



Avaya Solution & Interoperability Test Lab

Application Notes for IPC UnigyV2 with Avaya Aura® Session Manager 6.3 using SIP Trunks – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for IPC UnigyV2 to interoperate with Avaya Aura® Session Manager 6.3 using SIP trunks.

IPC UnigyV2 is a trading communication solution. In the compliance testing, IPC UnigyV2 used SIP trunks to Avaya Aura® Session Manager, for turrel users on IPC to reach users on Avaya Aura® Communication Manager and on the PSTN.

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 IPC UnigyV2 to interoperate with Avaya Aura® Communication Manager via Avaya Aura® Session Manager.

The Unigy Platform is a unified trading communications system designed specifically to make the entire trading ecosystem more productive, intelligent and efficient. Based on an SIP-enabled, open and distributed architecture, Unigy utilizes the latest, standards-based technology to create a groundbreaking, innovative Unified Trading Communications (UTC) solution.

Unigy offers a portfolio of devices and applications that serve the entire trading workflow, across the front, middle and back offices.

2. General Test Approach and Test Results

The feature test cases were performed manually. Calls were manually established among IPC turrent users with Avaya SIP, Avaya H.323, and/or PSTN users. Call controls were performed from various users to verify the call scenarios.

The serviceability test cases were performed manually by disconnecting and reconnecting the Ethernet cable to IPC UnigyV2.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing included basic call, display, G.711MU, hold/reconnect, DTMF, call forwarding unconditional/ring-no-answer/busy, blind/attended transfer, and attended conference.

The serviceability testing focused on verifying the ability of IPC UnigyV2 to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to IPC UnigyV2.

2.2. Test Results

All test cases were executed and verified. The following were the observations on IPC UnigyV2 from the compliance testing:

- Even when IPC UnigyV2 is configured with UDP, the TCP protocol must be configured to be allowed on Avaya Session Manager as UnigyV2 switches over to use TCP for diversions.
- During the compliance test, shuffling was disabled, as shown in **Section 5.4**.
- During the compliance test, Network Call Redirection (shuffling) was disabled, as shown in **Section 5.3**. (IPC requested)

2.3. Support

Technical support on IPC UnigyV2 can be obtained through the following:

- **Phone:** (800) NEEDIPC, (203) 339-7800
- **Email:** systems.support@ipc.com

3. Reference Configuration

As shown in the test configuration below, IPC UnigyV2 at the Remote Site consists of the Media Manager, Converged Communication Manager, and Turrets. The Media Manager and Converged Communication Manager are typically deployed on separate servers. In the compliance testing, the same server hosted the Media Manager and Converged Communication Manager.

SIP trunks are used from IPC UnigyV2 to Avaya Aura® Session Manager, to reach users on Avaya Aura® Communication Manager and on the PSTN.

A five digit Uniform Dial Plan (UDP) was used to facilitate dialing between the Central and Remote sites. Unique extension ranges were associated with Avaya Aura® Communication Manager users at the Central site (7200x and 7202x), and IPC turret users at the Remote site (7205x).

The detailed administration of basic connectivity between Avaya Aura® Communication Manager and Avaya Aura® Session Manager is not the focus of these Application Notes and will not be described.

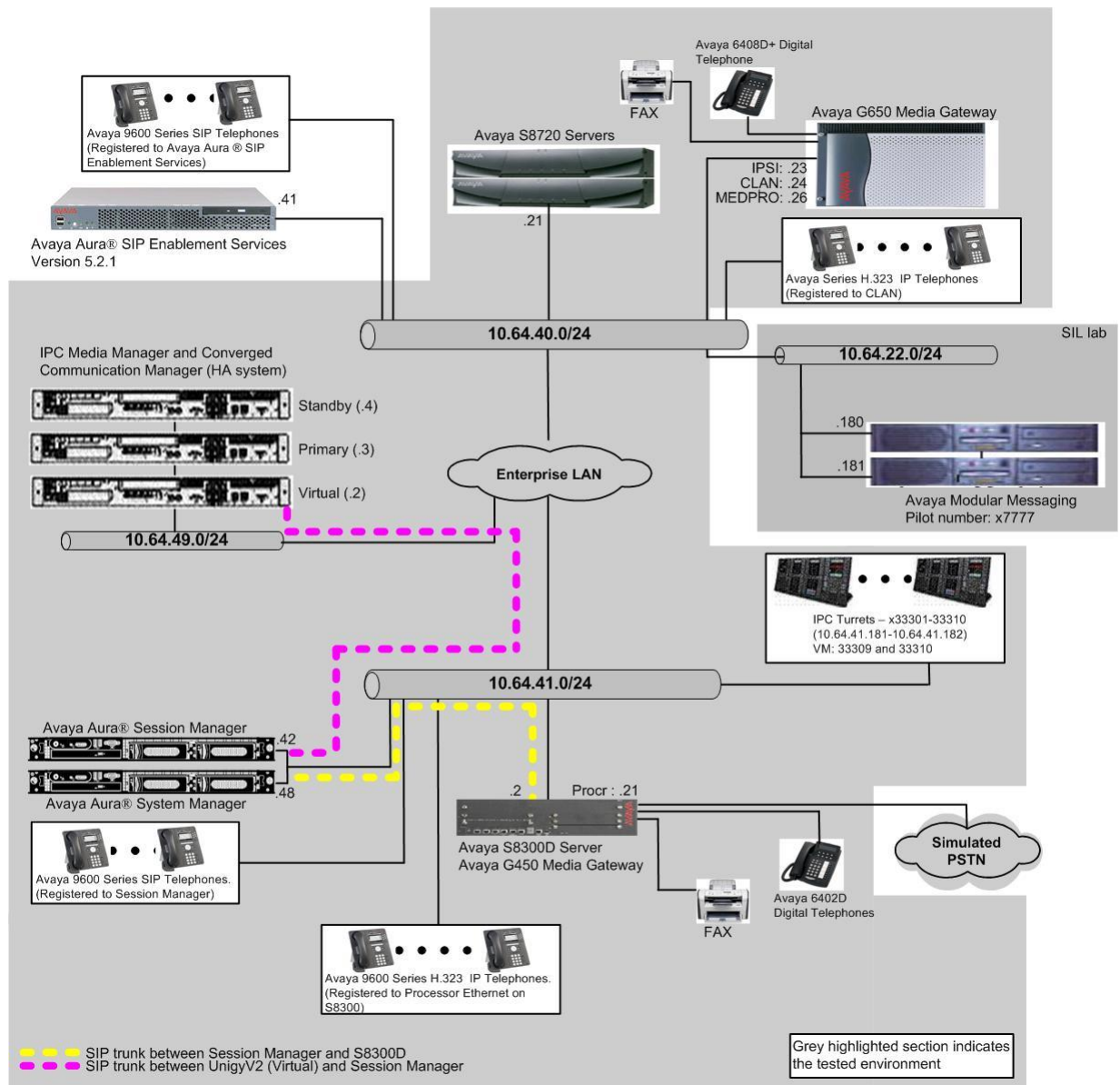


Figure 1: Test Configuration of IPC UnigyV2

4. Equipment and Software Validated

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

Equipment	Software
Avaya Aura® Communication Manager on Avaya S8300D Server	R016x.03.0.124.0-20553
Avaya G450 Media Gateway <ul style="list-style-type: none">TN464HP DS1 Interface	HW02 FW024
Avaya Aura® Session Manager	6.3.2.0.632023
Avaya Aura® System Manager	6.3.2.4.1529
Avaya 96xx IP Telephone (H.323)	3.1
Avaya 96xx IP Telephone (SIP)	2.6.4
Avaya A175 Desktop Video Device (SIP)	1.0.2
IPC UnigyV2 <ul style="list-style-type: none">Media ManagerConverged Communication ManageTurret	02.00.00.05.0031 02.00.00.05.0031 02.00.00.05.0031

5. Configure Avaya Aura® Communication Manager

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

- Verify Communication Manager license
- Administer system parameters features
- Administer SIP trunk group
- Administer SIP signaling group
- Administer IP network region
- Administer IP codec set
- Administer route pattern
- Administer private numbering
- Administer uniform dial plan
- Administer AAR analysis
- Administer ISDN trunk group
- Administer tandem calling party number

In the compliance testing, a separate set of codec set, network region, trunk group, and signaling group were used for the IPC turret users.

5.1. Verify Communication Manager License

Log into the System Access Terminal (SAT) to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use 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.

The license file installed on the system controls the maximum permitted. If there is insufficient capacity, contact an authorized Avaya sales 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: 4000	27	
Maximum Concurrently Registered IP Stations: 2400	3	
Maximum Administered Remote Office Trunks: 4000	0	
Maximum Concurrently Registered Remote Office Stations: 2400	0	
Maximum Concurrently Registered IP eCons: 68	0	
Max Concur Registered Unauthenticated H.323 Stations: 100	0	
Maximum Video Capable Stations: 2400	2	
Maximum Video Capable IP Softphones: 2400	2	
Maximum Administered SIP Trunks: 4000	70	
Maximum Administered Ad-hoc Video Conferencing Ports: 4000	0	
Maximum Number of DS1 Boards with Echo Cancellation: 80	0	

5.2. Administer System Parameters Features

Use the “change system-parameters features” command to allow for trunk-to-trunk transfers.

This feature is needed to be able to transfer an incoming call from IPC back out to IPC (incoming trunk to outgoing trunk), and to transfer an outgoing call to IPC to another outgoing call to IPC (outgoing trunk to outgoing trunk). For ease of interoperability testing, the **Trunk-to-Trunk Transfer** field was set to “all” to enable all trunk-to-trunk transfers on a system wide basis. Note that this feature poses significant security risk, and must be used with caution. For alternatives, the trunk-to-trunk feature can be implemented on the Class Of Restriction or Class Of Service levels. Refer to [1] for more details.

```
change system-parameters features                               Page 1 of 19
      FEATURE-RELATED SYSTEM PARAMETERS
      Self Station Display Enabled? n
      Trunk-to-Trunk Transfer: all
      Automatic Callback with Called Party Queuing? n
      Automatic Callback - No Answer Timeout Interval (rings): 3
      Call Park Timeout Interval (minutes): 10
      Off-Premises Tone Detect Timeout Interval (seconds): 20
      AAR/ARS Dial Tone Required? y

      Music (or Silence) on Transferred Trunk Calls? no
      DID/Tie/ISDN/SIP Intercept Treatment: attendant
      Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
      Automatic Circuit Assurance (ACA) Enabled? n
```

5.3. Administer SIP Trunk Group

Use the “add trunk-group n” command, where “n” is an available trunk group number, in this case “92”. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Group Type:** “sip”
- **Group Name:** A descriptive name.
- **TAC:** An available trunk access code.
- **Service Type:** “tie”

```
add trunk-group 92                                           Page 1 of 21
      TRUNK GROUP
      Group Number: 92
      Group Name: SM 41 42
      Direction: two-way
      Dial Access? n
      Queue Length: 0
      Service Type: tie
      Group Type: sip
      COR: 1
      Outgoing Display? y
      Auth Code? n
      CDR Reports: y
      TN: 1
      TAC: 1092
      Night Service:
      Member Assignment Method: auto
      Signaling Group: 92
      Number of Members: 10
```


Navigate to **Page 3**, and enter “private” for **Numbering Format**.

add trunk-group 92		Page 3 of 21
TRUNK FEATURES		
ACA Assignment? n	Measured: none	Maintenance Tests? y
Numbering Format: private		UUI Treatment: service-provider
		Replace Restricted Numbers? n
		Replace Unavailable Numbers? n
Modify Tandem Calling Number: no		
Show ANSWERED BY on Display? y		

Navigate to **Page 4**, and disable **Network Call Redirection (REFER)** since REFER did not work with Unigy V2. Enter “101” for **Telephone Event Payload Type**.

add trunk-group 92		Page 4 of 21
PROTOCOL VARIATIONS		
Mark Users as Phone? y		
repend '+' to Calling/Alerting/Diverting/Connected Number? n		
Send Transferring Party Information? y		
Network Call Redirection? n		
Send Diversion Header? n		
Support Request History? y		
Telephone Event Payload Type: 101		
Convert 180 to 183 for Early Media? n		
Always Use re-INVITE for Display Updates? n		
Identity for Calling Party Display: P-Asserted-Identity		
Block Sending Calling Party Location in INVITE? n		
Accept Redirect to Blank User Destination? n		
Enable Q-SIP? n		

5.4. Administer SIP Signaling Group

Use the “add signaling-group n” command, where “n” is an available signaling group number, in this case “92”. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Group Type:** “sip”
- **Transport Method:** “tls”
- **Near-end Node Name:** An existing C-LAN node name or procr.
- **Far-end Node Name:** The existing Session Manager node name.
- **Near-end Listen Port:** An available port for integration on Communication Manager.
- **Far-end Listen Port:** The same port number as in **Near-end Listen Port**.
- **Far-end Network Region:** Set to “1”.
- **Direct IP-IP Audio Connection:** Disable the field by entering “n” (Unigy V2 does not fully support shuffling).

add signaling-group 92		Page 1 of 2
SIGNALING GROUP		
Group Number: 92	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		
IP Video? y	Priority Video? y	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: SM-1
Near-end Listen Port: 5061		Far-end Listen Port: 5061
		Far-end Network Region: 1
Far-end Secondary Node Name:		
Far-end Domain:		
Incoming Dialog Loopbacks: eliminate		Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload		RFC 3389 Comfort Noise? n
Session Establishment Timer(min): 3		Direct IP-IP Audio Connections? n
Enable Layer 3 Test? y		IP Audio Hairpinning? n
Alternate Route Timer(sec): 6		

5.5. Administer IP Network Region

Use the “change ip-network-region n” command, where “n” is the existing far-end network region number used by the SIP signaling group from **Section 5.4**.

For **Authoritative Domain**, set to “avaya.com”. Enter a descriptive **Name**. Enter “yes” for **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio**, as shown below. For **Codec Set**, enter an available codec set number for integration with IPC UnigyV2.

```
change ip-network-region 1                                     Page 1 of 20
                                                                IP NETWORK REGION
Region: 1
Location: 1           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
                      IP Audio Hairpinning? n
UDP Port Min: 16390
UDP Port Max: 16999
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
Audio PHB Value: 46
Video PHB Value: 26
```

5.6. Administer IP Codec Set

Use the “change ip-codec-set n” command, where “n” is the codec set number from **Section 5.5**. Update the audio codec types in the **Audio Codec** fields as necessary. Note that IPC UnigyV2 supports G.711.

```
change ip-codec-set 1                                         Page 1 of 2
                                                                IP Codec Set

Codec Set: 1

Audio      Silence      Frames      Packet
Codec      Suppression   Per Pkt    Size(ms)
1: G.711MU      n           2          20
2:
3:
4:
5:
6:
7:
```

5.7. Administer Route Pattern

Use the “change route-pattern n” command, where “n” is an existing route pattern number to be used to reach IPC, in this case “92”. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Pattern Name:** A descriptive name.
- **Grp No:** The SIP trunk group number from **Section 5.3**.
- **FRL:** A level that allows access to this trunk, with 0 being least restrictive.

change route-pattern 92										Page 1 of 3		
Pattern Number: 92 Pattern Name: no IMS SIP trk												
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:	92	0								n	user	
2:											n	user
3:											n	user
4:											n	user
5:											n	user
6:											n	user
BCC		VALUE	TSC	CA-TSC	ITC		BCIE	Service/Feature	PARM	No.	Numbering	LAR
0		1	2	M	4	W	Request		Dgts		Format	
										Subaddress		
1:	y	y	y	y	y	n	n	rest			none	
2:	y	y	y	y	y	n	n	rest			none	

5.8. Administer Private Numbering

Use the “change private-numbering 0” command, to define the calling party number to send to IPC. Add an entry for the trunk group defined in **Section 5.3**. In the example shown below, all calls originating from a 5-digit extension beginning with 720 and routed to trunk group 92 will result in a 5-digit calling number. The calling party number will be in the SIP “From” header.

change private-numbering 0					Page 1 of 2	
NUMBERING - PRIVATE FORMAT						
Ext	Ext	Trk	Private	Total		
Len	Code	Grp(s)	Prefix	Len		
5	720	92		5	Total Administered: 10	
5	720	93		5	Maximum Entries: 540	

5.9. Administer Uniform Dial Plan

This section provides a sample AAR routing used for routing calls with dialed digits 7205x to IPC. Note that other methods of routing may be used. Use the “change uniform-dialplan 0” command, and add an entry to specify the use of AAR for routing digits 7205x, as shown below.

change uniform-dialplan 0						Page	1 of	2
UNIFORM DIAL PLAN TABLE						Percent Full: 0		
Matching Pattern	Len	Del	Insert Digits	Net	Conv	Node Num		
141044	11	0		ars	n			
2	5	0		aar	n			
20004	5	0		aar	n			
50000	5	0		aar	n			
53005	5	0		aar	n			
7050	4	0		aar	n			
7202	5	0		aar	n			
7203	5	0		aar	n			
7204	5	0		aar	n			
7205	5	0		aar	n			

5.10. Administer AAR Analysis

Use the “change aar analysis 7” command, and add an entry to specify how to route calls to 7205x. In the highlighted example shown below, calls with digits 7205x will be routed using route pattern “92” from **Section 5.7**.

change aar analysis 7						Page	1 of	2
AAR DIGIT ANALYSIS TABLE						Percent Full: 3		
Location: all								
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Reqd		
7202	5	5	92	unku		n		
7203	5	5	92	unku		n		
7204	5	5	92	unku		n		
7205	5	5	92	unku		n		
7206	5	5	92	unku		n		
7301	5	5	92	unku		n		
770	5	5	26	aar		n		
7777	4	4	92	unku		n		
780	5	5	92	unku		n		
79000	5	5	99	aar		n		
						n		
						n		
						n		

5.11. Administer ISDN Trunk Group

Use the “change trunk-group n” command, where “n” is the existing ISDN trunk group number used to reach the PSTN, in this case “80”.

Navigate to **Page 3**. For **Modify Tandem Calling Number**, enter “tandem-cpn-form” to allow for the calling party number from IPC to be modified.

change trunk-group 80		Page 3 of 21
TRUNK FEATURES		
ACA Assignment? n	Measured: none	Wideband Support? n
	Internal Alert? n	Maintenance Tests? y
	Data Restriction? n	NCA-TSC Trunk Member:
	Send Name: y	Send Calling Number: y
Used for DCS? n		Send EMU Visitor CPN? y
Suppress # Outpulsing? n	Format: natl-pub	
Outgoing Channel ID Encoding: preferred	UII IE Treatment: service-provider	
	Replace Restricted Numbers? n	
	Replace Unavailable Numbers? n	
	Send Connected Number: y	
Network Call Redirection: none	Hold/Unhold Notifications? n	
Send UII IE? y	Modify Tandem Calling Number: tandem-cpn-form	
Send UCID? n		
Send Codeset 6/7 LAI IE? y	Dsl Echo Cancellation? n	
Apply Local Ringback? n	US NI Delayed Calling Name Update? n	
Show ANSWERED BY on Display? y		
	Network (Japan) Needs Connect Before Disconnect? n	

5.12. Administer Tandem Calling Party Number

Use the “change tandem-calling-party-num” command to define the calling party number to send to the PSTN for tandem calls from IPC turret users.

In the example shown below, all calls originating from a 5-digit extension beginning with 7205 and routed to trunk group 80 will result in a 10-digit calling number. For **Number Format**, use an applicable format, in this case “pub-unk”.

change tandem-calling-party-num		Page 1 of 8			
CALLING PARTY NUMBER CONVERSION FOR TANDEM CALLS					
CPN	Incoming	Trk			Outgoing
Len Prefix	Number	Format	Grp(s)	Delete Insert	Number Format
5 33			80	3035383547	pub-unk
5 7205			80	3035383547	pub-unk

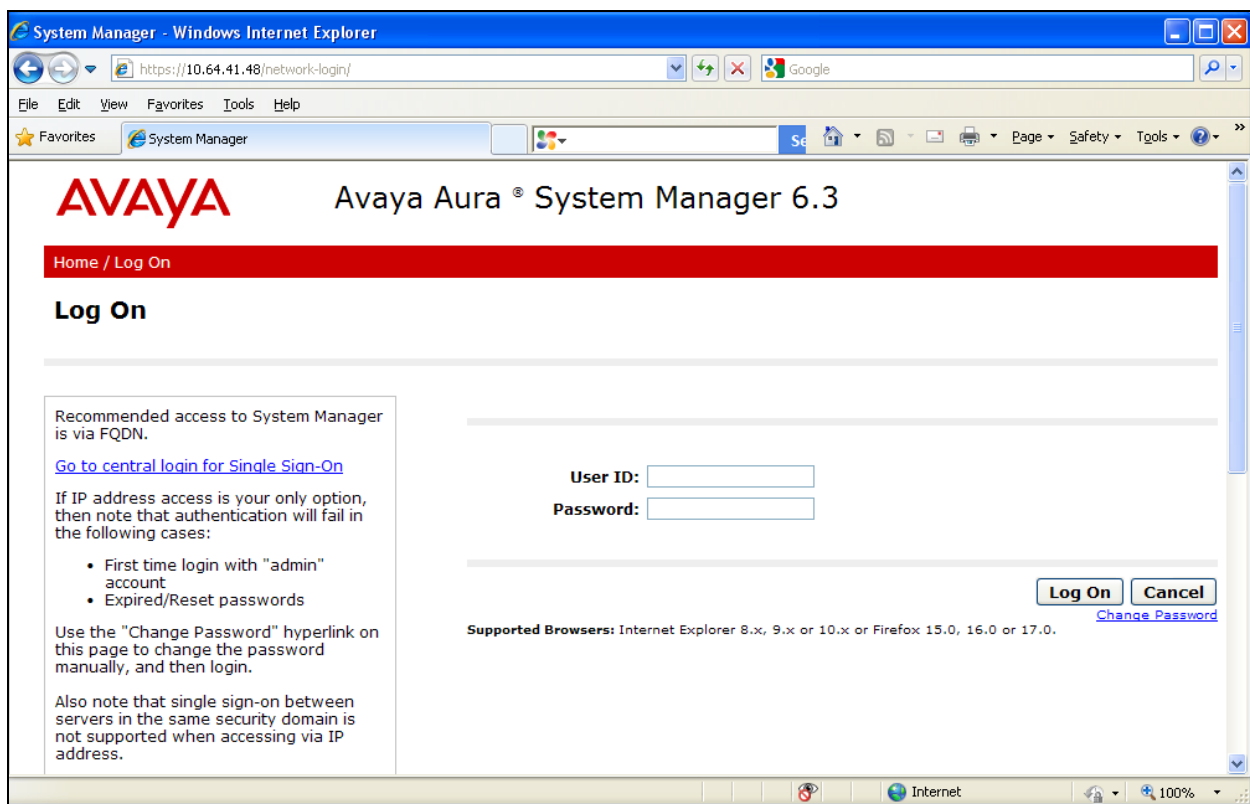
6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Avaya Aura® Session Manager. It is assumed that the basic configuration is already in place. This Section discusses the following area:

- Administer locations
- Administer adaptations
- Administer SIP entities
- Administer entity links
- Administer routing policies
- Administer dial patterns

6.1. Launch System Manager

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



6.2. Administer Locations

In the subsequent screen (not shown), select **Elements** → **Routing** to display the **Introduction to Network Routing Policy** screen below. Select **Routing** → **Locations** from the left pane, and click **New** in the subsequent screen (not shown) to add a new location for IPC.

The screenshot shows the Avaya Aura System Manager 6.3 web interface. The top header includes the Avaya logo, the title 'Avaya Aura® System Manager 6.3', and a user status bar indicating 'Last Logged on at October 18, 2013 2:40 PM' with links for 'Help', 'About', 'Change Password', and 'Log off admin'. The left navigation pane is expanded to 'Routing', showing a list of sub-items: Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area displays the 'Introduction to Network Routing Policy' page. It includes a breadcrumb trail 'Home / Elements / Routing' and a 'Help ?' link. The page title is 'Introduction to Network Routing Policy'. The text explains that Network Routing Policy consists of several routing applications like 'Domains', 'Locations', 'SIP Entities', etc., and provides a recommended order for configuration: Step 1: Create 'Domains' of type SIP, Step 2: Create 'Locations', Step 3: Create 'Adaptations', and Step 4: Create 'SIP Entities'. A note specifies that SIP Entities used as 'Outbound Proxies' include 'Gateway' or 'SIP Trunk'.

The **Location Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name** and optional **Notes**. In the **Location Pattern** sub-section, click **Add** and enter the applicable **IP Address Pattern** (not shown). Retain the default values in the remaining fields.

The screenshot shows the 'Location Details' screen in the Avaya Aura System Manager 6.3 web interface. The top header is identical to the previous screenshot. The left navigation pane is expanded to 'Routing' and 'Locations' is selected. The main content area displays the 'Location Details' page with a breadcrumb trail 'Home / Elements / Routing / Locations' and a 'Help ?' link. The page title is 'Location Details'. There are 'Commit' and 'Cancel' buttons. The 'General' sub-section contains a form with a required field '* Name:' with the value '49-subnet' and an optional 'Notes:' field with the value 'Unigy/Alliance'. The 'Dial Plan Transparency in Survivable Mode' sub-section contains an 'Enabled:' checkbox (unchecked), a 'Listed Directory Number:' text box, and an 'Associated CM SIP Entity:' dropdown menu.

6.3. Administer Adaptations

During the compliance test, the adaption was not administered. Instead, in **Section 5.4** of the signal group form, the Far-end Domain field was set to blank, which means “catch all”.

6.4. Administer SIP Entities

Add two new SIP entities, one for IPC, and another for the new SIP trunks for Communication Manager.

6.4.1. IPC SIP Entity

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

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

- **Name:** A descriptive name.
- **FQDN or IP Address:** The IP address of the IPC Media Manager server.
- **Type:** “Other”
- **Location:** Select the IPC location name from **Section 6.2**.
- **Time Zone:** Select the applicable time zone.

AVAYA Avaya Aura® System Manager 6.3 Last Logged on at October 18, 2013 2:40 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Routing × **Home**

Home / Elements / Routing / SIP Entities [Help ?](#)

SIP Entity Details Commit Cancel

General

* **Name:** IPC Unigy HA

* **FQDN or IP Address:** 10.64.49.2

Type: Other

Notes: IPC Unigy HA system

Adaptation:

Location: 49-subnet

Time Zone: America/Denver

Override Port & Transport with DNS SRV: ☐

* **SIP Timer B/F (in seconds):** 4

Credential name:

Call Detail Recording: none

CommProfile Type Preference:

Loop Detection

Loop Detection Mode: Off

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

6.4.2. Communication Manager SIP Entity

Select **Routing** → **SIP Entities** from the left pane, and click **New** in the subsequent screen (not shown) to add a new SIP entity for Communication Manager. Note that this SIP entity is used for integration with IPC.

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

- **Name:** A descriptive name.
- **FQDN or IP Address:** The IP address of an existing CLAN or procr.
- **Type:** “CM”
- **Notes:** Any descriptive notes.
- **Location:** Select the applicable location for Communication Manager.
- **Time Zone:** Select the applicable time zone.

AVAYA Avaya Aura® System Manager 6.3 Last Logged on at October 18, 2013 2:40 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Routing × **Home**

Home / Elements / Routing / SIP Entities [Help ?](#)

SIP Entity Details [Commit](#) [Cancel](#)

General

* **Name:** S8300D-G450-TLS

* **FQDN or IP Address:** 10.64.41.21

Type: CM

Notes: CM in D4H26 lab

Adaptation:

Location: 41-subnet

Time Zone: America/Denver

Override Port & Transport with DNS SRV: ☐

* **SIP Timer B/F (in seconds):** 4

Credential name:

Call Detail Recording: both

Loop Detection

Loop Detection Mode: Off

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

6.5. Administer Entity Links

Add three new entity links, two for IPC, and another for Communication Manager.

6.5.1. IPC Entity Links

Select **Routing** → **Entity Links** from the left pane, and click **New** in the subsequent screen (not shown) to add a new entity link for IPC. The **Entity Links** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **SIP Entity 1:** The Session Manager entity name
- **Protocol:** “UDP”
- **Port:** “5060”
- **SIP Entity 2:** The IPC entity name from **Section 6.4.1**.
- **Port:** “5060”
- **Connection Policy:** “Trusted”

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left navigation pane has 'Routing' expanded, with 'Entity Links' selected. The main content area is titled 'Entity Links' and shows a table with one item. The table has columns for Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, and Connection Policy. The values in the table are: Name: *SM63_IPC Unigy HA, SIP Entity 1: *SM63, Protocol: UDP, Port: *5060, SIP Entity 2: *IPC Unigy HA, Port: *5060, and Connection Policy: trusted. There are 'Commit' and 'Cancel' buttons at the bottom right of the table.

	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
<input type="checkbox"/>	*SM63_IPC Unigy HA	*SM63	UDP	*5060	*IPC Unigy HA	*5060	trusted

Repeat and add another entity link for IPC with “TCP” as Protocol, as shown below.

AVAYA

Avaya Aura® System Manager 6.3

Last Logged on at October 18, 2013 2:40 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Routing

Home

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home / Elements / Routing / Entity Links

Entity Links

Commit Cancel

1 Item Refresh Filter: Enable

	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
<input type="checkbox"/>	*SM63_IPC Unigy HA	*SM63	TCP	*5060	*IPC Unigy HA	*5060	trusted

Select : All, None

Commit Cancel

6.5.2. Communication Manager Entity Links

Select **Routing** → **Entity Links** from the left pane, and click **New** in the subsequent screen (not shown) to add a new entity link for Communication Manager. The **Entity Links** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **SIP Entity 1:** The Session Manager entity name, in this case “SM63”.
- **Protocol:** The signaling group transport method from **Section 5.4**.
- **Port:** The signaling group listen port number from **Section 5.4**.
- **SIP Entity 2:** The Communication Manager entity name from **Section 6.4.2**.
- **Port:** The signaling group listen port number from **Section 5.4**.
- **Connection Policy:** **Trusted**

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left navigation pane is expanded to 'Routing', and 'Entity Links' is selected. The main content area shows the 'Entity Links' configuration page. At the top, there are tabs for 'Routing', 'Session Manager', and 'Home'. Below the tabs, there is a breadcrumb trail: 'Home / Elements / Routing / Entity Links'. The page title is 'Entity Links'. There are 'Commit' and 'Cancel' buttons at the top right. Below the title, there is a table with the following columns: 'Name', 'SIP Entity 1', 'Protocol', 'Port', 'SIP Entity 2', 'Port', and 'Connection Policy'. The table contains one row with the following values: '00D-G450-TLS_5061', 'SM63', 'TLS', '5061', 'S8300D-G450-TLS', '5061', and 'trusted'. There are 'Commit' and 'Cancel' buttons at the bottom right.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
*00D-G450-TLS_5061	*SM63	TLS	*5061	*S8300D-G450-TLS	*5061	trusted

6.6. Administer Routing Policies

Add two new routing policies, one for IPC, and another for Communication Manager.

6.6.1. IPC Routing Policy

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

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

In the **SIP Entity as Destination** sub-section, click **Select** and select the IPC entity name from **Section 6.4.1** in the listing (not shown).

Retain the default values in the remaining fields.

AVAYA Avaya Aura® System Manager 6.3 Last Logged on at October 18, 2013 2:40 PM
Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Routing Policies

Routing Policy Details Commit Cancel Help ?

General

* Name: Route2Unigy-HA

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
IPC Unigy HA	10.64.49.2	Other	IPC Unigy HA system

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"/>	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	

Select : All, None

6.6.2. Communication Manager Routing Policy

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

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

In the **SIP Entity as Destination** sub-section, click **Select** and select the Communication Manager entity name from **Section 6.4.2** in the listing (not shown).

Retain the default values in the remaining fields.

AVAYA Avaya Aura® System Manager 6.3 Last Logged on at October 18, 2013 2:40 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Routing × **Home**

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
S8300D-G450-TLS	10.64.41.21	CM	CM in D4H26 lab

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"/>	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	

Select : All, None

6.7. Administer Dial Patterns

Add a new dial pattern for IPC, and update the existing dial pattern for Communication Manager.

6.7.1. IPC Dial Pattern

Select **Routing → Dial Patterns** from the left pane, and click **New** in the subsequent screen (not shown) to add a new dial pattern to reach IPC turret users. The **Dial Pattern Details** screen is displayed. In the **General** sub-section, enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Pattern:** A dial pattern to match.
- **Min:** The minimum number of digits to be matched.
- **Max:** The maximum number of digits to be matched.
- **SIP Domain:** Select “ALL”.
- **Notes:** Any desired description.

In the **Originating Locations and Routing Policies** sub-section, click **Add** and create a new policy for reaching IPC turret users. In the compliance testing, the policy allowed for call origination from all locations, and the IPC routing policy from **Section 6.6.1** was selected as shown below.

Avaya Aura® System Manager 6.3

Last Logged on at October 18, 2013 2:40 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Routing * **Home**

Home / Elements / Routing / Dial Patterns

Dial Pattern Details [Help ?](#)

General

* **Pattern:** 7205

* **Min:** 5

* **Max:** 5

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes:

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-	Route2Unigy -HA	IPC Unigy HA		<input type="checkbox"/>		

Select : All, None

6.7.2. Communication Manager Dial Pattern

Select **Routing** → **Dial Patterns** from the left pane, and click on the existing dial pattern for Communication Manager in the subsequent screen, in this case dial pattern “7200” (not shown). The **Dial Pattern Details** screen is displayed.

In the **Originating Locations and Routing Policies** sub-section, click **Add** and create a new policy as necessary for calls from IPC turret users. In the compliance testing, the policy allowed for call origination from the IPC location from **Section 6.2**, and the Communication Manager routing policy from **Section 6.6.2** was selected as shown below. Retain the default values in the remaining fields.

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 October 18, 2013 2:40 PM", "Help | About | Change Password | Log off", and the user "admin". The left sidebar shows a tree view with "Routing" selected, and sub-items: 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 "Home / Elements / Routing / Dial Patterns" and a "Dial Pattern Details" header with "Commit" and "Cancel" buttons. The "General" section contains fields for: * Pattern: 7200, * Min: 5, * Max: 5, Emergency Call: ☐, Emergency Priority: 1, Emergency Type: (empty), SIP Domain: avaya.com (dropdown), and Notes: (empty). Below this is the "Originating Locations and Routing Policies" section with "Add" and "Remove" buttons. It shows a table with 1 item, a "Refresh" button, and a "Filter: Enable" link. The table has columns: Originating Location Name, Originating Location Notes, Routing Policy Name, Rank, Routing Policy Disabled, Routing Policy Destination, and Routing Policy Notes. One row is visible with Originating Location Name "-ALL-", Routing Policy Name "Route2G450 via TLS", Routing Policy Disabled ☐, and Routing Policy Destination "S8300D-G450 -TLS". At the bottom, there is a "Select : All, None" option.

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
-ALL-		Route2G450 via TLS		<input type="checkbox"/>	S8300D-G450 -TLS	

7. Configure IPC Converged Communication Manager

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

- Launch Unigy Management System
- Administer SIP trunks
- Administer trunk groups
- Administer route lists
- Administer dial patterns
- Administer route plans

The configuration of Media Manager and/or Converged Communication Manager is typically performed by IPC installation technicians. The procedural steps are presented in these Application Notes for informational purposes.

7.1. Launch Unigy Management System

Access the UnigyV2 Management System web interface by using the URL “http://ip-address” in an Internet browser window, where “ip-address” is the IP address of the Media Manager. Log in using the appropriate credentials.

The screen below is displayed. Enter the appropriate credentials. Check **I agree with the Terms of Use**, and click **Login**.

In the subsequent screen (not shown), click **Continue**.



The image shows a web-based login interface for the Unigy Management System. On the left is the Unigy logo, a blue circle with the word 'unigy' in white. To the right of the logo are two input fields: 'User Name:' and 'Password:'. Below these fields is a checkbox labeled 'I agree with the' followed by a blue underlined link 'Terms of Use'. To the right of the checkbox is a small square icon. Below the checkbox and link is a 'Login' button. At the bottom of the form, there is a block of text: 'IPC Unigy™ Management System', 'Unigy™ Version 02.00.00.05.0031', 'COP Version 02.00.00.00.1888', and '© Copyright 2011-2013 IPC Systems, Inc. All rights reserved.'

The following screen (Tools -> Monitoring) displays. Navigate to **Configuration** → **Site** under the main menu.

Instances


Instance	Total Devices	Devices i...
Default Instance	6	0

Locations

Location	Instance	Total ...	Devices in... 1 ▼
Default Back Roo	Default Instance	4	0
Default Front Roo	Default Instance	2	0

Refresh

7.2. Administer SIP Trunks

Select **Trunks** → **SIP Trunks** in the left pane, and click the **Add** icon () in the lower left pane to add a new SIP trunk. Select “Dial Tone” from the **Select Connection Type** drop-down list.

Instance: All Instance ▼


Site Configuration: Location ▼

Location: All Locations ▼

▼ Trunks

- SIP Trunks
- Alliance Trunks
- Media Gateways

► Communication Devices

SIP Trunks 

UI Name	Last Used
Unigy-IPO-TRK	

Select Connection Type: ▼

The screen below is displayed next. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Trunk Name:** A descriptive name.
- **Destination Address:** IP address of the Session Manager signaling interface.
- **Destination Port:** The port number from **Section 6.5.1**.
- **Zone:** An available zone, in this case “Default Zone 1”.
- **Channels:** The number of SIP trunk group members from **Section 5.3**.
- **Reason Protocol** “SIP”
- **PBX Provider:** “Avaya”
- **Connected Party Update:** “UPDATE”

Retain the default values in the remaining fields.

The screenshot shows the UniQy Configuration -> Sites interface. On the left, a navigation pane lists various configuration categories, with 'SIP Trunks' selected. Below this, a table lists existing trunks: 'Unigy-SIP-TRK' and 'Unigy-IPO-TRK'. The main area displays the configuration for 'Trunk: Unigy-SIP-TRK' in 'Basic' mode. The configuration fields are as follows:

Field	Value
Trunk Name	Unigy-SIP-TRK
Connection Type	Dial Tone
Destination Address	10.64.41.42
Destination Port	5060
Media Manager Profile	Safe
Zone	Default Zone 1
Channels	30
Reason Protocol	SIP
PBX Provider	Avaya
Connected Party Update	UPDATE
Subscribe to MWI	<input checked="" type="checkbox"/>
MWI Subscription Time	0
Vendor	
A/B Side	<input type="checkbox"/>
Distant End Name	
PBX Trunk Group Reference	
Trunk Info	
ReINVITE For Media Update	<input checked="" type="checkbox"/>
Options Supported	<input checked="" type="checkbox"/>
Equipped	<input checked="" type="checkbox"/>

At the bottom right, there are buttons for 'Delete', 'Revert', and 'Save'.


Select the Advance tab in the upper right. .Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Diversion Header:** “History-Info.
- **Outgoing Transport Type:** “UDP”.

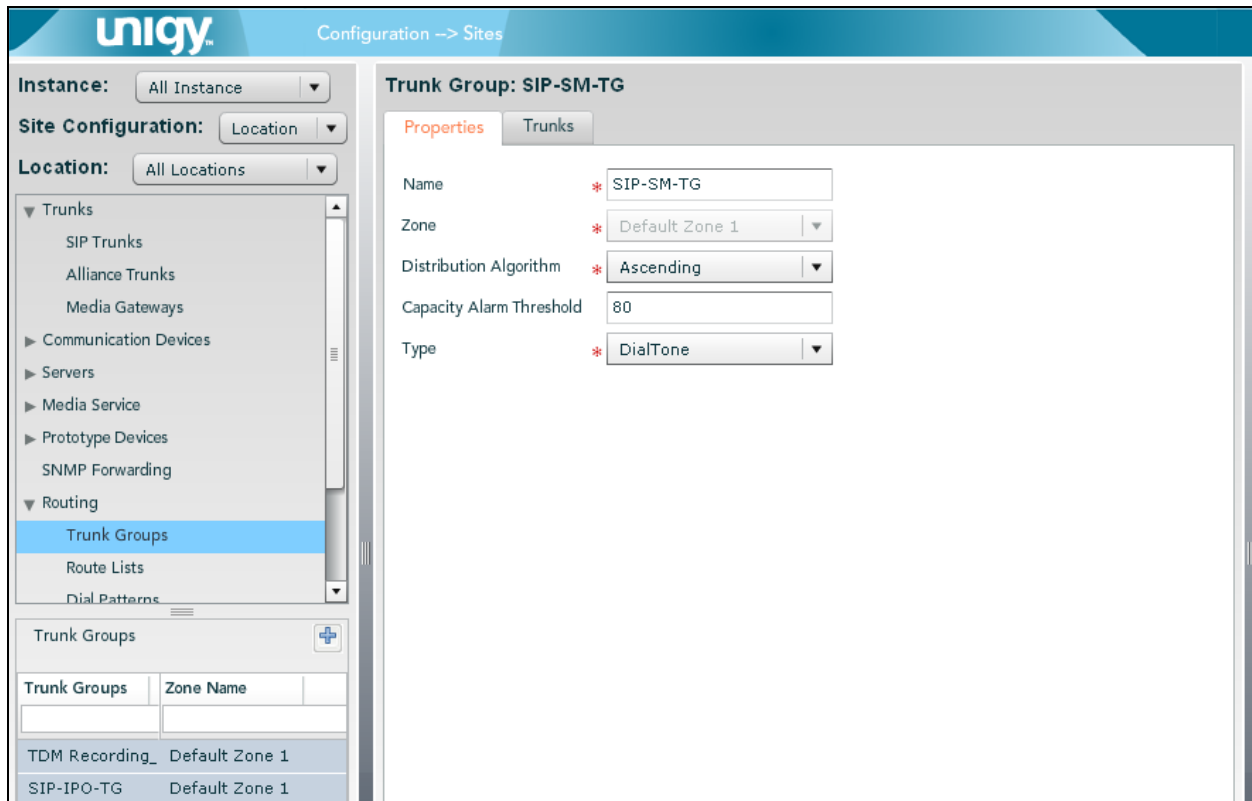
The screenshot shows the Unigy configuration interface. On the left, a navigation tree under 'Trunks' has 'SIP Trunks' selected. Below it, a table lists 'Unigy-SIP-TRK' and 'Unigy-IPO-TRK'. The main area is titled 'Trunk: Unigy-SIP-TRK' with 'Basic' and 'Advanced' tabs. The 'Advanced' tab is active, showing the 'DialTone Trunk Configuration' form. The form contains various fields with their current values or default settings.

Field	Value
Trunk Name	* Unigy-SIP-TRK
Connection Type	Dial Tone
Destination Address	* 10.64.41.42
Destination Port	* 5060
Media Manager Profile	* Safe
Zone	* Default Zone 1
Channels	30
Reason Protocol	* SIP
PBX Provider	* Avaya
Connected Party Update	* UPDATE
Subscribe to MWI	<input checked="" type="checkbox"/>
MWI Subscription Time	0
Vendor	
A/B Side	<input type="checkbox"/>
Distant End Name	
PBX Trunk Group Reference	
Trunk Info	
Diversion Header	* History-Info
Indicate PRACK Support	<input checked="" type="checkbox"/>
Outgoing Transport Type	* UDP
ReINVITE For Media Update	<input checked="" type="checkbox"/>
Options Supported	<input checked="" type="checkbox"/>

7.3. Administer Trunk Groups

Select **Routing** → **Trunk Groups** in the left pane, and click the **Add** icon () in the lower left pane to add a new trunk group.

The **Trunk Group** screen is displayed in the right pane. In the **Properties** tab, enter a descriptive **Name**, select “Default Zone 1” for the **Zone** field, select “Ascending” for the **Distribution Algorithm** field, and click **Save** (not shown). Select the **Trunks** tab in the right pane.



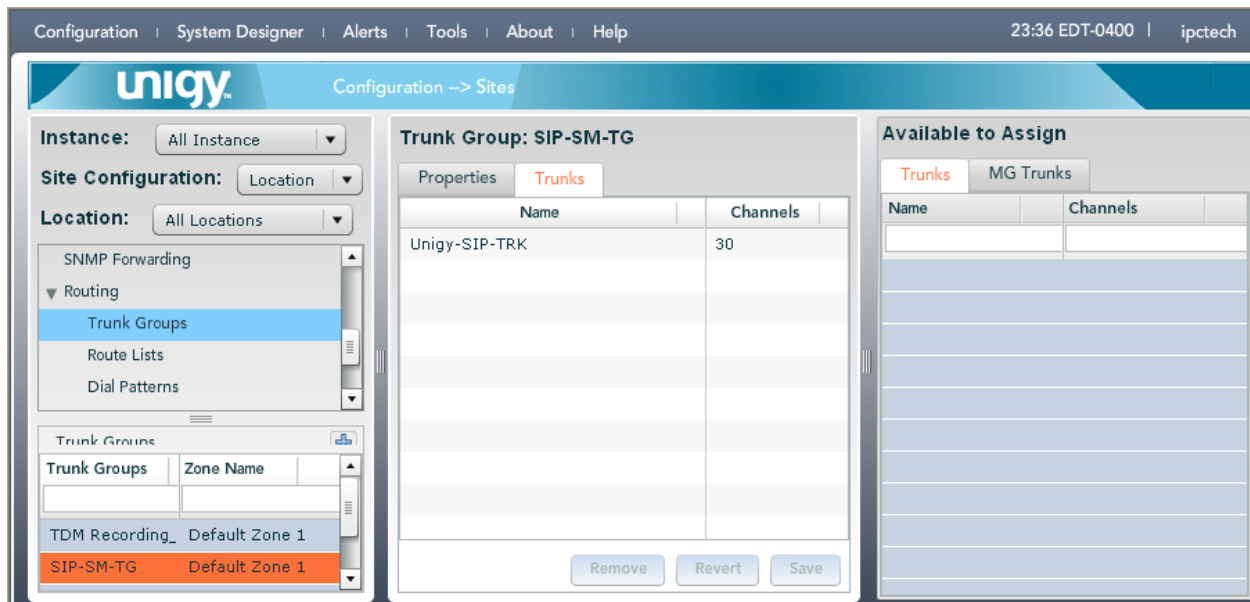
The screenshot shows the UniV2 configuration interface. The left pane displays a navigation tree with 'Trunk Groups' selected under 'Routing'. The right pane shows the 'Trunk Group: SIP-SM-TG' configuration screen. The 'Properties' tab is active, displaying the following fields:

- Name: * SIP-SM-TG
- Zone: * Default Zone 1
- Distribution Algorithm: * Ascending
- Capacity Alarm Threshold: 80
- Type: * DialTone


Below the configuration fields, there is a table with the following data:

Trunk Groups	Zone Name
TDM Recording_	Default Zone 1
SIP-IPO-TG	Default Zone 1

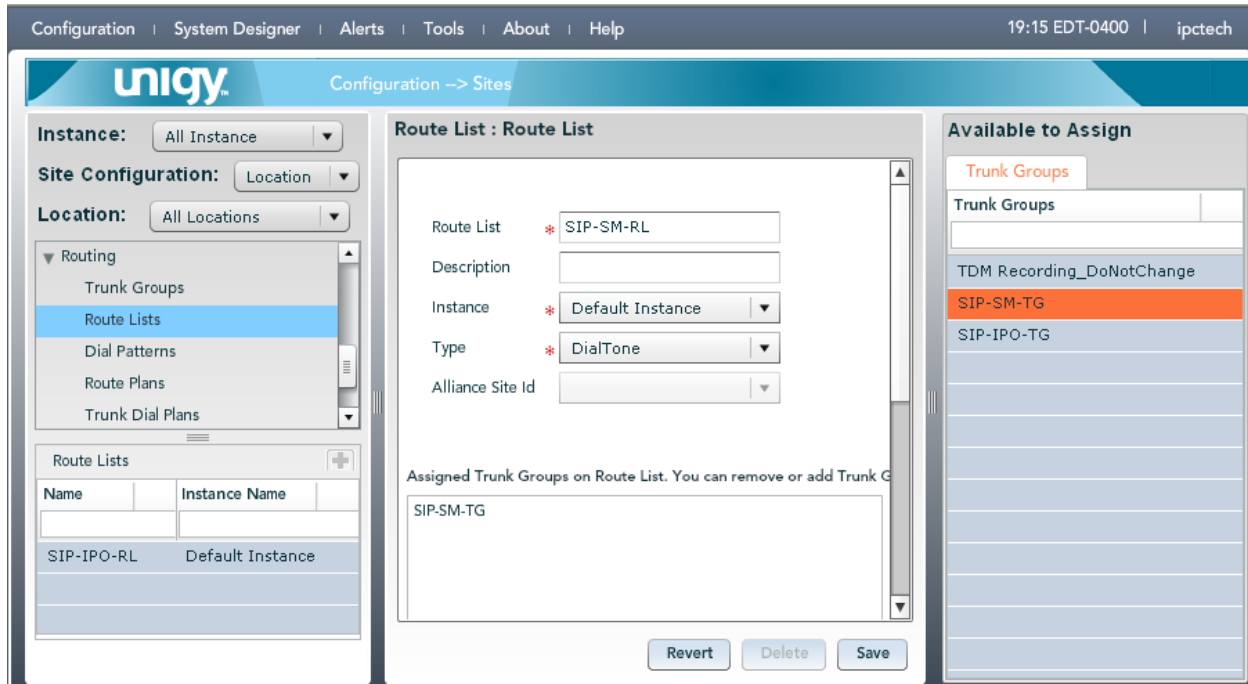
The screen is updated with three panes. In the rightmost pane, select the Trunks tab to display a list of trunks. Select the SIP trunk from **Section 7.2** in the rightmost pane and drag to the middle pane as shown below. Click Save.



7.4. Administer Route Lists

Select **Routing** → **Route Lists** in the left pane, and click the **Add** icon () in the lower left pane to add a new route list.

The **Route List** screen is displayed in the middle pane. For **Route List**, enter a descriptive name. In the right pane, select the trunk group from **Section 7.3** and drag into the **Assigned Trunk Groups on Route List** sub-section in the middle pane, as shown below. Click **Save**.



7.5. Administer Dial Patterns

Select **Routing → Dial Patterns** in the left pane, to display the **Dial Patterns** screen in the right pane. Click **Add New** in the upper right pane.

In the **Dial pattern Details** sub-section in the lower right pane, enter the desired **Name** and **Description**. For **Pattern String**, enter the dial pattern to match for Avaya endpoints, in this case “*” meaning any digits will be sent to Session Manager. Click **Save**. Once the **Save** button is clicked, the newly created Dial pattern should be displayed under the Dial Patterns section.

The screenshot shows the UniQy Configuration interface. The top navigation bar includes links for Configuration, System Designer, Alerts, Tools, About, and Help, along with the time 23:39 EDT-0400 and the user ipctech. The main header displays the UniQy logo and the path Configuration → Sites.

On the left side, there is a navigation pane with the following structure:

- Instance: All Instance (dropdown)
- Site Configuration: Location (dropdown)
- Location: All Locations (dropdown)
- Trunks
 - SIP Trunks
 - Alliance Trunks
 - Media Gateways
- Communication Devices
- Servers
- Media Service
- Prototype Devices
- SNMP Forwarding
- Routing
 - Trunk Groups
 - Route Lists
 - Dial Patterns** (highlighted)
 - Route Plans
 - Trunk Dial Plans
 - Trunk Dial Plan Rules

The main content area is divided into two sections:

- Dial Patterns**: A table with columns Name, Pattern String, Description, and Zone Name. Below the table are buttons for Add New and Delete.
- Dial pattern Details**: A sub-section with a Properties tab. It contains the following fields:
 - Name: All Dial Pattern
 - Zone: Default Zone 1 (dropdown)
 - Description: all
 - Pattern String: *Buttons for Revert and Save are located at the bottom right of this section.

Repeat this section to add another dial pattern to reach the PSTN, and include any required prefix by Avaya Aura® Communication Manager.

7.6. Administer Route Plans

Select **Routing** → **Route Plans** in the left pane, and click **Add New** (not shown) in the right pane to create a new route plan.

The screen is updated with three panes, as shown below. In the **Route Plan** middle pane, enter a descriptive **UI Name** and optional **Description**. For **Calling Party**, enter “*” to denote any calling party from UnigyV2. For **Destination** select the dial pattern for Avaya endpoints from **Section 7.5**. Select “Forward” for **Action**, and click **Save**.

The screenshot shows the Unigy Configuration interface. The top navigation bar includes links for Configuration, System Designer, Alerts, Tools, About, and Help, along with the time 23:46 EDT-0400 and the user ipctech. The main header displays the Unigy logo and the path Configuration → Sites.

The left pane, titled 'Instance: All Instance', contains 'Site Configuration: Location' and 'Location: All Locations'. A tree view on the left lists various configuration categories, with 'Routing' expanded and 'Route Plans' selected.

The middle pane, titled 'Route Plan', contains a 'Create New Route Plan' form. The form fields are as follows:

- UI Name: Route2SM
- Description: (empty)
- Calling Party: *
- Destination: *
- Action: Forward (dropdown menu)
- Route List: (empty table)

At the bottom of the form are buttons for 'Back', 'Revert', and 'Save'. Below the form is a section for 'Assign Trunk Groups'.

The right pane, titled 'Available to Assign', contains a 'Route Lists' table. The table has a 'Name' column and lists the following entries:

Name
TDM Recording_DoNotChange
SIP-SM-RL
SIP-IPO-RL

The screen is updated with the newly created route plan. Select the route plan, and click **Edit** toward the bottom of the screen.

The screenshot shows the UniV2 configuration interface. The top header includes navigation links: Configuration | System Designer | Alerts | Tools | About | Help, and the current time: 23:56 EDT-0400 | ipctech. The main content area is titled 'Configuration --> Sites' and 'Route Plan'.

On the left, there is a navigation menu with the following items:

- Trunks
- Communication Devices
- Servers
- Media Service
- Prototype Devices
- SNMP Forwarding
- Routing
 - Trunk Groups
 - Route Lists
 - Dial Patterns
 - Route Plans** (selected)
 - Trunk Dial Plans
 - Trunk Dial Plan Rules

The main content area is divided into two sections:

List of Route Plans

UI Name	Calling Party	Destination	Action	Instance Name
Route2MM	*	*	FORWARD	Default Instance
Route2IPO	*	*	FORWARD	Default Instance
Route2SM	*	*	FORWARD	Default Instance

Below the table are buttons: Delete, Add New, Revert, and Save Sequence Change.

Route Plan Details

Calling Party : *

Destination : *

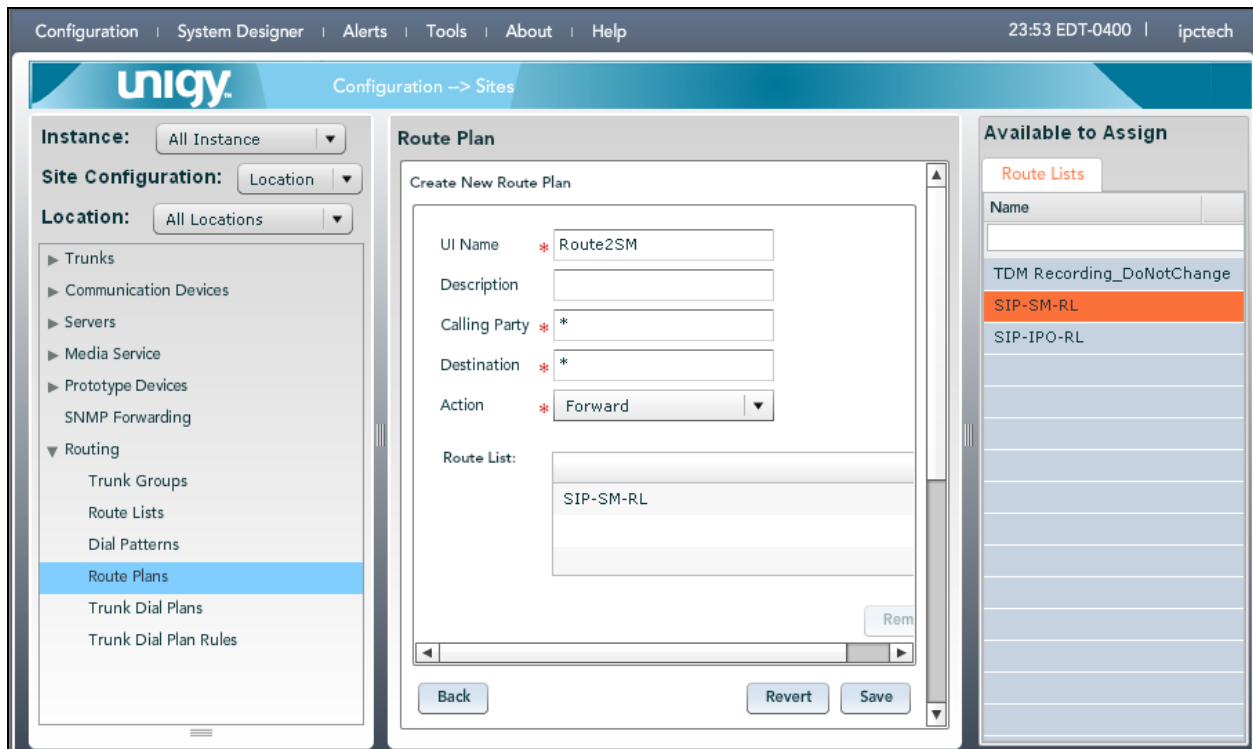
Action : FORWARD

RouteList:

Trunk Group:

At the bottom right of the details section is an **Edit** button.

The screen is updated with three panes again, as shown below. In the right pane, select the route list from **Section 7.4** and drag into the **Route List** sub-section in the middle pane, as shown below. Click **Save**.



8. Verification Steps

This section provides tests that can be performed to verify proper configuration of Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and IPC UnigyV2.

8.1. Verify Avaya Aura® Communication Manager

From the SAT interface, verify the status of the SIP trunk groups by using the “status trunk n” command, where “n” is the trunk group number administered in **Section 5.3**. Verify that all trunks are in the “in-service/idle” state as shown below.

```
status trunk 92
```

TRUNK GROUP STATUS			
Member	Port	Service State	Mtce Connected Ports Busy
0092/001	T00135	in-service/idle	no
0092/002	T00136	in-service/idle	no
0092/003	T00137	in-service/idle	no
0092/004	T00138	in-service/idle	no
0092/005	T00139	in-service/idle	no
0092/006	T00140	in-service/idle	no
0092/007	T00141	in-service/idle	no
0092/008	T00142	in-service/idle	no
0092/009	T00143	in-service/idle	no
0092/010	T00144	in-service/idle	no

Verify the status of the SIP signaling groups by using the “status signaling-group n” command, where “n” is the signaling group number administered in **Section 5.4**. Verify that the signaling group is “in-service” as indicated in the **Group State** field shown below.

```
status signaling-group 92
```

STATUS SIGNALING GROUP	
Group ID:	92
Group Type:	sip
Group State:	in-service

8.2. Verify Avaya Aura® Session Manager

From the System Manager home page (not shown), select **Elements** → **Session Manager** to display the **Session Manager Dashboard** screen (not shown). Select **Session Manager** → **System Status** → **SIP Entity Monitoring** from the left pane to display the **SIP Entity Link Monitoring Status Summary** screen. Click on the IPC entity name from **Section 6.4.1**.

AVAYA

Avaya Aura® System Manager 6.3

Last Logged on at October 19, 2013 9:06 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Session Manager ×

Routing ×

Session Manager ×

Home

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

Help ?

Session Manager

Dashboard

Session Manager

Administration

Communication Profile Editor

Network Configuration

Device and Location Configuration

Application Configuration

System Status

SIP Entity Monitoring

Managed Bandwidth Usage

Security Module Status

Registration Summary

User Registrations

Session Counts

System Tools

Performance

SIP Entity Link Monitoring Status Summary

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

SIP Entities Status for All Monitoring Session Manager Instances

Run Monitor

1 Items | Refresh

Filter: Enable

<input type="checkbox"/>	Session Manager	Type	Monitored Entities					Deny	Total
			Down	Partially Up	Up	Not Monitored			
<input type="checkbox"/>	SM63	Core	3	2	6	0	0	11	

Select: All, None

All Monitored SIP Entities

Run Monitor

11 Items | Refresh

Filter: Enable

<input type="checkbox"/>	SIP Entity Name
<input type="checkbox"/>	SB300D-G450-TLS
<input type="checkbox"/>	SB300D-G450-TCP
<input type="checkbox"/>	IPC Uniqy HA

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

Avaya Aura® System Manager 6.3

Last Logged on at October 19, 2013 9:06 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Session Manager

Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
System Status
SIP Entity Monitoring
Managed Bandwidth Usage
Security Module Status
Registration Summary
User Registrations
Session Counts
System Tools
Performance

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

SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

All Entity Links to SIP Entity: IPC Unigy HA

Status Details for the selected Session Manager:

Summary View

2 Items | Refresh

Filter: Enable

Session Manager I	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/> SM63	10.64.49.2	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/> SM63	10.64.49.2	5060	UDP	FALSE	UP	200 OK	UP

8.3. Verify IPC UnigyV2

Make a call from an IPC turret user to an Avaya endpoint. Verify that the call can be connected with two-way talk paths.

9. Conclusion

These Application Notes describe the configuration steps required for IPC UnigyV2 to successfully interoperate with Avaya Aura® Communication Manager 6.3 using Avaya Aura® Session Manager 6.3. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

10. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Document 03-300509, Release 6.3, May 2013, available at <http://support.avaya.com>.
2. *Administering Avaya Aura® System Manager*, Release 6.3, Issue 3, October 2013, available at <http://support.avaya.com>
3. *UnigyV2 1.1 System Configuration*, Part Number B02200187, Release 00, upon request to IPC Support.

©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.