



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Rauland-Borg Responder[®] 5 to Interoperate with Avaya Communication Server 1000 and Avaya Aura[®] Session Manager– Issue 1.0

Abstract

These Application Notes describe a compliance-tested configuration consisting of the Rauland-Borg Responder[®] 5 solution, Avaya Communication Server 1000 and Avaya Aura[®] Session Manager.

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 (hereafter known as Responder) solution, Avaya Communication Server 1000 (hereafter known as Communication Server 1000) and Avaya Aura[®] Session Manager (hereafter known as Session Manager).

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 and/or Rauland-Borg authorized distributors, 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 Server 1000, 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 Avaya Communication Server 1000 via Avaya Aura[®] Session 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 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 and passed.

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 Communication Server 1000 R7.6
- Avaya Aura® Session Manager R7.0
- Avaya Aura® System Manager R7.0
- Various UNISim and SIP endpoints
- Brekeke SIP Server (registrar)
- Responder® 5 Gateway Server
- Responder® 5 Branch Regional Controller
- Responder® 5 Communication Endpoints

Calls routed to and from the Communication Server 1000 used SIP trunks between the Brekeke SIP server and Session Manager, and in turn SIP trunks between Session Manager and Communication Server 1000.

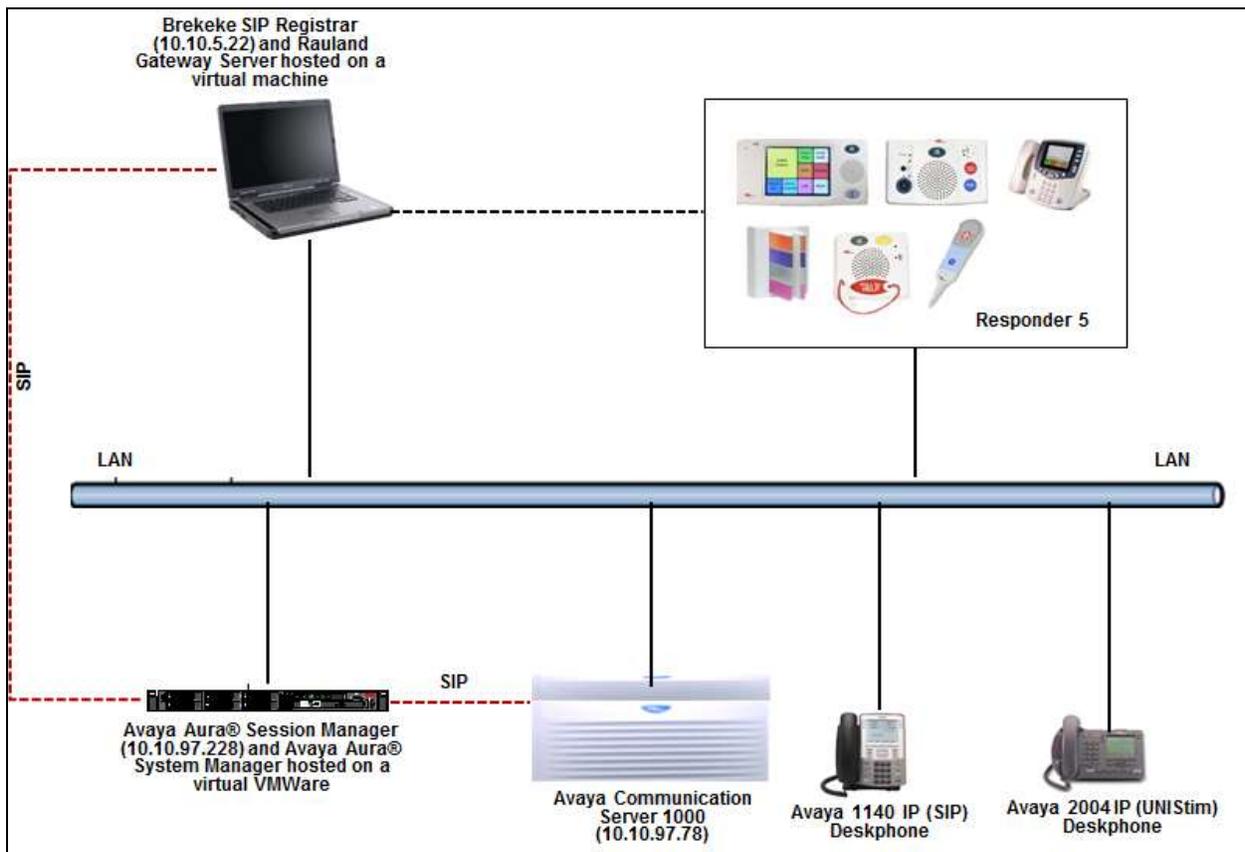


Figure 1 – Rauland-Borg Responder® 5 Compliance Test Configuration

4. Equipment and Software Validated

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

Equipment	Version
Avaya Communication Server 1000	7.65.16 SP7
Avaya Aura® Session Manager	7.0.0.0.700007
Avaya Aura® System Manager	7.0.0.0
Avaya IP Deskphones: 1140 (SIP) 2004P1 (UNISim)	4.03.09 0602B76
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 Communication Server 1000

This section describes the Communication Server 1000 configuration necessary to interoperate with Session Manager and Responder. It provides the procedures for configuring Avaya Communication Server 1000 system. The procedures include the following areas:

- Logging into the Element Manager via Unified Communication Manager
- Configuring the SIP Signaling Gateway.
- Configuring a D-Channel.
- Configuring Route and Trunks.
- Configuring Digit Manipulation Block.
- Configuring Route List Block.
- Configuring Distant Steering Code.

For detail configuration details of the Communication Server 1000 refer to **Section 10**.

5.1. Logging into Element Manager via Unified Communication Manager

User can login to the Element Manager via System Manager or Unified Communication Manager (UCM). During this compliance testing UCM was used to login to the Element Manager. To login to the UCM, open a browser and type in the IP address of the UCM in the URL (not shown). Screen below shows the main dashboard.

The screenshot shows the Avaya Unified Communications Management interface. The top navigation bar includes the Avaya logo and the title "Avaya Unified Communications Management". Below the navigation bar, the main content area is titled "Elements". It displays a table of registered elements with columns for Element Name, Element Type, Release, Address, and Description. The first row is highlighted, showing "EM on sip175" as the Element Name, "CS1000" as the Element Type, "7.6" as the Release, and "10.10.97.78" as the Address. The description for this element is "New element".

Element Name	Element Type	Release	Address	Description
EM on sip175	CS1000	7.6	10.10.97.78	New element.
com3.bvwddev.com (member)	Linux Base	7.6		Base OS element.
sip175.bvwddev.com (primary)	Linux Base	7.6		Base OS element.
	Media Gateway Controller	7.6		New element.

From the **Elements** page of UCM as shown in screen below, click on the Element **EM on sip175**. This is the element which is configured to access the Element Manager (EM) for the Communication Server 1000 Call Server.

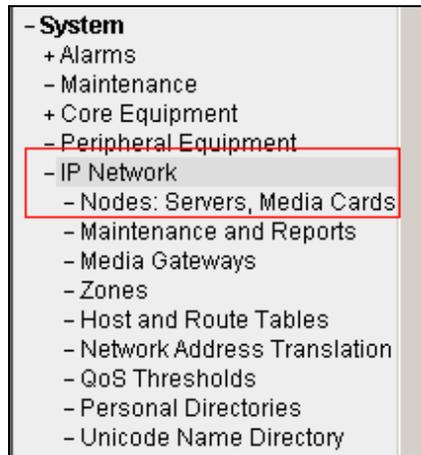
This screenshot is identical to the one above, but with a red box highlighting the first row of the table, which corresponds to the "EM on sip175" element. This indicates the element that the user is instructed to click on.

Element Name	Element Type	Release	Address	Description
EM on sip175	CS1000	7.6	10.10.97.78	New element.
com3.bvwddev.com (member)	Linux Base	7.6		Base OS element.
sip175.bvwddev.com (primary)	Linux Base	7.6		Base OS element.
	Media Gateway Controller	7.6		New element.

5.2. Configuring the SIP Signaling Gateway

This section describes the configuration required on the SIP Signaling Gateway so that the Communication Server 1000 can communicate with the Session Manager via SIP Trunks.

To add a Node, from the EM left navigator screen, navigate to **System → IP Network → Nodes: Servers, Media Cards** as shown below.



Assumption is made here that the IP Telephony node is already added.

During compliance testing Node **510** was added. Click on this Node as shown in screen below to view the configured values.

Managing: Username: admin
System » IP Network » IP Telephony Nodes

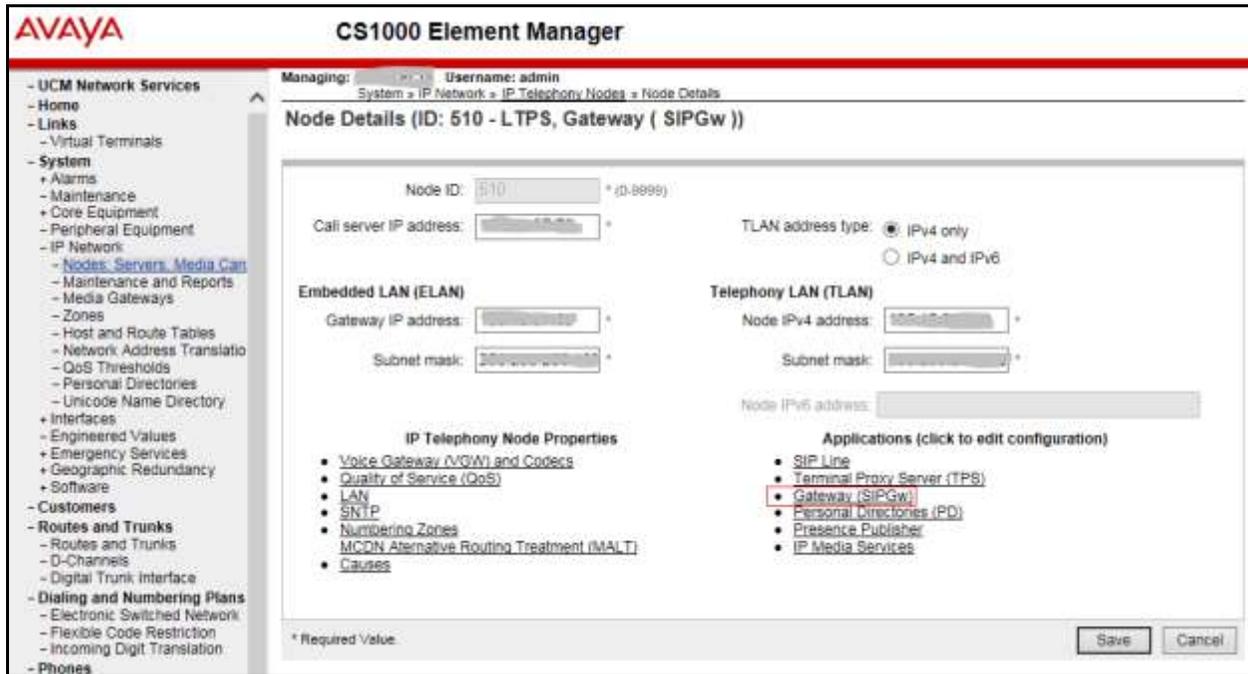
IP Telephony Nodes

Click the Node ID to view or edit its properties.

<input type="checkbox"/> Node ID	Components	Enabled Applications	ELAN IP	Node/TLAN IPv4	Node/TLAN IPv6	Status
<input type="checkbox"/> 510	1	LTPS, Gateway (SiPGw)	-	-	-	Synchronized
<input type="checkbox"/> 512	1	SIP Line, LTPS, Presence Publisher	-	-	-	Synchronized

Show: Nodes Component servers and cards IPv6 address

Open the SIP Signaling Gateway configuration by clicking on **Gateway (SIPGw)** as shown below from the Node Details page.



The following values were configured during compliance testing as shown in the screen below.

- **Vtrk gateway application:** Check the *Enable gateway service on this node* box.
- **Vtrk gateway application:** Select *SIP Gateway (SIPGw)* from the drop down menu.
- **SIP domain name:** *bvwdev.com*. This will be the same domain name that will be configured on the Session Manager.
- **Local SIP port:** *5060*.
- **Gateway endpoint name:** *cppm3*.
- **Application node ID:** *510*.

Retain default values for other fields.

The screenshot displays the AVAYA CS1000 Element Manager interface. The main window title is "CS1000 Element Manager". The breadcrumb navigation shows: "System > IP Network > IP Telephony Nodes > Node Details > Virtual Trunk Gateway Configuration". The page title is "Node ID: 510 - Virtual Trunk Gateway Configuration Details".

The configuration is organized into two main sections: "General" and "Virtual Trunk Network Health Monitor".

General Section:

- Vtrk gateway application:** A dropdown menu is set to "SIP Gateway (SIPGw)".
- SIP domain name:** A text field contains "bvwdev.com".
- Local SIP port:** A text field contains "5060".
- Gateway endpoint name:** A text field contains "cppm3".
- Gateway password:** A text field is empty.
- Application node ID:** A text field contains "510".
- Enable failsafe NRS:** An unchecked checkbox.

Virtual Trunk Network Health Monitor Section:

- Monitor IP addresses (listed below):** An unchecked checkbox.
- Monitor IP:** A text field is empty, with an "Add" button to its right.
- Monitor addresses:** A large empty text area with a "Remove" button to its right.

At the top of the configuration area, there is a checkbox labeled "Vtrk gateway application: Enable gateway service on this node".

At the bottom of the page, there are two notes: "* Required Value." and "Note: Changes made on this page will NOT be transmitted until the Node is also saved." There are "Save" and "Cancel" buttons at the bottom right.

Scroll down to the **Proxy or Redirect Server** section. The following values were configured during compliance testing.

- **Primary TLAN IP address:** 10.10.97.228. This is the IP address of the Session Manager.
- **Port:** 5060
- **Transport protocol:** Select *UDP* from the drop down menu.

Retain default values for other fields.

The screenshot displays the AVAYA CS1000 Element Manager interface. The main title is "CS1000 Element Manager". The breadcrumb trail is "System > IP Network > IP Telephony Nodes > Node Details > Virtual Trunk Gateway Configuration". The page title is "Node ID: 510 - Virtual Trunk Gateway Configuration Details". The "Proxy Or Redirect Server" section is highlighted with a red box. The configuration details for this section are as follows:

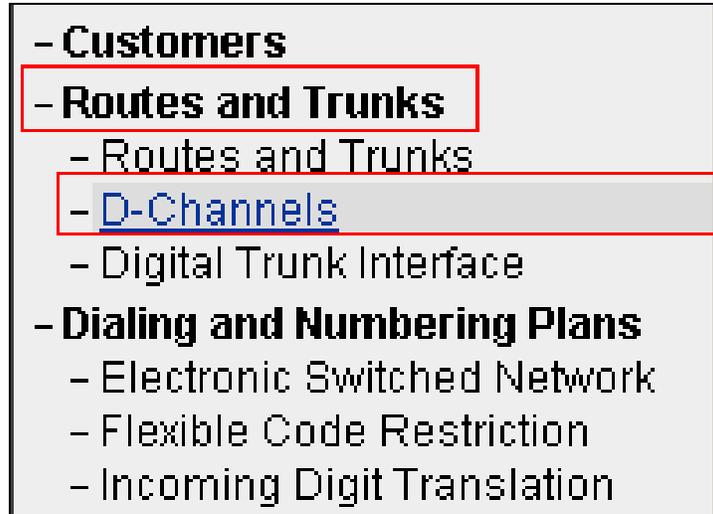
Field	Value
Primary TLAN IP address	10.10.97.228
Port	5060 (1 - 65535)
Transport protocol	UDP
Options	<input type="checkbox"/> Support registration <input type="checkbox"/> Primary CDS proxy
Secondary TLAN IP address	0.0.0.0
Port	5060 (1 - 65535)
Transport protocol	UDP

Additional information from the screenshot includes a "Save" and "Cancel" button at the bottom right, and a note: "Note: Changes made on this page will NOT be transmitted until the Node is also saved." A red asterisk indicates a required value.

Save and transmit (not shown) these Node properties to complete the SIPGw configuration.

5.3. Configuring D-Channel

This section explains the configuration of a D-Channel for a SIP Trunk. From the EM navigation screen, navigate to **Routes and Trunks** → **D-Channels** as shown below.



Choose an available D-Channel number to add as shown in the screen below. During compliance testing D-Channel number **1** was configured. Click on **Edit** to view its configuration.



The following values were configured in **Basic Configuration** for the D-Channel as shown below.

- **Action Device And Number (ADAN):** *DCH*.
- **D channel Card Type:** *DCIP*.
- **Designator:** A descriptive name.
- **Interface type for D-channel:** Select *Meridian Meridian1 (SL1)* from the drop down menu.
- **Meridian 1 node type:** Select *Slave to the controller (USR)* from the drop down menu.
- **Release ID of the switch at the far end:** Select *25* from the drop down menu.

Retain default values for all other fields.

Input Description	Input Value
Action Device And Number (ADAN):	DCH
D channel Card Type:	DCIP
Designator:	SIP
Recovery to Primary:	<input type="checkbox"/>
PRI loop number for Backup D-channel:	
User:	Integrated Services Signaling Link Dedicated (ISLD)
Interface type for D-channel:	Meridian Meridian1 (SL1)
Country:	ETS 300 =102 basic protocol (ETSI)
D-Channel PRI loop number:	
Primary Rate Interface:	<input type="button" value="more PRI"/>
Secondary PRI2 loops:	
Meridian 1 node type:	Slave to the controller (USR)
Release ID of the switch at the far end:	25
Central Office switch type:	100% compatible with Bellcore standard (STD)

Scroll down to edit the **Remote Capabilities** of the D-Channel that is seen under the **Basic options (BSCOPT)** section. Click on **Edit** button as shown in the screen below.

- Basic options (BSCOPT)

Primary D-channel for a backup DCH: Range: 0 - 254

- PINX customer number:

- Progress signal:

- Calling Line Identification :

- Output request Buffers: 32

- D-channel transmission Rate: 56 kb/s when LCMT is AMI (56K)

- Channel Negotiation option: No alternative acceptable, exclusive. (1)

- Remote Capabilities:

Enable the **Network name display method 2 (ND2)** option. Now click on **Return - Remote Capabilities** button (not shown) to return back to the main screen.

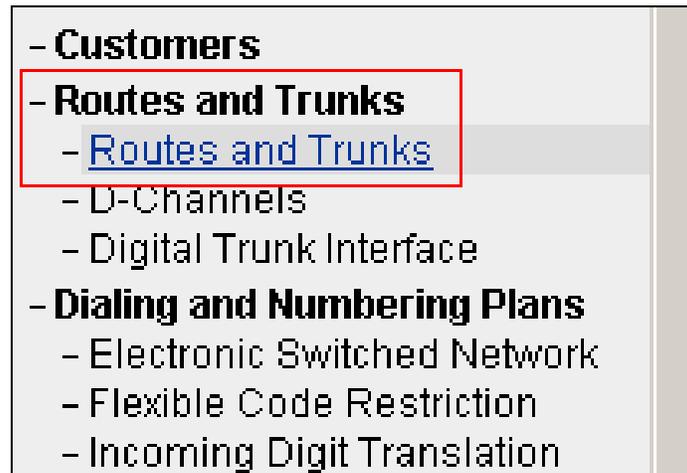
- Remote Capabilities Configuration

Input Description	Input Value
Basic rate interface (BRI)	<input type="checkbox"/>
Call completion on busy using integer value (CCBI)	<input type="checkbox"/>
Call completion on busy using object identifier (CCBO)	<input type="checkbox"/>
Call completion on busy for QSIG and EuroISDN BRI (CCBS)	<input type="checkbox"/>
Call completion on no response using integer value (CCNI)	<input type="checkbox"/>
Call completion on no response using object identifier (CCNO)	<input type="checkbox"/>
Call completion to no reply for QSIG and EuroISDN BRI (CCNR)	<input type="checkbox"/>
Network call park (CPK)	<input type="checkbox"/>
Connected line identification presentation (COLP)	<input type="checkbox"/>
Call transfer integer (CTI)	<input type="checkbox"/>
Call transfer object (CTO)	<input type="checkbox"/>
Diversion info. is sent using integer value (DV1I)	<input type="checkbox"/>
Diversion info. is sent using object identifier (DV1O)	<input type="checkbox"/>
Rerouting requests processed using integer value (DV2I)	<input type="checkbox"/>
Rerouting requests processed using object identifier (DV2O)	<input type="checkbox"/>
Diversion info. sent. rerouting requests processed (DV3I)	<input type="checkbox"/>
EuroISDN - div. info sent. rerouting req. processed (DV3O)	<input type="checkbox"/>
Call transfer notification and invocation to EuroISDN (ECTO)	<input type="checkbox"/>
Malicious call identification (MCID)	<input type="checkbox"/>
MCDN QSIG conversion (MQC)	<input type="checkbox"/>
Remote D-channel is on a MSDL card (MSL)	<input type="checkbox"/>
Message waiting interworking with DMS-100 (MWI)	<input type="checkbox"/>
Network access data (NAC)	<input type="checkbox"/>
Network call trace supported (NCT)	<input type="checkbox"/>
Network name display method 1 (ND1)	<input type="checkbox"/>
Network name display method 2 (ND2)	<input checked="" type="checkbox"/>

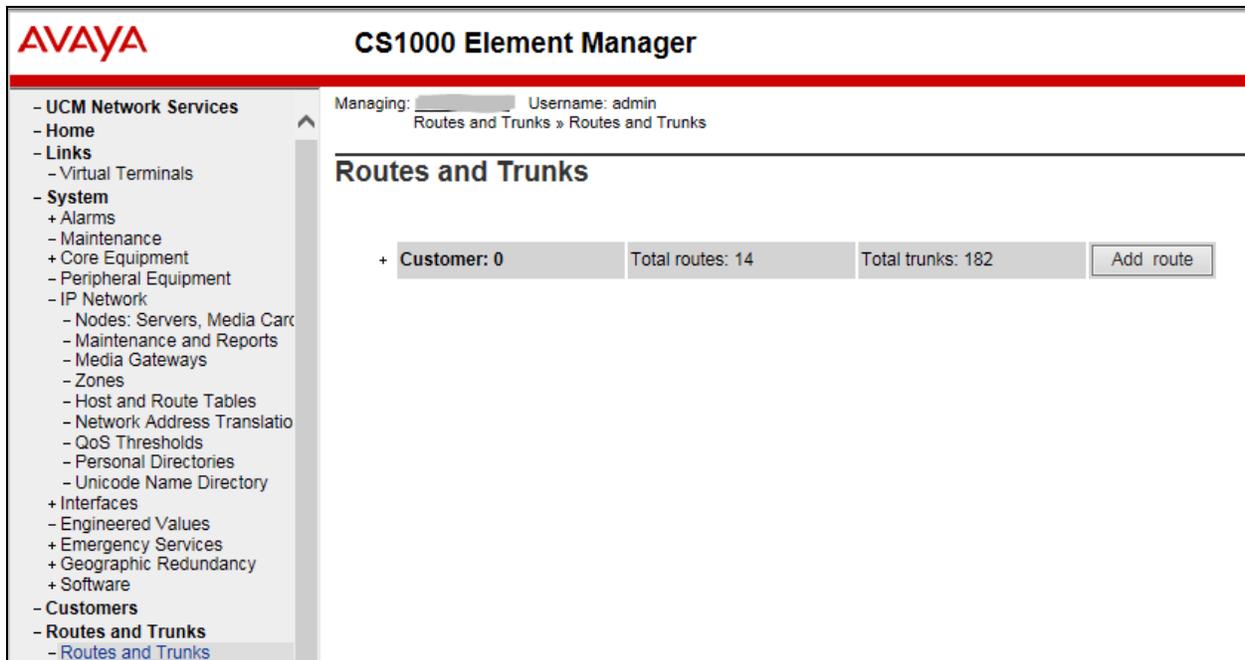
Now click on the **Submit** button (not shown) to complete the D-channel configuration.

5.4. Configuring Route and Trunks

This section explains the configuration of the SIP route and trunks which will be used by Communication Server 1000 to communicate with the Session Manager. To add a new route, navigate to **Routes and Trunks** → **Routes and Trunks** from the EM left hand navigator window as shown in screen below.



Now from the **Routes and Trunks** screen as shown below click on **Add route** button to start configuring a new route.



During compliance testing route 1 was added. The next three screens below shows the configuration for route 1 used during compliance testing.

- **Route data block (RDB) (TYPE):** *RDB*
- **Customer number (CUST):** *00*
- **Route number (ROUT):** *1*
- **Designator field for trunk (DES):** A descriptive name.
- **Trunk type (TKTP):** *TIE*
- **Incoming and outgoing trunk (ICOG):** Select *Incoming and Outgoing (IAO)* from the drop down menu.
- **Access code for the trunk route (ACOD):** An available Directory number from the system.
- **The route is for a virtual trunk route (VTRK):** Enable the box.
- **Zone for codec selection and bandwidth management (ZONE):** A number configured in the system.
- **Node ID of signaling server of this route (NODE):** *510*; this is the same node added in **Section 5.2**.
- **Protocol ID for the route (PCID):** Select *SIP (SIP)* from the drop down menu.
- **Integrated services digital network option (ISDN):** Enable the box.
- **D channel number (DCH):** *1*; this is the same D channel added in **Section 5.3**.
- **Interface type for route (IFC):** Select *Meridian M1 (SL1)* from the drop down menu.
- **Private network identifier (PNI):** A value configured in the system.
- **Call type for outgoing direct dialed TIE route (CTYP):** Select *Coordinated Dialing Plan (CDP)* from the drop down menu.
- **Calling number dialing plan (CNDP):** Select *Coordinated dialing plan (CDP)* from the drop down menu.
- **Signaling arrangement (SIGO):** Select *Standard (STD)* from the drop down menu.
- **Route class (RCLS):** Select *Route Class marked as external (EXT)* from the drop down menu.

Retain default values for other fields.

Now click on the **Submit** button (not shown) to complete the configuration.

Customer 0, Route 1 Property Configuration

- Basic Configuration

Route data block (RDB) (TYPE) : RDB

Customer number (CUST) : 00

Route number (ROUT) : 1

Designator field for trunk (DES) : SIP

Trunk type (TKTP) : TIE

Incoming and outgoing trunk (ICOG) : Incoming and Outgoing (IAO) ▾

Access code for the trunk route (ACOD) : 8001 *

Trunk type M911P (M911P) :

The route is for a virtual trunk route (VTRK) :

- Zone for codec selection and bandwidth management (ZONE) : 00002 (0 - 8000)

- Node ID of signaling server of this route (NODE) : 510 (0 - 9999)

- Protocol ID for the route (PCID) : SIP (SIP) ▾

- Print correlation ID in CDR for the route (CRID) :

- Enable Shared Bandwidth Management for the route (SBWM) :

Integrated services digital network option (ISDN) :

- Mode of operation (MODE) : Route uses ISDN Signaling Link (ISLD) ▾

- D channel number (DCH) : 1 (0 - 254)

- Interface type for route (IFC) : Meridian M1 (SL1) ▾

- Private network identifier (PNI) : 00001 (0 - 32700)

- Network calling name allowed (NCNA) :

- Call type for outgoing direct dialed TIE route (CTYP) : Coordinated Dialing Plan (CDP) ▾

- Insert ESN access code (INAC) :

- Integrated service access route (ISAR) :

- Display of access prefix on CLID (DAPC) :

- Mobile extension route (MBXR) :

- Mobile extension outgoing type (MBXOT) : National number (NPA) ▾

- Mobile extension timer (MBXT) : 0 (0 - 8000 milliseconds)

Calling number dialing plan (CNDP) : Coordinated dialing plan (CDP) ▾

- Network Options

Electronic switched network pad control (ESN) :

Signaling arrangement (SIGO) : Standard (STD) ▾

Route class (RCLS) : Route Class marked as external (EXT) ▾

After the route has been configured, trunks can be added that belongs to this route. The two screens below shows the configuration of the trunks that was used during compliance testing.

- **Auto increment member number:** Enable this box.
- **Trunk data block:** *IPTI*
- **Terminal number:** An available terminal number from the system.
- **Designator field for trunk:** A descriptive name.
- **Extended trunk:** *VTRK*
- **Member number:** *1*; this is the starting member number of the trunk.
- **Start arrangement Incoming:** Select *Immediate (IMM)* from the drop down menu.
- **Start arrangement Outgoing:** Select *Immediate (IMM)* from the drop down menu.
- **Class of Service:** Click on the **Edit** button.
- **Restriction level:** Select *Unrestricted (UNR)* from the drop down menu.

Retain default values for other fields.

Now click on **Return Class of Service** button (not shown) to return to the main page of trunks configuration. Click on **Save** button (not shown) to complete the trunks configuration.

Customer 0, Route 1, Trunk 1 Property Configuration

- Basic Configuration

Auto increment member number:

Trunk data block:

Terminal number:

Designator field for trunk:

Extended trunk:

Member number: *

Level 3 Signaling:

Card density:

Start arrangement Incoming:

Start arrangement Outgoing:

Trunk group access restriction:

Channel ID for this trunk:

Class of Service:

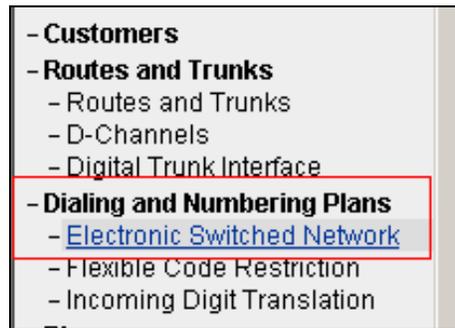
- Priority:

- Restriction level:

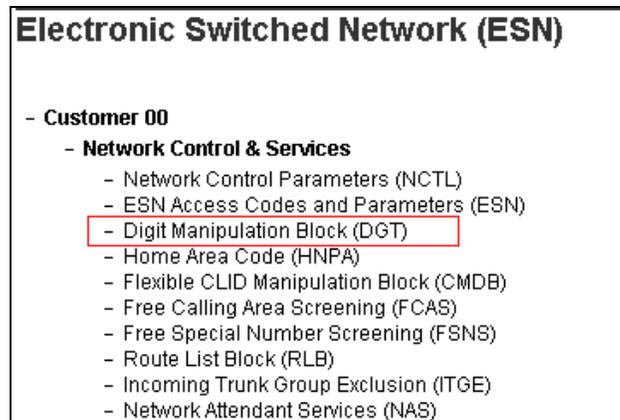
- Reversed Ear Piece:

5.5. Configuring Digit Manipulation Block

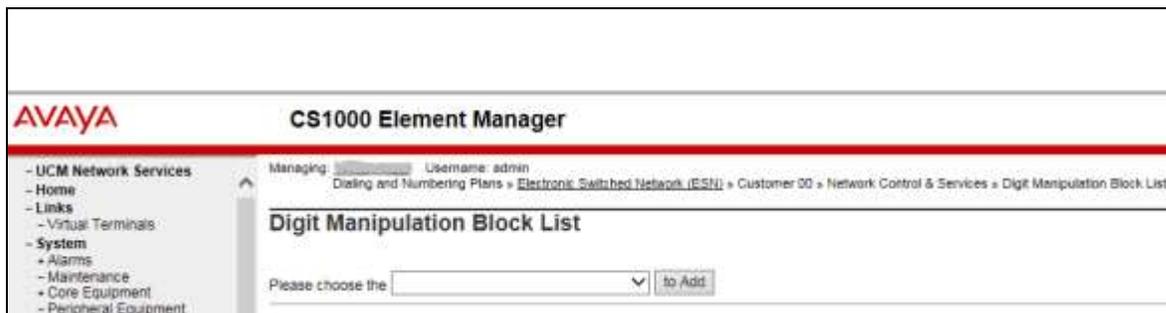
This section explains the digit manipulation block that is to be configured in the Communication Server 1000 dialing plan for its users to communicate with the Responder via the Session Manager. From the EM navigator pane, navigate to **Dialing and Numbering Plans** → **Electronic Switched Network** as shown below.



Click on **Digit Manipulation Block (DGT)** option as shown below.

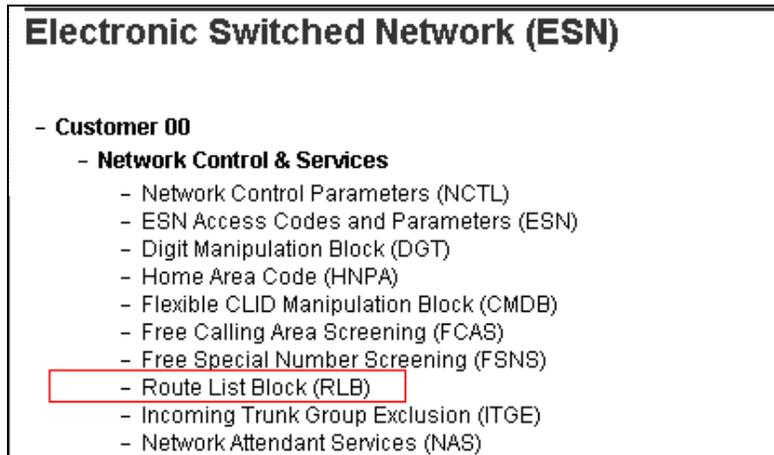


Screen below shows the **Digit Manipulation Block List** page where users can add a digit manipulation block index by selecting an available one from the drop down menu. During compliance testing **Digit Manipulation Block Index -- 0** was used which is already added in the Communication Server 1000 system by default.

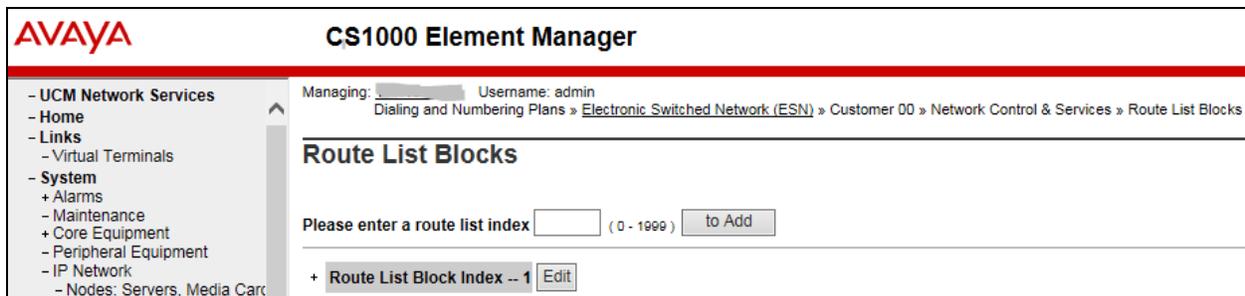


5.6. Configuring Route List Block

This section explains the route list block that is to be configured in the Communication Server 1000 dialing plan for its users to communicate with the Responder via Session Manager. From the EM navigator pane, navigate to **Dialing and Numbering Plans → Electronic Switched Network** as shown in **Section 5.5**. Click on **Route List Block (RLB)** option as shown below.



To add a route list index, enter a valid number in the **Please enter a route list index** box and click on **to Add** button as shown in the screen below. During compliance testing a route list block index of **1** was added.



Screen below show the values configured for the route list index block 1 added during compliance testing.

- **Digit Manipulation Index:** Select 0 from the drop down menu. This was configured in **Section 5.5**.
- **Route Number:** Select 1 from the drop down menu. This was configured in **Section 5.4**.

Retain default values for other fields.

Click on **Submit** to complete the configuration.

Data Entry of a Route List Block

Route List Block Index: 1

General Properties

Entry Number for the Route List:

Indexes

Time of Day Schedule: ▼

Facility Restriction Level: (0 - 7)

Digit Manipulation Index: ▼

ISL D-Channel Down Digit Manipulation Index: (0 - 1999)

Free Calling Area Screening Index: ▼

Free Special Number Screening Index: ▼

Business Network Extension Route:

Incoming CLID Table: (0 - 100)

Options

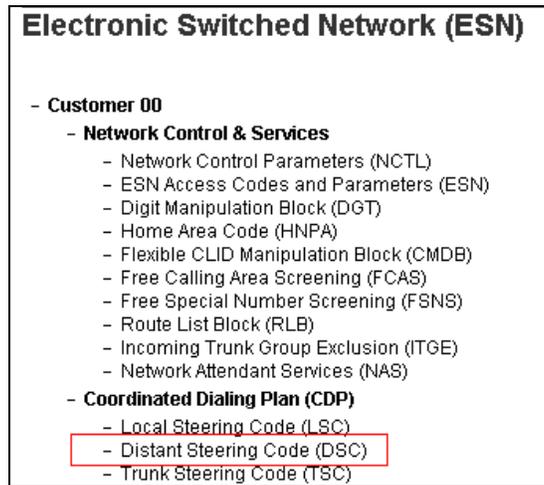
Local Termination entry:

Route Number: ▼

Skip Conventional Signaling:

5.7. Configuring Distant Steering Code

This section explains the distant steering code that is to be configured in the Communication Server 1000 dialing plan for its users to communicate with the Responder via Session Manager. From the EM navigator pane, navigate to **Dialing and Numbering Plans → Electronic Switched Network** as shown in **Section 5.5**. Click on **Distant Steering Code (DSC)** option as shown below.



To add a distant steering code, select **Add** from the drop down menu and enter an available distant steering code in the **Please enter a distant steering code** box and click on **Add** button to finish adding one as shown in the screen below. During compliance testing a code of **30** was added since the pilot number assigned to Responder was 30xxx.



Screen below show the values configured for the distant steering code of 30 added during compliance testing.

Enter the values as shown in screen below.

- **Flexible Length number of digits:** 5; since 30xxx the number to dial Responder is a 5 digit number.
- **Route List to be accessed for trunk steering code:** Select 1 from the drop down menu. This was configured in **Section 5.6**.

Retain default values for other fields.

Click on **Submit** to complete the configuration.

Distant Steering Code

Distant Steering Code:

Flexible Length number of digits: (0 - 10)

Display:

Remote Radio Paging Access:

Route List to be accessed for trunk steering code:

Collect Call Blocking:

Maximum 7 digit NPA code allowed:

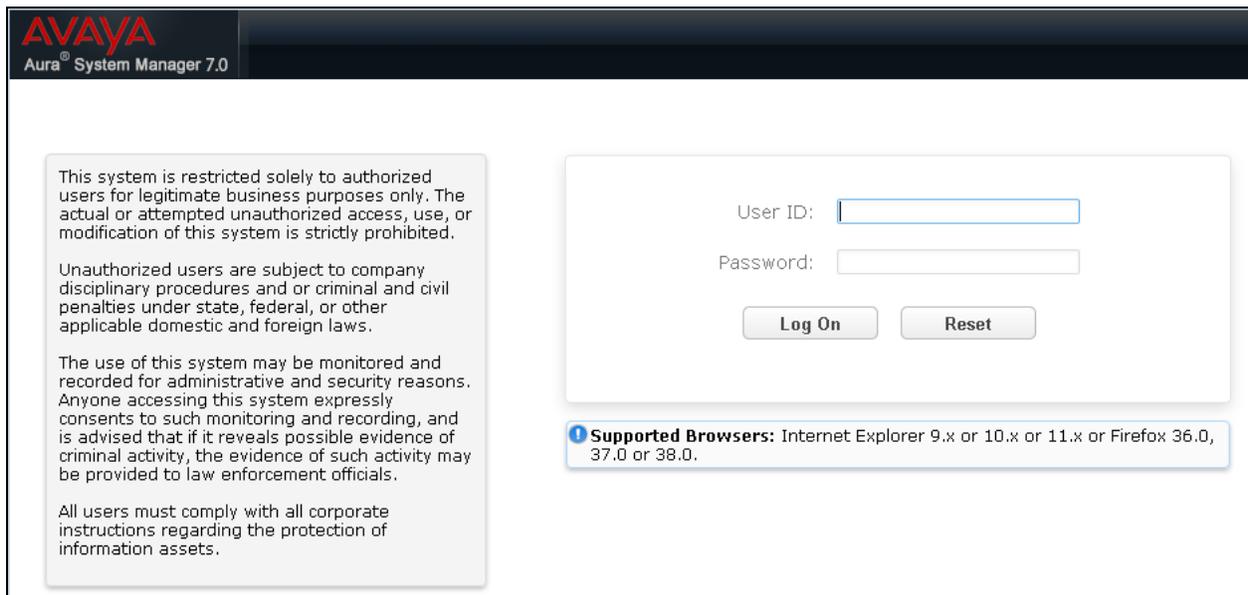
Maximum 7 digit NXX code allowed:

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.



AVAYA
Aura® System Manager 7.0

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

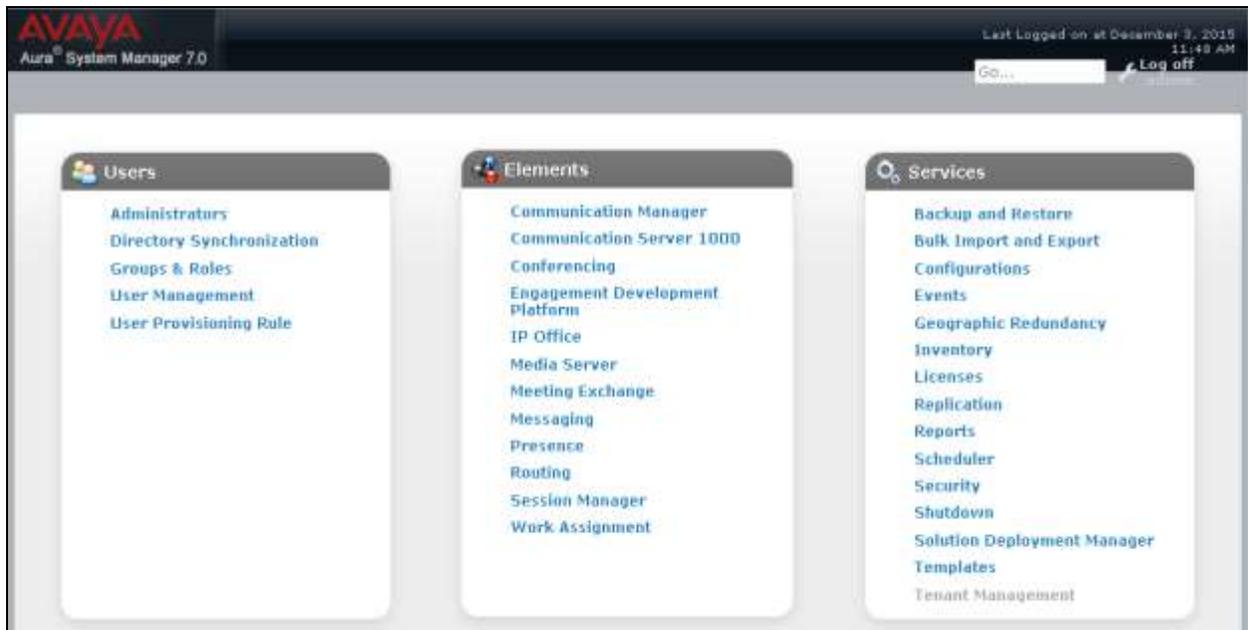
User ID:

Password:

Log On **Reset**

Supported Browsers: Internet Explorer 9.x or 10.x or 11.x or Firefox 36.0, 37.0 or 38.0.

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.



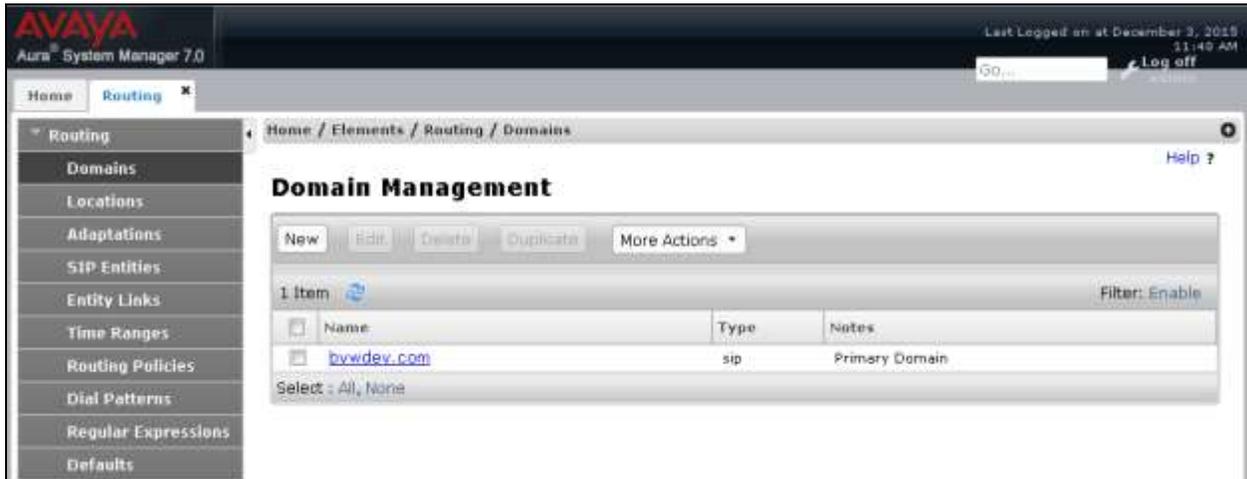
6.1. Configure Session Manager Details

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 **bvwddev.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 Server 1000, 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**.

The screenshot displays the 'Adaptation Details' configuration page in the Avaya Aura System Manager 7.0. The page is titled 'Adaptation Details' and has a 'General' tab selected. The 'Adaptation Name' field contains 'For_Rauland'. The 'Module Name' dropdown is set to 'DigitConversionAdapter'. The 'Module Parameter Type' dropdown is set to 'Name-Value Parameter'. Below these fields is a table with columns 'Name' and 'Value'. The table contains three rows: 'fromto' with value 'true', 'iodstd' with value 'bvwdev.com', and 'iosrcd' with value 'bvwdev.com'. There are 'Add' and 'Remove' buttons above the table. At the bottom of the form, there are fields for 'Egress URI Parameters' and 'Notes'. The interface includes a navigation menu on the left with options like 'Routing', 'Domains', 'Locations', 'Adaptations', etc. The top right shows the user is logged in as 'Left' on December 3, 2016, at 11:49 AM.

Screen below shows the Adaptation rule after it was Committed.

The screenshot shows the Avaya Aura System Manager 7.0 interface. The top navigation bar includes the Avaya logo, 'Aura System Manager 7.0', and a 'Log off' button. The breadcrumb trail is 'Home / Elements / Routing / Adaptations'. The main content area is titled 'Adaptations' and contains a table with the following data:

Name	Module Name	Module Parameters	Egress URI Parameters	Notes
CS1000Adapter	CS1000Adapter	fronto=true		CS1000 adapter for Phone Context
For Bauland	DigitConversionAdapter	fronto=true iodstd=bvwdev.com iosrcd=bvwdev.com odstd=10.10.5.22		

Below the table, there is a 'Select: All, None' option.

6.1.4. Add a SIP Entity

It is assumed that user has already configured SIP entities for Session Manager and Communication Server 1000. 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.

AVAYA
Aura System Manager 7.0

Last Logged on at December 3, 2015 11:48 AM
Go... Log off

Home Routing

Routing / Elements / Routing / SIP Entities

SIP Entity Details

Commit Cancel Help ?

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 Server 1000. 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.

name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy
DevvmSM_Rauland_5060_UDP	DevvmSM	UDP	5060	Rauland	<input type="checkbox"/>	5060	trusted

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 Server 1000. 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
Avaya System Manager 7.0

Last Logged on at December 3, 2015 11:45 AM
Log off admin

Home / Elements / Routing / Routing Policies

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

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	<input checked="" type="checkbox"/>	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
00	\$	\$	<input type="checkbox"/>	bxwdev.com	Befeville	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 Server 1000. 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.

The screenshot displays the 'Dial Pattern Details' configuration page in Avaya Aura System Manager 7.0. The left-hand navigation pane shows 'Dial Patterns' selected. The main area is titled 'Dial Pattern Details' and contains the following fields:

- Pattern:** 30
- Min:** 5
- Max:** 5
- Emergency Call:**
- Emergency Priority:** 1
- Emergency Type:** (empty)
- SIP Domain:** bvwdev.com
- Notes:** Dial pattern to reach Rauland server

Below the 'General' section is the 'Originating Locations and Routing Policies' section, which includes a table with the following data:

Item	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Belleville	Belleville DevConnect Lab	Route_to_Rauland_Server	0	<input type="checkbox"/>	Rauland	Route to a partner testing server

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.

Originating Location

Apply The Selected Routing Policies to All Originating Locations

1 Item [Refresh](#) Filter: Enable

<input type="checkbox"/>	Name	Notes
<input checked="" type="checkbox"/>	Belleville	Belleville DevConnect Lab

Select : All, None

Routing Policies

9 Items [Refresh](#) Filter: Enable

<input type="checkbox"/>	Name	Disabled	Destination	Notes
<input type="checkbox"/>	Route_to_CS1K_CPPM3	<input type="checkbox"/>	CS1K_Bottom	Route to the bottom CS1000
<input type="checkbox"/>	Route to DevAAM	<input type="checkbox"/>	DevAAM	
<input type="checkbox"/>	Route_to_DevCM	<input type="checkbox"/>	DevCM	Route to the main CM in the lab
<input type="checkbox"/>	RouteToDevvmCM	<input type="checkbox"/>	DevvmCM	
<input type="checkbox"/>	Route_to_IPO_36	<input type="checkbox"/>	IPO_36	Route to the top IP Office
<input type="checkbox"/>	Route_to_IPO_41_Server	<input type="checkbox"/>	IPO_41_Server	Route to the IP Office Server Edition
<input type="checkbox"/>	Route_to_IPO_44_Exp	<input type="checkbox"/>	IPO_44_Exp	Route to the IP Office Expansion
<input type="checkbox"/>	[REDACTED]	<input checked="" type="checkbox"/>	[REDACTED]	Route to a partner testing server
<input checked="" type="checkbox"/>	Route_to_Rauland_Server	<input type="checkbox"/>	Rauland	Route to a partner testing server

Select : All, None

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 Server 1000 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 UNISTim and SIP devices administered on Communication Server 1000.

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.

Employee #	User Name	Password	First Name	Middle Name	Last Name	Staff Level	Role	Permanent Device	Permanent Badge
00000001			Admin				Admin Role		
10001			Sharon		Strom	PCT	Surgery Clinical		
10003			Ann		Strom	RN	Surgery Clinical		
10006			Loise		Strom	PCT	Surgery Clinical		
10006			Rae		Strom	PCT	Surgery Clinical		
10007			Byth		Strom	PCT	Surgery Clinical		
10006			P	A	Strom	EVS	EVS		
10009			Van		Strom	EVS	EVS		
1001			Barbara		Strom	PCT	Surgery Clinical		
10010			Geoff		Strom	EVS	EVS		
10016			Philp		Strom	EVS Supervisor	EVS		
10017			Sue		Strom	RN	Surgery Clinical		
10018			Willy		Strom	RN	Surgery Clinical		
10018			Patricia		Strom	RN	Surgery Clinical		
10023			Tie		Strom	RN	Surgery Clinical		
10024			C	J	Strom	Nurse Manager	Nurse Manager		
10028			Jonathan		Strom	RN	Surgery Clinical		
10028			Rae		Strom	RN	Surgery Clinical		
10028			Maria		Strom	Unit Secretary	Surgery Clinical		
10029			Harold		Strom	RN	Surgery Clinical		
10030			Deryke		Strom	RN	Surgery Clinical		
10034			J	C	Strom	PCT	S East Clinical		
10036			Kathleen		Strom	PCT	S East Clinical		
10042			Zayd		Strom	PCT	S East Clinical		
10043			Garrett		Strom	RN	S East Clinical		
10044			Yanna		Strom	RN	S East Clinical		
10048			Mira		Strom	RN	S East Clinical		

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 members 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.

The screenshot shows the Brekeke SIP Server configuration interface. The left sidebar contains the following menu items: SIP Server (selected), SIP SERVER, Registered Clients, Active Sessions, User Authentication, Dial Plan, Aliases, Logs, Push Notification, Domains, Configuration, SYSTEM (+), MAINTENANCE (-), Start/Shutdown, and Software Maintenance. The main content area has tabs for System, SIP, RTP, Database/Radius, and Advanced. The System tab is active, displaying the following configuration sections:

- General**
 - Server Name: your-sip-sv
 - Server Description: your SIP Server
 - Server Location: your-place
 - Administrator SIP URI: your-sip-uri
 - Administrator Email Address: [empty]
 - Start up: manual auto
- Network**
 - Interface address 1: 10.10.5.34
 - Remote Address Pattern 1: [empty]
 - Interface address 2: [empty]
 - Remote Address Pattern 2: [empty]
 - Interface address 3: [empty]
 - Remote Address Pattern 3: [empty]
 - Interface address 4: [empty]
 - Remote Address Pattern 4: [empty]
 - Interface address 5: [empty]
 - Remote Address Pattern 5: [empty]
 - Auto interface discovery: on off
 - External IP address pattern: [empty]
 - Internal IP address pattern: [empty]
- IPv6**
 - IPv6: on off
 - RFC3484's policy table for Address Selection: on off
- DNS**
 - DNS SRV: on off
 - DNS AAAA: on off
 - DNS Server: [empty]
 - DNS SRV Failover: on off
 - Caching period for resolved name (sec): 3600

MENU	Caching period for unknown name (sec)	<input type="text" value="600"/>
	Caching period for error (sec)	<input type="text" value="10"/>
	UPnP	
	Enable/Disable	<input type="radio"/> enable <input checked="" type="radio"/> disable
	Default router IP address	<input type="text"/>
	Cache size	<input type="text" value="24"/>
	Cache period (sec,0=disable)	<input type="text" value="86400"/>
	Refresh Interval (sec,0=disable)	<input type="text" value="30"/>
	Java	
	Java VM arguments	<input type="text"/>
<input type="button" value="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.

The screenshot displays the Brekeke SIP Server configuration interface. The left sidebar contains a navigation menu with categories: SIP SERVER (Registered Clients, Active Sessions, User Authentication, Dial Plan, Aliases, Logs, Push Notification, Domains, Configuration), SYSTEM (+), MAINTENANCE (-), Start/Shutdown, and Software Maintenance. The main content area is titled 'SIP' and is divided into several sections:

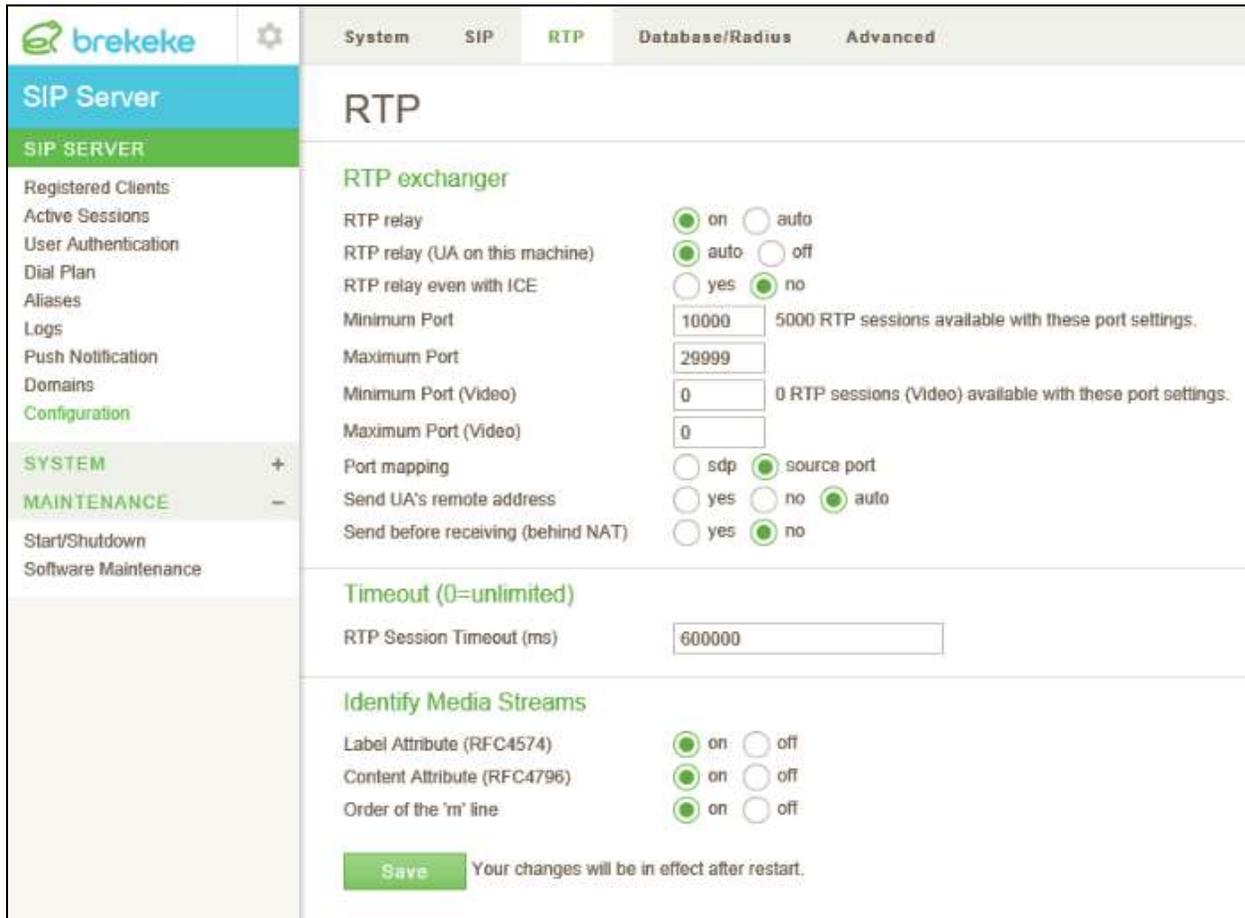
- SIP exchanger**:
 - Session Limit (-1=unlimited): -1
 - Local Port: 5060
 - B2B-UA mode: on off
 - Check Maximum UDP packet size: on off
 - Maximum UDP packet size: 1500
- NAT traversal**:
 - Keep address/port mapping: on off
 - Interval (ms): 12000
 - Method: Blank packet OPTIONS
 - Add 'rport' parameter (Send): on off
 - Add 'rport' parameter (Receive): on off
- Authentication**:
 - REGISTER: on off
 - INVITE: on off
 - MESSAGE: on off
 - SUBSCRIBE: on off
 - Realm (ex: domain name): [Empty text box]
 - Auth-user=user in "To:" (Register): yes no
 - Auth-user=user in "From:": yes no
 - FQDN only: yes no
 - Nonce Expires (seconds): 60
- Registration**:
 - Adjusted Expires: [Empty text box]
- Upper Registration**:
 - On/Off: on off
 - Register Server: [Empty text box]
 - Protocol: UDP TCP TLS

<ul style="list-style-type: none"> Registered Clients Active Sessions User Authentication Dial Plan Aliases Logs Push Notification Domains Configuration 	<h3>Thru Registration</h3> <p>On/Off <input checked="" type="radio"/> on <input type="radio"/> off</p>
	<h3>Timeout (0=unlimited)</h3> <p>Ringing Timeout (ms) <input type="text" value="240000"/></p> <p>Talking Timeout (ms) <input type="text" value="259200000"/></p> <p>Upper/Thru Timeout(ms) <input type="text" value="30000"/></p>
<p>SYSTEM +</p> <p>MAINTENANCE -</p> <p>Start/Shutdown</p> <p>Software Maintenance</p>	<h3>Dial Plan</h3> <p>Maximum history records <input type="text" value="10"/></p>
	<h3>Miscellaneous</h3> <p>100 Trying <input type="radio"/> any requests <input checked="" type="radio"/> only for initial INVITE</p> <p>Check Request-URI's validity <input type="radio"/> yes <input checked="" type="radio"/> no</p> <p>Server/User-Agent <input type="text"/></p>
	<h3>TCP</h3> <p>TCP-handling <input checked="" type="radio"/> on <input type="radio"/> off</p> <p>Queue Size <input type="text" value="50"/></p> <p>Maximum Active Connections (0=unlimited) <input type="text" value="0"/></p>
	<h3>TLS</h3> <p>TLS-handling <input type="radio"/> on <input checked="" type="radio"/> off</p> <p>Queue Size <input type="text" value="50"/></p> <p>Maximum Active Connections <input type="text"/></p>
	<h3>WS (WebSocket)</h3> <p>WS-handling <input type="radio"/> on <input checked="" type="radio"/> off</p> <p>Listen port <input type="text" value="10080"/></p> <p>Queue Size <input type="text" value="50"/></p> <p>Maximum Active Connections <input type="text"/></p>

Start/Shutdown Software Maintenance	WSS (WebSocket over TLS)	
	WSS-handling	<input type="radio"/> on <input checked="" type="radio"/> off
	Listen port	<input type="text" value="10081"/>
	Queue Size	<input type="text" value="50"/>
	Maximum Active Connections	<input type="text"/>
Key and Certificate		
Peer Certification Validation	<input checked="" type="radio"/> on <input type="radio"/> off	
File Type	<input checked="" type="radio"/> Certificate (.pem .der .cer. crt .cerf) and Key (.pem .key .der) <input type="radio"/> JKS <input type="radio"/> PKCS#12 (.p12 .pfx)	
Private Key File	<input type="text" value="No File"/>	<input type="button" value="Browse..."/>
Certificate File	<input type="text" value="No File"/>	<input type="button" value="Browse..."/>
Performance Optimization (Proxy)		
Initial threads	<input type="text"/>	Upgrade required
Maximum Sessions per thread	<input type="text"/>	Upgrade required
Performance Optimization (Registrar)		
Initial threads	<input type="text"/>	Upgrade required
Maximum Sessions per thread	<input type="text"/>	Upgrade required
<input type="button" value="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.



brekeke [Settings] System SIP **RTP** Database/Radius Advanced

SIP Server

SIP SERVER

- Registered Clients
- Active Sessions
- User Authentication
- Dial Plan
- Aliases
- Logs
- Push Notification
- Domains
- Configuration

SYSTEM +

MAINTENANCE -

- Start/Shutdown
- Software Maintenance

RTP

RTP exchanger

RTP relay on auto

RTP relay (UA on this machine) auto off

RTP relay even with ICE yes no

Minimum Port 5000 RTP sessions available with these port settings.

Maximum Port

Minimum Port (Video) 0 RTP sessions (Video) available with these port settings.

Maximum Port (Video)

Port mapping sdp source port

Send UA's remote address yes no auto

Send before receiving (behind NAT) yes no

Timeout (0=unlimited)

RTP Session Timeout (ms)

Identify Media Streams

Label Attribute (RFC4574) on off

Content Attribute (RFC4796) on off

Order of the 'm' line on off

Save Your changes will be in effect after restart.

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 Server 1000, the **To CS1000** rule was used.

The screenshot shows the Brekeke SIP Server Admin interface. The 'Rules' section is active, displaying a table of dial plan routing rules. The table has four main columns: Pri, Name, Matching Patterns, and Deploy Patterns. There are five rules listed, with the first and third rules highlighted with red boxes.

Pri	Name	Matching Patterns	Deploy Patterns
1	From Avaya	<pre>\$request = ^INVITE \$addr = 10.10.97.228 To = sip:30(.+)@ Alert-Info = .* P-Location = .* P-AV-Message-Id = .* x-nt-corr-id = .* AV-Global-Session-ID = .*</pre>	<pre>To = sip:%1@10.10.5.22 \$transport = UDP \$b2bua = true &net.sip.replacesdp.multipart = true Alert-Info = P-Location = P-AV-Message-Id = x-nt-corr-id = AV-Global-Session-ID = \$session = sdp &sdp.audio.a.1 =ptime:20</pre>
2	From IP Office	<pre>\$request = ^INVITE \$addr = [REDACTED] To = sip:30(.+)@ Alert-Info = .* P-Location = .* P-AV-Message-Id = .* x-nt-corr-id = .* AV-Global-Session-ID = .*</pre>	<pre>To = sip:%1@[REDACTED] \$transport = UDP \$b2bua = true &net.sip.replacesdp.multipart = true Alert-Info = P-Location = P-AV-Message-Id = x-nt-corr-id = AV-Global-Session-ID = \$session = sdp &sdp.audio.a.1 =ptime:20</pre>
3	To CS1000	<pre>\$request = ^INVITE To = sip:(56.+)@</pre>	<pre>To = sip:%1@10.10.97.228</pre>
4	To CM	<pre>\$request = ^INVITE To = sip:(56.+)@</pre>	<pre>To = sip:%1@[REDACTED]</pre>
5	To IP Office	<pre>\$request = ^INVITE To = sip:(26.+)@</pre>	<pre>To = sip:%1@[REDACTED]</pre>

At the bottom of the interface, there are settings for DNS SRV Failover (set to 'on') and Caching period for resolved name (set to '3600').

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.



The screenshot shows the Brekeke SIP Server Admin interface. The main content area is titled "Registered Clients" and displays a table of registered clients. The table has three columns: "User", "Contact URI (Source IP Address)", and "Detail". There are three rows of data, each representing a registered client. The "Detail" column for each row shows "Expires : 3600", "Priority : 1000", "User Agent :", "Transport : UDP", and "Time Update : Thu Dec 03 11:01:37 CST 2015".

User	Contact URI (Source IP Address)	Detail
5*501	sip:5*501@10.0.0.1:5064 (10.0.0.1:5064)	Expires : 3600 Priority : 1000 User Agent : Transport : UDP Time Update : Thu Dec 03 11:01:37 CST 2015
5*501*1	sip:5*501*1@10.0.0.1:5064 (10.0.0.1:5064)	Expires : 3600 Priority : 1000 User Agent : Transport : UDP Time Update : Thu Dec 03 11:01:37 CST 2015
5*501*101	sip:5*501*101@10.0.0.1:5064 (10.0.0.1:5064)	Expires : 3600 Priority : 1000 User Agent : Transport : UDP Time Update : Thu Dec 03 11:01:37 CST 2015

9. Conclusion

These Application Notes describe the procedures required to configure Rauland-Borg Responder® 5 to interoperate with endpoints registered to Avaya Communication Server 1000 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.

10. Additional References

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

Avaya

1. *Communication Server 1000E Installation and Commissioning*, Release 7.6, NN43041-310
2. *Element Manager System Reference – Administration - Avaya Communication Server 1000*, Release 7.6, NN43001-632.
3. *Avaya Communication Server 1000 Co-resident Call Server and Signaling Server Fundamentals* Release 7.6, NN43001-509.
4. *Avaya Communication Server 1000 Unified Communications Management Common Services Fundamentals -*, Release 7.6, NN43001-116.
5. *Avaya Communication Server 1000 - Software Input Output Reference — Administration* Release 7.6, NN43001-611.
6. *Avaya Communication Server 1000 - ISDN Primary Rate Interface Installation and Commissioning*, Release 7.6, NN43001-301.
7. *Implementing Avaya Aura® Session Manager* Document ID 03-603473.
8. *Administering Avaya Aura® Session Manager*, Doc ID 03-603324.
9. *Deploying Avaya Aura® System Manager*, Release 7.0.
10. *Administering Avaya Aura® System Manager for Release 7.0*, Release 7.0.

Rauland-Borg

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

©2016 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.