



**Application Notes for PatientSafe Solutions' PatientTouch[®]
Communications with Avaya Communication Server 1000
and Avaya Aura[®] Session Manager using SIP Trunks
– Issue 1.0**

Abstract

These Application Notes describe the configuration steps required for PatientSafe Solutions' PatientTouch Communications to interoperate with Avaya Communication Server 1000 and Avaya Aura[®] Session Manager using SIP trunks.

PatientTouch Clinical Communications solution facilitates hospital care team collaboration by combining real-time clinical context with intuitive technology with minimal IT requirements. In the compliance testing, PatientTouch Communications used SIP trunks to Avaya Aura[®] Session Manager, for PatientTouch users to reach users on Avaya Communication Server 1000 and on the PSTN.

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 the configuration steps required for PatientSafe Solutions' PatientTouch® Communications to interoperate with Avaya Communication Server 1000 (Communication Server 1000) and Avaya Aura® Session Manager (Session Manager) using SIP trunks.

PatientTouch Communications facilitates hospital care team collaboration by combining real-time clinical context with intuitive technology with minimal IT requirements. By delivering secured texting, voice, alerts, and critical context, PatientTouch Communications provides clinicians with the right information, at the right time, about the right patient, in the right way—to deliver better, safer, Connected Patient Care™. In the compliance tests, PatientTouch Communications used SIP trunks to Avaya Aura® Session Manager allowing PatientTouch users to reach users on Avaya Communication Server 1000 and on the PSTN.

2. General Test Approach and Test Results

The feature test cases were performed manually. Calls were manually established among PatientTouch users with Avaya SIP, Avaya UNiStim, and/or PSTN users.

The serviceability test cases were performed manually by disconnecting and reconnecting the LAN connection to PatientTouch Communications.

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 interoperability compliance test included feature and serviceability testing.

The feature testing included; basic call, display, G.711, hold/reconnect, call forwarding unconditional and call transfer.

The serviceability testing focused on verifying the ability of PatientTouch Communications to recover from adverse conditions, such as disconnecting/reconnecting the LAN connection.

2.2. Test Results

All test cases passed with following observations:

- During the compliance test, only G711MU was utilized.
- This version of PatientSafe Server (PSS) does not support the transfer feature. PatientTouch users can be the initiator or destination of a call flow, but not the transferee. All transfers were done via the Avaya phones.
- This version of PSS does not support conference feature and hence it was not tested.
- PatientTouch users are not members of voice messaging system and therefore Message Waiting Indicator (MWI) feature testing is not relevant for this compliance testing.
- Forwarding feature for PatientTouch users works in following scenarios, forward on manual decline, forward no answer, forward on busy, and forward on unavailable (i.e. user being logged out).

2.3. Support

Technical support on PatientTouch Communications can be obtained through the following:

- **Phone:** (858) 746-3100
- **Email:** support@patientsafesolutions.com

3. Reference Configuration

As shown in the test configuration below, PatientTouch Communications consists of the PatientTouch Server and clients. SIP trunks are used from PatientTouch Communications to Avaya Aura® Session Manager, to reach users on Avaya Communication Server 1000 and on the PSTN.

A five digit dialing plan was used to facilitate dialing between the Avaya and PatientTouch sites. Unique extension ranges were associated with Avaya Communication Server 1000 users (54xxx), and PatientTouch users (30xxx).

The configuration of Session Manager is performed via the web interface of Avaya Aura® System Manager (System Manager). The configuration of Communication Server 1000 is performed via the web interface of the Uniform Communication Manager (UCM). The detailed administration of basic connectivity between Communication Server 1000, System Manager, and Session Manager is not the focus of these Application Notes and will not be described.

The configuration of PatientTouch Communications and on wireless phones was performed by a PatientSafe Solutions engineer prior to the solution testing. During compliance testing the PSS was installed as a virtual machine on a VMWare host server.

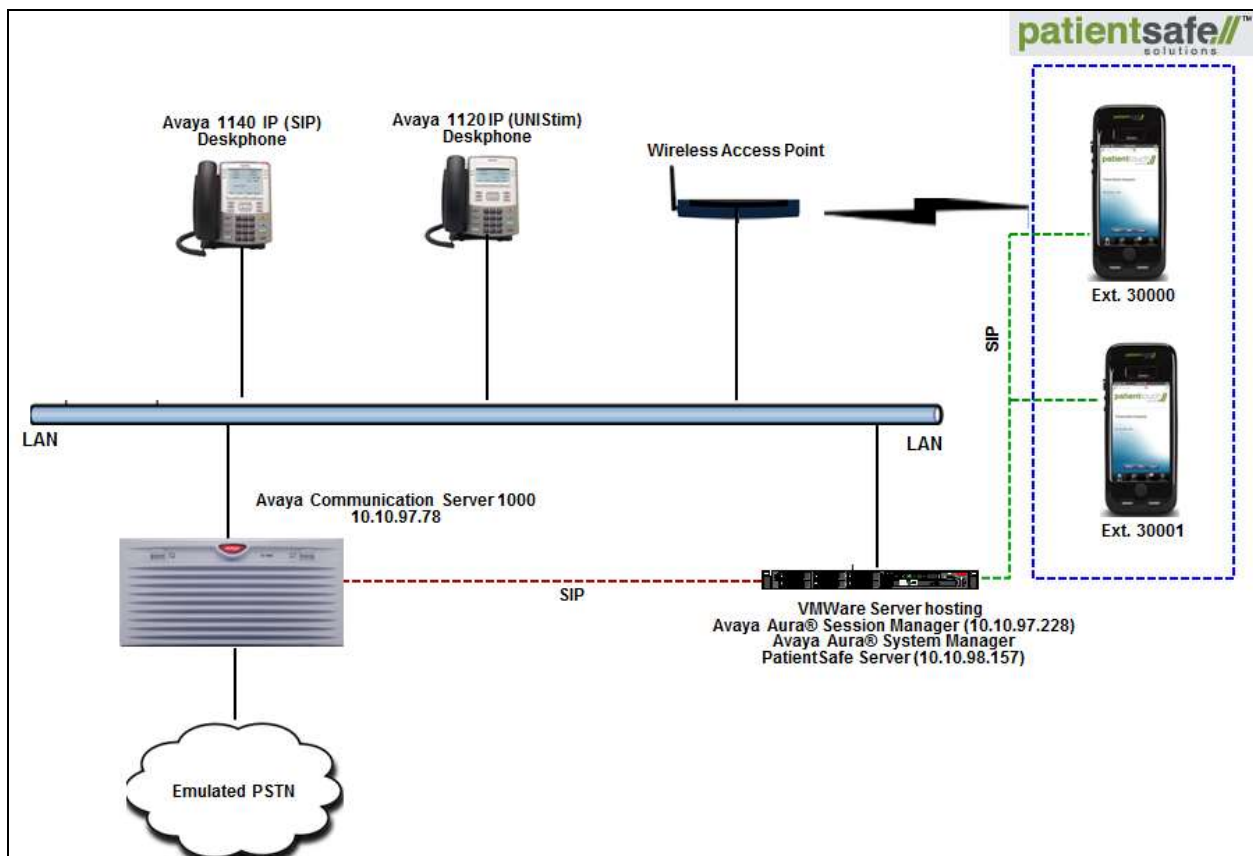


Figure 1: Avaya Communication Server 1000 and PatientSafe Reference Configuration

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment	Software
Avaya Communication Server 1000	7.65 SP7
Avaya Aura® Session Manager	7.0.0.0.700007
Avaya Aura® System Manager	7.0.0.0.16266
Avaya 1120E Deskphone (UNISim) Avaya 1140E Deskphone (SIP)	0624C8Q 04.03.12.00
PatientSafe Solutions • PatientTouch (Server/App) • iPhone 5s (ME296LL/A)	3.3.1(2719/2722) 9.0.2

5. Configure Avaya Communication Server 1000

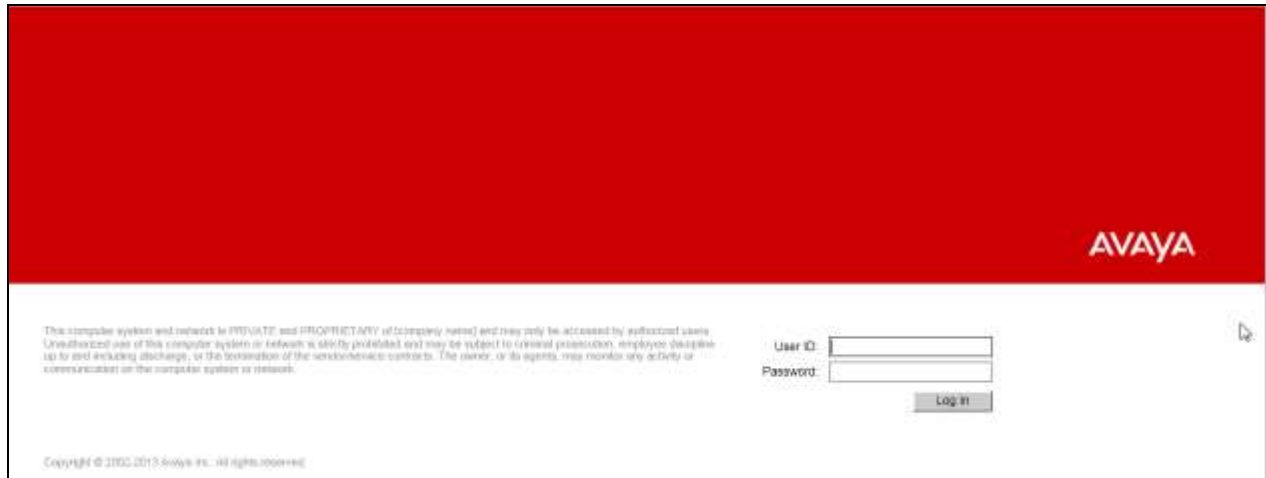
This section describes the Communication Server 1000 configuration necessary to interoperate with Session Manager and PSS. It provides the procedures for configuring Communication Server 1000 system. The procedures include the following areas:

- Logging into the Element Manager via UCM.
- Configuring the SIP Signaling Gateway.
- Configuring Voice Codecs on Media Gateways.
- Configuring Zones.
- Configure Integrated Services Digital Network (ISDN).
- Configuring a D-Channel.
- Configuring Route and Trunks.
- Configuring Digit Manipulation Block.
- Configuring Route List Block.
- Configuring Dialing Plan.

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

5.1. Logging into Element Manager via Unified Communication Manager

To login to the UCM open an IE browser and type in the IP address of the UCM in the URL. Screen below shows the main login screen. Enter the correct credentials to login.

The image shows the Avaya login interface. It features a prominent red header bar with the 'AVAYA' logo in white on the right side. Below the header, on the left, is a block of small, grey text containing a legal disclaimer. To the right of this text is a login form with two input fields: 'User ID' and 'Password'. A 'Log in' button is positioned below the password field. In the bottom left corner, there is a small copyright notice: 'Copyright © 2002-2013 Avaya Inc. All rights reserved.'

This computer system and network is PRIVATE and PROPRIETARY (if necessary items) and may only be accessed by authorized users. Unauthorized use of this computer system or network is strictly prohibited and may be subject to criminal prosecution, employee discipline up to and including discharge, or the termination of the vendor/service contracts. The owner, or its agents, may monitor any activity or communication on the computer system or network.

User ID:

Password:

Log in

Copyright © 2002-2013 Avaya Inc. All rights reserved.

From the **Elements** page 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.

AVAYA Avaya Unified Communications Management

Host Name: sip175.bvwdev.com Software Version: 02.30.0096.00(6706) User Name admin

Elements

New elements are registered into the security framework, or may be added as simple hyperlinks. Click an element to enter a search term.

Search Reset

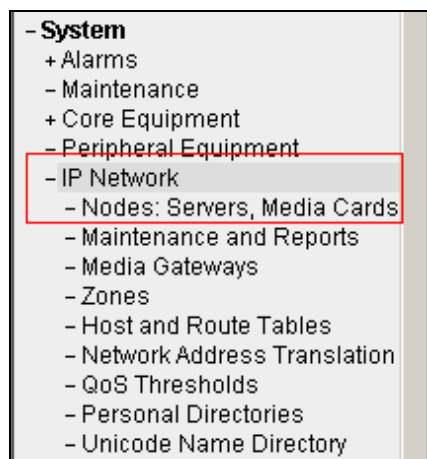
Add... Edit... Delete

	Element Name	Element Type ^	Release
1	EM on sip175	CS1000	7.6
2	cpdm3.bvwdev.com (member)	Linux Base	7.6
3	sip175.bvwdev.com (primary)	Linux Base	7.6

5.2. Configuring the SIP Signaling Gateway

This section describes the configuration required on the SIP Signaling Gateway present on the Communication Server 1000 so that 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: 10.10.97.78 Username: admin						
System » IP Network » IP Telephony Nodes						
IP Telephony Nodes						
Click the Node ID to view or edit its properties.						
Add... Import... Export... Delete Print Refresh						
☐ Node ID ▲	Components	Enabled Applications	ELAN IP	Node/TLAN IPv4	Node/TLAN IPv6	Status
☐ 510	1	LTPS, Gateway (SIPGw)	-	10.10.97.149	-	Synchronized

On the **Node Details** page, select the **Terminal Proxy Server (TPS)** link as shown in screen below. In the field **UNISTim Line Terminal Proxy Server** check the box for *Enable proxy server on this node* (not shown) and then click the **Save** button (not shown).

AVAYA

CS1000 Element Manager

Managing: 10.10.97.78 Username: admin
System » IP Network » IP Telephony Nodes » Node Details

Node Details (ID: 510 - LTPS, Gateway (SIPGw))

Subnet mask: 255.255.255.192 *

Subnet mask: 255.255.255.192 *

Node IPv6 address:

IP Telephony Node Properties

- Voice Gateway (VGVW) and Codecs
- Quality of Service (QoS)
- LAN
- SNTP
- Numbering Zones
- MCDN Alternative Routing Treatment (MALT) Causes

Applications (click to edit configuration)

- SIP Line
- Terminal Proxy Server (TPS)**
- Gateway SIP User
- Personal Directories (PD)
- Presence Publisher
- IP Media Services

* Required Value

On the **Node Details** page, select the **Quality of Service (QoS)** link as shown in screen below. Retain default values under the **Diffserv Codepoint (DSCP)** section (not shown). Click on the **Save** button (not shown).

AVAYA CS1000 Element Manager

Managing: 10.10.97.78 Username: admin
System > IP Network > IP Telephony Nodes > Node Details

Node Details (ID: 510 - LTPS, Gateway (SIPGW))

Subnet mask: 255.255.255.192 * Subnet mask: 255.255.255.192 *
Node IPv6 address: [Empty field]

IP Telephony Node Properties

- Voice Gateway (VGW) and Codecs
 - Quality of Service (QoS)**
 - LBN
 - SNTP
 - Numbering Zones
 - MCQD Alternative Routing Treatment (MALT) Causes

Applications (click to edit configuration)

- SIP Line
- Terminal Proxy Server (TPS)
- Gateway (SIPGW)
- Personal Directories (PD)
- Presence Publisher
- IP Media Services

* Required Value. [Save] [Cancel]

On the **Node Details** page as shown in the screen above select **Voice Gateway (VGW) and Codecs** link. The following values were configured during compliance testing as shown in the screen below.

Codec G711: Enabled by default.

Voice payload size: Select 20 from the drop down menu.

Voice Activity Detection (VAD): Uncheck this box.

Click on **Save** button.

AVAYA CS1000 Element Manager

Managing: 10.10.97.78 Username: admin
System > IP Network > IP Telephony Nodes > Node Details > VGW and Codecs

Node ID: 510 - Voice Gateway (VGW) and Codecs

General | Voice Codecs | Fax

Voice Codecs

Codec G711: ☒ Enabled (required)
Voice payload size: 20 (milliseconds per frame)
Voice playout (jitter buffer) delay: 40 60 (milliseconds)
Nominal Maximum
Maximum delay may be automatically adjusted based on nominal settings.
☐ Voice Activity Detection (VAD)

Codec G722: ☐ Enabled
Voice payload size: 20 (milliseconds per frame)
Voice playout (jitter buffer) delay: 40 60 (milliseconds)
Nominal Maximum
Maximum delay may be automatically adjusted based on nominal settings.

Codec G729: ☒ Enabled
Voice payload size: 20 (milliseconds per frame)

* Required Value. Note: Changes made on this page will NOT be transmitted until the Node is also saved. [Save] [Cancel]

Select **Gateway (SIPGw)** link as shown below from the Node Details page.

AVAYA CS1000 Element Manager

Managing: 10.10.97.78 Username: admin
System > IP Network > IP Telephony Nodes > Node Details

Node Details (ID: 510 - LTPS, Gateway (SIPGw))

Subnet mask: 255.255.255.192 * Subnet mask: 255.255.255.192 *

Node IPv6 address: []

IP Telephony Node Properties

- Voice Gateway (VGW) and Coders
- Quality of Service (QoS)
- LAN
- SNTP
- Numbering Zones
- MCDN Alternative Routing Treatment (MALT) Causes

Applications (click to edit configuration)

- SIP Line
- Terminal Proxy Server (TPS)
- Gateway (SIPGw)**
- Personal Directories (PD)
- Presence Publisher
- IP Media Services

* Required Value. [Save] [Cancel]

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.

AVAYA CS1000 Element Manager

Managing: 10.10.97.78 Username: admin
System > IP Network > IP Telephony Nodes > Node Details > Virtual Trunk Gateway Configuration

Node ID: 510 - Virtual Trunk Gateway Configuration Details

General | SIP Gateway Settings | SIP Gateway Services

Vtrk gateway application: ☒ Enable gateway service on this node

General

Vtrk gateway application: SIP Gateway (SIPGw) [v]
SIP domain name: bvwdev.com *
Local SIP port: 5060 * (1 - 65535)
Gateway endpoint name: cppm3 *
Gateway password: [] *
Application node ID: 510 * (0-9999)
Enable failsafe NRS: ☐

Note: Failsafe NRS will be enabled only on those servers in the node where NRS application is not deployed.

Virtual Trunk Network Health Monitor

☐ Monitor IP addresses (listed below)
Information will be captured for the IP addresses listed below.
Monitor IP: [] Add
Monitor addresses: [] Remove

* Required Value. Note: Changes made on this page will NOT be transmitted until the Node is also saved. [Save] [Cancel]

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.

Transport protocol: Select *UDP* from the drop down menu.

Retain default values for other fields.

AVAYA CS1000 Element Manager

Managing: 10.10.97.78 Username: admin
System > IP Network > IP Telephony Nodes > Node Details > Virtual Trunk Gateway Configuration

Node ID: 510 - Virtual Trunk Gateway Configuration Details

General | SIP Gateway Settings | SIP Gateway Services

Proxy or Redirect Server:

Proxy Server Route 1:

Primary TLAN IP address: 10.10.97.228
The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"

Port: 5060 (1 - 65535)

Transport protocol: UDP

Options: ☐ Support registration
☐ Primary CDS proxy

Scroll down to the **SIP URI Map** section. The following values were configured under the **Private domain names** during compliance testing.

UDP: udp

CDP: cdp.udp

Retain default values for other fields.

AVAYA CS1000 Element Manager

Managing: 10.10.97.78 Username: admin
System > IP Network > IP Telephony Nodes > Node Details > Virtual Trunk Gateway Configuration

Node ID: 510 - Virtual Trunk Gateway Configuration Details

General | SIP Gateway Settings | SIP Gateway Services

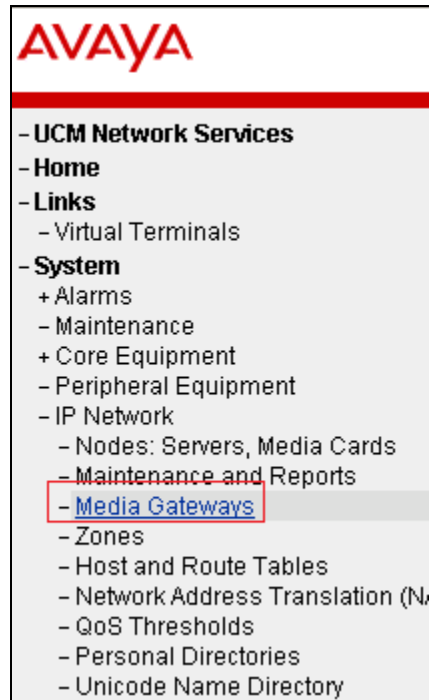
SIP URI Map:

Public E.164 domain names		Private domain names	
National:		UDP:	udp
Subscriber:		CDP:	cdp.udp
Special number:	PublicSpecial	Special number:	PrivateSpecial
Unknown:	PublicUnknown	Vacant number:	PrivateUnknown
		Unknown:	UnknownUnknown

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

5.3. Configuring Voice Codecs on Media Gateways

To configure voice codecs on Media Gateway Card (MGC) from the EM left navigator screen, navigate to **System → IP Network → Media Gateways** as shown below.



Screen below shows an already added MGC **004 00**. Click on the same to view the MGC configuration page. Click on the link **VGW and IP phone codec profile** (not shown).



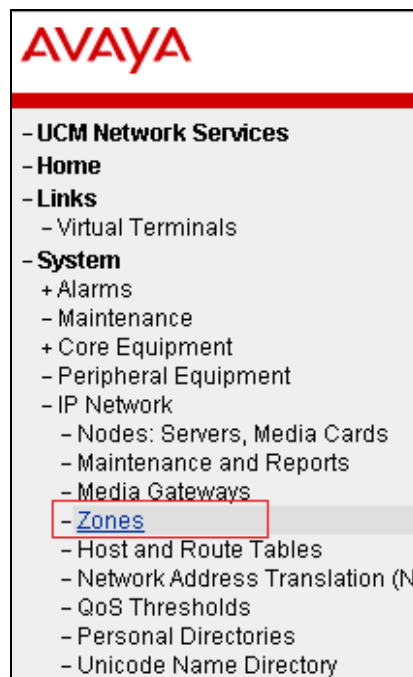
Ensure that the Codec G711 is selected as shown in the screen below. Note that the MGC has to be rebooted for the changes to take effect.

The screenshot shows the AVAYA CS1000 Element Manager interface. On the left is a navigation tree with the following items: - UCM Network Services, - Home, - Links, - Virtual Terminals, - System, + Alarms, - Maintenance, + Core Equipment, - Peripheral Equipment, - IP Network, - Nodes: Servers, Media Cards, - Maintenance and Reports, - Media Gateways, and - Zones. The main area displays settings for the selected codec, G711. It includes a 'FAX packet size' dropdown set to 30, a 'Codec name' field showing G711 with a 'Select' button, a 'Voice payload size' dropdown set to 20 (ms/frame), a 'Voice playout (jitter buffer) nominal delay' dropdown set to 40, and a 'Voice playout (jitter buffer) maximum delay' dropdown set to 80. Red text below the delay settings states 'Modifications may cause changes to dependent settings'. At the bottom right, there is a 'VAD' checkbox which is currently unchecked.

5.4. Configuring Zones

This section describes the steps to create 2 zones: One for Voice Gateways (VGW)/ IP phones, and the other for SIP Trunk.

To configure zones, from the EM left navigator screen, navigate to **System → IP Network → Zones** as shown below.



During compliance testing zone 1 was configured for VGW/IP phones and zone 2 was configured for SIP trunks.

Screen below shows the configuration used for Zone number **1**. For **Zone Intent (ZBRN)** field select **MO (MO)** from the drop down list. Retain default values for other fields.

Configuration for Zone number **2** is similar to the screen below; except for **Zone Intent (ZBRN)** field select **VTRK** from the drop down list (not shown).

AVAYA CS1000 Element Manager

Managing: 10.10.10.10 Username: admin
System > IP Network > Zones > Bandwidth Zones > Bandwidth Zones 1 > Edit Bandwidth Zone > Zone Basic Property and Bandwidth Management

Zone Basic Property and Bandwidth Management

Input Description	Input Value
Zone Number (ZONE):	1 * (1 - 9999)
Intrazone Bandwidth (INTRA_BW):	1000000 (0 - 10000000)
Intrazone Strategy (INTRA_STGY):	Best Quality (BQ)
Interzone Bandwidth (INTER_BW):	1000000 (0 - 10000000)
Interzone Strategy (INTER_STGY):	Best Quality (BQ)
Resource Type (RES_TYPE):	Shared (SHARED)
Zone Intent (ZBRN):	MO (MO)
Description (ZDESC):	
Location Name (ZNAME):	
Reserved BW Block Size (RESERVED_BW_SIZE):	0 (200 - 9999999)

Submit Refresh Cancel

5.5. Configure Integrated Services Digital Network (ISDN)

This section ensures that the ISDN option under the Features package is selected. From the EM left navigator screen, navigate to **Customers** as shown below.

AVAYA

- UCM Network Services
- Home
- Links
 - Virtual Terminals
- System
 - + Alarms
 - Maintenance
 - + Core Equipment
 - Peripheral Equipment
 - + IP Network
 - + Interfaces
 - Engineered Values
 - + Emergency Services
 - + Geographic Redundancy
 - + Software
- **Customers**
- Routes and Trunks
 - D-Channels

Select a customer and click on it to navigate to the **Customer Details** page (not shown). Click on the **Feature Packages** link (not shown) and from this page click on **Integrated Services Digital Network** link. Ensure that the **Integrated Services Digital Network** box is checked as shown in the screen below.

AVAYA CS1000 Element Manager

Integrated Services Digital Network

Feature Packages:

- Package: 123
- Package: 125
- Package: 128
- Package: 131
- Package: 133
- Package: 145

Configuration Fields:

- Integrated Services Digital Network: ☒
- Virtual private network identifier: 1 (1 - 16383)
- Private network identifier: 1 (1 - 16383)
- Node DN:
- Multi-location business group: 0 (0 - 65535)
- Business sub group consult-only: 65535 (0 - 65535)
- Prefix 1:
- Prefix 2:
- Home number plan area code: (200 - 999)
- Prefix for central office: (100 - 9999)
- Home location code: (100 - 99999999)
- Local steering code:
- Calling number type: CLID feature displays the set's Prime DN
- Redirection count for ISDN calls: 5
- CLID information for incoming/outgoing calls: No manipulation is done
- Public service telephone networks: ☐

5.6. 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.

Navigation Tree:

- Customers
- **Routes and Trunks**
 - Routes and Trunks
 - **D-Channels**
 - Digital Trunk Interface
- Dialing and Numbering Plans
 - Electronic Switched Network
 - Flexible Code Restriction
 - Incoming Digit Translation

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.



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

- PINK customer number:

- Progress signal:

- Calling Line Identification:

- Output request Buffers: 32

- D-channel transmission Rate: 56 kbit/s when LCMT is AMI (56k)

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

- Remote Capabilities: **Edit**

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

AVAYA CS1000 Element Manager

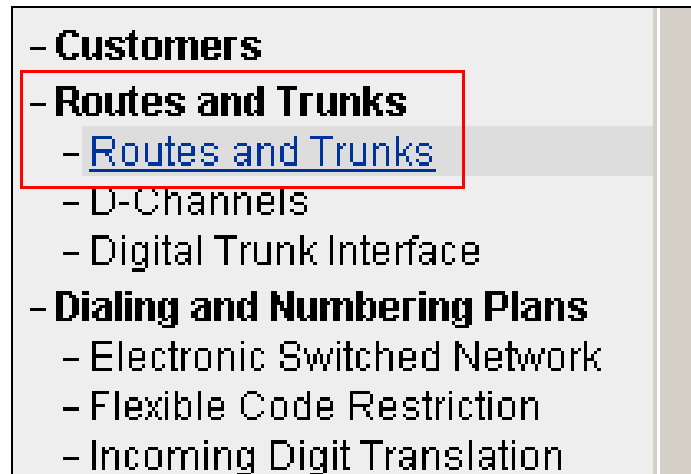
- Remote Capabilities Configuration

Input Description	
Basic rate interface (BRI)	☐
Call completion on busy using integer value (CCBI)	☐
Call completion on busy using object identifier (CCBO)	☐
Call completion on busy for QSIG and EuroISDN BRI (CCBS)	☐
Call completion on no response using integer value (CCNI)	☐
Call completion on no response using object identifier (CCNO)	☐
Call completion to no reply for QSIG and EuroISDN BRI (CCNR)	☐
Network call park (CPK)	☐
Connected line identification presentation (COLP)	☐
Call transfer integer (CTI)	☐
Call transfer object (CTO)	☐
Diversion info. is sent using integer value (DV1)	☐
Diversion info. is sent using object identifier (DV10)	☐
Forwarding requests processed using integer value (DV2)	☐
Forwarding requests processed using object identifier (DV20)	☐
Diversion info. sent, forwarding requests processed (DV3)	☐
EuroISDN - div. info sent, forwarding req. processed (DV30)	☐
Call transfer notification and invocation to EuroISDN (ECTO)	☐
Malicious call identification (MCID)	☐
MCDN QSIG conversion (MOC)	☐
Remote D-channel is on a MSOL card (MSL)	☐
Message waiting interworking with DMS-100 (MWM)	☒
Network access data (NAC)	☐
Network call trace supported (NCT)	☐
Network name display method 1 (ND1)	☐
Network name display method 2 (ND2)	☒
Network name display method 3 (ND3)	☐

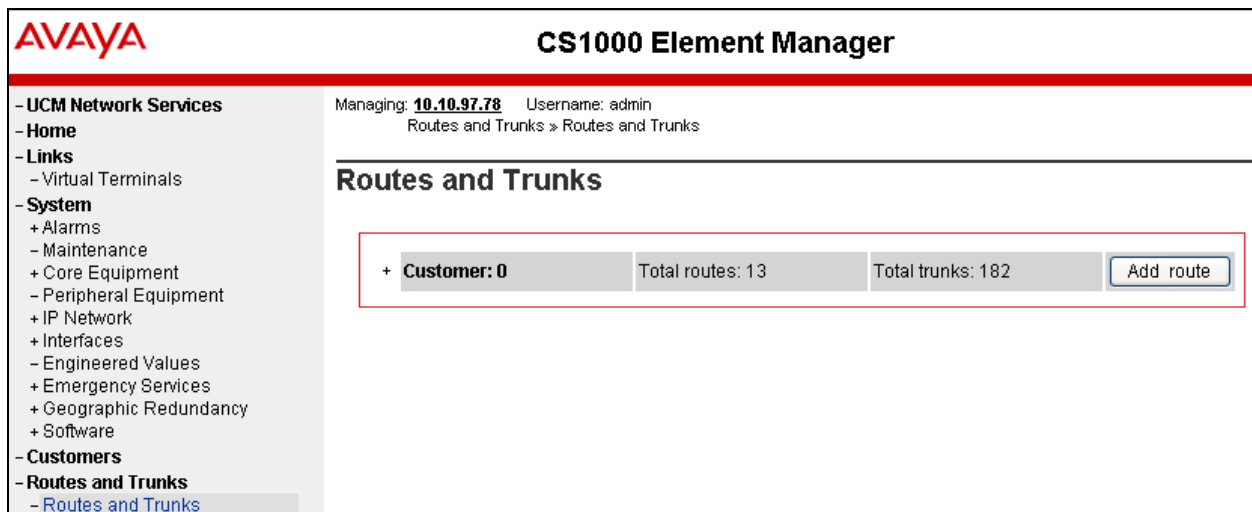
Click on the **Submit** button (not shown) to complete the D-channel configuration.

5.7. 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.



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): The *VTRK* zone, which is zone 2 in the system as explained in **Section 5.4**.

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 5.6**.

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.

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

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.

Click on **Return Class of Service** button to return to the main page of trunks configuration.

Click on **Save** button (not shown) to complete the trunks configuration.

Avaya CS1000 Element Manager

Managing: 10.10.10.78 Username: admin
Routes and Trunks > Routes and Trunks > Customer 0, Route 1, Trunk 1 Property Configuration

Customer 0, Route 1, Trunk 1 Property Configuration

- Basic Configuration

Auto increment member number: ☒

Trunk data block: IPTI

Terminal number: 10000000

Designator field for trunk: SP

Extended trunk: VTRK

Member number: 1

Level 3 Signaling: ISDN

Card density: 1

Start arrangement Incoming: Immediate (IMM)

Start arrangement Outgoing: Immediate (IMM)

Trunk group access restriction: 1

Channel ID for this trunk: 1

Class of Service: E88

- Priority: Low Priority (LPR)

- Restriction level: Unrestricted (UNR)

- Reversed Ear Piece: Reversed Ear Piece denied (REP)

- Short or long line: Short or long line

- Transmission Class of Service: Non-Transmission Compensated (NTC)

- Warning Tone: Warning Tone Allowed (WTA)

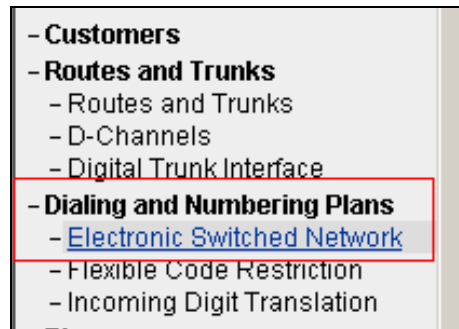
- Reversed Ear Piece: Reversed Ear Piece denied (REP)

- ARF Supervised COT: ARF Supervised COT

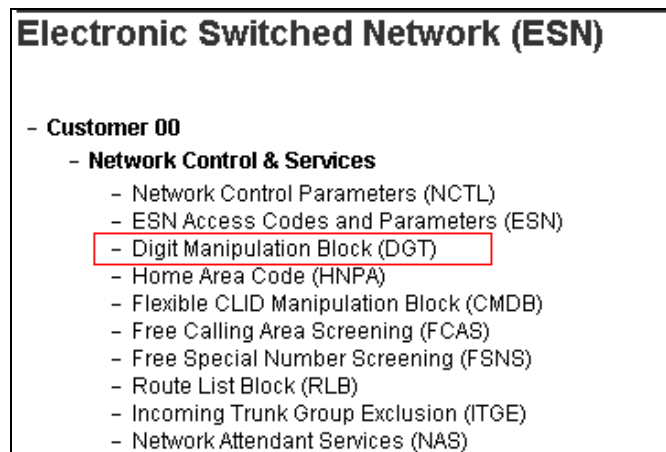
Return Class of Service Cancel

5.8. Configuring Digit Manipulation Block

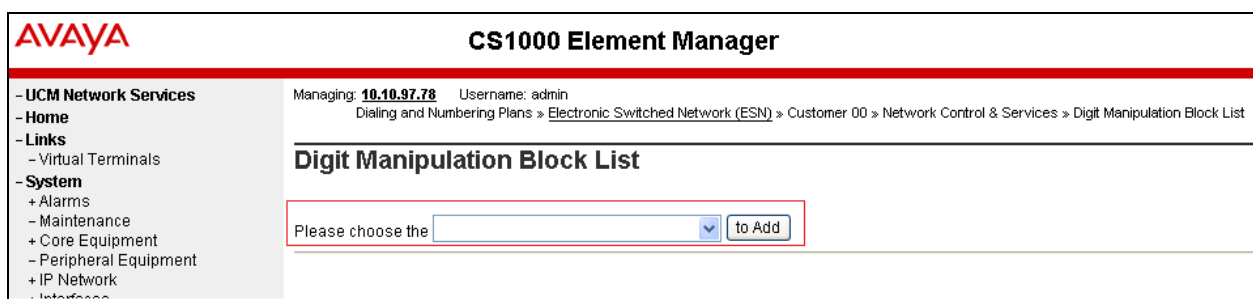
This section explains the digit manipulation block that is to be configured in the Communication Server 1000 dialing plan for its users to communicate with the PSS via the Session Manager. From the EM navigator pane, navigate to **Dialing and Numbering Plans → Electronic Switched Network** as shown below.



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

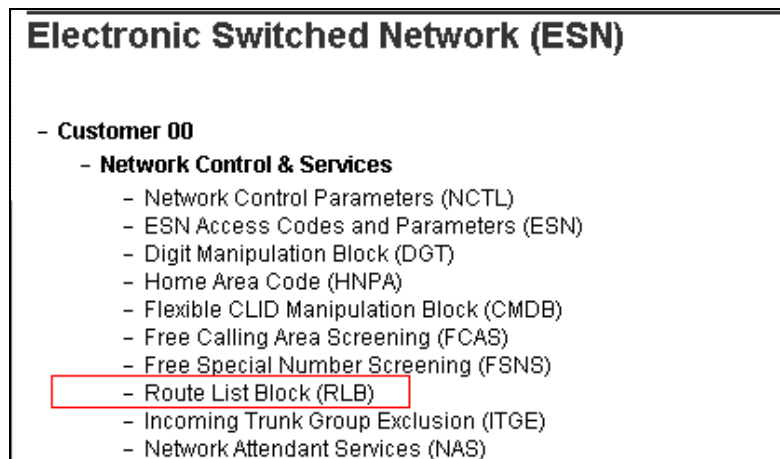


Screen below shows the **Digit Manipulation Block List** page where users can add a digit manipulation block index by selecting an available one from the drop down menu. During compliance testing **Digit Manipulation Block Index -- 0** was used which is already added in the Communication Server 1000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

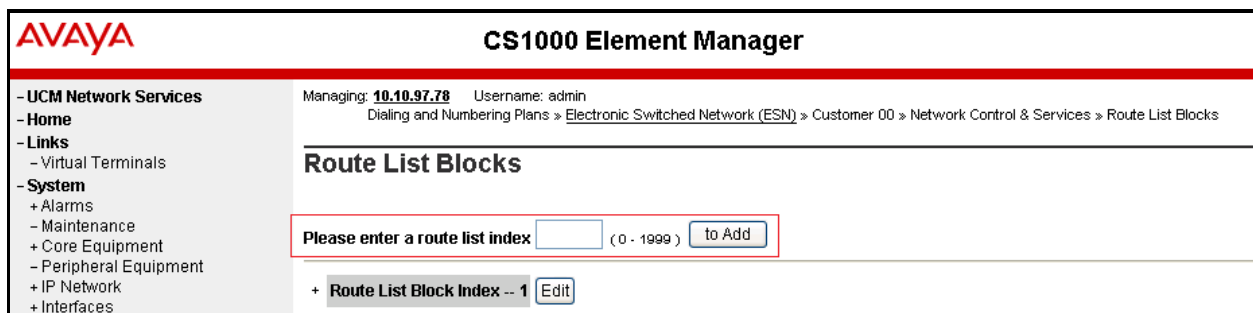


5.9. Configuring Route List Block

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 PSS via Session Manager. From the EM navigator pane, navigate to **Dialing and Numbering Plans** → **Electronic Switched Network** as shown in **Section 5.8**. 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 5.8**.

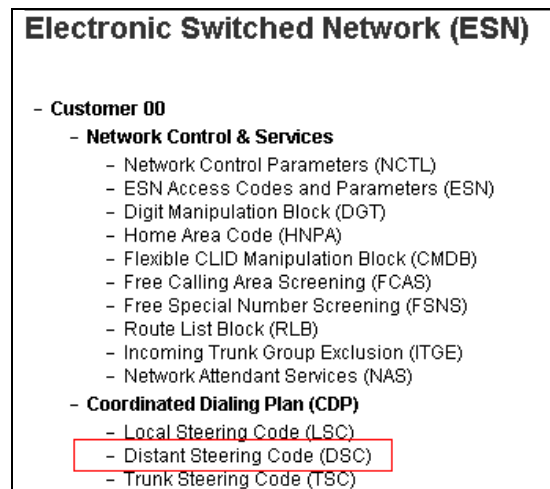
Route Number: Select 1 from the drop down menu. This was configured in **Section 5.7**. Retain default values for other fields.

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

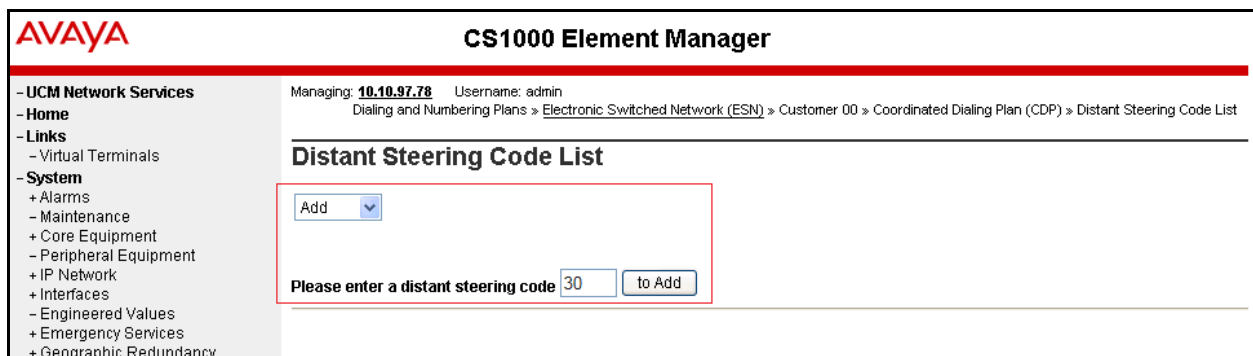
The screenshot shows the Avaya CS1000 Element Manager interface. The left sidebar contains a navigation menu with categories like Network Services, Features, and Troubleshooting. The main area is titled 'Index' and contains configuration fields for various services. The 'Options' section is expanded, showing fields for 'Route Number' (set to 1) and 'Digit Manipulation Index' (set to 0). Other fields include 'Time of Day Schedule', 'Priority Restriction Level', 'ISL D-Channel Down Digit Manipulation Index', 'Time Calling Area Screening Index', 'Free Special Number Screening Index', 'Business Network Extension Route', 'Incoming CLID Table', 'Local Termination only', 'Skip Conversion of Signaling', 'Use Tone Detector', 'Conversion to LDM', 'Supervise Route', 'Strategy on Congestion', 'GOS Alternate Routing Cause', 'GOS Alternate Routing Cause 1', 'Preferential Routing', 'Preferential Route 1', 'ISDN Drop Back Rule', 'Drop Back Disabled (GOS)', 'ISDN Off-Hook Seizure Option', 'Off-Hook Seizure Allowed', 'Call Back Seizure Allowed', and 'VMS Options' (set to 'Only if a VMS Route'). The bottom right corner has buttons for 'Submit', 'Refresh', 'Delete', and 'Cancel'.

5.10. 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 PSS via Session Manager. From the EM navigator pane, navigate to **Dialing and Numbering Plans → Electronic Switched Network** as shown in Section 5.8. 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 **to Add** button to finish adding one as shown in the screen below. During compliance testing a code of **30** was added since the users assigned on PSS started with 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 PSS 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 5.9**.

Retain default values for other fields.

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

The screenshot shows the Avaya CS1000 Element Manager interface. The left sidebar contains a navigation menu with categories like 'Network Services', 'Links', 'Systems', 'Features', 'Call Services', 'Routing and Forwarding Plans', and 'Monitoring'. The main content area is titled 'Distant Steering Code' and contains the following configuration fields:

- Distant Steering Code: 30
- Flexible Length number of digits: 5
- Display: Local Steering Code 5,000
- Remote Radio Paging Access: ☐
- Route List to be accessed for trunk steering code: 1
- Collect Call Blocking: ☐
- Maximum 7 digit NPA code allowed: [empty]
- Maximum 7 digit FOD code allowed: [empty]

At the bottom right of the form are four buttons: Submit, Rollback, Cancel, and Cancel.

6. Configure Avaya Aura® Session Manager

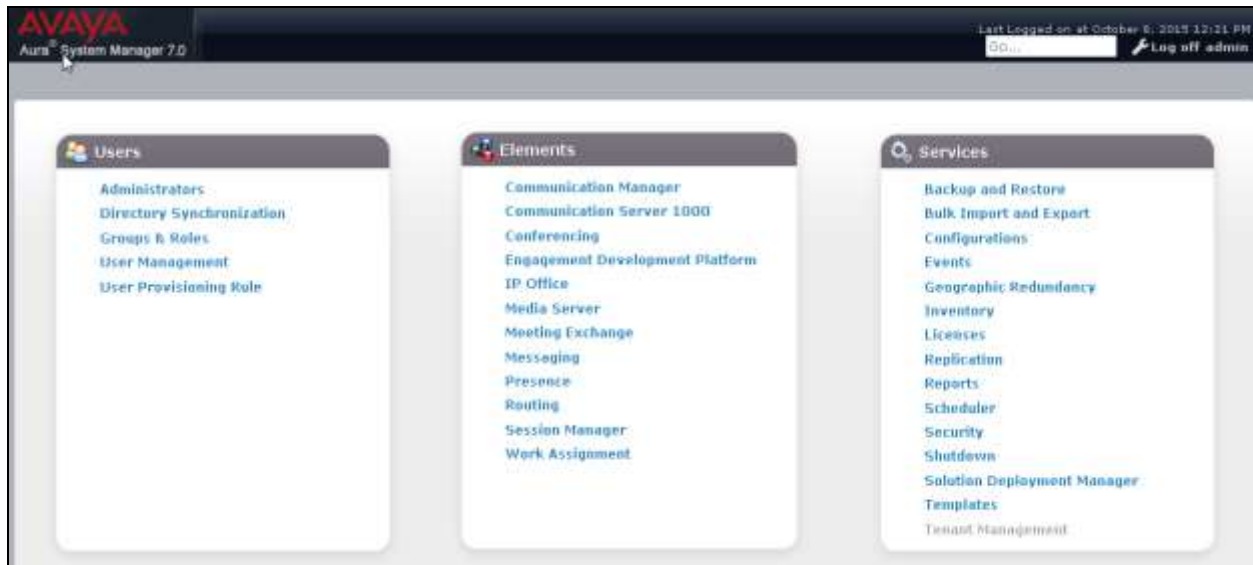
This section provides the procedures for configuring Avaya Aura® Session Manager. The procedures include the following areas:

- Launch System Manager
- Add a Domain
- Add a Location
- Administer Adaptations
- Administer SIP entities
- Administer entity links
- Administer routing policies
- Administer dial patterns

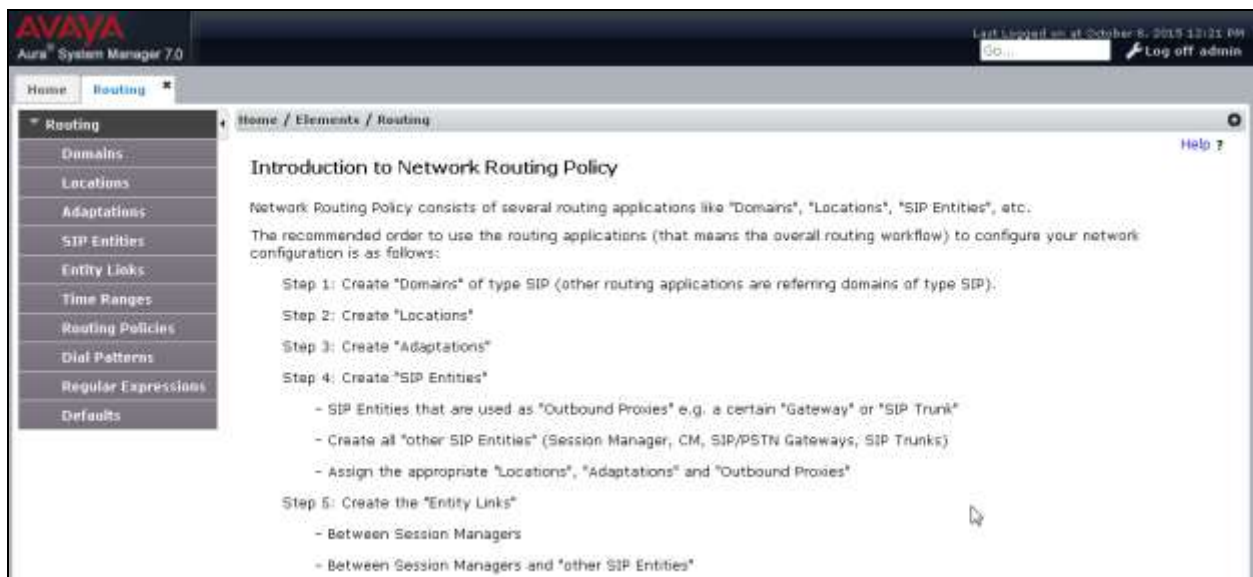
6.1. Launch System Manager

Access the System Manager web interface by using the URL <https://ip-address> in an Internet browser window, where “ip-address” is the IP address of the System Manager server. Log in using the appropriate credentials.

The System Manager main page is displayed next. Navigate to **Elements** → **Routing**.



The **Introduction to Network Routing Policy** page is displayed.



6.2. Add a Domain

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



6.3. 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.



6.4. Administer Adaptations

To enable calls between stations on Communication Server 1000 and other SIP entities registered to Session Manager, Session Manager should be configured to use an Adaptation Module designed for Communication Server 1000.

To configure an adaptation, select **Adaptations** from the left hand window of the Routing screen and click on **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Adaptation Name:** Enter an identifier for the Adaptation Module
- **Module Name:** Select “CS1000Adapter” from drop-down menu
- **Module Parameter:** Enter “fromto=true. This will modify the FROM and TO headers in the SIP messages.

In the **Digit Conversion for Incoming Calls to SM** section, click **Add** and enter the following values.

- **Matching Pattern** Enter dialed prefix for calls to SIP endpoints registered to Session Manager. During compliance testing, 30 was used as per the configuration in **Section 5.10**.

- **Min** Enter minimum number of digits that must be dialed
- **Max** Enter maximum number of digits that may be dialed

In the sample configuration, 5 was used.

- **Phone Context** Enter value of **Private CDP domain name** defined in **Section 5.2**.

- **Delete Digits** Enter 0, unless digits should be removed from dialed number before call is routed by Session Manager

- **Address to modify** Select *both*

Click **Commit**. The Adaptation Module defined during compliance testing is shown below.

The screenshot displays the Avaya Aura System Manager 7.0 interface. The left-hand navigation pane shows the 'Routing' menu expanded, with 'Adaptations' selected. The main content area is titled 'Adaptation Details' and includes a 'General' tab. The 'General' section contains the following fields: 'Adaptation Name' (CS1000Adapter), 'Module Name' (CS1000Adapter), 'Module Parameter Type' (empty), 'Egress URI Parameters' (fromto=true), and 'Notes' (CS1000 adapter for Phone Context). Below this is the 'Digit Conversion for Incoming Calls to SM' section, which features a table with columns: Matching Pattern, Min, Max, Phone Context, Delete Digits, Insert Digits, Address to modify, Adaptation Data, and Notes. The table contains one row with values: Matching Pattern: 30, Min: 5, Max: 5, Phone Context: cdp.cdp, Delete Digits: 0, Insert Digits: (empty), Address to modify: both, Adaptation Data: (empty), and Notes: Calls to PatientSafe. The interface also shows a top bar with the Avaya logo and a user profile section.

6.5. Administer SIP Entities

Select **Routing** → **SIP Entities** from the left pane, and click **New** in the subsequent screen (not shown) to add a new SIP entity for PatientTouch Communications.

The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **FQDN or IP Address:** The IP address of the PatientTouch server.
- **Type:** Select *Other*.
- **Location:** Select the PatientTouch location name.
- **SIP Link Monitoring:** Select *Use Session Manager Configuration*.

Click the **Commit** button.

The screenshot shows the Avaya Aura System Manager 7.0 interface. The left navigation pane has 'Routing' selected. The main content area is titled 'SIP Entity Details' and has a 'General' tab. The form contains the following fields and values:

- Name:** PatientSafe Solutions
- FQDN or IP Address:** 10.10.98.157
- Type:** Other
- Notes:** SIP entity for a partner testing
- Adaptation:** (empty)
- Location:** Belleville
- Time Zone:** America/Fortaleza
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty)
- Securable:** (unchecked)
- Call Detail Recording:** none
- CommProfile Type Preference:** (empty)
- Loop Detection Mode:** On
- Loop Count Threshold:** 5
- Loop Detection Interval (in msec):** 200
- SIP Link Monitoring:** Use Session Manager Configuration

The 'Commit' and 'Cancel' buttons are located at the top right of the form.

6.6. Administer Entity Links

Select **Routing** → **Entity Links** from the left pane, and click **New** in the subsequent screen (not shown) to add a new entity link for PatientTouch Communications.

The **Entity Links** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **SIP Entity 1:** The Session Manager entity name.
- **Protocol:** The signaling group transport method. During the compliance test, the UDP protocol was used between Session Manager and Patient Touch.
- **Port:** An appropriate signaling group listen port number is displayed.
- **SIP Entity 2:** Select the PatientTouch entity name.
- **Port:** An appropriate signaling group listen port number is displayed.
- **Connection Policy:** Select *trusted*

Click the **Commit** button.

The screenshot shows the Avaya Aura System Manager 7.0 interface. The left navigation pane has 'Entity Links' selected under the 'Routing' section. The main area is titled 'Entity Links' and contains a table with one item. The table has columns for Name, SIP Entity 1, Protocol, Port, SIP Entity 2, DNS Override, Port, and Connection Policy. The values in the table are: Name: DevmSM_PatientSafe, SIP Entity 1: DevmSM, Protocol: UDP, Port: 5060, SIP Entity 2: PatientSafe Solutions, DNS Override: (unchecked), Port: 5060, and Connection Policy: trusted. There are 'Commit' and 'Cancel' buttons at the top and bottom of the table area.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Conn. Pol.
DevmSM_PatientSafe	DevmSM	UDP	5060	PatientSafe Solutions	☐	5060	trusted

6.7. Administer Routing Policies

Select **Routing** → **Routing Policies** from the left pane, and click **New** in the subsequent screen (not shown) to add a new routing policy for PatientTouch Communications.

The **Routing Policy Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name**.

In the **SIP Entity as Destination** sub-section, click **Select** and select the PatientTouch entity name from **Section 6.5** in the listing (not shown).

Retain the default values in the remaining fields.

Click the **Commit** button.

Routing Policy Details

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
PatientSafe Solutions	10.10.36.157	Other	SIP entity for a partner testing

6.8. Administer Dial Patterns

Select **Routing** → **Dial Patterns** from the left pane, and click **New** in the subsequent screen (not shown) to add a new dial pattern to reach PatientTouch users.

The **Dial Pattern Details** screen is displayed. In the **General** sub-section, enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Pattern:** A dial pattern to match.
- **Min:** The minimum number of digits to be matched.
- **Max:** The maximum number of digits to be matched.
- **SIP Domain:** During the compliance test, *bwdev.com* was selected for the sip domain.
- **Notes:** Any desired description.

In the **Originating Locations and Routing Policies** sub-section, click **Add** and create a new policy for reaching PatientTouch users.

The screenshot shows the Avaya Aura System Manager 7.0 interface. The left-hand navigation pane has 'Dial Patterns' selected under the 'Routing' category. The main content area is titled 'Dial Pattern Details' and contains a 'General' tab. The fields in the 'General' tab are: 'Pattern' (text box with '30'), 'Min' (text box with '5'), 'Max' (text box with '5'), 'Emergency Call' (checkbox), 'Emergency Priority' (text box with '1'), 'Emergency Type' (dropdown menu), 'SIP Domain' (dropdown menu with 'bwdev.com' selected), and 'Notes' (text box with 'Dial pattern to reach PatientSafe server'). At the top right of the main area are 'Commit' and 'Cancel' buttons. Below the 'General' tab is a section titled 'Originating Locations and Routing Policies' with 'Add' and 'Remove' buttons. The top of the screen shows the Avaya logo and 'Aura System Manager 7.0'. The top right corner shows a user login 'Log on at October 8, 2014 12:11 PM' and a 'Log off admin' button.

In the **Originating Location** sub-section, check the *Belleville* location checkbox.
In the **Routing Policies** sub-section, check an appropriate routing policy from **Section 6.7**.

Click the **Select** button. From the **Dial Pattern Details** screen seen above, select **Commit**.

The screenshot shows the Avaya Aura System Manager 7.0 interface. The left sidebar contains a navigation menu with options: Home, Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Home / Elements / Routing / Dial Patterns'. It features two sub-sections: 'Originating Location' and 'Routing Policies'. In the 'Originating Location' section, there is a checkbox labeled 'Apply The Selected Routing Policies to All Originating Locations' and a table with one item, 'Belleville', which is selected. In the 'Routing Policies' section, there is a table with four items, including 'Route_to_PatientSafe_Server', which is selected. Both tables have a 'Select: All, None' link at the bottom. The interface also includes a 'Select' button and a 'Cancel' button at the bottom right.

Name	Notes
Belleville	Belleville DevConnect Lab

Name	Disabled	Destination	Notes
Route_to_CS1K_CP9MG	☐	CS1K_Bottom	Route to the bottom CS1KMG
Route_to_DevCM	☐	DevCM	Route to the main CM in the lab
Route_to_IP0_36	☐	IP0_36	Route to the top IP Office
Route_to_PatientSafe_Server	☐	PatientSafe Solutions	Route to a partner testing server

7. Configure PatientSafe's PatientTouch Communications

PatientSafe engineers install, configure, and customize the PatientTouch applications for their end customers. By PatientSafe Solutions request, installation/configuration steps were not included in these Application Notes. To acquire above information, please contact PatientSafe Solutions.

8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya Aura® Session Manager.

8.1. Verify Avaya Aura® Session Manager

From the System Manager home page, select **Elements** → **Session Manager** to display the **Session Manager Dashboard** screen (not shown). Select **Session Manager** → **System Status** → **SIP Entity Monitoring** from the left pane to display the **SIP Entity Link Monitoring Status Summary** screen. Click on the PatientTouch entity name from **Section 6.25**.

AVAYA
Aura® System Manager 7.0

Home / Elements / Session Manager / System Status / SIP Entity Monitoring

SIP Entity Link Monitoring Status Summary

This page provides a summary of Session Manager SIP entity link monitoring status.

SIP Entities Status for All Monitoring Session Manager Instances

Run Monitor

Session Manager	Type	Down	Partially Up	Up	Not Monitored	Down	Total
☐ Devvsm	Core	2	0	2	0	0	4

Select: All, None

All Monitored SIP Entities

Run Monitor

SIP Entity Name
☐ DevCM
☐ IPO_36
☐ CS1K_Bottom
☐ PatientSafe Solutions

The **SIP Entity, Entity Link Connection Status** screen is displayed. Verify that **Conn. Status** and **Link Status** are *Up*, as shown below.



8.2. Verify PatientSafe Solutions' PatientTouch Communications

Please contact PatientSafe Solutions for information.

9. Conclusion

These Application Notes describe the configuration steps required for PatientSafe's PatientTouch Communications to successfully interoperate with Avaya Communication Server 1000 and Avaya Aura® Session Manager using SIP trunks.

All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

10. Additional References

This section references the product documentation relevant to these Application Notes.

1. *Communication Server 1000E Installation and Commissioning*, NN46041-310
2. *Element Manager System Reference – Administration - Avaya Communication Server 1000*, NN43001-632.
3. *Co-resident Call Server and Signaling Server Fundamentals - Avaya Communication Sever 1000*, NN43001-509.
4. *Unified Communications Management Common Services Fundamentals - Avaya Communication Server 1000*, NN43001-116.
5. *Administering Avaya Aura® System Manager*, October 2013, Release 6.3.
6. *ISDN Primary Rate Interface Installation and Commissioning - Avaya Communication Server 1000*, NN43001-301.
7. *Administering Avaya Aura® Session Manager*, 03-603324.

For PatientTouch Communications, please contact PatientSafe Solutions.

©2015 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.