip:%1@10.64.21.31	
2	Avaya SES 28	$request=^INVITE To=sip:(28.+)@	$transport=tcp To=sip:%1@10.64.40.41	
3	Avaya SES	$request=^INVITE To=sip:(22.+)@	$transport=tcp To=sip:%1@10.64.40.41	
4	Avaya CM6	$request=^INVITE To=sip:(60.+)@	$transport=tcp To=sip:%1@10.64.21.31	
5	To_WSM	$request=^INVITE To=sip:(847.+)@	$transport=tcp To=sip:%1@192.168.27.20	
7	To_Outside_ThruWSM	$request=^INVITE To=sip:(91.+)@	$transport=tcp To=sip:%1@192.168.27.20	
9	Cisco CM	$request=^INVITE To=sip:(534.+)@	To=sip:%1@10.1.2.100	

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 **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.



Dial Plan > **Edit Rule**

Enter the details of your rule below.

Rule name: Avaya SES 28

Description:

Priority: 1

□ Disabled

Matching Patterns:

```
$request=^INVITE
To=sip:(28,+)@
```

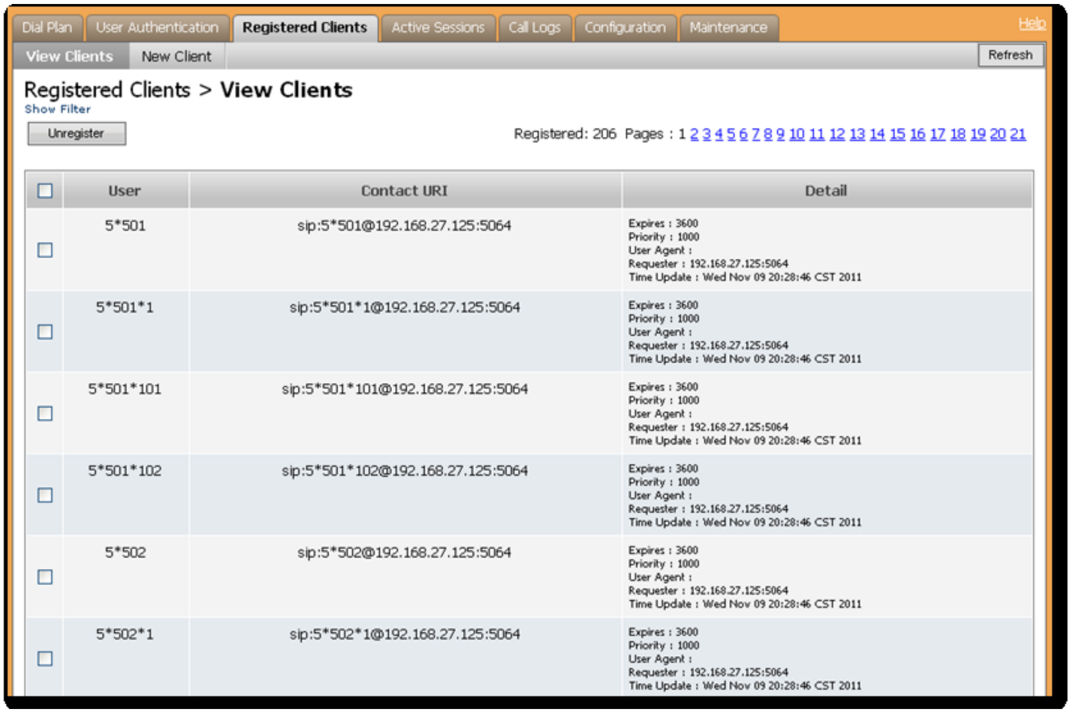
Deploy Patterns:

```
$transport=tcp
To=sip:%1@10.64.40.41
```

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.



Registered Clients > View Clients

Registered: 206 Pages : 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21

□	User	Contact URI	Detail
□	5*501	sip:5*501@192.168.27.125:5064	Expires : 3600 Priority : 1000 User Agent : Requester : 192.168.27.125:5064 Time Update : Wed Nov 09 20:28:46 CST 2011
□	5*501*1	sip:5*501*1@192.168.27.125:5064	Expires : 3600 Priority : 1000 User Agent : Requester : 192.168.27.125:5064 Time Update : Wed Nov 09 20:28:46 CST 2011
□	5*501*101	sip:5*501*101@192.168.27.125:5064	Expires : 3600 Priority : 1000 User Agent : Requester : 192.168.27.125:5064 Time Update : Wed Nov 09 20:28:46 CST 2011
□	5*501*102	sip:5*501*102@192.168.27.125:5064	Expires : 3600 Priority : 1000 User Agent : Requester : 192.168.27.125:5064 Time Update : Wed Nov 09 20:28:46 CST 2011
□	5*502	sip:5*502@192.168.27.125:5064	Expires : 3600 Priority : 1000 User Agent : Requester : 192.168.27.125:5064 Time Update : Wed Nov 09 20:28:46 CST 2011
□	5*502*1	sip:5*502*1@192.168.27.125:5064	Expires : 3600 Priority : 1000 User Agent : Requester : 192.168.27.125:5064 Time Update : Wed Nov 09 20:28:46 CST 2011

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

[1] *Administering Avaya Aura™ Communication Manager*, Doc # 03-300509, Release 5.2, Issue 5.0, May 2009.

[2] *Installing, Administering, Maintaining, and Troubleshooting Avaya Aura® SIP Enablement Services,* Doc # 03-600768, January 2011

[3] *Application Notes for Configuring Rauland-Borg Responder® 5 to Interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager R6.0.1.*

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.