



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Dialogic® BorderNet™ 2020 Integrated Media Gateway with Avaya Aura® Session Manager and Avaya Aura® Communication Manager - Issue 1.0

Abstract

These Application Notes describe the procedure to configure Dialogic® BorderNet™ 2020 Integrated Media Gateway to interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager as an ISDN PRI/SIP gateway using SIP trunking.

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 procedure to configure Dialogic® BorderNet™ 2020 Integrated Media Gateway to interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager as an ISDN PRI/SIP gateway using SIP trunking.

Dialogic® BorderNet™ 2020 Integrated Media Gateway combines integrated media and signaling, IP and TDM gateway capabilities with session border controller functionality in a compact 1U form factor appliance.

The compliance testing of the Dialogic® BorderNet™ 2020 Integrated Media Gateway focused on its ISDN PRI/SIP gateway functions.

2. General Test Approach and Test Results

The interoperability compliance test included feature and serviceability. During the test, various call scenarios were exercised to verify call and feature interoperability of BorderNet 2020 and Avaya products. Network and server outage conditions were used to verify serviceability of the joint solution.

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 primary focus of the feature testing was to verify SIP trunking interoperability between an Avaya SIP-based network and BorderNet 2020. Test cases were selected to verify the following areas.

Basic Interoperability:

- PSTN calls from and to Avaya IP/SIP telephones via BorderNet 2020. Some sample testing with traditional analog and Avaya digital phones were also performed.
- Multiple codecs support, e.g. G.711MU and G.729AB
- Various PTSN dialing plans including national and international calling, toll-free, and direct inward dialed calling
- SIP transport using UDP

Advanced Interoperability:

- Codec negotiation
- Quality of Service
- Telephony supplementary features, such as Hold, Blind Transfer, Attended Transfer, Conference, and Call Forwarding
- DTMF Support using RFC 2833

- T.38 Fax support
- Voicemail Coverage and Retrieval
- Calling Number Block
- Direct IP-to-IP Media (also known as “Shuffling”) over SIP Trunk. Direct IP-to-IP media allows a RTP path to be established directly between Avaya phones and BorderNet 2020 gateway and release media processing resources on the Avaya Media Gateway

The serviceability testing focused on verifying the ability of the solution to recover from adverse conditions, such as network failures and BorderNet 2020 reboot.

2.2. Test Results

All test cases were executed and verified. The following observation was made during the compliance test:

Initially, the RFC 2833 method of passing DTMF digits did not work for both inbound and outbound calls when shuffling was enabled on the SIP trunk. Dialogic provided a patch with the version 2.2 SP2 b1561, which is slated to be part of 2.2 SP3.

2.3. Support

Technical Support on Dialogic BorderNet 2020 can be obtained through the following phone contacts:

- Phone: +1 781 433 9600
- E-mail: americas.support@dialogic.com

3. Reference Configuration

The reference configuration consists of Communication Manager, Session Manager, System Manager, Messaging, BorderNet 2020, and a number of Avaya telephones. BorderNet 2020 is used as a SIP/ISDN gateway for PSTN access. The Session Manager in the right block, managed through the System Manager in the same block, routes the calls between the different entities using SIP Trunks. The management interface of BorderNet 2020 has to be on a different subnet from the signaling and media interfaces. The Messaging server resides in another subnet and is connected to Communication Manager via a different Session Manager (not shown).

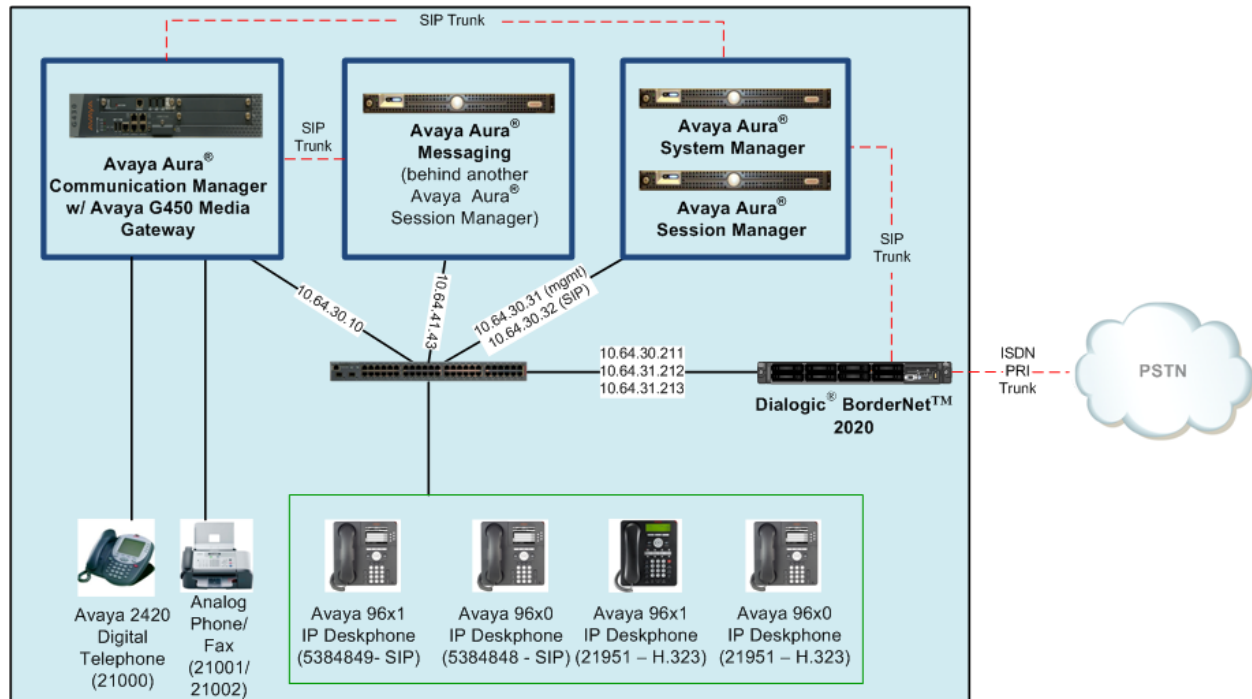


Figure 1 – Sample configuration for Dialogic® BorderNet™ 2020 with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using Sip Trunking

4. Equipment and Software Validated

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

Equipment/Software	Version
Avaya Aura [®] Communication Manager running on Avaya S8300D Server	6.3 SP1
Avaya G450 Media Gateway MGP MM711AP (ANA)	HW 1 FW 31.20.0 HW 27, FW 073
Avaya Aura [®] Session Manager	6.3.3
Avaya Aura [®] System Manager	6.3.3
Avaya Aura [®] Messaging	6.2
Avaya 96x0 Series IP Telephones (H.323) - Avaya one-X Deskphone Edition	3.1.5
Avaya 96x0 Series IP Telephones (SIP) - Avaya one-X Deskphone Edition SIP	2.6
Avaya 96x1 Series IP Telephones (H.323) - Avaya one-X Deskphone Edition	6.2.2
Avaya 96x1 Series IP Telephones (SIP) - Avaya one-X Deskphone Edition SIP	6.2.1
Avaya 2420 Digital Telephone	NA
Dialogic [®] BorderNet [™] 2020 Integrated Media Gateway Dialogic [®] WebUI	2.2 SP2 b1561 2.2 SP2

5. Configure Avaya Aura[®] Communication Manager

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

- Verify Avaya Aura[®] Communication Manager License
- Configure IP Node Names
- Configure IP Codec Set
- Configure IP Network Region
- Configure SIP Trunks with Session Manager
- Configure Route Pattern
- Configure Public Unknown Numbering
- Administer ARS Analysis
- Administer Feature Access Code

Throughout this section the administration of Communication Manager is performed using a System Access Terminal (SAT). Some administration screens have been abbreviated for clarity. These instructions assume that Communication Manager has been installed, configured, licensed and provided with a functional dial plan. In these Application Notes, Communication Manager was configured with 5-digit extension **21xxx** for IP stations and 7-digit extension **538xxxx** for SIP stations. Other numbers on PSTN (accessible from BorderNet 2020) were reachable via the **ars** table with the use of **feature access code 9**.

These Application Notes will focus on the configuration of the SIP trunk and related call routing. It is assumed that the following administration is already in place and will not be described in this section.

- H.323 and SIP stations
- Routing to SIP stations
- Voice Mail server connectivity

5.1. Verify Avaya Aura[®] Communication Manager License

Enter the **display system-parameters customer-options** command. Navigate to **Page 2** and verify that there is sufficient remaining capacity for SIP trunks by comparing the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column. If there is insufficient capacity of SIP Trunks or a required feature is not enabled, contact an Avaya representative to make the appropriate changes.

display system-parameters customer-options		Page	2 of	11
OPTIONAL FEATURES				
IP PORT CAPACITIES		USED		
Maximum Administered H.323 Trunks:		12000	50	
Maximum Concurrently Registered IP Stations:		18000	3	
Maximum Administered Remote Office Trunks:		12000	0	
Maximum Concurrently Registered Remote Office Stations:		18000	0	
Maximum Concurrently Registered IP eCons:		414	0	
Max Concur Registered Unauthenticated H.323 Stations:		100	0	
Maximum Video Capable Stations:		41000	0	
Maximum Video Capable IP Softphones:		18000	0	
Maximum Administered SIP Trunks:		24000	108	

5.2. Configure IP Node Names

All calls from and to Communication Manager are signalled over a SIP trunk to Session Manager. The signalling interface on Session Manager is provided by the SM100 security module. Use the **change node-names ip** command to add the **Name** and **IP Address** for the SM100 security module of Session Manager. **SM1** and **10.64.30.32** was used in this example.

change node-names ip		Page	1 of	2
		IP NODE NAMES		
Name	IP Address			
default	0.0.0.0			
procr	10.64.30.10			
procr6	::			
sm1	10.64.30.32			

5.3. Configure IP Codec Set

Use the **change ip-codec-set n** command to specify **G.711MU** and **G.729AB** codecs under **Audio Codec** where **n** is the codec set used in this configuration. Retain the default values for the remaining fields.

change ip-codec-set 1		Page	1 of	2
		IP Codec Set		
Codec Set: 1				
Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size(ms)	
1: G.711MU	n	2	20	
2: G.729AB	n	2	20	

To configure fax support, navigate to **Page 2** and change **FAX** to **t.38-standard**. Use default values for all other fields.

change ip-codec-set 1		Page 2 of 2	
IP Codec Set			
Allow Direct-IP Multimedia? y			
Maximum Call Rate for Direct-IP Multimedia:		384:Kbits	
Maximum Call Rate for Priority Direct-IP Multimedia:		384:Kbits	
	Mode	Redundancy	
FAX	t.38-standard	0	ECM: n
Modem	off	0	
TDD/TTY	US	3	
Clear-channel	n	0	

5.4. Configure IP Network Region

Use the **change ip-network-region n** command where **n** is the number of the network region used. Set the **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** fields to **yes**. For **Codec Set**, enter the codec set configured in **Section 5.3**. Set the **Authoritative Domain** to a domain name, e.g. avaya.com in this case. Retain the default values for the remaining fields.

change ip-network-region 1		Page 1 of 20	
IP NETWORK REGION			
Region: 1			
Location:	Authoritative Domain: avaya.com		
Name:	Stub Network Region: n		
MEDIA PARAMETERS		Intra-region IP-IP Direct Audio: yes	
Codec Set: 1		Inter-region IP-IP Direct Audio: yes	
UDP Port Min: 2048		IP Audio Hairpinning? y	
UDP Port Max: 3329			

5.5. Configure SIP Trunk with Session Manager

To administer a SIP Trunk on Communication Manager, two intermediate steps are required, creation of a signaling group and trunk group.

5.5.1. Configure Signaling Group

Use the **add signaling-group n** command, where **n** is an available signaling group number, and fill in the indicated fields. Default values can be used for the remaining fields:

- **Group Type:** **sip**
- **Transport Method:** **tls**
- **Near-end Node Name:** **procr**
- **Far-end Node Name:** Session Manager node name from **Section 5.2**
- **Near-end Listen Port:** **5061**
- **Far-end Listen Port:** **5061**
- **Far-end Network Region:** Network Region configured in **Section 5.4**
- **Far-end Domain:** Authoritative Domain configured in **Section 5.4**
- **DTMF over IP:** **rtp-payload** (or **in-band**, see note in **Section 2.2**)

add signaling-group 91		Page 1 of 2
SIGNALING GROUP		
Group Number: 91	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? y	
Peer Detection Enabled? y	Peer Server: SM	
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y		
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n		
Near-end Node Name: procr	Far-end Node Name: sml	
Near-end Listen Port: 5061	Far-end Listen Port: 5061	
	Far-end Network Region: 1	
	Far-end Secondary Node Name:	
Far-end Domain: avaya.com		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
	RFC 3389 Comfort Noise? n	
DTMF over IP: rtp-payload	Direct IP-IP Audio Connections? y	
Session Establishment Timer(min): 3	IP Audio Hairpinning? n	
Enable Layer 3 Test? y	Initial IP-IP Direct Media? n	

5.5.2. Configure SIP Trunk Group

Add the corresponding trunk group controlled by the above signaling group via the **add trunk-group n** command, where **n** is an available trunk group number and fill in the indicated fields.

- **Group Type:** sip
- **Group Name:** A descriptive name (e.g. **SM1**)
- **TAC:** An available trunk access code (e.g. **191**)
- **Service Type:** tie
- **Signaling Group:** Number of the signaling group added in **Section 5.5.1** (i.e. **91**)
- **Number of Members:** The number of SIP trunks to be allocated to calls routed to **Session Manager** (must be within the limits of the total trunks available from licensed verified in **Section 5.1**)

add trunk-group 91		Page 1 of 21	
TRUNK GROUP			
Group Number: 91	Group Type: sip	CDR Reports: y	
Group Name: SM1	COR: 1	TN: 1	TAC: 191
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
Service Type: tie	Auth Code? n		
	Member Assignment Method: auto		
	Signaling Group: 91		
	Number of Members: 48		

Navigate to **Page 3** and change **Numbering Format** to **public**. Use default values for all other fields.

add trunk-group 91		Page 3 of 21	
TRUNK FEATURES			
ACA Assignment? n	Measured: none	Maintenance Tests? y	
Numbering Format: public			
UUI Treatment: service-provider			
Replace Restricted Numbers? n			
Replace Unavailable Numbers? N			

5.6. Configure Route Pattern

Configure a route pattern to correspond to the newly added SIP trunk group. Use **change route pattern n** command, where **n** is an available route pattern. When changing the route pattern, enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Grp No:** The trunk group number from **Section 5.5.2**
- **FRL:** Enter a level that allows access to this trunk, with **0** being least restrictive

change route-pattern 91															Page		1 of 3			
Pattern Number: 91															Pattern Name:					
SCCAN? n															Secure SIP? n					
Grp		FRL	NPA	Pfx	Hop	Toll	No.	Inserted							DCS/		IXC			
No				Mrk	Lmt	List	Del	Digits							QSIG					
Dgts															Intw					
1:		91		0												n		user		
2:															n		user			
		BCC VALUE			TSC	CA-TSC			ITC BCIE			Service/Feature			PARM	No.	Numbering	LAR		
		0	1	2	M	4	W	Request									Dgts	Format		
															Subaddress					
1:		y	y	y	y	y	n	n		rest									none	
2:		y	y	y	y	y	n	n		rest									none	

5.7. Configure Public Unknown Numbering

Use the **change public-unknown-numbering 0** command to assign number presented by Communication Manager for calls leaving for Session Manager. Add an entry for the extensions configured in the dialplan. Enter the following values for the specified fields, and retain default values for the remaining fields.

- **Ext Len:** Number of digits of the extension i.e. **5**
- **Ext. Code:** Leading digits of the extension number, i.e. **2**
- **Total CPN Len:** Total number of digits i.e. **5**

Repeat the procedure for seven-digit extensions with **Ext Len 7, Ext. Code 5, CPN Prefix 303, and Total CPN Len 10**.

change public-unknown-numbering 0					Page 1 of 2	
NUMBERING - PUBLIC/UNKNOWN FORMAT						
				Total		
Ext	Ext	Trk	CPN	CPN		
Len	Code	Grp(s)	Prefix	Len		
				Total Administered: 2		
5	2			5		
				Maximum Entries: 9999		
7	5	303		10		

5.8. Administer ARS Analysis

This section shows a sample Auto Route Selection (ARS) entry used for routing calls with dialed digits beginning with **1720**. Use the **change ars analysis 1720** command to add an entry and specify how to route calls. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Dialed String:** Dialed prefix digits to match on, in this case **1720**
- **Total Min:** Minimum number of digits, in this case **11**
- **Total Max:** Maximum number of digits, in this case **11**
- **Route Pattern:** The route pattern number from **Section 5.6**, i.e. **91**
- **Call Type:** **hnpa**

Note that additional entries may be added for different number destinations.

change ars analysis 1720							Page 1 of 2
ARS DIGIT ANALYSIS TABLE							
Location: all							Percent Full: 0
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd	
1720	11	11	91	hnpa		n	

5.9. Administer Feature Access Code

Use the **change feature access code** command to define a feature access code for **Auto Route Selection (ARS)**. In the test, **9** was used.

change feature-access-codes		Page 1 of 11
FEATURE ACCESS CODE (FAC)		
Abbreviated Dialing List1 Access Code:		
Abbreviated Dialing List2 Access Code:		
Abbreviated Dialing List3 Access Code:		
Abbreviated Dial - Prgm Group List Access Code:		
Announcement Access Code:		
Answer Back Access Code:		
Attendant Access Code:		
Auto Alternate Routing (AAR) Access Code: 8		
Auto Route Selection (ARS) - Access Code 1: 9		Access Code 2:

6. Configure Avaya Aura® Session Manager

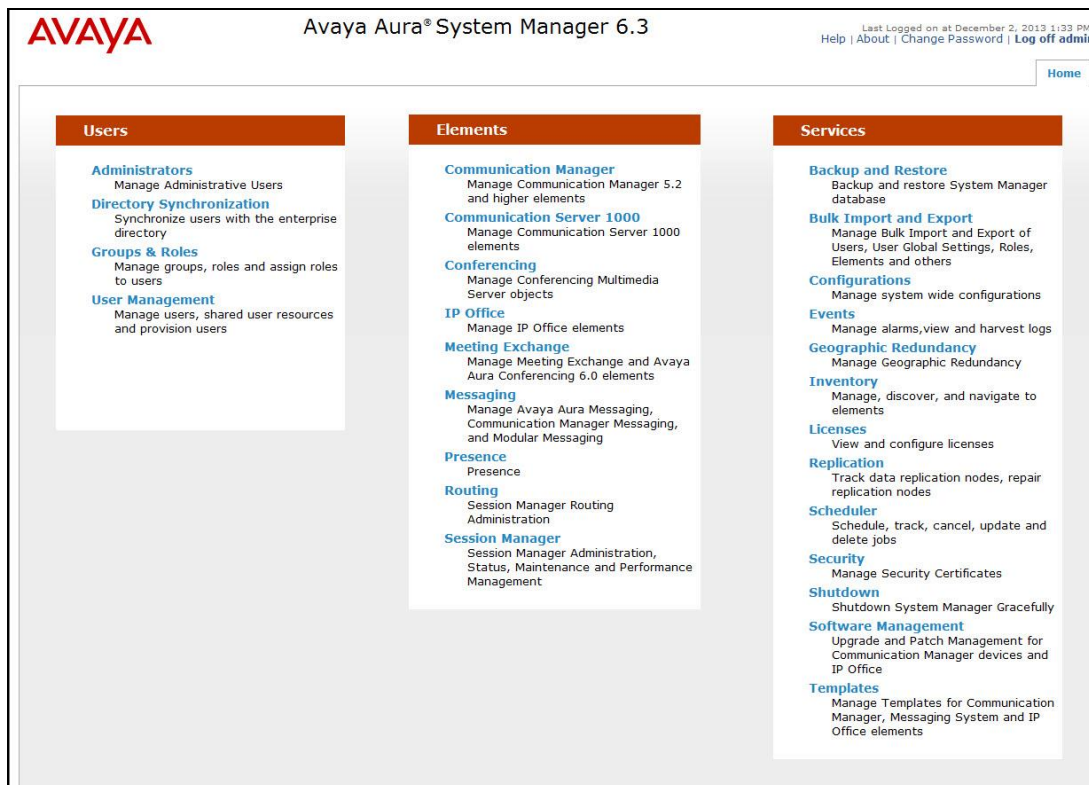
This section provides the procedures for configuring Session Manager, assuming it has been installed and licensed. The procedures include the following items:

- Specify SIP Domain
- Add Locations
- Add SIP Entities
- Add Entity Links
- Add Routing Policies
- Add Dial Patterns

It is assumed that the following items that are required for SIP stations configuration has been configured and not described in this section:

- Communication Manager as an Application
- Application Sequence Configuration
- Users for SIP stations

Configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL **http://<ip-address>**, where **<ip-address>** is the IP address of System Manager. Log in with the appropriate credentials. The menu shown below is displayed. Click on **Elements** → **Routing**.



6.1. Specify SIP Domain

Add the SIP domain for which the communications infrastructure will be authoritative. Select **Domains** on the left and click the **New** button on the right (not shown). The following screen will be shown. Fill in the following fields and click **Commit**.

- **Name:** The authoritative domain name configured in **Section 5.4** (e.g. **avaya.com**)
- **Type:** Select **sip**
- **Notes:** Descriptive text (optional)

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left sidebar contains a navigation menu with the following items: Routing, Domains (selected), Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Domain Management' and includes a 'Commit' button and a 'Cancel' button. Below this is a table with the following columns: Name, Type, and Notes. The table contains one row with the value 'avaya.com' in the Name column, 'sip' in the Type column, and an empty Notes column. Above the table is a '1 Item Refresh' button. To the right of the table is a 'Filter: Enable' button. At the bottom of the main content area are 'Commit' and 'Cancel' buttons. The top of the page features the Avaya logo, the title 'Avaya Aura System Manager 6.3', and a user status bar indicating 'Last Logged on at December 2, 2013 1:33 PM' with links for 'Help', 'About', 'Change Password', and 'Log off admin'.

6.2. Add Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside, for the purpose of bandwidth management. A single location is added to the configuration for Communication Manager and BorderNet 2020. To add a location, select **Locations** on the left and click on the **New** button on the right (not shown). The following screen will be shown. Fill in the following fields:

Under **General**:

- **Name:** A descriptive name
- **Notes:** Descriptive text (optional)

Under **Location Pattern**:

- **IP Address Pattern:** A pattern used to logically identify the location. In these Application Notes, the pattern represented the networks involved, i.e. **10.64.30.*** and **10.64.31.***.
- **Notes:** Descriptive text (optional)

The screen below shows addition of the **Site 2** location, which includes all the components of the compliance environment. Click **Commit** to save.

AVAYA

Avaya Aura[®] System Manager 6.3

Last Logged on at December 2, 2013 1:33 PM

[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Routing

Home

Routing

Elements / Routing / Locations

Help ?

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Location Details

Commit

Cancel

General

Name:

Site 2

Notes:

Dial Plan Transparency in Survivable Mode

Enabled:

☐

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units:

Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth:

☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location):

1000

Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location):

1000

Kbit/Sec

Minimum Multimedia Bandwidth:

64

Kbit/Sec

Default Audio Bandwidth:

80

Kbit/sec

Alarm Threshold

Overall Alarm Threshold:

80

%

Multimedia Alarm Threshold:

80

%

Latency before Overall Alarm Trigger:

5

Minutes

Latency before Multimedia Alarm Trigger:

5

Minutes

Location Pattern

Add

Remove

2 Items

Refresh

Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	10.64.30.*	
<input type="checkbox"/>	10.64.31.*	

Select :

All, None

6.3. Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP-based telephony system connected to it using SIP trunks. In the sample configuration, a SIP Entity is added for Communication Manager, BorderNet 2020, and Session Manager.

6.3.1. Adding Avaya Aura® Communication Manager

Select **SIP Entities** on the left and click on the **New** button on the right (not shown). Fill in the following fields.

Under **General**:

- **Name:** A descriptive name
- **FQDN or IP Address:** IP address of the procr interface of Communication Manager, i.e. **10.64.30.10**
- **Type:** Select **CM**
- **Location:** Select the location defined in **Section 6.2**
- **Time Zone:** Time zone for this entity

Defaults can be used for the remaining fields. Click **Commit** to save the SIP Entity definition. The following screen shows the configuration of the Communication Manager SIP Entity.

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The top navigation bar includes the Avaya logo, the title "Avaya Aura® System Manager 6.3", and a user status bar indicating "Last Logged on at December 2, 2013 11:33 PM" with links for "Help", "About", "Change Password", and "Log off admin". A secondary navigation bar shows "Routing" and "Home" tabs. The left sidebar contains a menu with "Routing" selected, and sub-items: "Domains", "Locations", "Adaptations", "SIP Entities" (highlighted), "Entity Links", "Time Ranges", "Routing Policies", "Dial Patterns", "Regular Expressions", and "Defaults". The main content area is titled "SIP Entity Details" and includes "Commit" and "Cancel" buttons. The "General" tab is active, showing fields for: "Name" (CM-virtual), "FQDN or IP Address" (10.64.30.10), "Type" (CM), "Notes" (empty), "Adaptation" (empty), "Location" (Site 2), "Time Zone" (America/Denver), "Override Port & Transport with DNS SRV" (unchecked), "SIP Timer B/F (in seconds)" (4), "Credential name" (empty), "Call Detail Recording" (none), "Loop Detection Mode" (Off), and "SIP Link Monitoring" (Use Session Manager Configuration). The "Loop Detection" and "SIP Link Monitoring" sections are partially visible at the bottom.

6.3.2. Adding Dialogic BorderNet 2020

Select **SIP Entities** on the left and click on the **New** button on the right (not shown).

Under **General**:

- **Name:** A descriptive name
- **FQDN or IP Address:** IP address of the signaling interface of BorderNet 2020, i.e. **10.64.31.212**
- **Type:** Select **SIP Trunk**
- **Location:** Select the location defined in **Section 6.2**
- **Time Zone:** Time zone for this entity

Defaults can be used for the remaining fields. Click **Commit** to save the SIP Entity definition. The screen below shows the configuration of the BorderNet 2020 SIP Entity.

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The top navigation bar includes the Avaya logo, the title 'Avaya Aura® System Manager 6.3', and user information: 'Last Logged on at December 2, 2013 1:33 PM', 'Help | About | Change Password | Log off admin'. The left sidebar shows a tree view with 'Routing' expanded, containing sub-items: Domains, Locations, Adaptations, SIP Entities (highlighted), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area has a breadcrumb trail 'Home / Elements / Routing / SIP Entities' and a 'Help ?' link. Below the breadcrumb is the 'SIP Entity Details' section with 'Commit' and 'Cancel' buttons. The 'General' tab is active, showing the following configuration fields: 'Name' (Dialogic BorderNet 2020), 'FQDN or IP Address' (10.64.31.212), 'Type' (SIP Trunk), 'Notes' (empty), 'Adaptation' (empty dropdown), 'Location' (Site 2), 'Time Zone' (America/Denver), 'Override Port & Transport with DNS SRV' (unchecked checkbox), 'SIP Timer B/F (in seconds)' (4), 'Credential name' (empty text field), 'Call Detail Recording' (egress dropdown), 'Loop Detection Mode' (Off dropdown), and 'SIP Link Monitoring' (Use Session Manager Configuration dropdown). The 'Loop Detection' and 'SIP Link Monitoring' sections are also visible below the main configuration area.

6.3.3. Adding Avaya Aura® Session Manager

Select **SIP Entities** on the left and click on the **New** button on the right (not shown).

Under **General**:

- **Name:** A descriptive name
- **FQDN or IP Address:** IP address of the Session Manager signaling interface i.e. **10.64.30.32**
- **Type:** Select **Session Manager**
- **Location:** Select the location defined in **Section 6.2**
- **Time Zone:** Time zone for this entity

Create three Port definitions for **TLS**, **TCP**, and **UDP**. Under **Port**, click **Add**, and edit the fields in the resulting new row as shown below:

- **Port:** Port number on which the system listens for SIP requests
- **Protocol:** Transport protocol to be used to send SIP requests
- **Default Domain** The domain used (e.g., **avaya.com**)

Defaults can be used for the remaining fields. Click **Commit** to save the SIP Entity definition.

Avaya Aura® System Manager 6.3

Last Logged on at December 2, 2013 1:33 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Routing | **Home**

Routing | **Elements** | **Routing** | **SIP Entities**

SIP Entity Details Commit Cancel Help ?

General

* Name:

* FQDN or IP Address:

Type:

Notes:

Location:

Outbound Proxy:

Time Zone:

Credential name:

SIP Link Monitoring

SIP Link Monitoring:

Entity Links

Add Remove

0 Items Refresh Filter: Enable

	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
<input type="checkbox"/>							

Port

TCP Failover port:

TLS Failover port:

Add Remove

3 Items Refresh Filter: Enable

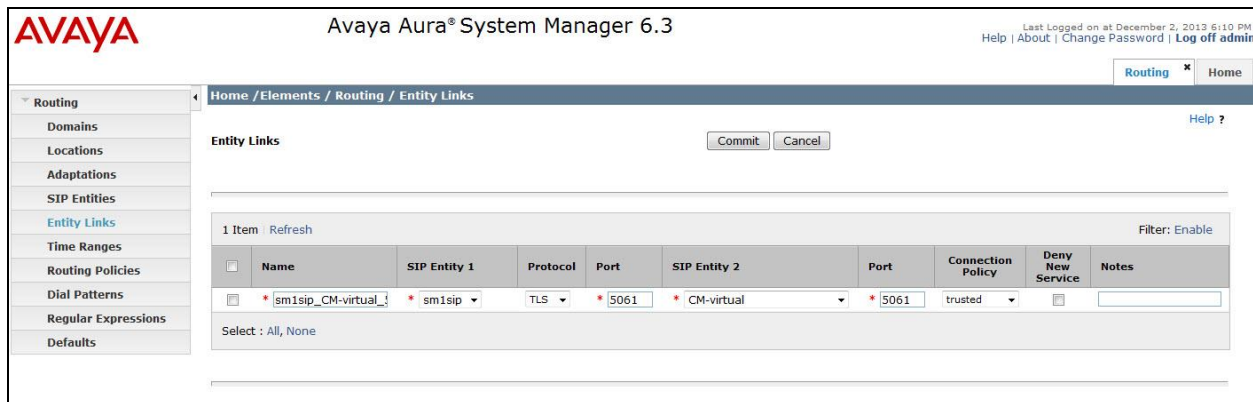
	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	<input type="text" value="5060"/>	<input type="text" value="UDP"/>	<input type="text" value="avaya.com"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="5060"/>	<input type="text" value="TCP"/>	<input type="text" value="avaya.com"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="5061"/>	<input type="text" value="TLS"/>	<input type="text" value="avaya.com"/>	<input type="text"/>

6.4. Add Entity Links

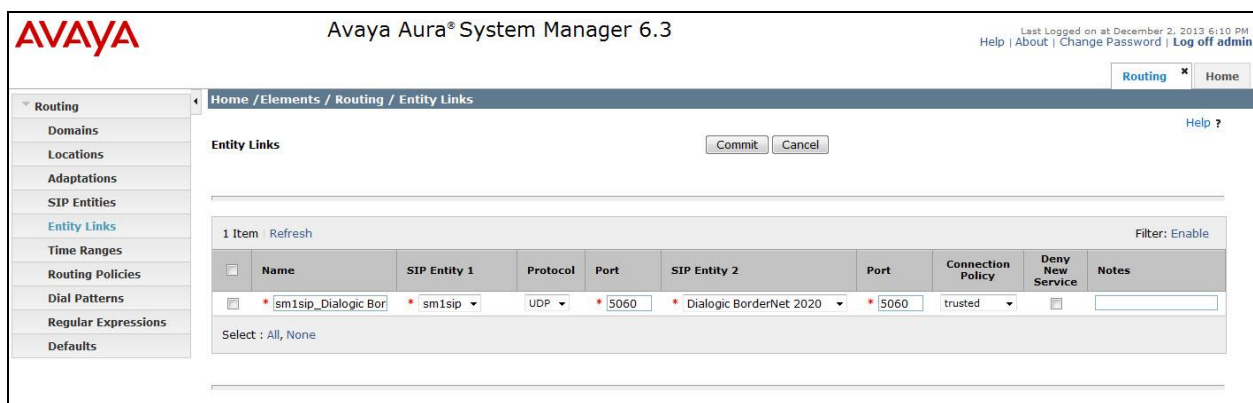
A SIP trunk between Session Manager and a telephony system is described by an Entity link. To add an Entity Link, select **Entity Links** on the left and click on the **New** button on the right (not shown). Fill in the following fields in the new row that is displayed:

- **Name:** A descriptive name
- **SIP Entity 1:** Select the **SessionManager** SIP Entity from **Section 6.3.3**
- **Protocol:** Select the transport protocol to align with the far end. In these Application Notes **TLS** was used for Communication Manager and **UDP** for BorderNet 2020.
- **Port:** Port number to which the far end system sends SIP requests
- **SIP Entity 2:** Select the name of the far end system
- **Port:** Port number on which the far end system receives SIP requests

Click **Commit** to save each Entity Link definition. The following screen illustrates adding the Entity Link for Communication Manager.



The screen below illustrates the Entity Link for BorderNet 2020.



6.5. Add Routing Policies

Routing policies describe the condition under which calls will be routed to the SIP Entities specified in **Section 6.3**. Two routing policies were added: one for Communication Manager and another for BorderNet 2020. To add a routing policy, select **Routing Policies** on the left and click on the **New** button on the right (not shown). The following screen is displayed. Fill in the following fields:

Under **General**:

- Enter a descriptive name in **Name**

Under **SIP Entity as Destination**:

- Click **Select**, and then select the appropriate SIP entity to which this routing policy applies

Under **Time of Day**:

- Click **Add**, and select the time range configured. In these Application Notes, the predefined **24/7** Time Range is used

Defaults can be used for the remaining fields. Click **Commit** to save each Routing Policy definition. The following picture shows the Routing Policy for Communication Manager.

[Routing](#) [Home](#)

- Routing
- Domains
- Locations
- Adaptations
- SIP Entities
- Entity Links
- Time Ranges
- Routing Policies
- Dial Patterns
- Regular Expressions
- Defaults

[Home](#) / [Elements](#) / [Routing](#) / [Routing Policies](#)[Help ?](#)

Routing Policy Details

[Commit](#) [Cancel](#)

General

* Name: Disabled: ☐* Retries: Notes:

SIP Entity as Destination

[Select](#)

Name	FQDN or IP Address	Type	Notes
CM-virtual	10.64.30.10	CM	

Time of Day

[Add](#)[Remove](#)[View Gaps/Overlaps](#)

1 Item [Refresh](#)

Filter: [Enable](#)

<input type="checkbox"/>	Ranking ▲	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	<input type="text" value="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](#)

The following screen shows the Routing Policy for BorderNet 2020.

AVAYA

Avaya Aura® System Manager 6.3

Last Logged on at December 2, 2013 8:12 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home / Elements / Routing / Routing Policies

Routing Policy Details

CommitCancel

Help ?

General

* Name:

to Dialogic

Disabled:

☐

* Retries:

0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Dialogic BorderNet 2020	10.64.31.212	SIP Trunk	

Time of Day

AddRemoveView Gaps/Overlaps

1 Item RefreshFilter: Enable

<input type="checkbox"/>	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	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

6.6. Add Dial Patterns

Dial patterns must be defined that will direct calls to the appropriate SIP Entity. To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button on the right (not shown). Fill in the following fields as specified for the dial pattern that routes calls to Communication Manager:

Under **General**:

- **Pattern:** Dialed number or prefix, **21**
- **Min:** Minimum length of dialed number, **5**
- **Max:** Maximum length of dialed number, **5**
- **SIP Domain:** Select domain from **Section 6.1**.

Under **Originating Locations and Routing Policies**, click **Add**, and then select the appropriate location and routing policy from the list. Default values can be used for the remaining fields. Click **Commit** to save the dial pattern. The following screen shows the configured dial pattern.

AVAYA Avaya Aura® System Manager 6.3 Last Logged on at December 2, 2013 8:12 PM
Help | About | Change Password | Log off admin

Routing x Home

Home / Elements / Routing / Dial Patterns Help ?

Dial Pattern Details Commit Cancel

General

* Pattern: 21

* Min: 5

* Max: 5

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: avaya.com

Notes: to CM_30_10

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	~ALL-		to_CM_Virtual		<input type="checkbox"/>	CM-virtual	

Select : All, None

Denied Originating Locations

Add Remove

0 Items Refresh Filter: Enable

<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------

Commit Cancel

Repeat the process to add one or more dial patterns for routing calls to PSTN numbers via BorderNet 2020. Fill in the following fields as specified that routes calls to BorderNet 2020:

Under **General**:

- **Pattern:** Dialed number or prefix, **1**
- **Min:** Minimum length of dialed number, **11**
- **Max:** Maximum length of dialed number, **11**
- **SIP Domain:** Select **-ALL-**

Under **Originating Locations and Routing Policies**, click **Add**, and then select the appropriate location and routing policy from the list. Default values can be used for the remaining fields. Click **Commit** to save the dial pattern. The following screen shows the configured dial pattern.

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The top navigation bar includes the Avaya logo, the title "Avaya Aura® System Manager 6.3", and a user status bar indicating "Last Logged on at December 2, 2013 8:12 PM" with links for "Help", "About", "Change Password", and "Log off admin". The main interface is divided into a left sidebar with a tree view containing "Routing", "Domains", "Locations", "Adaptations", "SIP Entities", "Entity Links", "Time Ranges", "Routing Policies", "Dial Patterns" (highlighted), "Regular Expressions", and "Defaults". The main content area has a breadcrumb trail "Home / Elements / Routing / Dial Patterns" and a "Help ?" link. The "Dial Pattern Details" section includes "Commit" and "Cancel" buttons. The "General" tab is active, showing fields for "Pattern" (value: 1), "Min" (value: 11), "Max" (value: 11), "Emergency Call" (checkbox), "Emergency Priority" (value: 1), "Emergency Type" (text field), "SIP Domain" (dropdown menu with "-ALL-" selected), and "Notes" (text area). Below this is the "Originating Locations and Routing Policies" section, which includes "Add" and "Remove" buttons, a "1 Item" count, and a "Refresh" button. A table lists the configured policy:

	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		to Dialogic		<input type="checkbox"/>	Dialogic BorderNet 2020	

Below the table is a "Select : All, None" option. The "Denied Originating Locations" section at the bottom shows "0 Items" and a "Refresh" button, with a table header for "Originating Location" and "Notes". "Commit" and "Cancel" buttons are at the bottom right of the interface.

During the compliance test, additional dial patterns were also created for other destinations (e.g. **011** for international calls).

7. Configure Dialogic® BorderNet™ 2020 Integrated Media Gateway

For the compliance test, two trunking interfaces were configured on BorderNet 2020. A SIP trunk interface was used to connect to Session Manager and an ISDN PRI interface was used to connect to PSTN. This section focuses on the configuration at the SIP side which enabled BorderNet 2020 to interoperate with Session Manager.

It is assumed that basic administration such as IP addresses, Default Gateways, and VLAN IDs for the SIP signaling and media interfaces, Serial number, Security ID, and Packet Facility have been configured during installation.

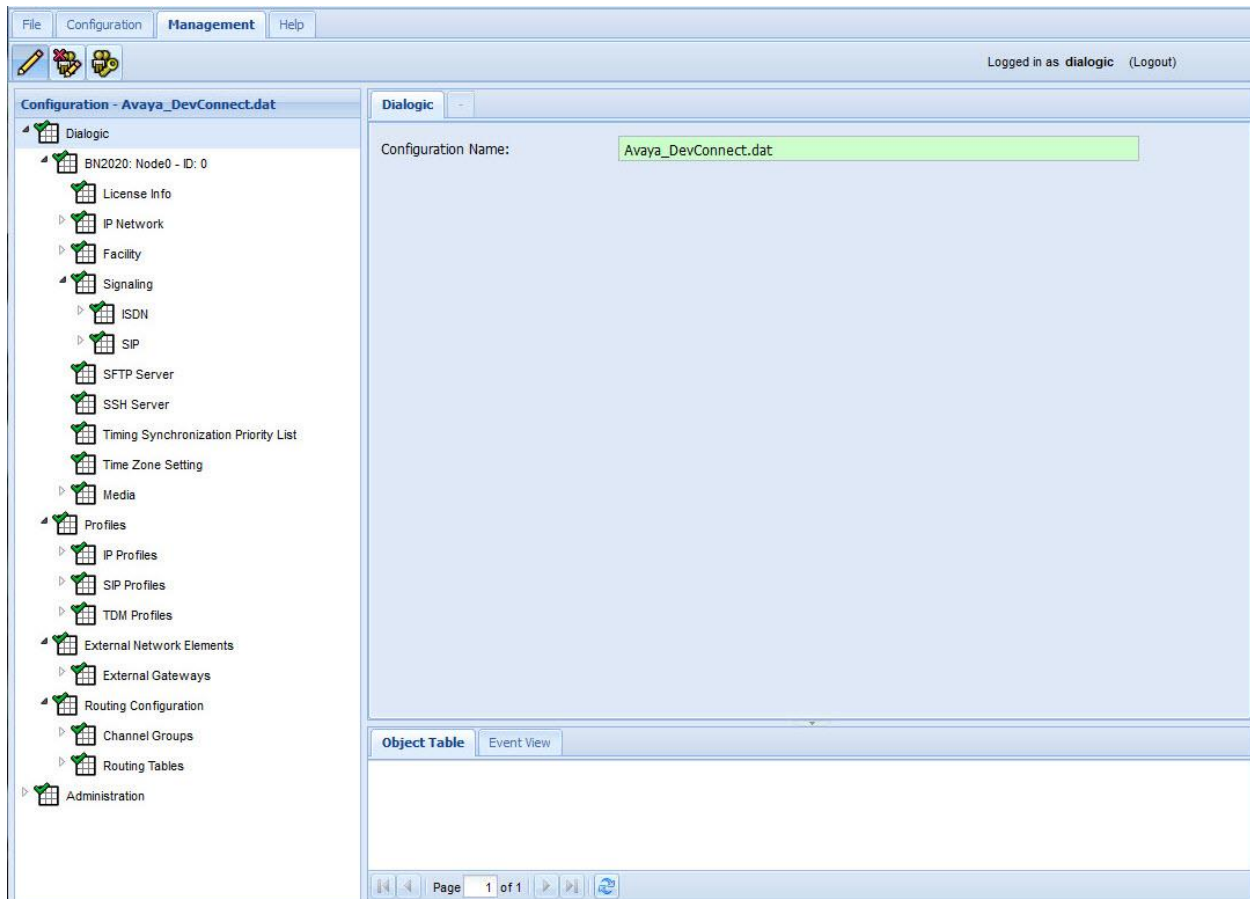
It is also assumed that the PSTN trunk has been properly configured, which includes the ISDN PRI interface, TDM Profile, associated Channel Group, and the underlining T1 interface.

This section provides the procedures for configuring BorderNet 2020, assuming it has been installed and licensed. The procedures include the following items:

- Launch Management Interface
- Configure BN2020 Node
- Configure Profiles
- Configure External Network Element
- Configure Routing Configuration

7.1. Launch Management Interface

BorderNet 2020 is administered using a built-in web based management user interface. To access the interface, enter <http://<ip-addr>> as the URL in a Firefox web browser where <ip-addr> is the IP address of the Dialogic management port. Currently Firefox and Internet Explorer are the only officially supported web browsers for BorderNet 2020. Enter the appropriate credentials to log in. The following screen is displayed.



7.2. Configure BN2020 Node

From the configuration tree in the left pane, navigate to **Dialogic** → **BN2020 Node0** → **Signaling**. If a SIP object is already present, skip the rest of this section and continue on **Section 7.3**. Otherwise, right click **Signaling** and select **New SIP**. The **SIP** screen is displayed. For **IP Operation Mode**, select **Multiple IP** from the dropdown menu. Keep the default values for the remaining fields. The following shows the completed **SIP** screen.

Note: For the compliance test there is only one IP address defined on this **SIP** screen. But it is a recommended practice to set the **IP Operation Mode** field to **Multiple IP** to allow another SIP address to be added in the future without having to perform a major reconfiguration.

The screenshot shows the Avaya DevConnect Manager interface. The left pane displays the configuration tree with 'Dialogic' expanded, showing 'BN2020: Node0 - ID: 0' and its sub-items: 'License Info', 'IP Network', 'Facility', 'Signaling', 'ISDN', 'SIP', 'SFTP Server', 'SSH Server', and 'Timing Synchronization Priority List'. The 'SIP' item is selected. The right pane shows the 'SIP' configuration form with the following fields and values:

Field	Value
Compact Header:	Disable
Message Restriction Setting:	Default
UserName (AOR):	DIALOGIC-BDN0
Authentication User Name:	
Authentication Password:	
SIP-T Enabled:	No
SIP-T Behavior:	Not Used
IP Operation Mode:	Multiple IP
Retry-After (# of Seconds):	5

Right click **Dialogic** → **BN2020 Node0** → **Signaling** → **SIP** and select **New SIP IP Address**. The **SIP IP Address** screen is displayed. For **IP Address**, select the signaling IP address from the dropdown menu. Set **Transport Type** to **UDP** and **Port** to **5060**. Please note that the transport type and port should match the configured SIP Entity Link in **Section 6.4**. Keep the default values for the remaining fields. The following shows the completed **SIP IP Address** screen.

The screenshot shows the Avaya DevConnect Manager interface. The left pane displays the configuration tree with 'Dialogic' expanded, showing 'BN2020: Node0 - ID: 0' and its sub-items: 'License Info', 'IP Network', 'Facility', 'Signaling', 'ISDN', 'SIP', 'SFTP Server', 'SSH Server', and 'Timing Synchronization Priority List'. The 'SIP' item is selected, and 'SIP IP Address: 10.64.31.212' is highlighted. The right pane shows the 'SIP IP Address: 10.64.31.212' configuration form with the following fields and values:

Field	Value
IP Type:	IPv4
IP Address:	10.64.31.212
Transport Type:	UDP
Port:	5060
TLS Port:	5061
DNS Client:	Not Used
DNS Query Mode:	MIX
Secure Profile:	Not Used
Default Secure Profile:	Not Used
Fully Qualified Domain Name:	

7.3. Configure Profiles

7.3.1. Configure IP Profiles

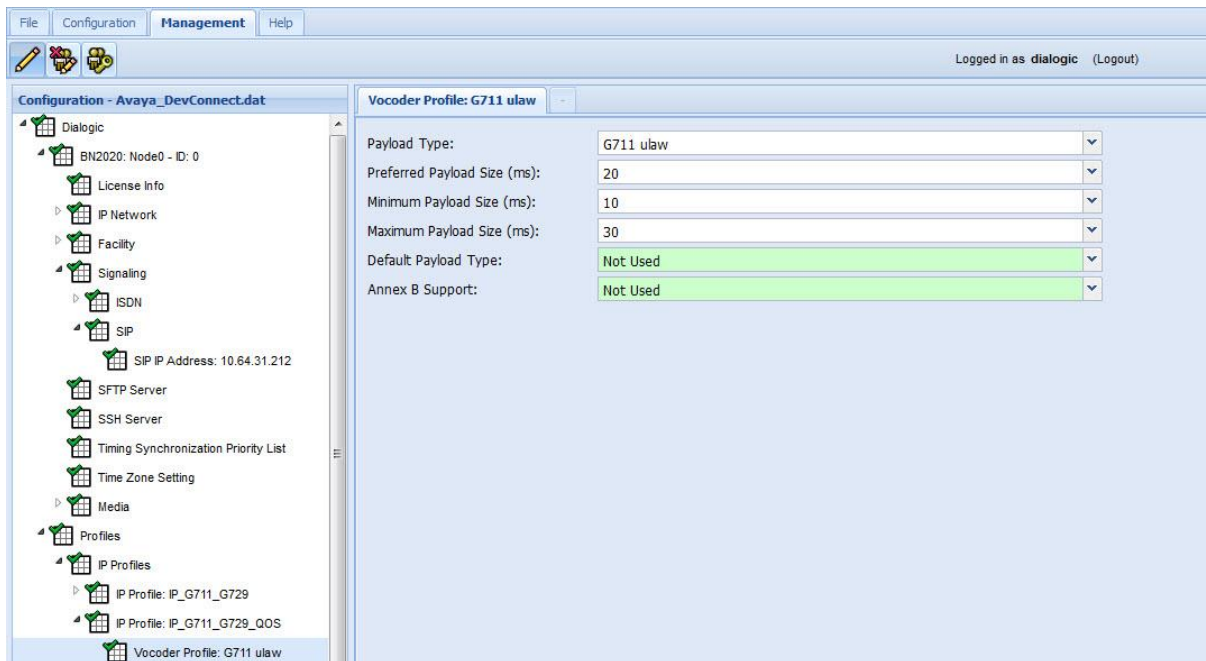
From the configuration tree in the left pane, right click **Dialogic** → **Profiles** → **IP Profiles** and select **New IP Profile**. The **IP Profile** screen is displayed. Enter a descriptive name in the **Name** field. For **Digit Relay**, select **DTMF Packetized** to use the RFC 2833 method (or select **DTMF In-band** for in-band DTMF, see note in **Section 2.2**). For **Fax Mode**, select **Enable Relay (T.38)**. For **Digit Relay Packet Type**, select a proper value. Keep the default values for the remaining fields. The following shows the completed **IP Profile** screen.

The screenshot shows the Avaya DevConnect Manager interface. The left pane displays the configuration tree with 'Dialogic' expanded, showing 'IP Profiles' and 'IP Profile: IP_G711_G729_QOS' selected. The right pane shows the configuration for 'IP Profile: IP_G711_G729_QOS'. The configuration fields are as follows:

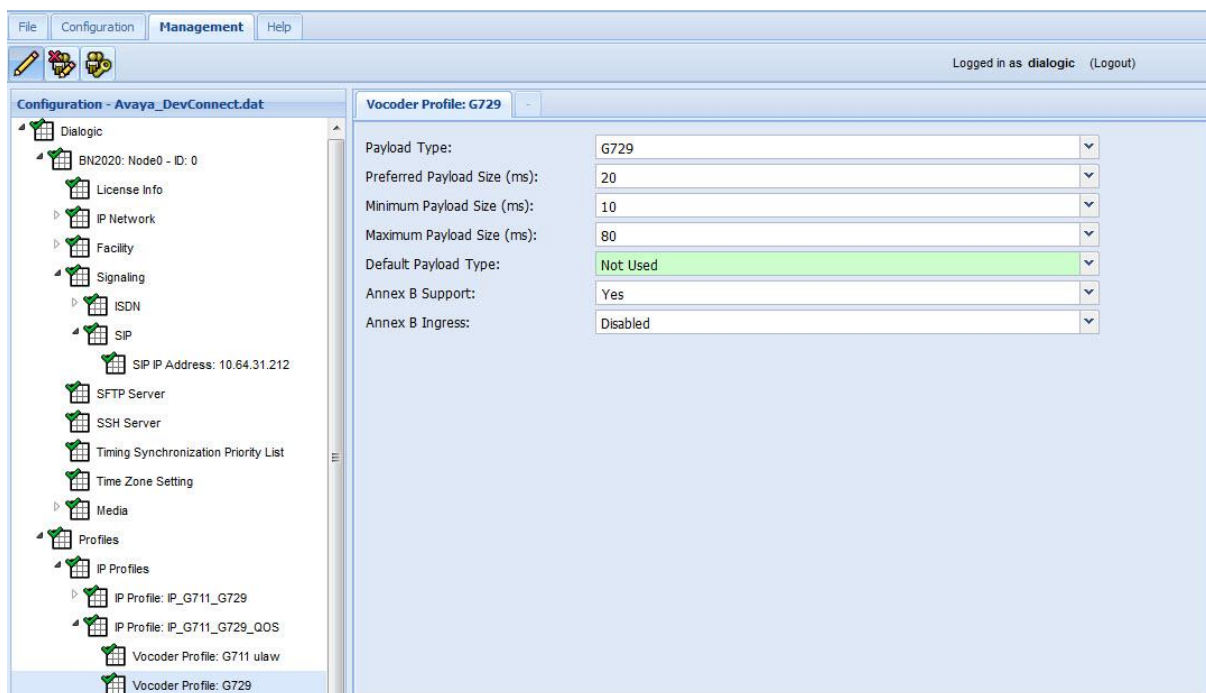
Field	Value
Name	IP_G711_G729_QOS
Silence Suppression	Disable
Echo Cancellation	Enabled (NLP Enabled)
RTP Redundancy	No Redundancy
RTP Payload Type for Redundancy	Not Used
Digit Relay	DTMF Packetized
Fax Mode	Enable Relay (T.38)
Fax Bypass Codec	G711 ulaw
Fax Packet Redundancy	No Redundancy
Initial Media Inactivity Timer	Disable
Initial Media Inactivity Timer Value	Seconds: 181
Media Inactivity Timer	Disable
Media Inactivity Timer Value	Seconds: 30
Digit Relay Packet Type	127
Modem Behavior	Bypass
Source Port Validate	Enable
High Jitter	Disable

7.3.1.1 Configure IP Codecs in IP Profile

From the configuration tree in the left pane, right click the newly created IP Profile and select **New Vocoder Profile**. The **Vocoder Profile** screen is displayed. For **Payload Type**, select **G711 ulaw**. Keep the default values for the remaining fields. The following shows the completed **Vocoder Profile** screen.

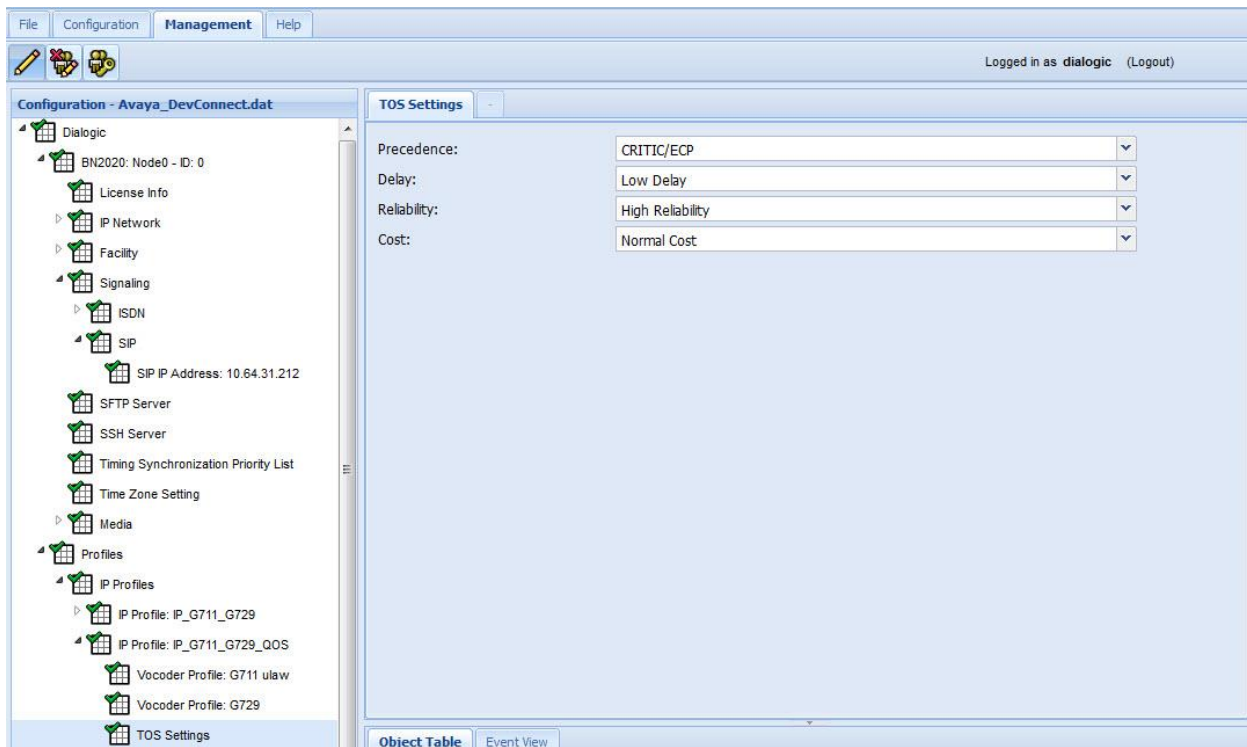


Repeat the procedure for the **G.729** codec and set **Annex B Support** to **Yes**.



7.3.1.2 Configure TOS Settings in IP Profile

From the configuration tree in the left pane, right click the newly created IP Profile and select **New TOS Settings**. The **TOS Settings** screen is displayed. For the **Precedence**, **Delay**, **Reliability**, and **Cost** fields, select **CRITIC/ECP**, **Low Delay**, **High Reliability**, and **Normal Cost** respectively. The following shows the completed **TOS Settings** screen.



7.3.2. Configure SIP Profiles

From the configuration tree in the left pane, right click **Dialogic** → **Profiles** → **SIP Profiles** and select **New SIP Profile**. The **SIP Profile** screen is displayed. Enter a descriptive name in the **Name** field. For **Codec Priority**, select **Remote**. This gives the codecs in the far end higher priority during codec negotiation. Keep the default values for the remaining fields. The following shows the completed **SIP Profile** screen.

The screenshot displays the Avaya DevConnect Manager configuration interface. The left pane shows the configuration tree with the following structure:

- Dialogic
 - BN2020: Node0 - ID: 0
 - License Info
 - IP Network
 - Facility
 - Signaling
 - ISDN
 - SIP
 - SIP IP Address: 10.64.31.212
 - SFTP Server
 - SSH Server
 - Timing Synchronization Priority List
 - Time Zone Setting
 - Media
 - Profiles
 - IP Profiles
 - IP Profile: IP_G711_G729
 - IP Profile: IP_G711_G729_QOS
 - Vocoder Profile: G711 ulaw
 - Vocoder Profile: G729
 - TOS Settings
 - SIP Profiles
 - SIP Profile: SIP Default
 - SIP Profile: SIP_Remote_Codec

The right pane shows the configuration for the selected SIP Profile: **SIP_Remote_Codec**. The configuration fields are as follows:

Field	Value
Name	SIP_Remote_Codec
PRACK Support	Disabled
PRACK Timer (s)	150
Precondition Support	Disabled
Codec Priority	Remote
3XX Redirect Support	Enabled
Loop Detection	Enabled
Loop Detection Method	To Header
INVITE Retransmission Attempts	Retransmit All
Trusted	Enabled
Privacy	Disabled
PAID RPID Display Name	When none received send user part of URI
INFO Keep-Alive Support	Disabled
Outbound Delayed Media	Disabled
SRTP Mode	Disabled
180 Ringing Behavior	Send 183 Progress w/SDP

At the bottom of the right pane, there are two tabs: **Object Table** and **Event View**.

7.4. Configure External Network Element

From the configuration tree in the left pane, right click **Dialogic** → **External Network Elements** → **External Gateways** and select **New External Gateway**. The **ExternalGateway** screen is displayed (not shown). Enter a descriptive name in the **Name** field such as **Avaya_Session_Manager**. For **Protocol**, select **SIP**. For **IP Address**, enter the IP address of the Session Manager signaling interface. For **Profile**, select the SIP Profile configured in **Section 7.3.2**. For **OPTIONS Keep Alive**, select **Enable** to enable sending SIP Options messages. Keep the default values for the remaining fields. The following shows the completed **ExternalGateway** screen for **Avaya_Session_Manager**.

The screenshot displays the Avaya Session Manager configuration interface. The left pane shows the configuration tree with the following structure:

- Configuration - Avaya_DevConnect.dat
 - Signaling
 - ISDN
 - SIP
 - SIP IP Address: 10.64.31.212
 - SFTP Server
 - SSH Server
 - Timing Synchronization Priority List
 - Time Zone Setting
 - Media
 - Profiles
 - IP Profiles
 - IP Profile: IP_G711_G729
 - IP Profile: IP_G711_G729_QOS
 - Vocoder Profile: G711 ulaw
 - Vocoder Profile: G729
 - TOS Settings
 - SIP Profiles
 - SIP Profile: SIP Default
 - SIP Profile: SIP_Remote_Codec
 - TDM Profiles
 - External Network Elements
 - External Gateways
 - Avaya_Session_Manager

The right pane shows the configuration for **Avaya_Session_Manager**:

Name:	Avaya_Session_Manager
Protocol:	SIP
Address Type:	IP Address
IP Type:	IPv4
IP Address:	10.64.30.32
Allowed Gateway Subnet Prefix:	32
HostName:	
Transport Type:	UDP
Transport Port:	Port: 5060 Increment: 1
Registration Required:	No
Registration Interval:	Seconds: 3600 Increment: 1
Profile:	ID: 1 - SIP_Remote_Codec
Secure Profile:	Not Used
OPTIONS Keep Alive:	Enable

At the bottom, there are tabs for **Object Table** and **Event View**.

7.5. Configure Routing Configuration

7.5.1. Configure Channel Group

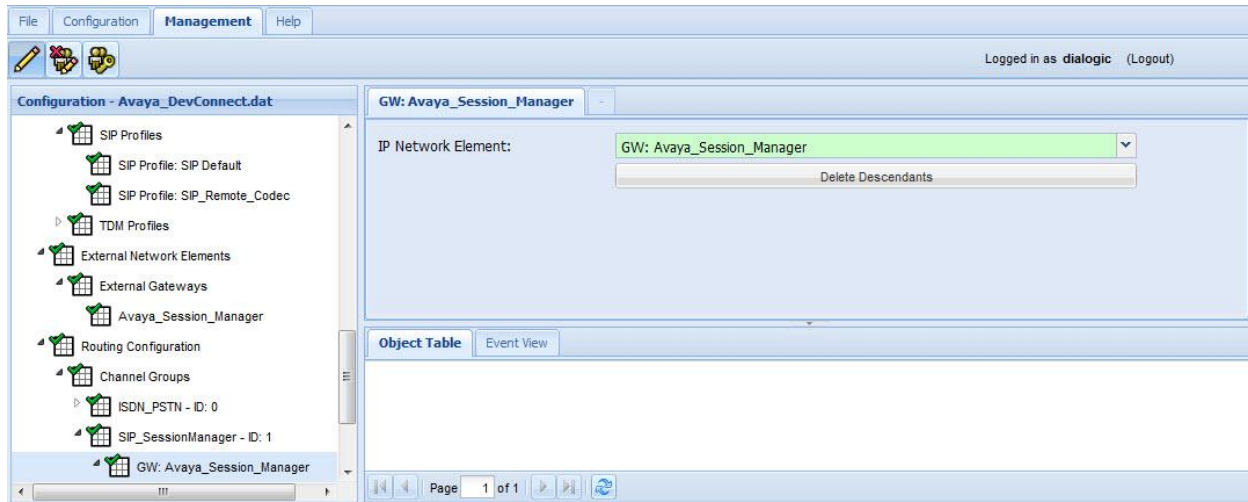
From the configuration tree in the left pane, right click **Dialogic** → **Routing Configuration** → **Channel Groups** and select **New Channel Group**. The **ChannelGroup** screen is displayed (not shown). Enter a descriptive name in the **Name** field such as **SIP_SessionManager**. For **Signaling Type**, select **SIP**. For **Incoming IP Profile** and **Outgoing IP Profile**, select the IP Profile configured in **Section 7.3.1**. Keep the default values for the remaining fields. The following shows the completed **ChannelGroup** screen for **SIP_SessionManager**.

The screenshot displays the Avaya DevConnect configuration interface. The left pane shows the configuration tree with 'Dialogic' expanded, and 'SIP_SessionManager - ID: 1' selected under 'Channel Groups'. The right pane shows the configuration for 'SIP_SessionManager - ID: 1'.

Field	Value
ID:	1
Name:	SIP_SessionManager
Trunk Direction:	Incoming/Outgoing
Signaling Type:	SIP
Route Table:	None
Cause Code Table:	None
Incoming IP Profile:	IP_G711_G729_QOS
Outgoing IP Profile:	IP_G711_G729_QOS
Incoming Treatment:	Release w/Cause
Outgoing Treatment:	Release w/Cause
Incoming Translation Table:	None
Outgoing Translation Table:	None
Hunting Options:	Round Robin Clockwise
Ingress Side will Play Call Progress Tones:	False
Re-Attempt Cause Code:	Not Used 000 - Reserved 001 - Unallocated 002 - No Route to Specified Transit Network 003 - No Route to Destination
Support Digit A to F:	False
Channel Transfer:	Not Used
Overlap Enable:	Disabled
Termination Digit:	Not Used
Minimum # of Digits:	Not Used
Inter SAM Timeout (Seconds):	4
Total Overlap Timeout (Seconds):	6
Multi-Level Precedence and Preemption (MLPP) Support:	Not Used
CPN/CPC retrieval via INR/INF:	Disabled

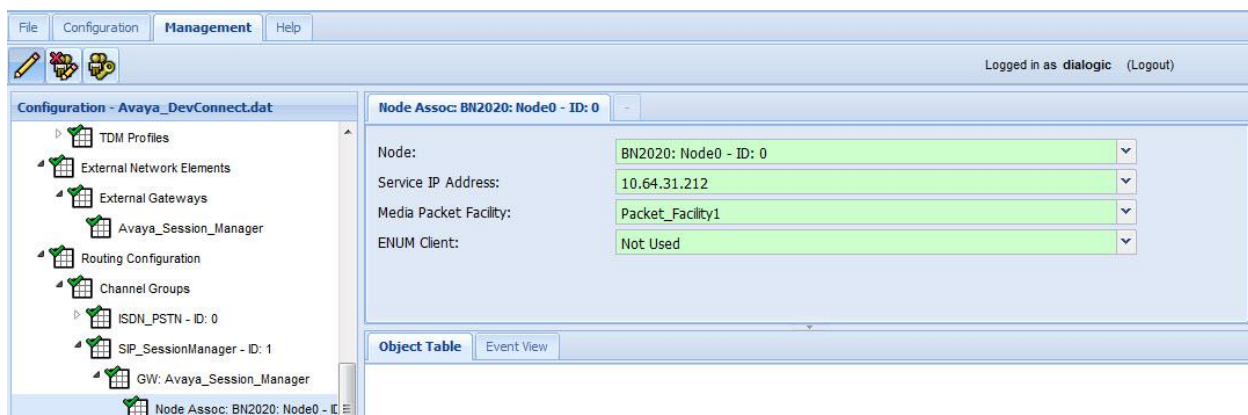
At the bottom of the right pane, there are two tabs: 'Object Table' and 'Event View'.

Right click the newly configured Channel Group in the left pane and select **New IP Network Element**. The **NetworkElement** screen is displayed (not shown). For **IP Network Element**, select the External Gateway configured in **Section 7.4**. The following shows the completed **NetworkElement** screen.



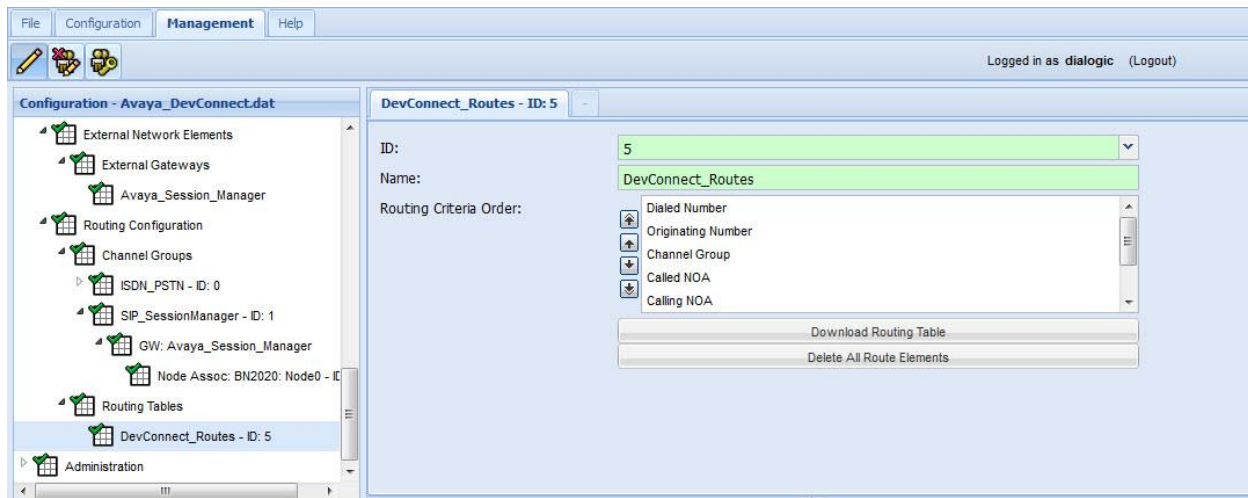
Right click the newly configured IP Network Element in the left pane and select **New Node Association**. The **Node Assoc** screen is displayed. For **Node**, **Service IP Address**, and **Media Packet Facility**, select proper values. Keep the default values for the remaining fields. The following shows the completed **Node Assoc** screen.

Please note that packet facility was pre-configured and is not shown in this document.

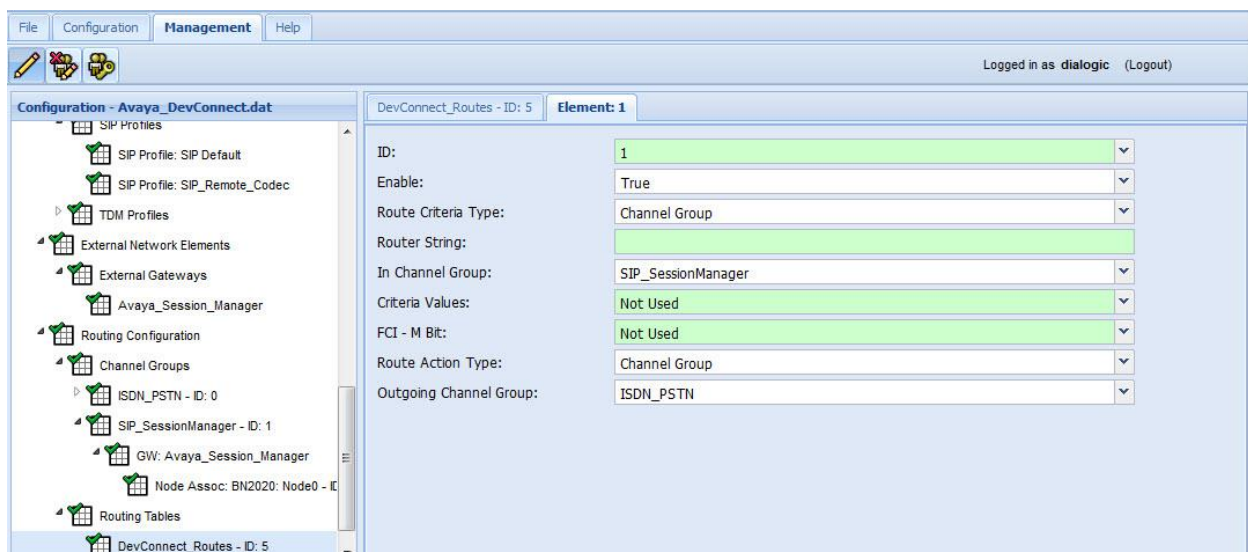


7.5.2. Configure Routing Tables

From the configuration tree in the left pane, right click **Dialogic** → **Routing Configuration** → **Routing Tables** and select **New Routing Table**. The **Table** screen is displayed (not shown). Enter a descriptive name in the **Name** field. Keep the default values for the remaining fields. The following shows the completed **Table** screen.



Right click the newly configured Routing Table in the left pane and select **New Route Element**. The **Element** tab is displayed. For **Route Criteria Type**, select **Channel Group**. For **In Channel Group**, select the channel group configured in **Section 7.5.1**. For **Outgoing Channel Group**, select the channel group pre-configured for the ISDN PRI interface. Keep the default values for the remaining fields. The following shows the completed **Element** tab.



Repeat the above procedure for a second Route Element which routes calls from the ISDN PRI channel group to the Session Manager channel group.

The screenshot displays the Avaya DevConnect configuration tool. The left pane shows a tree view of the configuration hierarchy under 'Configuration - Avaya_DevConnect.dat'. The right pane shows the configuration for 'DevConnect_Routes - ID: 5', specifically 'Element: 2'. The configuration fields are as follows:

Field	Value
ID:	2
Enable:	True
Route Criteria Type:	Channel Group
Router String:	
In Channel Group:	ISDN_PSTN
Criteria Values:	Not Used
FCI - M Bit:	Not Used
Route Action Type:	Channel Group
Outgoing Channel Group:	SIP_SessionManager

Bring up the Channel Group configured in **Section 7.5.1** by right clicking **Dialogic** → **Routing Configuration** → **Channel Groups** → **SIP_SessionManager**. For **Route Table**, select the Route Table configured above. The following shows the updated **ChannelGroup** screen for **SIP_SessionManager**.

The screenshot displays the Avaya DevConnect configuration interface. The left pane shows a tree view under 'Configuration - Avaya_DevConnect.dat' with 'Dialogic' expanded, leading to 'Routing Configuration' and then 'Channel Groups', where 'SIP_SessionManager - ID: 1' is selected. The right pane shows the configuration for 'SIP_SessionManager - ID: 1'.

ID:	1
Name:	SIP_SessionManager
Trunk Direction:	Incoming/Outgoing
Signaling Type:	SIP
Route Table:	DevConnect_Routes - ID: 5
Cause Code Table:	None
Incoming IP Profile:	IP_G711_G729_QOS
Outgoing IP Profile:	IP_G711_G729_QOS
Incoming Treatment:	Release w/Cause
Outgoing Treatment:	Release w/Cause
Incoming Translation Table:	None
Outgoing Translation Table:	None
Hunting Options:	Round Robin Clockwise
Ingress Side will Play Call Progress Tones:	False
Re-Attempt Cause Code:	Not Used 000 - Reserved 001 - Unallocated 002 - No Route to Specified Transit Network 003 - No Route to Destination
Support Digit A to F:	False
Channel Transfer:	Not Used
Overlap Enable:	Disabled
Termination Digit:	Not Used
Minimum # of Digits:	Not Used
Inter SAM Timeout (Seconds):	4
Total Overlap Timeout (Seconds):	6
Multi-Level Precedence and Preemption (MLPP) Support:	Not Used
CPN/CPC retrieval via INR/INF:	Disabled

At the bottom, there are tabs for 'Object Table' and 'Event View'.

Repeat the above procedure for the Channel Group pre-configured for the ISDN PRI interface.

8. Verification Steps

This section provides the verification steps that may be performed to verify that Avaya Aura[®] enterprise network can establish and receive calls with BorderNet 2020.

8.1. Verify Signaling Group Status on Avaya Aura[®] Communication Manager

Enter the command **status signalling-group n**, where **n** is the signalling group configured in **Section 5.5.1**, to ensure that the **Group State** is **in-service**.

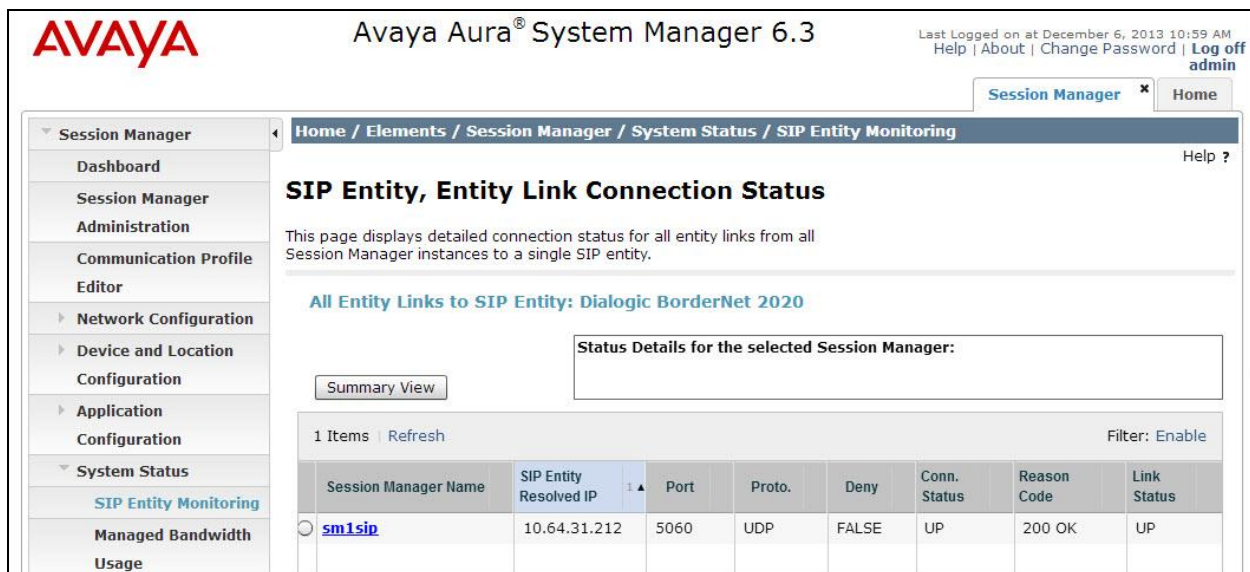
```
status signaling-group 91
                        STATUS SIGNALING GROUP

      Group ID: 91
      Group Type: sip

      Group State: in-service
```

8.2. Verify Entity Link Status on Avaya Aura[®] Session Manager

To verify connectivity to BorderNet 2020, click **Session Manager** on the Home page of System Manager web interface. Navigate to **Session Manager → System Status → SIP Entity Monitoring**. Locate and click the SIP Entity for BorderNet 2020 under **All Monitored SIP Entities** (not shown). Both the **Conn. Status** and **Link Status** fields should display **UP**.



The screenshot shows the Avaya Aura System Manager 6.3 web interface. The top navigation bar includes the Avaya logo, the title "Avaya Aura[®] System Manager 6.3", and user information: "Last Logged on at December 6, 2013 10:59 AM", "Help | About | Change Password | Log off admin". The left sidebar contains a menu with categories: Session Manager, System Status, and SIP Entity Monitoring. The main content area shows the "SIP Entity, Entity Link Connection Status" page. It includes a breadcrumb trail: "Home / Elements / Session Manager / System Status / SIP Entity Monitoring". Below the breadcrumb, there is a description: "This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity." A section titled "All Entity Links to SIP Entity: Dialogic BorderNet 2020" contains a "Summary View" button and a table. The table has a "Filter: Enable" option and shows 1 item. The table columns are: Session Manager Name, SIP Entity Resolved IP, Port, Proto., Deny, Conn. Status, Reason Code, and Link Status. The data row shows: sm1sip, 10.64.31.212, 5060, UDP, FALSE, UP, 200 OK, and UP.

Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
sm1sip	10.64.31.212	5060	UDP	FALSE	UP	200 OK	UP

9. Conclusion

These Application Notes describe the configuration steps required for Dialogic® BorderNet™ 2020 Integrated Media Gateway to successfully interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager. All feature and serviceability test cases were completed with an observation noted in **Section 0**.

10. Additional References

Avaya references are available at <http://support.avaya.com>

- [1] “Administering Avaya Aura® Session Manager”, Release 6.3, Issue 4, June 2014
- [2] “Administering Avaya Aura® Communication Manager”, Document Number 03-300509, Issue 9.0, Release 6.3, October 2013

Dialogic® BorderNet™ 2020 Integrated Media Gateway references are available on <http://www.dialogic.com/en/products/session-border-controllers/bordernet-2020.aspx>.

©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.