



Avaya Solution & Interoperability Test Lab

Application Notes for IPC UnigyV3P2 with Avaya Aura® Session Manager 7.0 using SIP Trunks – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for IPC UnigyV3P2 to interoperate with Avaya Aura® Session Manager 7.0 using SIP trunks.

IPC UnigyV3P2 is a trading communication solution. In the compliance testing, IPC UnigyV3P2 used SIP trunks to Avaya Aura® Session Manager. Using the SIP trunks, UnigyV3P2 users on IPC were able to reach users on Avaya Aura® Communication Manager and on the PSTN.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration steps required for IPC UnigyV3P2 to interoperate with Avaya Aura® Session Manager, and 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 turrel 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 UnigyV3P2.

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, G.711A, hold/reconnect, DTMF, call forwarding unconditional/ring-no-answer/busy, blind/attended transfer, blinded/attended conference, barge-in, and long duration calls.

The serviceability testing focused on verifying the ability of IPC UnigyV3P2 to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to IPC UnigyV3P2.

2.2. Test Results

All test cases were executed and verified. The following were the observations on IPC UnigyV3P2 from the compliance testing:

- Even when IPC UnigyV3P2 is configured with UDP, the TCP protocol must be configured to be allowed on Session Manager as UnigyV3P2 switches over to use TCP for diversions.
- During the compliance test, Network Call Redirection (shuffling) was disabled, as shown in **Section 5.3**. (IPC requested)
- A blind conference initiated by an IPC turret with 96x1 Avaya SIP Deskphones did not work. This issue is being investigated by Avaya. A supervised conference from IPC turret with Avaya 96x1 SIP Deskphones worked properly. Also with 96x0 Avaya SIP Deskphones blind and supervised conferences worked as expected.

2.3. Support

Technical support on IPC UnigyV3P2 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 UnigyV3P2 consists of the Media Manager (MM), Converged Communication Manager (CCM), 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 UnigyV3P2 to Session Manager, to reach users (SIP and H.323) and on the PSTN.

A five digit Uniform Dial Plan (UDP) was used to facilitate dialing between the Avaya and IPC. Unique extension ranges were associated with Communication Manager users (7200x for H.323 and 7202x for SIP), and IPC turret users (7205x).

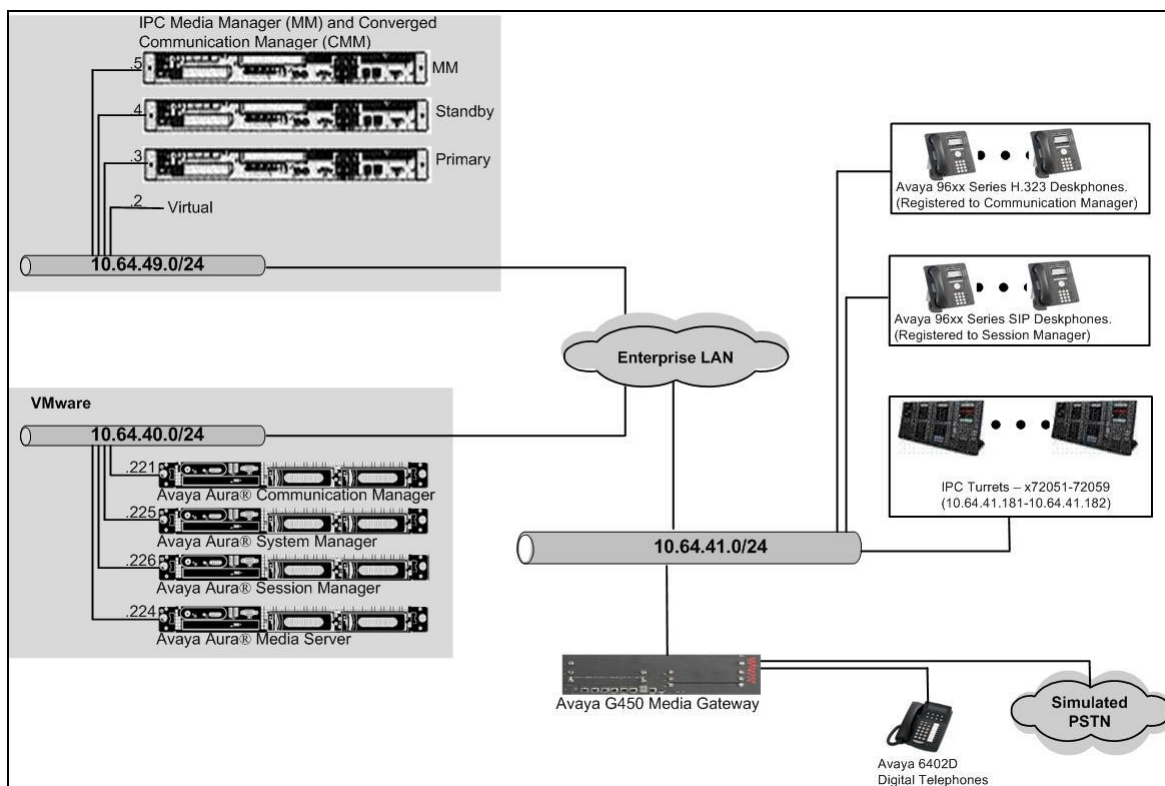


Figure 1: Test Configuration of IPC UnigyV3P2

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	R017x.00.0.441.0-22477
Avaya G450 Media Gateway	37.19
Avaya Aura® Media Server	7.7.0.226
Avaya Aura® Session Manager	7.0.0.0.700007
Avaya Aura® System Manager	7.0.0.0.3929
Avaya 96xx IP Deskphone (H.323)	
9621G	6.6
9650C	3.25
Avaya 96x1 IP Deskphone (SIP)	7.0.0.39
IPC UnigyV3P2	
• Media Manager	03.00.00.02.0006
• Converged Communication Manage	03.00.00.02.0006
• Turret	03.00.00.02.0006

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 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:** Enable or Disable the field by entering “y” or “n”.

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? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
	Alternate Route Timer(sec): 6	

5.4. 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 Type: sip          CDR Reports: y
Group Name: SM_41_42                                COR: 1                 TN: 1                 TAC: 1092
Direction: two-way                                Outgoing Display? y
Dial Access? n                                     Night Service:
Queue Length: 0
Service Type: tie                                   Auth Code? n
                                                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	

5.5. 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 UnigyV3P2.

```
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
UDP Port Min: 16390   IP Audio Hairpinning? n
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 UnigyV3P2 supports G.711 and G.729. For G.729, IPC needs to install a license.

```
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			
								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 Req'd		
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				Outgoing
Len Prefix	Number	Trk			Number
	Format	Grp(s)	Delete	Insert	Format
5	7205	80		303xxxxyyy	pub-unk

6. Configure Avaya Aura® Session Manager

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

- Administer locations
- 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.

AVAYA
Aura® System Manager 7.0

Recommended access to System Manager is via FQDN.
[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

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

Internet Explorer 11 is not using the compatibility view to display the System Manager Web pages. To prevent undesirable effects, enable the compatibility view. For information about how to enable the compatibility view, see the related documentation details.

User ID:

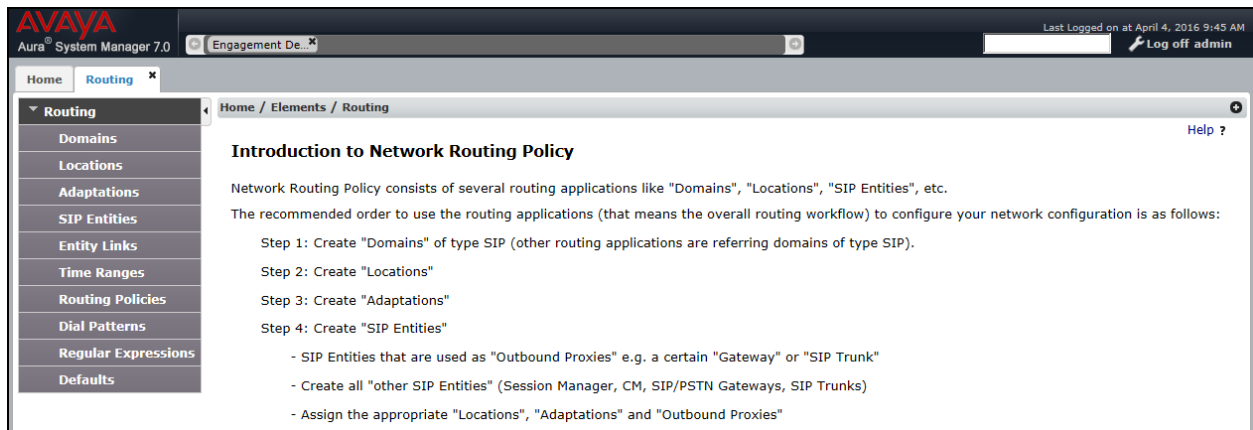
Password:

[Change Password](#)

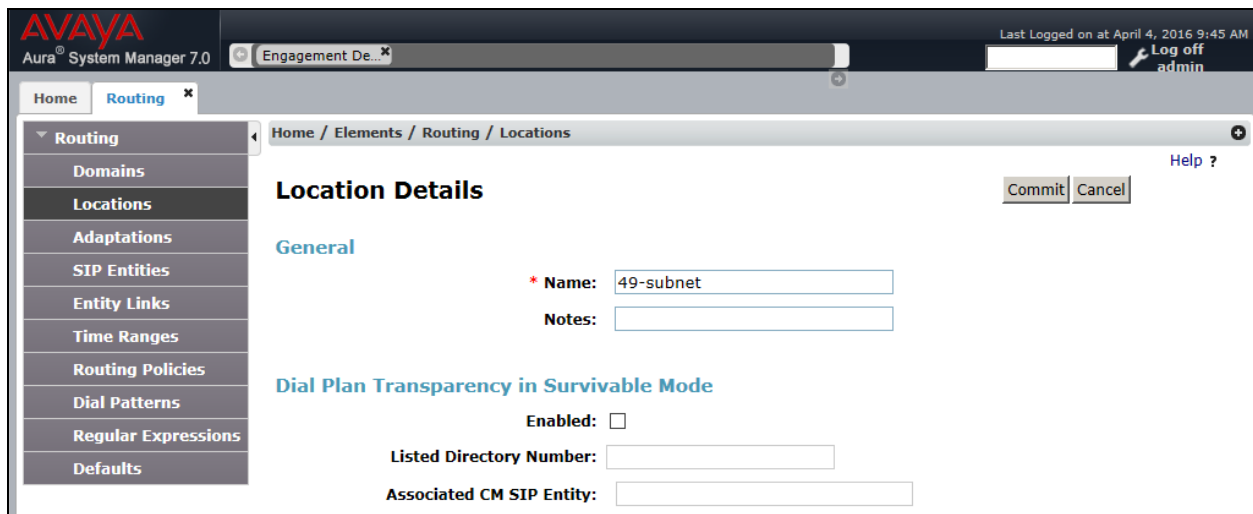
Supported Browsers: Internet Explorer 9.x, 10.x or 11.x or Firefox 36.0, 37.0 and 38.0.

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 **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.



6.3. Administer SIP Entities

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

6.3.1. 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.

The screenshot shows the Avaya Aura System Manager 7.0 interface. The top navigation bar includes the Avaya logo, 'Aura System Manager 7.0', a search bar, and a 'Log off admin' button. The left sidebar shows a tree view with 'Routing' expanded and 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and contains a 'General' tab. The form fields are as follows:

Field	Value
Name	Unigy-IPC
FQDN or IP Address	10.64.49.2
Type	Other
Notes	
Adaptation	
Location	49-subnet
Time Zone	America/Denver
SIP Timer B/F (in seconds)	4
Credential name	
Securable	<input type="checkbox"/>
Call Detail Recording	none
CommProfile Type Preference	

6.3.2. 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
Aura® System Manager 7.0

Engagement ...

Last Logged on at April 13, 2016 1:25 PM
Log off
admin

Home Routing

Home / Elements / Routing / SIP Entities

SIP Entity Details Commit Cancel

General

* Name: CM7.x

* FQDN or IP Address: 10.64.40.221

Type: CM

Notes: Avaya 7.x Communication Manag

Adaptation:

Location: 40-subnet

Time Zone: America/Denver

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

Credential name:

Securable: ☐

Call Detail Recording: both

Loop Detection

Loop Detection Mode: On

Loop Count Threshold: 5

Loop Detection Interval (in msec): 200

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

6.4. Administer Entity Links

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

6.4.1. 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 6.3.1**.
- **Port:** “5060”
- **Connection Policy:** “Trusted”

Avaya Aura System Manager 7.0

Home / Elements / Routing / Entity Links

Entity Links

Commit Cancel

1 Item Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy
<input type="checkbox"/>	* SM70Unigy-UDP	* SM7.x	UDP	* 5060	* Unigy-IPC	<input type="checkbox"/>	* 5060	trusted

Select : All, None

Commit Cancel

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

The screenshot shows the Avaya Aura System Manager 7.0 interface. The left sidebar contains a navigation menu with options: Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links (selected), Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Entity Links' and shows a table with one item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, DNS Override, Port, and Connection Policy. The item shows a link between *SM70Unigy-TCP and *Q Unigy-IPC using the TCP protocol on port 5060, with a trusted connection policy. There are 'Commit' and 'Cancel' buttons at the top and bottom of the table.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy
*SM70Unigy-TCP	*Q SM7.x	TCP	5060	*Q Unigy-IPC		5060	trusted

6.4.2. 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 “SM7.x”.
- **Protocol:** The protocol used between Communication Manager and Session Manager is “TLS”.
- **Port:** Enter an appropriate port used, in this case “5061”.
- **SIP Entity 2:** The Communication Manager entity name from **Section 6.3.2**.
- **Port:** Enter an appropriate port used, in this case “5061”.
- **Connection Policy:** **Trusted**

The screenshot displays the Avaya Aura System Manager 7.0 interface. The left navigation pane shows the 'Routing' menu expanded, with 'Entity Links' selected. The main content area is titled 'Entity Links' and contains a table with one item. The table columns are: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, DNS Override, Port, and Connection Policy. The item in the table is 'SM70CM70-TLS', linking 'SM7.x' to 'CM7.x' via 'TLS' on port '5061' with a 'trusted' connection policy. The page includes 'Commit' and 'Cancel' buttons at the top right and bottom right.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy
* SM70CM70-TLS	* SM7.x	TLS	* 5061	* CM7.x	<input type="checkbox"/>	* 5061	trusted

6.5. Administer Routing Policies

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

6.5.1. 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 6.3.1** in the listing (not shown).

Retain the default values in the remaining fields.

AVAYA
Aura® System Manager 7.0

Home / Elements / Routing / Routing Policies

Routing Policy Details [Commit] [Cancel] [Help ?]

General

* Name: Route2Unigy

Disabled: ☐

* Retries: 0

Notes: Route to Unigy

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Unigy-IPC	10.64.49.2	Session Manager	IPC Unigy system 3.0

Time of Day

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

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

6.5.2. 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 6.3.2** in the listing (not shown).

Retain the default values in the remaining fields.

AVAYA
Aura® System Manager 7.0

Engagement... x

Last Logged on at April 6, 2016 9:33 AM
Log off admin

Home Routing x

Home / Elements / Routing / Routing Policies

Routing Policy Details

Commit Cancel

Help ?

General

* Name: Route2CM70

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
CM7.x	10.64.40.221	CM	Avaya 7.x Communication Manager

Time of Day

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<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. Administer Dial Patterns

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

6.6.1. 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 6.5.1** was selected as shown below.

The screenshot displays the Avaya Aura System Manager 7.0 interface. The top navigation bar shows 'Home' and 'Routing'. The left sidebar lists various configuration options, with 'Dial Patterns' selected. The main content area is titled 'Dial Pattern Details' and includes a 'General' sub-section. The 'General' section contains the following fields:

- Pattern:** 7205
- Min:** 5
- Max:** 5
- Emergency Call:** ☐
- Emergency Priority:** 1
- Emergency Type:** (empty)
- SIP Domain:** -ALL- (selected from a dropdown)
- Notes:** (empty)

Below the 'General' section is the 'Originating Locations and Routing Policies' sub-section. It features an 'Add' button and a table with one item:

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/> -ALL-		Route2Unigy	0	<input type="checkbox"/>	Unigy-IPC	Route to Unigy

At the bottom of the table, there is a 'Select : All, None' option.

6.6.2. 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 all locations, and the Communication Manager routing policy from **Section 6.5.2** was selected as shown below. Retain the default values in the remaining fields.

AVAYA
Aura® System Manager 7.0

Engagement... Last Logged on at April 6, 2016 9:33 AM Log off admin

Home Routing

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

Commit Cancel

Help ?

General

* Pattern: 7200

* Min: 5

* Max: 5

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL- ▼

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item 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-		Route2CM70	0	<input type="checkbox"/>	CM7.x	

Select : All, None

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

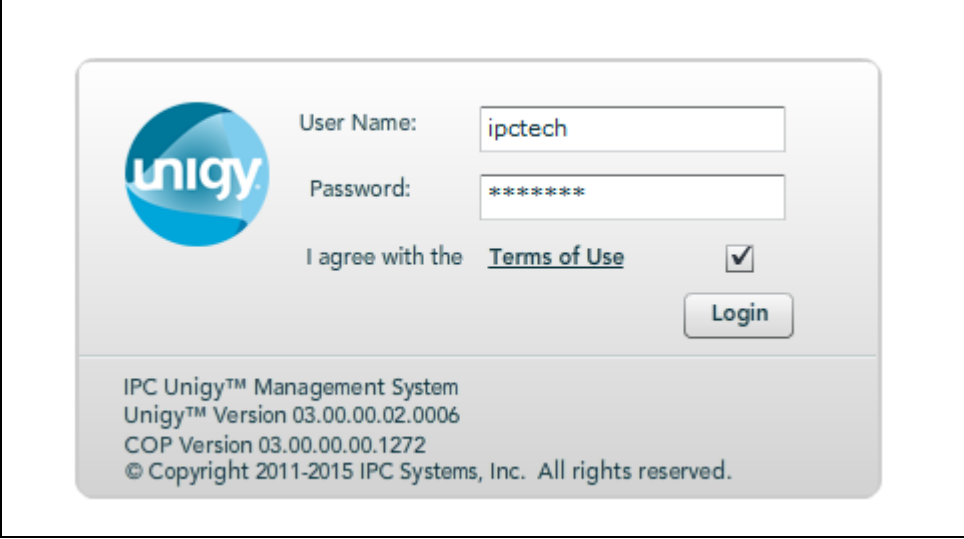
The installation/configuration of Media Manager and/or Converged Communication Manager is typically performed by IPC installation engineers. The procedural steps are presented in these Application Notes for informational purposes.

7.1. Launch Unigy Management System

Access the UnigyV3P2 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 screenshot shows the Unigy Management System login page. On the left is the Unigy logo. To its right are two input fields: 'User Name:' with the value 'ipctech' and 'Password:' with masked characters '*****'. Below these is a checkbox labeled 'I agree with the' followed by a link 'Terms of Use' and a checked checkbox. A 'Login' button is positioned to the right of the checkbox. At the bottom, a footer contains the text: 'IPC Unigy™ Management System', 'Unigy™ Version 03.00.00.02.0006', 'COP Version 03.00.00.00.1272', and '© Copyright 2011-2015 IPC Systems, Inc. All rights reserved.'

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

Configuration | System Designer | Alerts | Tools | About | Help 11:51 EDT-0400 | ipctech

Enterprise
Sites
Users
Configuration Groups
Roles

Tools -> Monitoring

Summary Backroom Portal Zones

Instances

View All

Instance	Total Devices	Device Alerts High	Device Alerts
Default Instance	7	3	2


Locations

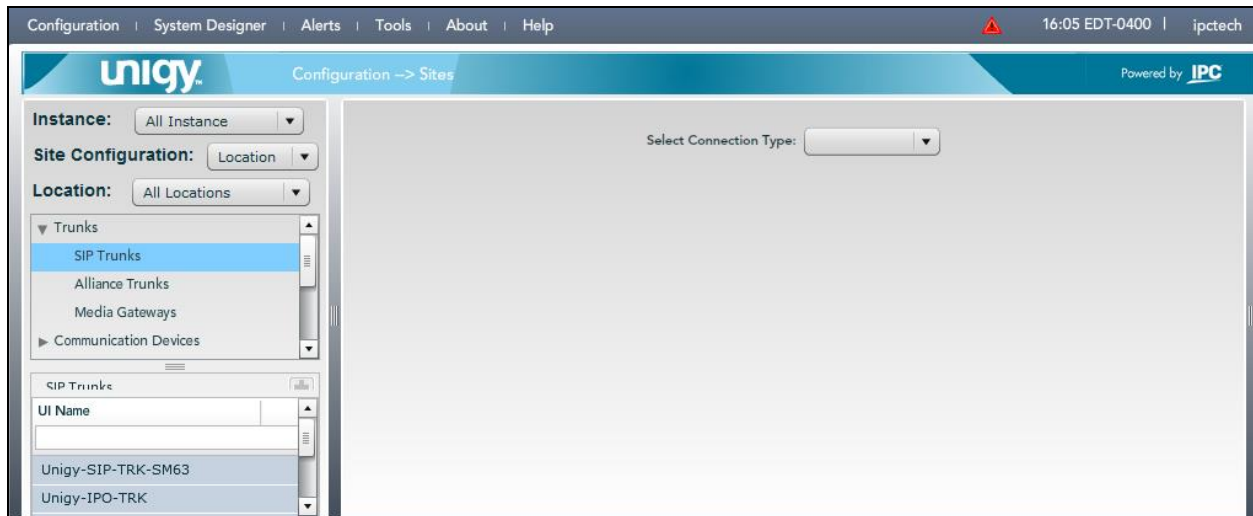
Location	Instance	Total Devices	Device Alerts High
Default Back Room	Default Instance	4	3
Default Front Room	Default Instance	3	0

Alerts

Ack	Clear Pending	Time	Alert Name	Severity	Count	Device Name	Device Type	Inst
<input type="checkbox"/>	<input type="checkbox"/>	03-22-2016 06	CCM-Hardware-137615-Pc	SEV1PLUS	4	ccm-2	CCM-Hardwar	De
<input type="checkbox"/>	<input type="checkbox"/>	03-22-2016 06	APP-DS-ds_ha-140025-sta	SEV1	1	ccm-2	SERVER	De
<input type="checkbox"/>	<input type="checkbox"/>	03-24-2016 10	APP-DS-ds_ha-140025-sta	SEV1	2	ccm-1	SERVER	De
<input type="checkbox"/>	<input type="checkbox"/>	03-24-2016 10	Turret-IQ/MAX-101040-co	SEV1	3	10500E0A7069	TURRET	De
<input type="checkbox"/>	<input type="checkbox"/>	03-22-2016 05	MediaGateway-Media Gate	SEV1	4	MG1Z1	MEDIA_GATEV	De

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.



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 6.4.1**.
- **Zone:** An available zone, in this case “Default Zone 1”.
- **Channels:** The number of SIP trunk group members.
- **Reason Protocol:** “SIP”
- **PBX Provider:** “Avaya”
- **Connected Party Update:** “UPDATE”

Retain the default values in the remaining fields.

The screenshot displays the Unigy Configuration web interface. The top navigation bar includes links for Configuration, System Designer, Alerts, Tools, About, and Help. The main header shows 'Configuration -> Sites' and 'Powered by IP'. The left sidebar contains a tree view with categories like Trunks, SIP Trunks, Alliance Trunks, Media Gateways, Communication Devices, Servers, Media Service, Prototype Devices, SNMP Forwarding, and Routing. The 'SIP Trunks' section is expanded, showing a list of trunks: Unigy-SIP-TRK-SM63, Unigy-IPO-TRK, Unigy-SIP-TRK-SM62, and Unigy-SIP-Trk-SM70 (highlighted in orange). The main content area is titled 'Trunk: Unigy-SIP-Trk-SM70' and features a 'Basic' tab. The 'Dial Tone Trunk Configuration' section contains the following fields and values:

Field	Value
Trunk Name	Unigy-SIP-Trk-SM70
Connection Type	Dial Tone
Destination Address	10.64.40.226
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 of the configuration area 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 web interface. The top navigation bar includes links for Configuration, System Designer, Alerts, Tools, About, and Help. The main header displays the Unigy logo and the current configuration path: Configuration --> Sites. The sidebar on the left contains a tree view of configuration categories, with 'SIP Trunks' selected. The main configuration area is titled 'Trunk: Unigy-SIP-Trk-SM70' and has two tabs: 'Basic' and 'Advanced'. The 'Advanced' tab is active, showing the 'Dial Tone Trunk Configuration' section. The configuration fields are as follows:

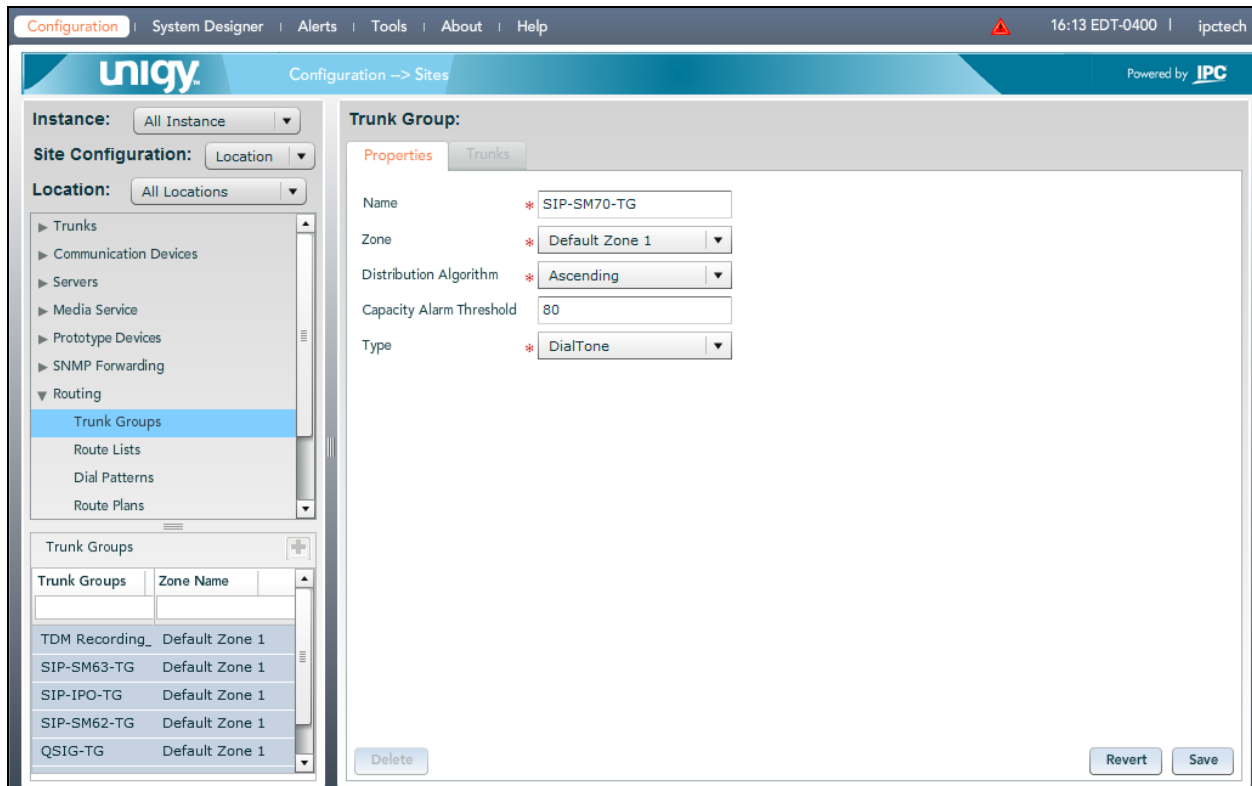
Field	Value
Trunk Name	Unigy-SIP-Trk-SM70
Connection Type	Dial Tone
Destination Address	10.64.40.226
Destination Port	5060
Media Manager Profile	Safe
Zone	Default Zone 1
Channels	30
Reason Protocol	SIP
PBX Provider	Avaya
Connected Party Update	UPDATE
Subscribe to MWI	<input checked="" type="checkbox"/>
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 type="checkbox"/>
Outgoing Transport Type	UDP
ReINVITE For Media Update	<input checked="" type="checkbox"/>
Options Supported	<input checked="" type="checkbox"/>
Equipped	<input checked="" type="checkbox"/>

At the bottom of the configuration area, there are three buttons: Delete, Revert, and Save.

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**. Select the **Trunks** tab in the right pane.




The screenshot shows the UniV3P2-SM70-S Configuration interface. The left pane displays the navigation tree with 'Trunk Groups' selected under 'Routing'. The right pane shows the 'Trunk Group: Properties' configuration screen. The 'Name' field is set to 'SIP-SM70-TG', 'Zone' is 'Default Zone 1', 'Distribution Algorithm' is 'Ascending', 'Capacity Alarm Threshold' is '80', and 'Type' is 'DialTone'. A table at the bottom left lists existing trunk groups, and buttons for 'Delete', 'Revert', and 'Save' are at the bottom right.

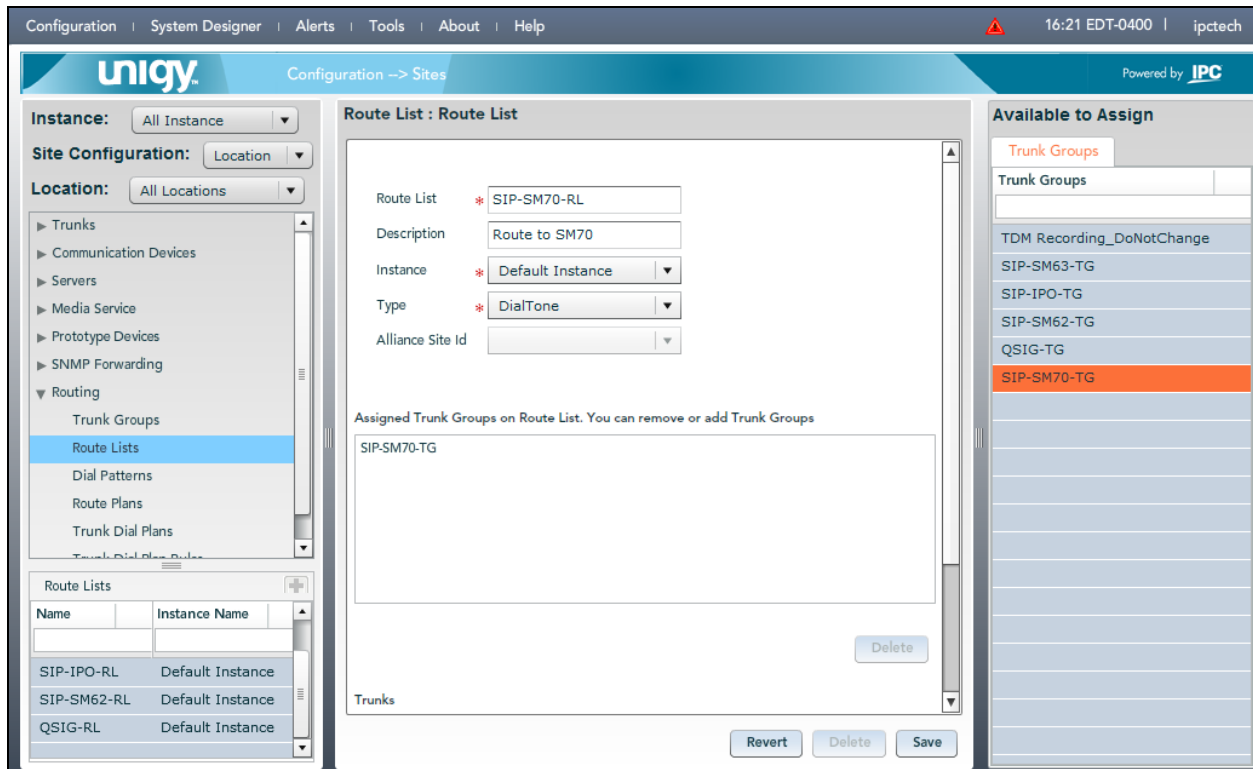
Trunk Groups	Zone Name
TDM Recording_	Default Zone 1
SIP-SM63-TG	Default Zone 1
SIP-IPO-TG	Default Zone 1
SIP-SM62-TG	Default Zone 1
QSIG-TG	Default Zone 1

[illegible]

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**.



The screenshot shows the UniQy Configuration interface. The top navigation bar includes links for Configuration, System Designer, Alerts, Tools, About, and Help. The main header displays the UniQy logo, the current path 'Configuration --> Sites', and the text 'Powered by IPC'. The interface is divided into three main panes:

- Left Pane:** Contains a tree view of configuration categories. Under 'Routing', 'Route Lists' is selected and highlighted in blue. Below the tree is a table titled 'Route Lists' with columns 'Name' and 'Instance Name'. It lists three entries: 'SIP-IPO-RL' (Default Instance), 'SIP-SM62-RL' (Default Instance), and 'QSIG-RL' (Default Instance). At the bottom of this pane is an 'Add' icon (a square with a plus sign).
- Middle Pane:** Titled 'Route List : Route List', it contains a form for configuring a route list. The fields are: 'Route List' (text input with value 'SIP-SM70-RL'), 'Description' (text input with value 'Route to SM70'), 'Instance' (dropdown menu with 'Default Instance' selected), 'Type' (dropdown menu with 'DialTone' selected), and 'Alliance Site Id' (text input). Below the form is a section titled 'Assigned Trunk Groups on Route List. You can remove or add Trunk Groups'. It contains a list box with 'SIP-SM70-TG' and a 'Delete' button. At the bottom of the middle pane are 'Revert', 'Delete', and 'Save' buttons.
- Right Pane:** Titled 'Available to Assign', it contains a list of trunk groups. The first group is 'Trunk Groups' (highlighted in orange). Below it are several other groups: 'TDM Recording_DoNotChange', 'SIP-SM63-TG', 'SIP-IPO-TG', 'SIP-SM62-TG', 'QSIG-TG', and 'SIP-SM70-TG' (highlighted in orange).

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. The main header displays the UniQy logo, the path Configuration → Sites, and the text "Powered by IPC".

On the left sidebar, the "Routing" section is expanded, showing options like Trunk Groups, Route Lists, **Dial Patterns** (selected), Route Plans, Trunk Dial Plans, and Trunk Dial Plan Rules.

The main content area is divided into two sections:

- Dial Patterns**: A table with columns for Name, Pattern String, Description, and Zone Name. It contains one entry: "ALL Dial Pattern" with a "*" pattern string, "all" description, and "Default Zone 1". Buttons for "Add New" and "Delete" are at the bottom right of the table.
- Dial pattern Details**: A sub-section with a "Properties" tab. It contains four fields, each marked with a red asterisk: "Name" (ALL Dial Pattern), "Zone" (Default Zone 1), "Description" (all), and "Pattern String" (*). "Revert" and "Save" buttons are at the bottom right.

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 UnigyV3P2. For **Destination** select the dial pattern for Avaya endpoints from **Section 7.5**. Select “Forward” for **Action**, and click **Save**.

The screenshot displays the Unigy Configuration web interface. The top navigation bar includes links for Configuration, System Designer, Alerts, Tools, About, and Help, along with a status bar showing the time (16:30 EDT-0400) and the user (ipctech). The main interface is divided into three panes:

- Left Pane:** A navigation tree under the 'Routing' section. The 'Route Plans' option is highlighted. Other options include Trunks, Communication Devices, Servers, Media Service, Prototype Devices, SNMP Forwarding, Trunk Groups, Route Lists, Dial Patterns, Trunk Dial Plans, and Trunk Dial Plan Rules.
- Center Pane:** Titled 'Route Plan', it contains a 'Create New Route Plan' form. The fields are as follows:
 - UI Name:** * Route-2-SM70
 - Description:** (empty)
 - Calling Party:** *
 - Destination:** *
 - Action:** * Forward (selected from a dropdown)
 - Instance:** * Default Instance (selected from a dropdown)
 - Route List:** (empty table with a 'Remove' button below it)
- Right Pane:** Titled 'Available to Assign', it shows a list of route lists. The 'Route Lists' tab is active, displaying a table with the following entries:

Name
TDM Recording_DoNotChange
SIP-SM70-RL
SIP-IPO-RL
SIP-SM62-RL
QSIG-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 UniQy Configuration -> Sites interface. The left sidebar contains a tree view with the following categories: Trunks, Communication Devices, Servers, Media Service, Prototype Devices, SNMP Forwarding, and Routing. The Routing category is expanded, showing Trunk Groups, Route Lists, Dial Patterns, Route Plans (selected), Trunk Dial Plans, and Trunk Dial Plan Rules.

The main content area is titled "Route Plan" and contains a table of route plans. The table has the following columns: UI Name, Calling Party, Destination, Action, and Instance Name. The table lists several route plans, with "Route-2-SM70" selected.

UI Name	Calling Party	Destination	Action	Instance Name
Route-2-SM70	*	*	FORWARD	Default Instance
Route-2-IPO	*	*	FORWARD	Default Instance
Route2SM63	*	*	FORWARD	Default Instance
QSIG2CM63	*	*	FORWARD	Default Instance
QSIG2CM601	*	*	FORWARD	Default Instance
Route2SM62	*	*	FORWARD	Default Instance
Route-2-IPO 2	*	*	FORWARD	Default Instance

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

The "Route Plan Details" section shows the configuration for the selected route plan. It includes fields for "Calling Party" (set to *), "Destination" (set to *), "Action" (set to FORWARD), and "RouteList" (set to SIP-SM70-RL). The "Trunk Group" field is set to SIP-SM70-TG. An "Edit" button is located at the bottom right of the details section.

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**.

Configuration | System Designer | Alerts | Tools | About | Help 16:35 EDT-0400 | ipctech

Configuration -> Sites Powered by IPC

Instance: All Instance Site Configuration: Location Location: All Locations

Trunks
Communication Devices
Servers
Media Service
Prototype Devices
SNMP Forwarding
Routing
Trunk Groups
Route Lists
Dial Patterns
Route Plans
Trunk Dial Plans
Trunk Dial Plan Rules

Route Plan

Create New Route Plan

UI Name * Route-2-SM70
Description
Calling Party * *
Destination * *
Action * Forward
Route List: SIP-SM70-RL
Remove
Back Revert Save

Available to Assign
Route Lists
Name
TDM Recording_DoNotChange
SIP-SM70-RL
SIP-IPO-RL
SIP-SM62-RL
QSIG-RL

In the Route Plan page, verify the route plan that utilizes during the compliance test is at the top of the route plan list.

Configuration | System Designer | Alerts | Tools | About | Help 12:55 EDT-0400 | ipctech

Configuration -> Sites Powered by IPC

Instance: All Instance Site Configuration: Location Location: All Locations

Trunks
Communication Devices
Servers
Media Service
Prototype Devices
SNMP Forwarding
Routing
Trunk Groups
Route Lists
Dial Patterns
Route Plans

Route Plan

List of Route Plans

UI Name	Calling Party	Destination	Action	Instance Name
Route-2-SM70	*	*	FORWARD	Default Instance
Route-2-IPO	*	*	FORWARD	Default Instance
Route2SM63	*	*	FORWARD	Default Instance
QSIG2CM63	*	*	FORWARD	Default Instance
QSIG2CM601	*	*	FORWARD	Default Instance
Route2SM62	*	*	FORWARD	Default Instance
Route-2-IPO 2	*	*	FORWARD	Default Instance

8. Verification Steps

This section provides tests that can be performed to verify proper configuration of Communication Manager, Session Manager, and IPC UnigyV3P2.

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 6.3.1**.

The screenshot displays the Avaya Aura System Manager 7.0 web interface. The top navigation bar includes the Avaya logo, version information, and a user session summary (Last Logged on at April 6, 2016 9:33 AM, Log off admin). The left sidebar contains a tree view with categories like Session Manager, Network Configuration, Device and Location Configuration, Application Configuration, System Status, and System Tools. The 'System Status' category is expanded, showing 'SIP Entity Monitoring' as the selected option.

The main content area is titled 'SIP Entity Link Monitoring Status Summary'. It includes a sub-header 'SIP Entities Status for All Monitoring Session Manager Instances' and a 'Run Monitor' button. Below this is a table with 1 item, filtered by 'Enable'. The table has columns for Session Manager, Type, and Monitored Entities (Down, Partially Up, Up, Not Monitored, Deny, Total).

Session Manager	Type	Monitored Entities					Total
		Down	Partially Up	Up	Not Monitored	Deny	
SM7.x	Core	5	0	7	0	0	12

Below the table, there is a 'Select: All, None' option. Further down, the 'All Monitored SIP Entities' section is visible, featuring another 'Run Monitor' button and a list of 12 items, filtered by 'Enable'. The list includes SIP Entity Names: [IPOSE](#), [CM-601](#), [CI-eONE](#), and [Uniqy-IPC](#).

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 7.0

Engagement... Last Logged on at April 6, 2016 9:33 AM Log off admin

Home Routing Session Manager

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

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: Unigy-IPC

Summary View

Status Details for the selected Session Manager:

2 Items Refresh Filter: Enable

	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	SM7.x	10.64.49.2	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	SM7.x	10.64.49.2	5060	UDP	FALSE	UP	200 OK	UP

8.3. Verify IPC UnigyV3P2

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 UnigyV3P2 to successfully interoperate with Avaya Aura® Session Manager 7.0 and Avaya Aura® Communication Manager 7.0 via Avaya Aura® Session Manager. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

10. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Document 03-300509, Release 7.0, August 2015, available at <http://support.avaya.com>.
2. *Administering Avaya Aura® System Manage for Release 7.0*, , Issue 1, January 2016, available at <http://support.avaya.com>
3. *UnigyV3P2 1.1 System Configuration*, Part Number B02200187, Release 00, upon request to IPC Support.

©2016 Avaya Inc. All Rights Reserved.

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

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