



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for Amtelco Infinity Intelligent SIP Attendant Console with Avaya Aura® Session Manager – Issue 1.0**

### **Abstract**

These Application Notes describe the configuration steps required for Amtelco Infinity SIP Attendant Console to interoperate with Avaya Communication Server 1000 and Avaya Aura® Session Manager using SIP trunks. Amtelco Infinity SIP Attendant Console is a SIP-based soft phone solution that provides phone and operator state controls during call handling.

In the compliance testing, Amtelco Infinity SIP Attendant Console used the SIP trunks interface from Avaya Aura® Session Manager to provide attendant consoles for Avaya Communication Server 1000.

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 Amtelco Infinity SIP Attendant Console to interoperate with Avaya Communication Server 1000 (hereafter referred as Communication Server 1000) and Avaya Aura® Session Manager (hereafter referred to as Session Manager) using SIP trunks. Amtelco Infinity SIP Attendant Console (hereafter referred to as Infinity) is a SIP-based soft phone solution that provides phone and operator state controls during call handling.

In the compliance testing, Amtelco Infinity SIP Attendant Console used the SIP trunks interface from Avaya Aura® Session Manager to provide attendant consoles for Avaya Communication Server 1000.

The Amtelco Infinity SIP Attendant Console solution consists of an Infinity server and attendants with desktop computers running Amtelco Infinity Telephone Agent. The Infinity server controls routing of calls to/from the attendants, and with all attendant related activities such as answer/drop calls performed from Amtelco Infinity Telephone Agent.

## 2. General Test Approach and Test Results

The feature test cases were performed manually. Calls were placed manually with necessary attendant actions such as hold and transfer performed from the attendant desktops to verify various call scenarios. The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to the Infinity server and to the attendants.

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 G.711, G.729, codec negotiation, DTMF, hold/resume, drop, display, blind transfer, attended conference, inbound, outbound, multiple calls, and multiple agents.

The serviceability testing focused on verifying the ability of Infinity to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connections to the Infinity server and to the attendants.

## 2.2. Test Results

All test cases were executed and passed. The following were observations on Infinity from the compliance testing.

- Infinity needs to be configured to send OPTIONS, else won't respond to OPTIONS and Session Manager will assume the connectivity is down. Furthermore, enabling OPTIONS on Infinity requires configuration of an account, or else OPTIONS won't be sent.
- Infinity only supports G 7.11 for outgoing calls and G 7.11 and G 729 for incoming calls.
- There is no MUTE feature available on the Infinity GUI. Infinity expects agents to use this feature if available on their headsets locally.
- In case of Ethernet connectivity being lost to the Infinity Server during an active call, audio connection gets dropped, member graphical user interface (GUI) shows red OFF. Upon link restoration, member needs to end call, logout and login, and may see "Next Call Ring x yyyy" on screen, depending on whether the calling party held on to the call while Ethernet connectivity was lost.
- In case of Ethernet connectivity being lost to the Infinity Telephone agent during an active call, audio drops and agent sees a login screen. Upon link restoration and agent performing a login, GUI may appear as if call waiting and alerting tone applied, even when there is no active call. Agent will need to connect and end before returning back to normal. Upon agent pressing F1, alerting stops and GUI appears as if agent connected to a call when there is no call. If the caller on the other end is still on line, then call is presented to the next available agent.

## 2.3. Support

Technical support on Infinity can be obtained through the following:

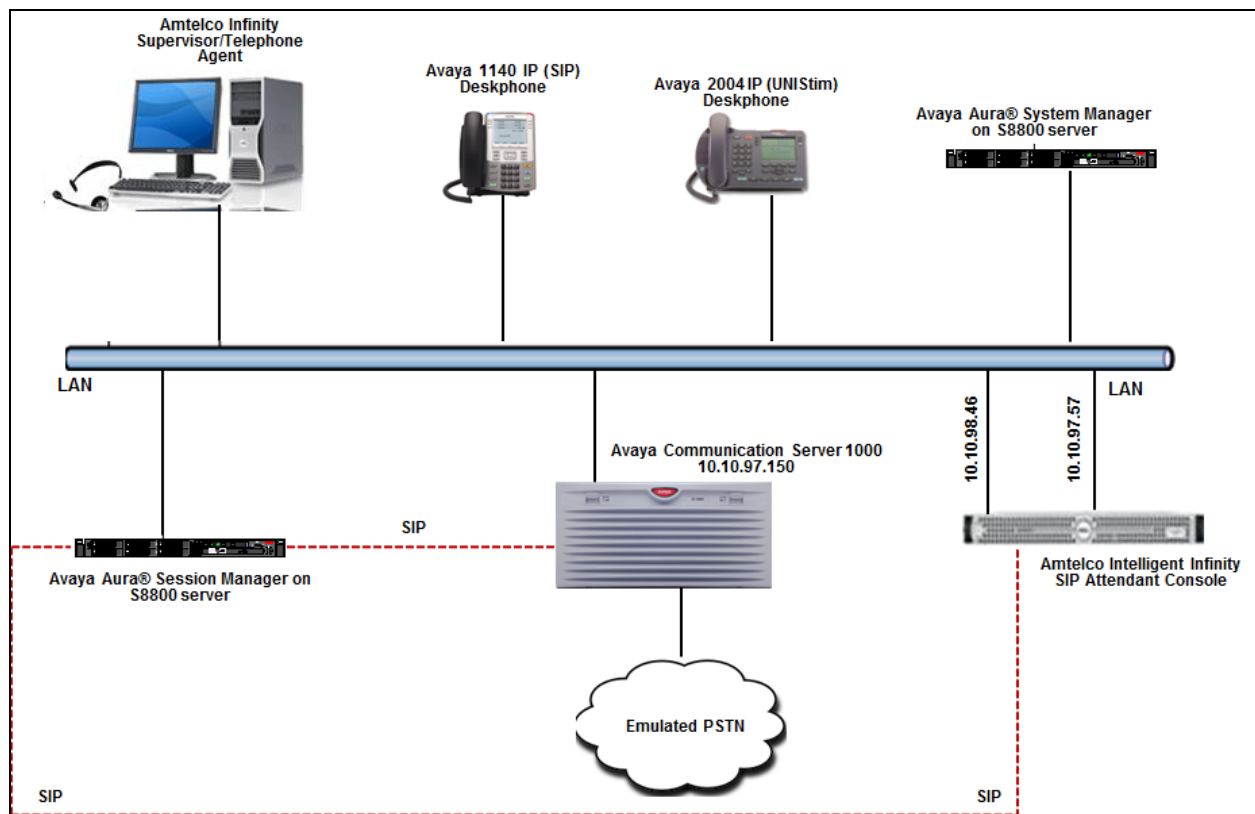
- **Phone:** (800) 553-7679
- **Email:** [service@amtelco.com](mailto:service@amtelco.com)
- **Web:** [www.amtelco.com/Welcome.htm](http://www.amtelco.com/Welcome.htm)

### 3. Reference Configuration

As shown in **Figure 1**, attendants are running the Infinity Telephone Agent soft phone application on the desktops, and the administrator is running the Infinity Supervisor.

SIP trunks are used between Infinity SIP Attendant Console and Session Manager. A five digit Uniform Dial Plan was used to facilitate dialing with Infinity. Calls to extensions 76xxx are routed over the SIP trunks to Infinity. Calls from internal/ external users will be routed with digits 76000 to Infinity. Infinity will route the received call to an available attendant, and populate the answering attendant with pertinent information for the call.

The detailed administration of connectivity between Communication Server 1000 and Session Manager are not the focus of these Application Notes and will not be described.



**Figure 1: Compliance Testing Configuration**

## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Communication Server 1000	7.65
Avaya Aura® Session Manager	6.3
Avaya Aura® System Manager	6.3
Avaya 2004 IP Deskphone (UNISlim)	0602B76
Avaya 1140 IP Deskphone (SIP)	04.03.12
Amtelco Infinity Intelligent SIP Attendant Console <ul style="list-style-type: none"><li>• XDS VoIP Card</li></ul>	5.61.08 4.48
Amtelco Infinity Supervisor	5.60.0020
Amtelco Infinity Telephone Agent	5.60.4364.53

## 5. Configure Avaya Communication Server 1000

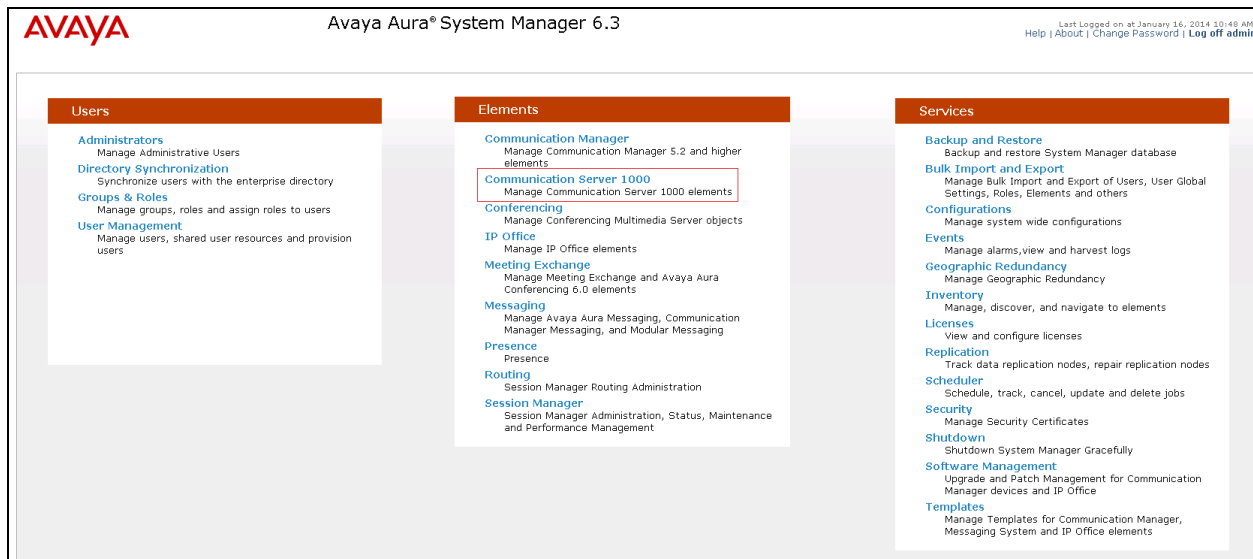
This section describes the Communication Server 1000 configuration necessary to interoperate with Session Manager and Infinity. It provides the procedures for configuring Avaya Communication Server 1000 system. The procedures include the following areas:

- Logging into the Element Manager via System Manager.
- 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.

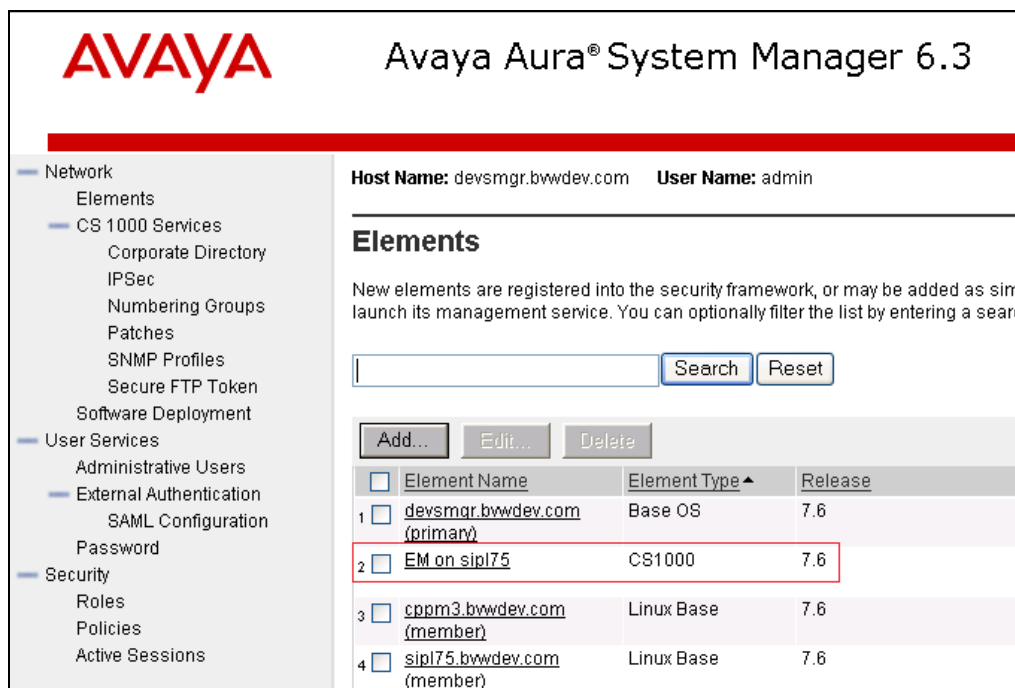
For detail configuration details of the Communication Server 1000 refer to **Section 10**.

## 5.1. Logging into Element Manager via Avaya Aura® System Manager

To login to the System Manager open an IE browser and type in the IP address of the System Manager in the URL (not shown). Screen below shows the main dashboard. Navigate to **Elements → Communication Server 1000**.



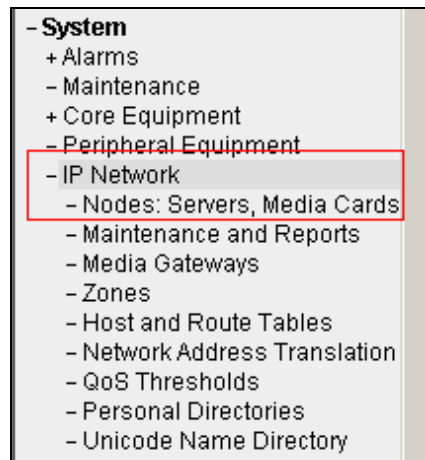
From the **Elements** page of Communication Server 1000 as shown in screen below, click on the Element **EM on sip175**. This is the element which is configured to access the Element Manager (EM) for the Communication Server 1000 Call Server.



## 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 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 **511** was added. Click on this Node as shown in screen below to view the configured values.

**AVAYA****CS1000 Element Manager**

- UCM Network Services
- Home
- Links
  - Virtual Terminals
- System
  - + Alarms
  - Maintenance
  - + Core Equipment
  - Peripheral Equipment
  - IP Network
    - Nodes: Servers, Media Cards

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

<input type="checkbox"/> Node ID ▲	Components	Enabled Applications	ELAN IP	Node/TLAN IPv4	Node/TLAN IPv6	Status
<input type="checkbox"/> 511	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: 511 - 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 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 (SIPGw)
- Personal Directories (PD)
- Presence Publisher
- IP Media Services

\* Required Value. Save Cancel

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: 511 - 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 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 (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.

Repeat the same for codec G729 and retain default values for other fields.

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: 511 - Voice Gateway (VGW) and Codecs**

General | **Voice Codecs** | Fax

**Voice Codecs**

Codec G711: ☒ Enabled (required)  
Voice payload size: 20 (milliseconds per frame)  
Voice playback (jitter buffer) delay: 40 80 (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 playback (jitter buffer) delay: 40 80 (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: 511 - 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 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 (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:** *bwdev.com*. This will be the same domain name that will be configured on Session Manager.

**Local SIP port:** *5060*.

**Gateway endpoint name:** *cppm3*.

**Application node ID:** *511*.

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: 511 - 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) \*  
SIP domain name: bwdev.com \*  
Local SIP port: 5060 \* (1 - 65535)  
Gateway endpoint name: cppm3 \*  
Gateway password: \*  
Application node ID: 511 \* (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:** *10.10.97.198*. This is the IP address of Session Manager.

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

Retain default values for other fields.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation menu with categories like UCM Network Services, Home, Links, and System. The main content area is titled 'Node ID: 511 - Virtual Trunk Gateway Configuration Details'. Under the 'Proxy or Redirect Server' section, the 'Proxy Server Route 1' configuration is visible. The 'Primary TLAN IP address' is set to '10.10.97.198', with a note indicating it can be IPv4 or IPv6. The 'Port' is '5060' (range 1-65535). The 'Transport protocol' is set to 'UDP' via a dropdown menu. There are also checkboxes for 'Support registration' and 'Primary CDS proxy', both of which are unchecked.

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*

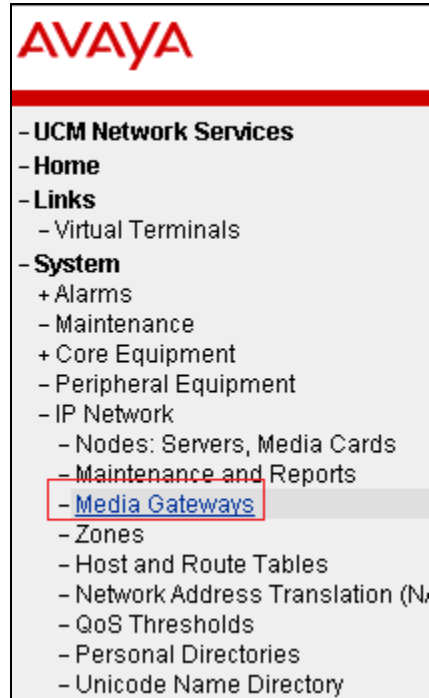
Retain default values for other fields.

The screenshot shows the AVAYA CS1000 Element Manager interface, specifically the 'SIP URI Map' section for Node ID: 511. It displays two columns: 'Public E.164 domain names' and 'Private domain names'. Under 'Public E.164 domain names', fields for 'National', 'Subscriber', 'Special number' (set to 'PublicSpecial'), and 'Unknown' (set to 'PublicUnknown') are visible. Under 'Private domain names', the 'UDP' field is set to 'udp' and the 'CDP' field is set to 'cdp.udp', both highlighted with red boxes. Other fields like 'Special number' (set to 'PrivateSpecial'), 'Vacant number' (set to 'PrivateUnknown'), and 'Unknown' (set to 'UnknownUnknown') are also present.

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 IPMG, in this case 004 00, to view the MGC configuration page. Click on the link **VGW and IP phone codec profile** (not shown).

The screenshot shows the AVAYA CS1000 Element Manager interface. The left navigation pane is visible on the left. The main content area is titled 'Media Gateways'. At the top of the main area, there are buttons: 'Add...', 'Digital Trunking...', 'Reboot', 'Delete', 'Virtual Terminal', and 'More Actions'. Below these buttons is a table with the following columns: IPMG, IP Address, Zone, and Type. The table contains one row with the following data: IPMG: 004 00, IP Address: 10.10.97.79, Zone: 1, Type: MGC. The 'Type' cell is highlighted with a red box.

IPMG	IP Address	Zone	Type
004 00	10.10.97.79	1	MGC

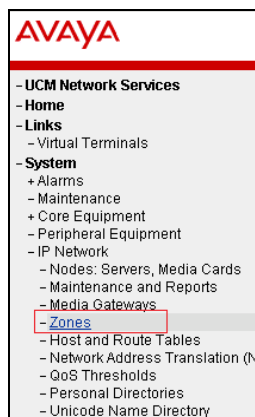
Ensure that the Codecs **G711** and **G729A** are selected as shown in the screen below. Note that the MGC has to be rebooted for the changes to take effect.

The screenshot displays the AVAYA CS1000 Element Manager interface. On the left is a navigation tree with categories like UCM Network Services, Home, Links, System, and Phones. The 'System' category is expanded, showing sub-items like Alarms, Maintenance, Core Equipment, Peripheral Equipment, IP Network, Nodes: Servers, Media Cards, Maintenance and Reports, Media Gateways, Zones, Host and Route Tables, Network Address Translation (NAT), QoS Thresholds, Personal Directories, and Unicode Name Directory. The 'Media Gateways' item is selected. The main panel shows configuration settings for 'Enable modems pass through mode' and 'Enable V.21 FAX tone detection', both checked. Below these are settings for 'Fax TCF method' (set to 2), 'FAX maximum rate' (14400 bps), 'FAX playback nominal delay' (100 ms), 'FAX no activity timeout' (20 ms), and 'FAX packet size' (30). A red box highlights the codec configuration section. It shows two codecs: G711 and G729A. For G711, the 'Codec name' is G711, 'Voice payload size' is 20 ms/frame, 'Voice playback (jitter buffer) nominal delay' is 40 ms, and 'Voice playback (jitter buffer) maximum delay' is 80 ms. For G729A, the 'Codec name' is G729A, 'Voice payload size' is 20 ms/frame, 'Voice playback (jitter buffer) nominal delay' is 40 ms, and 'Voice playback (jitter buffer) maximum delay' is 80 ms. Both codecs have 'VAD' (Voice Activity Detection) disabled. A third codec, G723.1, is listed at the bottom but is not selected.

## 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: 10.10.97.78 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 - 8000)
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 (ZDES):	
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

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

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

Routes and Trunks

D-Channels

Digital Trunk Interface

Dialing and Numbering Plans

Electronic Switched Network

Flexible Code Restriction

Incoming Digit Translation

Phones

Templates

Reports

Views

Lists

Properties

Migration

Tools

Backup and Restore

Date and Time

Logs and reports

Security

Passwords

Policies

Login Options

Integrated Digital Access

Digital Private Network Signaling System 1

Flexible Tones and Cadences

Multifrequency Compelled Signaling

International Supplementary Features

Enhanced Night Service

Integrated Services Digital Network

Dial Access Prefix on CLID table entry option

Package: 122

Package: 123

Package: 125

Package: 128

Package: 131

Package: 133

Package: 145

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: ☐

RS; Reviewed:  
SPOC 7/7/2014

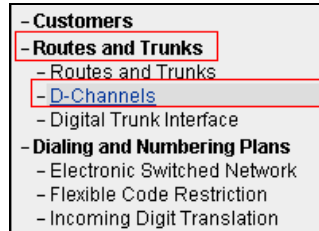
Solution & Interoperability Test Lab Application Notes  
©2014 Avaya Inc. All Rights Reserved.

16 of 50  
Infinity-CS1K76

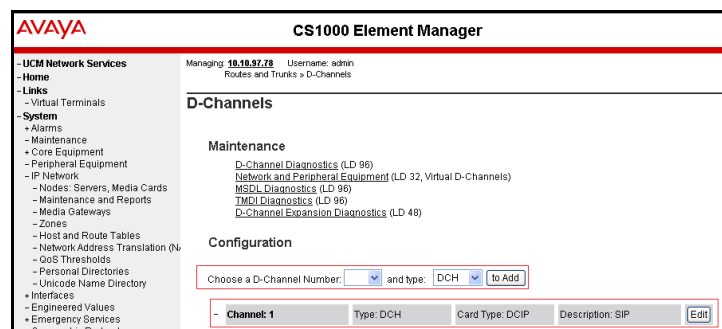


## 5.6. Configuring D-Channel

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.



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*.

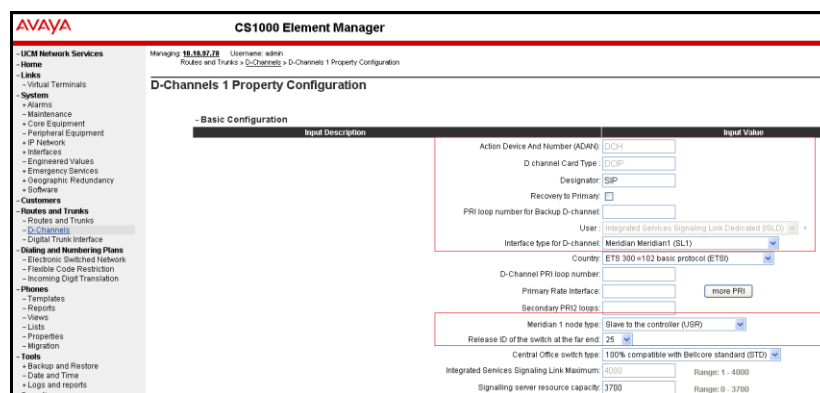
**Designator:** A descriptive name.

**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

- PINX customer number:

- Progress signal:

- Calling Line Identification:

- Output request Buffers:

- D-channel transmission Rate:

- Channel Negotiation option:

- Remote Capabilities:

Enable the **Message waiting interworking with DMS-100 (MWI)** and **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**

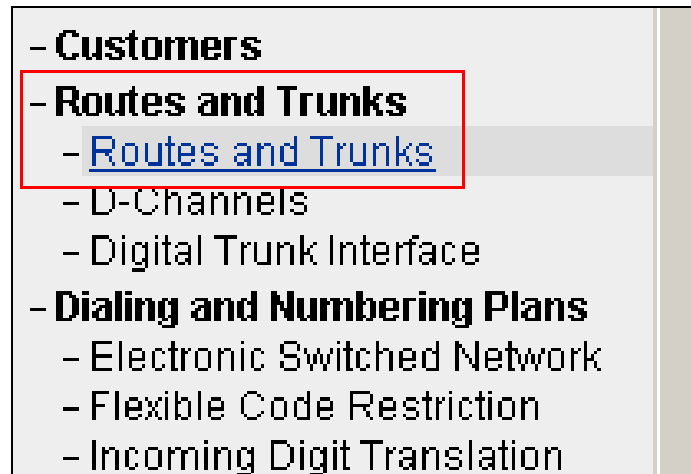
**- Remote Capabilities Configuration**

Input Description	
Basic rate interface (BRI)	<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 (DV1)	<input type="checkbox"/>
Diversion info. is sent using object identifier (DV10)	<input type="checkbox"/>
Rerouting requests processed using integer value (DV2)	<input type="checkbox"/>
Rerouting requests processed using object identifier (DV20)	<input type="checkbox"/>
Diversion info. sent. rerouting requests processed (DV3)	<input type="checkbox"/>
EuroISDN - div. info sent. rerouting req. processed (DV30)	<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 checked="" 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"/>
Network name display method 3 (ND3)	<input type="checkbox"/>

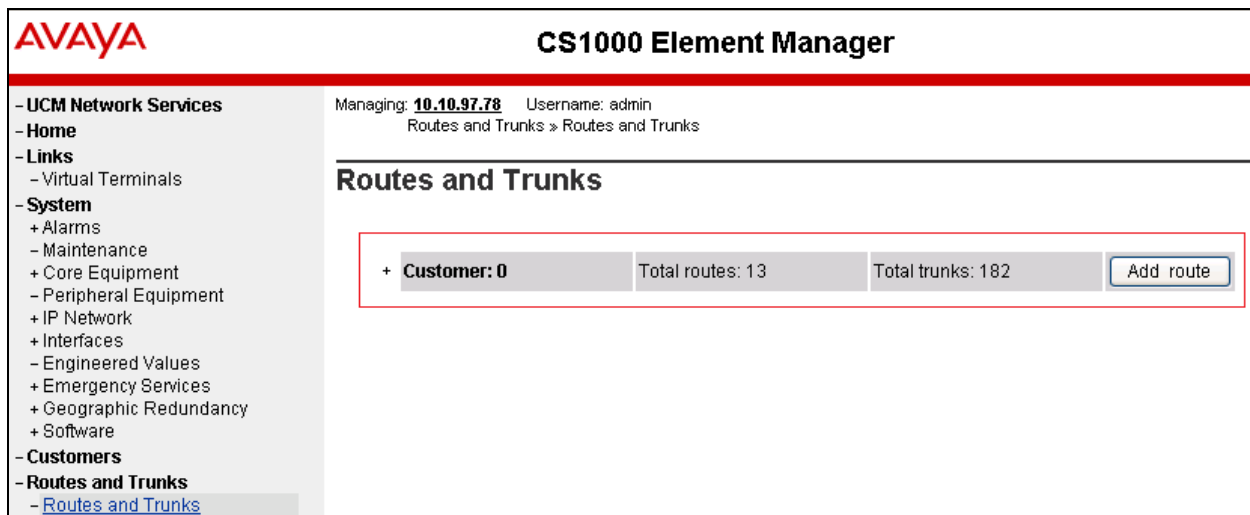
Click on the **Submit** button (not shown) to complete the D-channel configuration.

## 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 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):** A number configured in the system as explained in **Section 5.4**.
- **Node ID of signaling server of this route (NODE):** *511*; 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.

AVAYA		CS1000 Element Manager	
<b>- UCM Network Services</b> <b>- Home</b> <b>- Links</b> - Virtual Terminals <b>- System</b> + Alarms - Maintenance + Core Equipment - Peripheral Equipment + IP Network - Interfaces - Engineered Values + Emergency Services + Geographic Redundancy + Software <b>- Customers</b> <b>- Routes and Trunks</b> - Routes and Trunks - D-Channels - Digital Trunk Interface <b>- Dialing and Numbering Plans</b> - Electronic Switched Network - Flexible Code Restriction - Incoming Digit Translation <b>- Phones</b> - Templates - Reports - Views - Lists - Properties - Migration <b>- Tools</b> + Backup and Restore - Date and Time + Logs and reports <b>- Security</b> + Passwords + Policies + Login Options		Managing: <b>10.10.97.78</b> Username: admin Routes and Trunks > Routes and Trunks > Customer 0, Route 1 Property Configuration <h3>Customer 0, Route 1 Property Configuration</h3> <div> <b>- Basic Configuration</b> </div> <div>           Route data block (RDB) (TYPE): <input type="text" value="RDB"/>            Customer number (CUST): <input type="text" value="00"/>            Route number (ROUT): <input type="text" value="1"/>            Designator field for trunk (DES): <input type="text" value="SIP"/>            Trunk type (TKTP): <input type="text" value="TIE"/>            Incoming and outgoing trunk (ICOG): <input type="text" value="Incoming and Outgoing (IAO)"/>            Access code for the trunk route (ACOD): <input type="text" value="8001"/>            Trunk type M911P (M911P): <input type="checkbox"/>            The route is for a virtual trunk route (VTRK): <input checked="" type="checkbox"/>            - Zone for codec selection and bandwidth management (ZONE): <input type="text" value="00002"/> (0 - 8000)            - Node ID of signaling server of this route (NODE): <input type="text" value="511"/> (0 - 9999)            - Protocol ID for the route (PCID): <input type="text" value="SIP (SIP)"/>            - Print correlation ID in CDR for the route (CRID): <input checked="" type="checkbox"/>            - Enable Shared Bandwidth Management for the route (SBWM): <input type="checkbox"/>            Integrated services digital network option (ISDN): <input checked="" type="checkbox"/>            - Mode of operation (MODE): <input type="text" value="Route uses ISDN Signaling Link (ISLD)"/>            - D channel number (DCH): <input type="text" value="1"/> (0 - 254)            - Interface type for route (IFC): <input type="text" value="Meridian M1 (SL1)"/>            - Private network identifier (PNI): <input type="text" value="00001"/> (0 - 32700)            - Network calling name allowed (NCNA): <input checked="" type="checkbox"/>            - Network call redirection (NCRD): <input checked="" type="checkbox"/>            - Trunk route optimization (TRO): <input type="checkbox"/>            - Recognition of DTI2 ABCD FALT signal for ISL (FALT): <input type="checkbox"/>            - Recognition of DTI2 ABCD FALT signal for ISL (FALT): <input type="checkbox"/>            - Channel type (CHTY): <input type="text" value="B-channel (BCH)"/>            - Call type for outgoing direct dialed TIE route (CTYP): <input type="text" value="Coordinated Dialing Plan (CDP)"/>            - Insert ESN access code (INAC): <input checked="" type="checkbox"/>            - Integrated service access route (ISAR): <input type="checkbox"/>            - Display of access prefix on CLID (DAPC): <input type="checkbox"/>            - Mobile extension route (MBXR): <input type="checkbox"/>            - Mobile extension outgoing type (MBXOT): <input type="text" value="National number (NPA)"/>            - Mobile extension timer (MBXT): <input type="text" value="0"/> (0 - 8000 milliseconds)            Calling number dialing plan (CNDP): <input type="text" value="Coordinated dialing plan (CDP)"/>  <div> <b>- Network Options</b> </div> <div>           Electronic switched network pad control (ESN): <input checked="" type="checkbox"/>            Signaling arrangement (SIGO): <input type="text" value="Standard (STD)"/>            Route class (RCLS): <input type="text" value="Route Class marked as external (EXT)"/>            Off-hook queuing (OHQ): <input type="checkbox"/>            Off-hook queue threshold (OHQT): <input type="text" value="0"/>            Call back queuing (CBQ): <input checked="" type="checkbox"/>            Number of digits (NDIG): <input type="text" value="2"/>            Authcode (AUTH): <input type="checkbox"/> </div> </div>	

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: 10.10.97.76 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:

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:

- Short or long line:

- Transmission Class of Service:

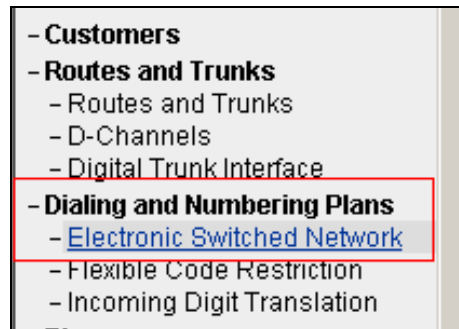
- Warning Tone:

- Reversed Ear Piece:

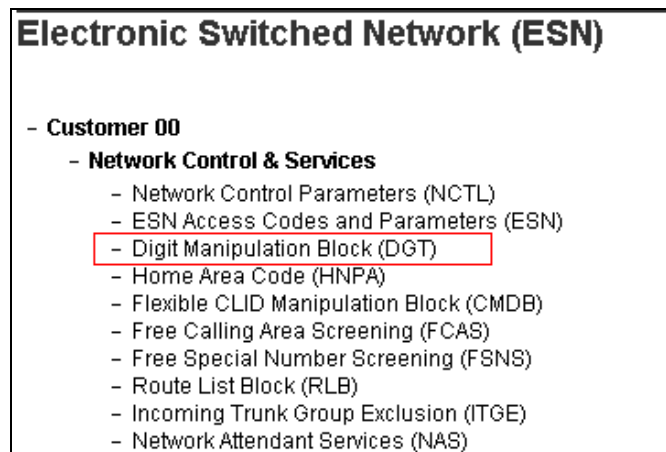
- ARF Supervised COT:

## 5.8. Configuring Digit Manipulation Block

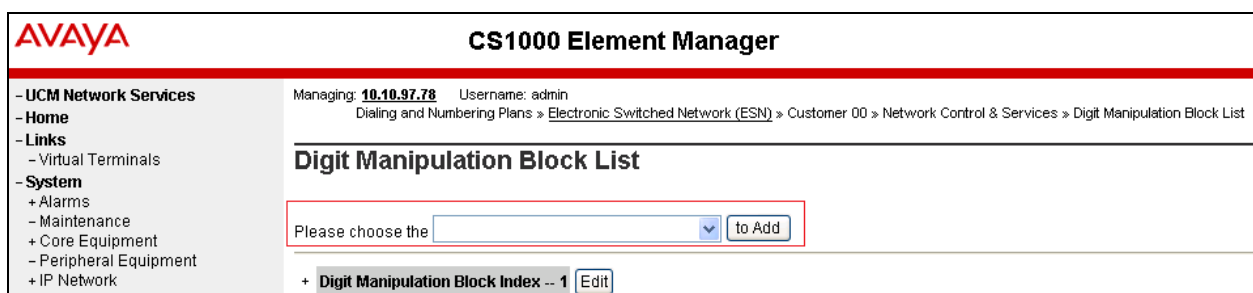
This section explains the digit manipulation block that is to be configured in the Communication Server 1000 dialing plan for its users to communicate with the Responder via Session Manager. From the EM navigator pane, navigate to **Dialing and Numbering Plans → Electronic Switched Network** as shown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



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

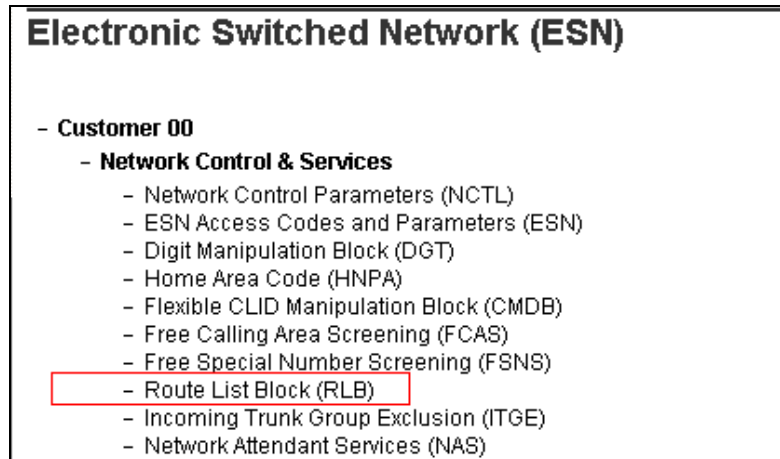


Screen below shows the **Digit Manipulation Block List** page where users can add a digit manipulation block index by selecting an available one from the drop down menu. During compliance testing **Digit Manipulation Block Index -- 0** was used which is already added in the Communication Server 1000 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 Responder 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 shows the values configured for the route list index block 1 added during compliance testing.

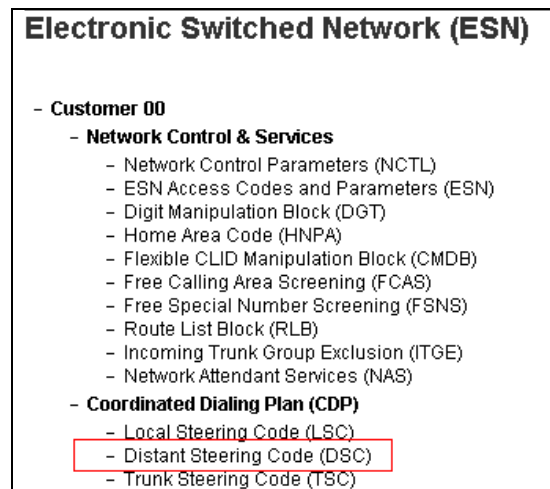
**Digit Manipulation Index:** Select *0* from the drop down menu. This was configured in **Section 5.8**.

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

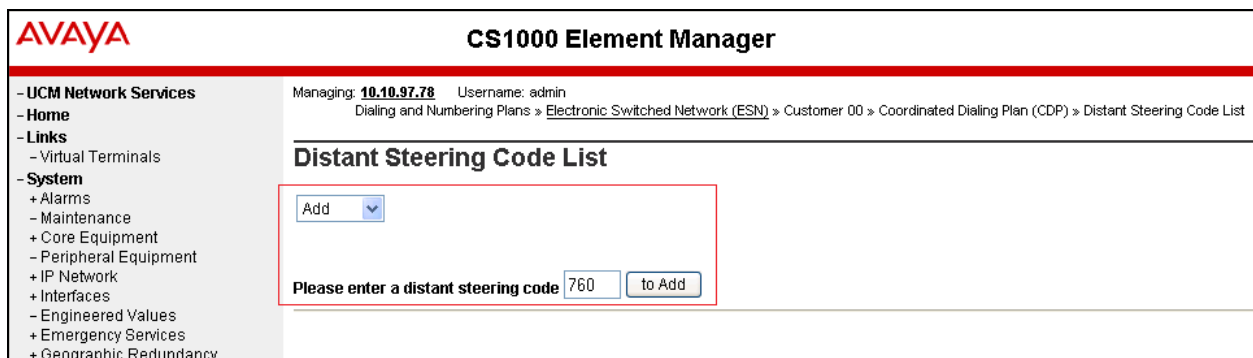
Click on **Submit** to complete the configuration.

## 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 Responder 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 **760** was added since the pilot number assigned to Infinity was 76000.



Screen below shows the values configured for the distant steering code of 760 added during compliance testing.

Enter the values as shown in screen below.

**Flexible Length number of digits:** 5; since 76000 the number to dial Infinity 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.

AVAYA CS1000 Element Manager

Managing: 10.10.87.78 Username: admin

Dialing and Numbering Plans > Electronic Switched Network (ESN) > Customer 00 > Coordinated Dialing Plan (CDP) > Distant Steering Code List > Distant Steering Code

### Distant Steering Code

Distant Steering Code: 76

Flexible Length number of digits: 5 (0 - 10)

Display: Local Steering Code (LSC)

Remote Radio Paging Access: ☐

Route List to be accessed for trunk steering code: 1

Collect Call Blocking: ☐

Maximum 7 digit NPA code allowed:

Maximum 7 digit NXX code allowed:

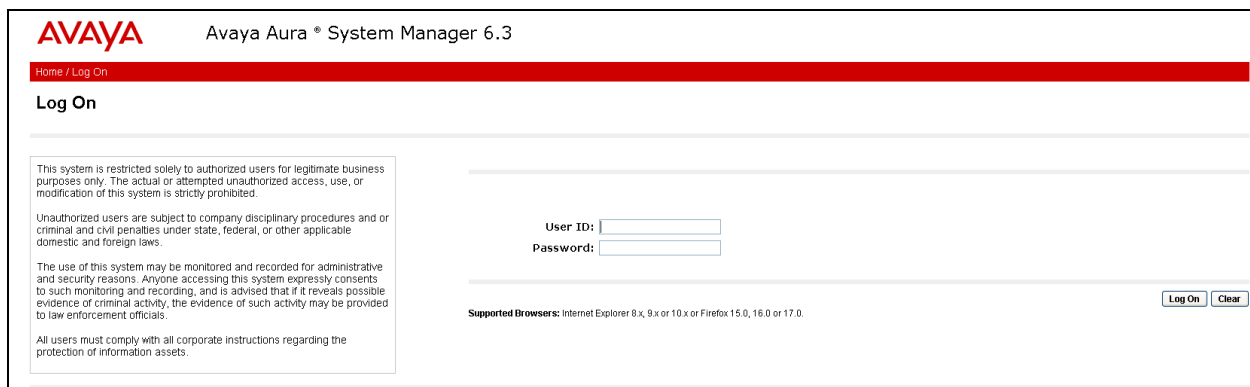
Submit Refresh Delete Cancel

## 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 Session Manager refer to **Section 10**

Session Manager is administered via 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.



The screenshot shows the Avaya Aura System Manager 6.3 login interface. At the top, the Avaya logo is on the left, and the text "Avaya Aura® System Manager 6.3" is on the right. Below the logo, there is a red navigation bar with the text "Home / Log On". Underneath the navigation bar, the text "Log On" is displayed. The main content area is divided into two columns. The left column contains a disclaimer box with the following text: "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." The right column contains the login fields: "User ID:" followed by a text input field, and "Password:" followed by a password input field. Below the password field, there is a "Supported Browsers:" label and a list of supported browsers: "Internet Explorer 8.x, 9.x or 10.x or Firefox 15.0, 16.0 or 17.0". At the bottom right of the login area, there are two buttons: "Log On" and "Clear".

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 Session Manager Routing Administration.

**AVAYA**

Avaya Aura® System Manager 6.3

Last Logged on at January 21, 2014 11:41 AM  
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

**Users**

[Administrators](#)  
Manage Administrative Users

[Directory Synchronization](#)  
Synchronize users with the enterprise directory

[Groups & Roles](#)  
Manage groups, roles and assign roles to users

[User Management](#)  
Manage users, shared user resources and provision users

**Elements**

[Communication Manager](#)  
Manage Communication Manager 5.2 and higher elements

[Communication Server 1000](#)  
Manage Communication Server 1000 elements

[Conferencing](#)  
Manage Conferencing Multimedia Server objects

[IP Office](#)  
Manage IP Office elements

[Meeting Exchange](#)  
Manage Meeting Exchange and Avaya Aura Conferencing 6.0 elements

[Messaging](#)  
Manage Avaya Aura Messaging, Communication Manager Messaging, and Modular Messaging

[Presence](#)  
Presence

[Routing](#)  
Session Manager Routing Administration

[Session Manager](#)  
Session Manager Administration, Status, Maintenance and Performance Management

**Services**

[Backup and Restore](#)  
Backup and restore System Manager database

[Bulk Import and Export](#)  
Manage Bulk Import and Export of Users, User Global Settings, Roles, Elements and others

[Configurations](#)  
Manage system wide configurations

[Events](#)  
Manage alarms, view and harvest logs

[Geographic Redundancy](#)  
Manage Geographic Redundancy

[Inventory](#)  
Manage, discover, and navigate to elements

[Licenses](#)  
View and configure licenses

[Replication](#)  
Track data replication nodes, repair replication nodes

[Scheduler](#)  
Schedule, track, cancel, update and delete jobs

[Security](#)  
Manage Security Certificates

[Shutdown](#)  
Shutdown System Manager Gracefully

[Software Management](#)  
Upgrade and Patch Management for Communication Manager devices and IP Office

[Templates](#)  
Manage Templates for Communication Manager, Messaging System and IP Office elements

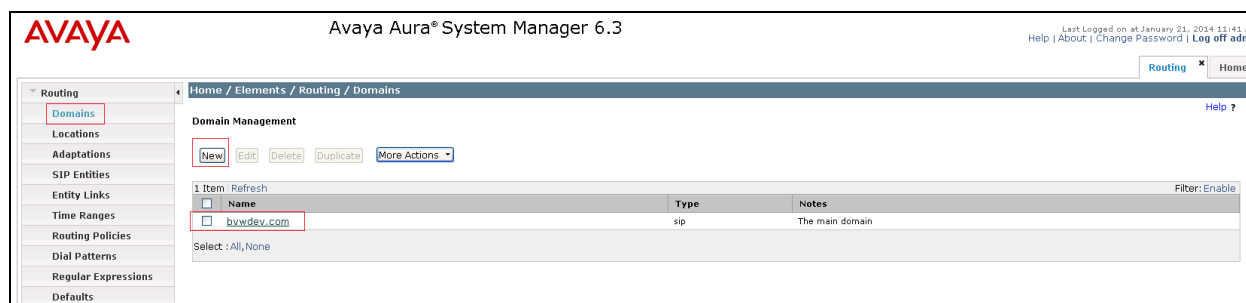
## 6.1. Configure Session Manager Details

Administration for the solution required the following steps:

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

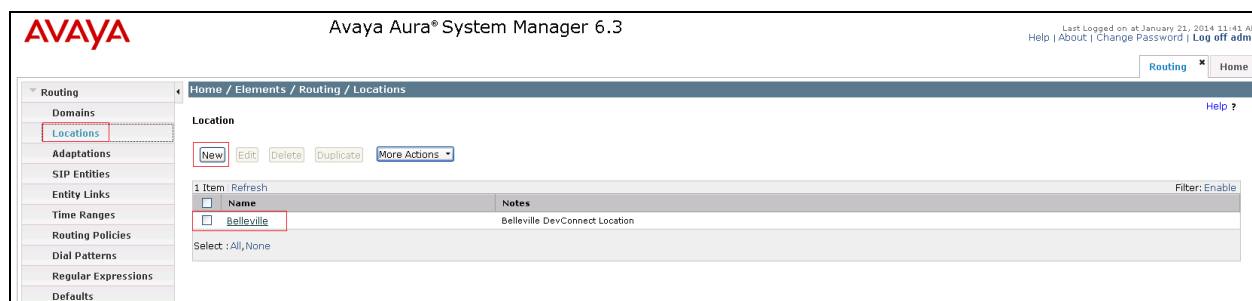
### 6.1.1. Add a Domain

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 **bwvdev.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. Add a SIP Entity

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 (*AmTelco*).

**FQDN or IP Address:** *10.10.97.57* was the address used by the Infinity server during compliance testing.

**Type:** Select *Other* from the drop down menu.

**Notes:** Useful for quick glance identification on other screens.

**Location:** Select *Belleville* from the drop down list.

**SIP Link Monitoring:** Select *Link Monitoring Enabled* from the drop down menu. The Infinity Server does support keep-alive messages and therefore we can 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 6.1.4** for how the Entity Link was created. Retain default values for other fields.

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

AVAYA Avaya Aura® System Manager 6.3

Routing Home

Home / Elements / Routing / SIP Entities

SIP Entity Details

General

Name: AmTelco

FQDN or IP Address: 10.10.97.57

Type: Other

Notes: SIP Entity for AmTelco testing

Adaptation: [v]

Location: Belleville

Time Zone: America/Portaleza

Override Port & Transport with DNS SRV: [x]

SIP Timer B/F (in seconds): 4

Credential name: [v]

Call Detail Recording: none

CommProfile Type Preference: [v]

Loop Detection

Loop Detection Mode: Off

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Supports Call Admission Control: [x]

Shared Bandwidth Manager: [x]

Primary Session Manager Bandwidth Association: [v]

Backup Session Manager Bandwidth Association: [v]

Entity Links

Add Remove

SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
DevSM	UDP	5060	AmTelco	5060	trusted	[x]

Select: All, None

SIP Responses to an OPTIONS Request

Add Remove

Response Code & Reason Phrase	Mark Entity Up/Down	Notes

Commit Cancel

### 6.1.4. Add Entity Links

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:** *AmTelco\_UDP* - A Descriptive name for the Entity Link.

**SIP Entity 1:** Select *DevSM* from the drop down menu – This is the existing Session Manager SIP Entity.

**SIP Entity 2:** Select *AmTelco* from the drop down menu – This is the newly created SIP entity in Section 6.1.3.

**Protocol:** Select *UDP* from the drop down menu.

**Port:** *5060* – Port 5060 is the standard listen port for the UDP SIP transport protocol.

Retain default values for other fields.

Click **Commit** to save the entries.

Avaya Aura® System Manager 6.3

Home / Elements / Routing / Entity Links

Entity Links

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service	Notes
*AmTelco_UDP	*DevSM	UDP	*5060	*AmTelco	*5060	trusted	<input type="checkbox"/>	

Commit Cancel



### 6.1.5. 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.

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 *AmTelco* 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 6.1.6** but is shown here for brevity.

AVAYA Avaya Aura® System Manager 6.3

Home / Elements / Routing / Routing Policies

Routing Policy Details

Commit Cancel

General

\* Name: Route\_To\_AmTelco\_Server

Disabled: ☐

\* Retries: 0

Notes: Routing to AmTelco server

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
AmTelco	10.10.97.57	Other	SIP Entity for AmTelco testing

Time of Day

Add Remove View Gaps/Overlaps

1 Item Refresh

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select: All, None

Dial Patterns

Add Remove

1 Item Refresh

Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
76	5	5	<input type="checkbox"/>	bvvidev.com	Belleville	Dial Pattern forAmTelco Infinity Server

Select: All, None

Regular Expressions

Add Remove

0 Items Refresh

Pattern	Rank Order	Deny	Notes
---------	------------	------	-------

Commit Cancel

### 6.1.6. Create Dial Pattern

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:** 76 – Pilot number to reach the Infinity Server was defined as 76000 during compliance testing.

**Min and Max:** 5 – The number of digits in the dialed number to match.

**SIP Domain:** Select *bwdev.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.

Avaya Aura® System Manager 6.3

Home / Elements / Routing / Dial Patterns

**Dial Pattern Details**

Commit Cancel

General

Pattern: 76

Min: 5

Max: 5

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: bwdev.com

Notes: Dial Pattern for AmTelco Infinity Server

Originating Locations and Routing Policies

Add Remove

1 Item Refresh

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 Location	Route_To_AmTelco_Server	0	<input type="checkbox"/>	AmTelco	Routing to AmTelco server

Select : All, None

Denied Originating Locations

Add Remove

0 Items Refresh

Originating Location	Notes
----------------------	-------

Commit Cancel

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\_AmTelco\_Server* policy defined in **Section 6.1.5** 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.

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The left sidebar contains a navigation menu with options: 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 a 'Routing' tab and a 'Home' button. The 'Originating Location' section includes a 'Select' button and a 'Cancel' button. Below this, there is a checkbox labeled 'Apply The Selected Routing Policies to All Originating Locations'. A table lists the available locations, with 'Belleville' highlighted. The 'Routing Policies' section shows a table of policies, with 'Route\_To\_AmTelco\_Server' highlighted. The table for 'Originating Location' has columns for 'Name' and 'Notes'. The table for 'Routing Policies' has columns for 'Name', 'Disabled', 'Destination', and 'Notes'.

Name	Notes
Belleville	Belleville DevConnect Location

Name	Disabled	Destination	Notes
IP_Office_Bottom	<input type="checkbox"/>	IP_Office_Bottom	Route to bottom IP Office
IP_Office_Top	<input type="checkbox"/>	IP_Office_Top	Route to top IP Office
Route_To_AmTelco_Server	<input type="checkbox"/>	AmTelco	Routing to AmTelco server

## 7. Configure Amtelco Infinity Intelligent SIP Attendant Console

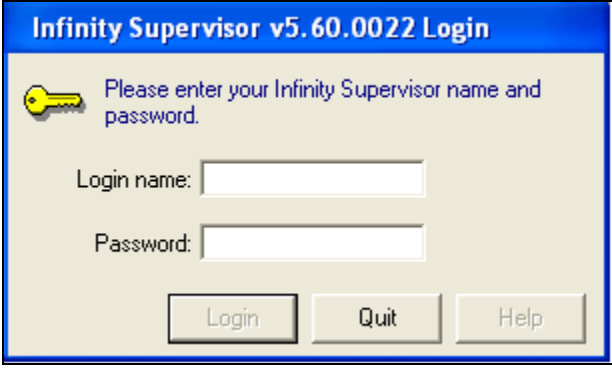
This section provides the procedures for configuring Infinity. The procedures include the following areas:

- Launch Infinity Supervisor
- Administer billing number and board settings
- Administer SIP route
- Administer clients
- Administer system settings

### 7.1. Launch Infinity Supervisor

From a PC running the Amtelco Infinity Supervisor application, select **Start → All Programs → AMTELCO → Infinity Supervisor** to display the **Infinity Supervisor Login** screen below.

Upon initial log in, prior to entering the credentials, press the **Ctrl** and **F12** key.



The screenshot shows a login window titled "Infinity Supervisor v5.60.0022 Login". Inside the window, there is a yellow key icon and the text "Please enter your Infinity Supervisor name and password." Below this, there are two input fields: "Login name:" and "Password:". At the bottom of the window, there are three buttons: "Login", "Quit", and "Help".

The **Setup Control Panel** screen is displayed. For **Server Name**, enter the IP address of the Infinity server that interfaces with attendants (SIP Card), in this case “10.10.98.46”. Retain the default values in the remaining fields. Click on the **OK** button.

The **Infinity Supervisor Login** screen shown earlier is displayed again. Log in using the appropriate credentials.

The screenshot shows the 'Setup Control Panel' dialog box with the following fields and options:

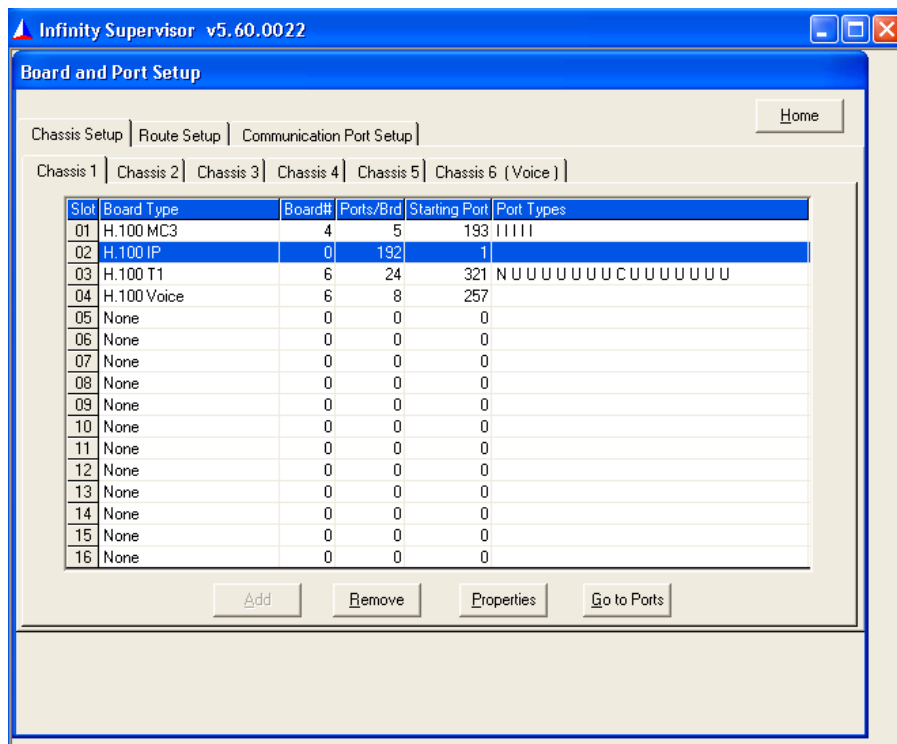
- Adapter:** 0 (dropdown menu)
- Network Type:** TCP/IP (dropdown menu)
- Server Name:** 10.10.98.46 (text field, highlighted with a red border)
- Port:** 5010 (text field, with a note '(Base Port + Str#)')
- Client Name:** (empty text field)
- Port:** 0 (text field)
- Op See Port:** 1000 (text field)
- ☒ **Replace permanent settings by writing these values to registry:**  
HKEY\_LOCAL\_MACHINE\Software\Amtelco\Inf5xSupervisor\0000
- Advanced** (button)
- OK** and **Cancel** (buttons)

## 7.2. Administer Billing Number and Board Settings

The **Infinity Supervisor** screen is displayed next. Select **BOARDS and PORTS**.



The **Board and Port Setup** screen pops up. Select the **H.100 IP** entry, and click **Properties**.



The **Board Properties** screen pops up next. For **Billing#**, enter the applicable number to use for outbound calls for billing purposes, and click **More**.

Infinity Supervisor v5.60.0022

**Board Properties**

Existing Board: H.100 IP Chassis: 01 Slot: 02 Port Range: 0001 to 0257

Step 1: Board Type:

Select the type of board for the above chassis and slot from the list of boards below. You can use the filter buttons to only display boards of a particular type.

H.100 IP Filter for: ☒ All ☐ MVIP ☐ APIB ☐ Voice

Step 2: Board Properties:

Brd ID: 0 Each board must be assigned a unique hardware number that matches the physical switch setting made on the board itself. (Range: 0-15)

Ports/Board: 192 Select the number of ports for this board. The list reflects the possible setting for this type of board.

Starting Port #: 1 Select a starting port for this board. For a map of ports for this chassis press the "... " button. The map shows all ports and their current usage.

Billing#: 33000

More >> H.100 IP parameter settings

READ ONLY MODE!  
You must remove the board to make board level changes because of the complexity of attached port information.

Ok Cancel Ports >>

The **Board Properties** screen is updated with the **H.100 IP Board Settings** sub-section. For **Port**, enter “32768”. Enter the pertinent network information (Server IP Address) for the remaining fields.

Infinity Supervisor v5.60.0022

**Board Properties**

Existing Board: H.100 IP Chassis: 01 Slot: 02 Port Range: 0001 to 0257

Step 1: Board Type:

Select the type of board for the above chassis and slot from the list of boards below. You can use the filter buttons to only display boards of a particular type.

H.100 IP Filter for: ☒ All ☐ MVIP ☐ APIB ☐ Voice

Step 2: Board Properties:

Brd ID: 0

Ports/Board: 192

Starting Port #: 1 ...

Billing#: 33000

<< Hide

H.100 IP Board Settings

Port: 32768

IP Address: 10.10.97.57

Mask: 255.255.255.240

Gateway: 10.10.97.49

DNS: 0.0.0.0

READ ONLY MODE!  
You must remove the board to make board level changes because of the complexity of attached port information.

Ok Cancel Ports >>

### 7.3. Administer SIP Route

The **Board and Port Setup** screen is displayed next. Select the **Route Setup** → **SIP** tab, followed by the **General** sub-tab.

Under **Options**, check **Send Options for Register**.

For **Register Time**, enter a desired interval for the Options message. Retain default values for other fields.

Infinity Supervisor v5.60.0022

Board and Port Setup

Chassis Setup | **Route Setup** | Communication Port Setup

Properties | Port Selection | Options | **SIP**

Save Undo

Route List

Name	Rte
CS1k	R0
ISDN	R1
	R2
	R3
	R4
	R5
	R6
	R7
DO NOT USE/P	R8
	R9
	R10
	R11
	R12
	R13
	R14

Edit Route Name

**General** Domains

SIP User Authentication

User: Password:

Miscellaneous Options

Register Time: 36000 DNS:

☒ No Alert  
☒ Send Options for Register  
☐ Assert



Select the **Domains** sub-tab. Enter the following values for the specified fields, and retain the default values for the remaining fields. Click on the **Save** button.

- **To Number:** 76000
- **To Domain:** IP address of Session Manager signaling interface.
- **From Number:** 33000
- **From Domain:** IP address of the IP board from **Section 7.2**.
- **Contact Number:** 33000
- **Contact Domain:** IP address of the IP board from **Section 7.2**.
- **URI Port:** Infinity SIP entity port number from **Section Error! Reference source not found.**
- **URI Domain:** IP address of Session Manager signaling interface.

Infinity Supervisor v5.60.0022

Board and Port Setup

Chassis Setup | Route Setup | Communication Port Setup

Properties | Port Selection | Options | SIP

Route List

Name	Rte
CS1k	R0
ISDN	R1
	R2
	R3
	R4
	R5
	R6
	R7
DO NOT USE/P	R8
	R9
	R10
	R11
	R12
	R13
	R14

Edit Route Name

General | Domains

Save Undo

**To**

Number: 76000 Domain: 10.10.97.198

**From**

Number: 33000 Domain: 10.10.97.57

**Contact**

Number: 33000 Domain: 10.10.97.57

**URI**

Port: 5060 [Default](#) Domain: 10.10.97.198

## 7.4. Administer Clients

From the **Infinity Supervisor** screen shown below, select **CLIENT**.



Enter an available client number, in this case “76000” and click on **Edit** to configure the values. If there is no available client then a **Client not found** pop-up window appears (not shown) asking user to confirm adding a new client, click on the **Yes** button to confirm.

The screen is updated as shown below. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name:** Name to display to the attendant when answering calls to this client.
- **Answer Phrase:** Guidance phrase for what to say when answering calls to this client.
- **Source ID:** The phone number identification for this client.

Repeat this section to administer all needed clients. In this compliance testing, calls from the PSTN will be routed with digits 76000 to Infinity.

The screenshot displays the 'Infinity Supervisor v5.60.0022' application window. At the top, the 'Client #' is set to '76000'. Below this, the 'Page: General Information' tab is active. The 'General Info' section contains the following fields and options:

- Name:** 'Client 76000' (with a tooltip: 'The name of the client. It is displayed along with the client number on the operator screen call line.')
- Answer Phrase:** 'This is Amtelco Infinity, how may I redirect your call' (with a tooltip: 'Enter what should be said when answering calls for this client.' and a link to 'More answer phrase options').
- Billing Number:** '0' (with a tooltip: 'A number used for billing purposes that may be different than the client number.')
- PBX Setup:** A link to 'PBX Setup'.
- This Client is a Template?** An unchecked checkbox with a tooltip: 'Client templates can only be edited by Supervisors with permission.'

The 'Client Identity' section includes:

- Source:** A dropdown menu set to 'ID' and a text field containing '76000' (with a link to 'Make Inactive').
- Secondary Sources:** Five input fields labeled 2), 3), 4), and 5).

The 'Client's Status' section shows:

- Current Status:** 'No Status' (with a tooltip: 'Client's current status (read only - set by client or oper)').

## 7.5. Administer System Settings

From the **Infinity Supervisor** screen shown below, select **SYSTEM SETTINGS**.



The screen below is displayed. For **Window**, select **System Options** from the drop-down list.

Select the **Telephony** tab, and enter a valid account number for **Reg. Account**.

Reboot the Infinity server.

The screenshot shows the 'Infinity Supervisor v5.60.0022' application window. The 'Window' dropdown is set to 'System Options'. The 'Telephony' tab is selected and highlighted with a red box. The 'Reg. Account' field is also highlighted with a red box and contains the value '1'. Other fields include 'Direct SMDI' (Called), 'Direct VBPC' (Called), 'Default Music Port' (199), 'Off Hook Time' (800 ms), 'Flash Hook Time' (0 ms), 'Flash Hook Delay' (0 ms), 'Flash Guard Time' (0 ms), 'Dialout Guard Time' (0 ms), and 'QSIG Timeout' (0 ms). Below these are sections for 'XDS & Voice Ports' and 'Digital Ports' with checkboxes for 'Run in ALAW?', 'Display Names?', and 'Display Sources?'. The 'amtelco' logo is visible in the top right of the window.

Field	Value	Description
Window	System Options	
Direct SMDI	Called	Select the SMDI line interface between Infinity and the PBX.
Direct VBPC	Called	Select the VBPC line interface between Infinity and the PBX.
Default Music Port	199	Select the default port to be used for Music on Hold and for Auto-Answer Music.
Off Hook Time	800 ms	Set how long to wait after sensing an off-hook to ensure it really is an off-hook.
Flash Hook Time	0 ms	Set the duration of the flash-hook.
Flash Hook Delay	0 ms	Set the length of time to wait after a flash-hook before continuing.
Flash Guard Time	0 ms	Set flash guard time.
Dialout Guard Time	0 ms	Set dialout guard time.
QSIG Timeout	0 ms	Set QSIG path replacement timeout.
Reg. Account	1	SIP Registration account.

**XDS & Voice Ports**

- Run in ALAW? ☐ Check for E1 (European) ISDN. (Requires a restart to enable)

**Digital Ports**

- Display Names? ☐ Use a disk file to fill the Calling, Called, and Reason fields.
- Display Sources? ☐ Parses the digital phone display to fill in the Called and Calling fields.

## 8. Verification Steps

This section provides tests that can be performed to verify proper configuration of Communication Manager, Session Manager, and Infinity.

### 8.1. Verify Avaya Communication Server 1000

On Communication Server 1000, verify the status of the DCH by the **stat dch** command. Verify that the DCH is in **OPER EST** and **ACTV** status as shown below.

```
.stat dch
DCH 001 : OPER      EST   ACTV  AUTO      DES : SIP
```

### 8.2. Verify Avaya Aura® Session Manager

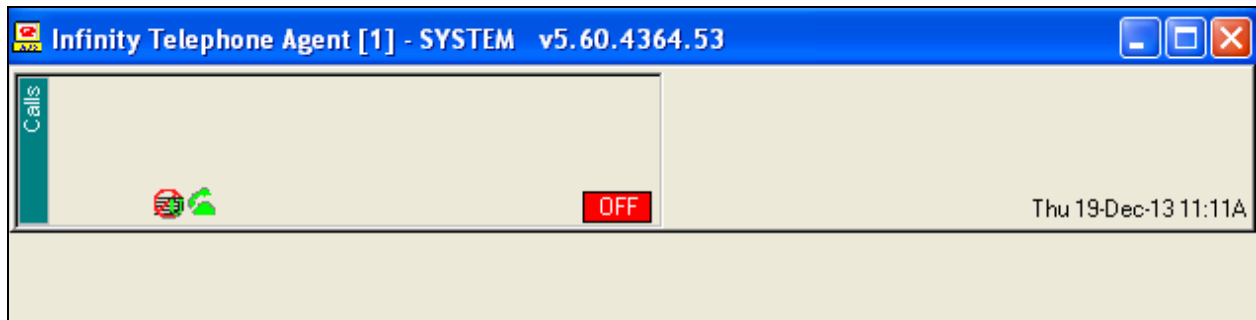
Navigate to **Elements → Session Manager → System Status → SIP Entity Monitoring** and select the Communication Server 1000 SIP Entity (not shown). Verify the **Link Status** is *Up*. Repeat the procedure above selecting the AmTelco Infinity server SIP Entity (not shown), and verify the **Link Status** is *Up*.

### 8.3. Verify Infinity Intelligent SIP Attendant Console

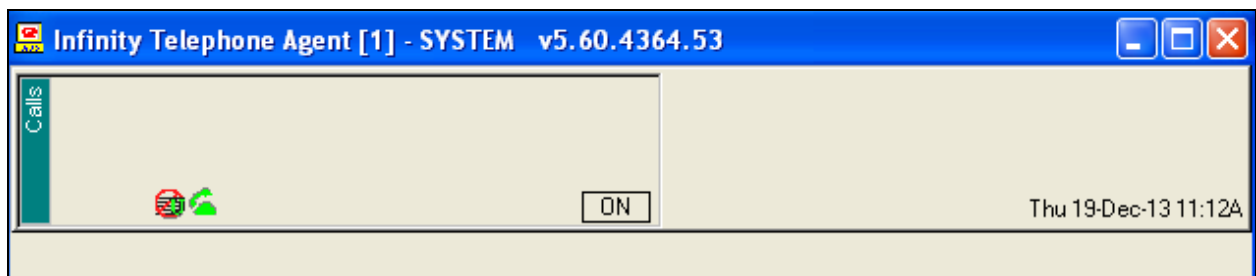
From an attendant PC running the Amtelco Infinity Telephone Agent application, select **Start → All Programs → AMTELCO → Infinity Telephone Agent** to display the **Infinity Telephone Agent** screen below. Log in using the appropriate credentials.



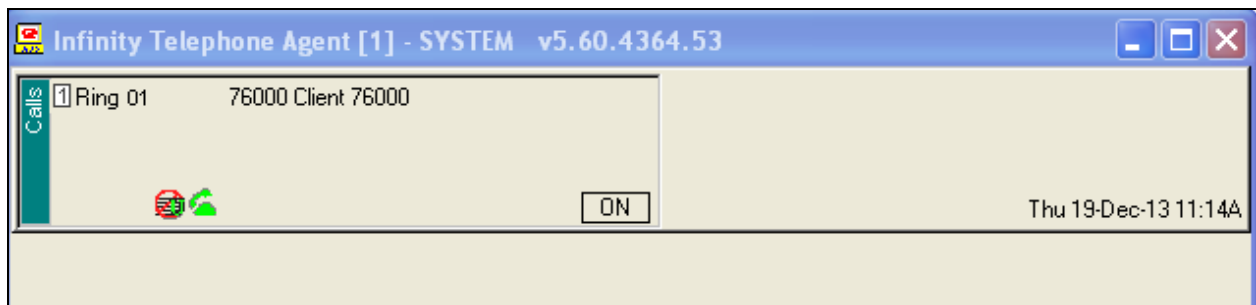
The screen below is displayed next. Click **OFF** to toggle into available.



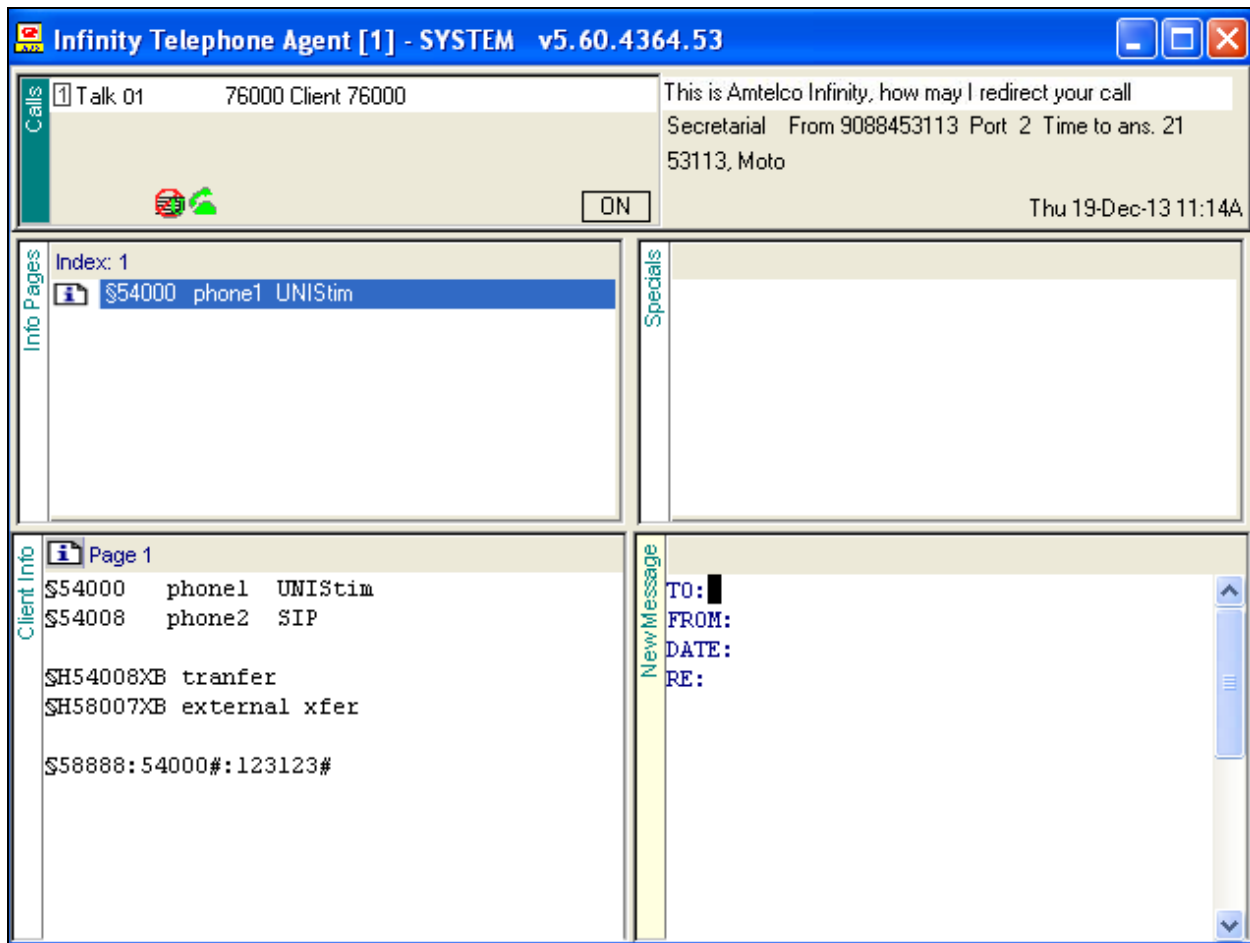
Verify the status is updated to **ON**, as shown below.



Make an incoming call from the PSTN to reach Infinity. Verify that an available attendant hears the alerting tone, and that the attendant screen is updated showing the alerting call. Also verify that the display information reflects the proper client ID and name from **Section 7.4**.



Press **F1** to answer the call. Verify that the attendant is connected to the PSTN with two-way talk paths, and that the screen is updated with the proper guidance phrase from **Section 7.4**.



## 9. Conclusion

These Application Notes describe the configuration steps required for Amtelco Infinity Intelligent SIP Attendant Console to successfully interoperate with Avaya Aura® Session Manager. 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.

### Avaya

*Communication Server 1000E Installation and Commissioning*, March 2013, Release 7.6, NN46041-310

*Element Manager System Reference – Administration - Avaya Communication Server 1000*, March 2013, Release 7.6, NN43001-632.

*Co-resident Call Server and Signaling Server Fundamentals - Avaya Communication Server 1000*, March 2013, Release 7.6, NN43001-509.

*Unified Communications Management Common Services Fundamentals - Avaya Communication Server 1000*, March 2013, Release 7.6, NN43001-116.

*Administering Avaya Aura® System Manager*, October 2013, Release 6.3.

*ISDN Primary Rate Interface Installation and Commissioning - Avaya Communication Server 1000*, March 2013, Release 7.6, NN43001-301.

*Administering Avaya Aura® Session Manager*, October 2013, Release 6.3, Document Number 03-603324.

### Amtelco

Product information for Amtelco Infinity can be found at <http://www.amtelco.com/>.

*Infinity Supervisor Reference Guide*, Version 232M072, November 2012, available at <http://service.amtelco.com>.

---

**©2014 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](mailto:devconnect@avaya.com).