



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Lane Telecommunications Passport 4000 Fax Server with Avaya Aura™ Session Manager and Avaya Aura™ Communication Manager - Issue 1.0

Abstract

These Application Notes describe the procedure to configure Avaya Aura™ Session Manager and Avaya Aura™ Communication Manager to work with Lane Telecommunications Passport 4000 Fax over IP solution using SIP (Session Initiation Protocol) connectivity.

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 present a sample configuration for a network that uses Lane Telecommunications Passport 4000 Fax Server through a SIP infrastructure consisting of Avaya Aura™ Session Manager and Avaya Aura™ Communication Manager. Lane Telecommunications Passport 4000 Fax Server provides a consolidated fax solution which improves productivity by integrating fax, email, telex, and SMS messaging systems. Passport 4000 Fax Server can reduce costs by consolidating communications into a single data network and takes advantage of new communications technologies such as Fax over IP (FoIP). Passport 4000 Fax Server is based on the Dialogic/Brooktrout SR140 Sip Stack. This solution allows Lane Telecommunications Passport 4000 Fax Server to send and receive faxes from a local Fax machine connected to Avaya Aura™ Communication Manager and the PSTN using SIP Trunks. In this configuration, the Passport 4000 Fax Server connects to telephony systems through SIP trunks on Avaya Aura™ Session Manager.

1.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. The feature testing focused on verifying the proper transmission, collection and reporting of fax by Passport 400 Fax Server. Tests were executed on bidirectional fax transmission between PSTN Fax or Communication Manager and Passport 4000 Fax Server, codec support and negotiation and reporting. The serviceability testing focused on verifying the ability of the Passport 4000 Fax Server to recover from adverse conditions, such as network failures.

1.2. Support

Technical Support on Lane Telecommunications Passport 4000 Fax Server can be obtained through the following phone contacts:

- Head Quarters United Kingdom EMEA region +44 1256 301550
- Americas Regional Office +1 973 526 2979
- Asia Pacific Regional Office +65 6353 0555

2. Reference Configuration

As shown in **Figure 1**, the Lane Telecommunications Passport 4000 Fax Server uses SIP trunking for call signaling. Session Manager using its SM-100 (Security Module) network interface, routes the calls between the different entities using SIP Trunks. All inter-system calls are carried over these SIP trunks. Session Manager supports flexible inter-system call routing based on the dialed number, the calling number and the system location; it can also provide protocol adaptation to allow multi-vendor systems to interoperate. Session Manager is managed by System Manager via the management network interface.

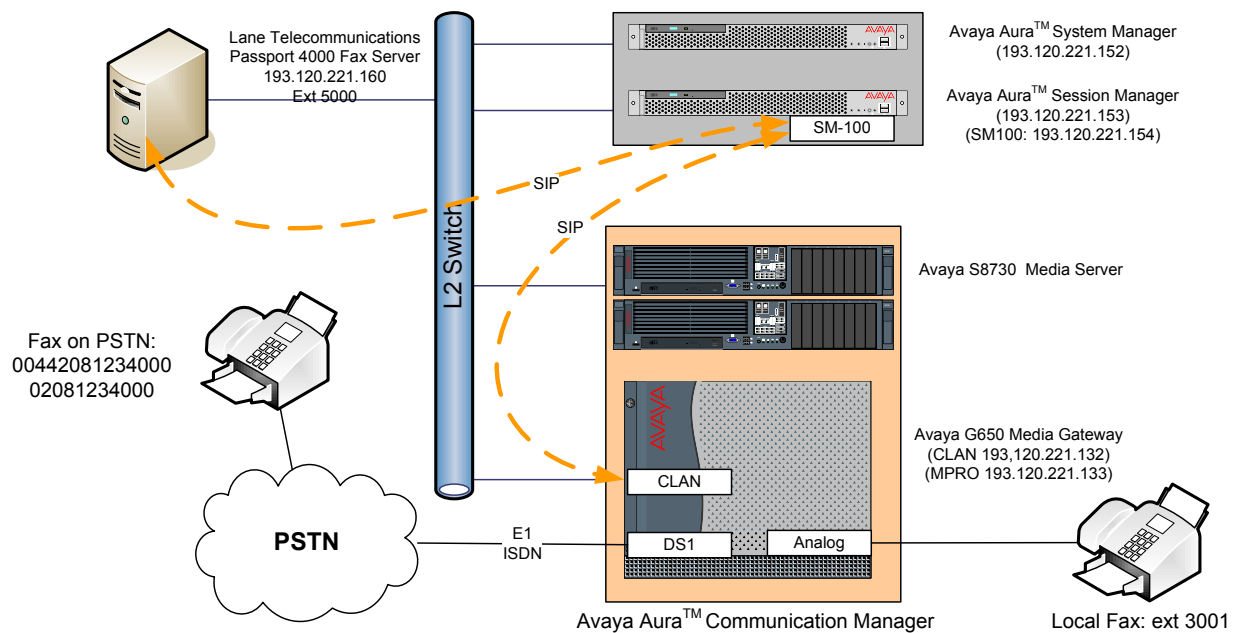


Figure 1 – Test Configuration of Passport 4000 Fax Server, Avaya Aura™ Communication Manager and Avaya Aura™ Session Manager

For the sample configuration shown in **Figure 1**, Session Manager run on an Avaya S8510 Server, Communication Manager 5.2 runs on an Avaya S8730 Server with an Avaya G650 Media Gateway, and Passport 4000 Fax Server runs on a personal computer equipped with Windows Operating System. The results in these Application Notes are applicable to other Communication Manager Server and Media Gateway combinations. These Application Notes will focus on the configuration of the SIP trunks and call routing. Detailed administration of the endpoint telephones or the PSTN interface will not be described. Refer to the appropriate documentation in **References [1] and [2]** for more details.

3. Equipment and Software Validated

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

Product / Hardware Platform	Software Version
Avaya Aura™ System Manager on S8510 Server	Avaya Aura™ System Manager 5.2 Service Pack 1 Patch 2 - 5.2.0.7.11
Avaya Aura™ Session Manager on S8510 Server	Avaya Aura™ Session Manager 5.2 Service Pack 1 Patch 2 - 5.2.0.1.520017
Avaya Aura™ Communication Manager on S8730 Servers	Avaya Aura™ Communication Manager 5.2.1 – S8730-15-02.1.016.4
AvayaG650 Media Gateway IPSI (TN2312BP) C-LAN (TN799DP) IP Media Resource 320 (TN2602AP) DS1 Interface (TN2464BP) Analog Line (TN2793B)	HW28 FW049 HW16 FW034 HW08 FW051 HW02 FW019 HW00005
Lane Telecommunications Passport 4000 Fax Server	Passport4000MessageServerManagement_2.1.3561.0 Passport4000MessageServer_2.1.3561.0 Passport4000FaxServiceManagement_2.1.3384.0 Passport4000FaxService6.2_2.1.3671
Dialogic Brooktrout SDK	6.2.2
Dialogic SR140 Sip Stack brktsip.dll	6.2.0.5
Analog Fax Device form Canon	FAX-JX500

4. Configure Avaya Aura™ Communication Manager

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

- Verify Avaya Aura™ Communication Manager License.
- Configure IP Node Names.
- Verify/List IP Interfaces.
- Configure IP Codec Set.
- Configure IP Network Region.
- Administer SIP Trunks with Session Manager.
- Configure Route Pattern.
- Configure Location and Public Unknown Numbering.
- Administer AAR Analysis.
- Save Translations.

Throughout this section the administration of Communication Manager is performed using a System Access Terminal (SAT), the following commands are entered on the system with the appropriate administrative permissions. Some administration screens have been abbreviated for clarity. These instructions assume that the Communication Manager has been installed, configured, licensed and provided with a functional dial plan. Refer to the appropriate documentation as described in **Reference [1]** and **[2]** for more details. In these Application Notes Communication Manager was configured with 4 digit extension **30xx** for stations (and analog line fax) while Passport 4000 Fax Server as **5000** reachable with **aar** table. Diaplan analysis can be verified with the **display dialplan analysis** command.

display dialplan analysis							Page 1 of 12		
DIAL PLAN ANALYSIS TABLE									
Location: all							Percent Full: 1		
Dialed	Total	Call	Dialed	Total	Call	Dialed	Total	Call	
String	Length	Type	String	Length	Type	String	Length	Type	
30	4	ext							
50	4	aar							
8	3	dac							
9	1	fac							

Other numbers on PSTN are reachable via **ars** table with the use of **feature access code 9**. The configuration of the PSTN side is not detailed as it is service provider dependent. Refer to **[1]** to configure the incoming ISDN trunk and the digit manipulations according to the numbering offered by the service provider.

4.1. Verify Avaya Aura™ Communication Manager License

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 difference between the two values needs to be greater than or equal to the desired number of simultaneous SIP trunk connections. Verify highlighted value, as shown below.

display system-parameters customer-options		Page	2 of	10
OPTIONAL FEATURES				
IP PORT CAPACITIES		USED		
Maximum Administered H.323 Trunks:		100	0	
Maximum Concurrently Registered IP Stations:		18000	2	
Maximum Administered Remote Office Trunks:		0	0	
Maximum Concurrently Registered Remote Office Stations:		0	0	
Maximum Concurrently Registered IP eCons:		0	0	
Max Concur Registered Unauthenticated H.323 Stations:		100	0	
Maximum Video Capable Stations:		100	0	
Maximum Video Capable IP Softphones:		100	9	
Maximum Administered SIP Trunks:		1000	300	

If there is insufficient capacity of SIP Trunks or a required feature is not enabled, contact an authorized Avaya sales representative to make the appropriate changes.

4.2. Configure IP Node Names

As SIP interaction with Session Manager is carried through the security module SM100 IP interface, in configuring the SIP Trunk refer to its IP address. Use the **change node-names ip** command to add the **Name** and **IP Address** for the Session Manager, in the example **SM100** and **193.120.221.154** was used.

change node-names ip		Page	1 of	2
IP NODE NAMES				
Name	IP Address			
Gateway001	193.120.221.129			
SM100	193.120.221.154			
clan	193.120.221.132			
default	0.0.0.0			
mpro	193.120.221.133			
procr	0.0.0.0			

Note: In the example some other values (CLAN, MedPro) have been already created as per installation and configuration of Communication Manager.

4.3. Verify/List IP Interfaces

Use the **list ip-interface all** command and note the **C-LAN** to be used for SIP trunks between the Communication Manager and the Session Manager.

list ip-interface all									
IP INTERFACES									
ON	Type	Slot	Code/Sfx	Node Name/ IP-Address	Mask	Gateway	Node	Net Rgn	VLAN
y	C-LAN	01A02	TN799 D	clan 193.120.221.132	/25	Gateway001		1	n
y	MEDPRO	01A03	TN2602	mpro 193.120.221.133	/25	Gateway001		1	n

4.4. Configure IP Codec Set

Use the **change ip-codec-set n** command where **n** is codec set used in the configuration. The Passport 4000 Fax Server supports both G.711A and G.711MU:

- **Audio Codec:** Set to the desired codec (i.e. G711A).

Retain the default values for the remaining fields.

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.711A	n	2	20		
2: G.711MU	n	2	20		
3:					

Navigate to **Page 2**; ensure that **FAX** has **Mode** set to **t.38-standard**. Submit these changes.

change ip-codec-set 1			Page	2 of	2
IP Codec Set					
Allow Direct-IP Multimedia? n					
	Mode	Redundancy			
FAX	t.38-standard	0			
Modem	off	0			
TDD/TTY	US	3			
Clear-channel	n	0			

4.5. Configure IP Network Region

Use the **change ip-network-region n** command where **n** is the number of the network region used. Set the **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** fields to **yes**. For the **Codec Set**, enter the corresponding audio codec set configured in **Section 4.4**. Set the **Authoritative Domain** to the SIP domain. Retain the default values for the remaining fields, and submit these changes.

Note: In the test configuration, **network region 1** was used. If a new network region is needed or an existing one is modified, ensure to configure it with the correct parameters.

change ip-network-region 1		Page 1 of 19
IP NETWORK REGION		
Region: 1		
Location: 1	Authoritative Domain: avaya.com	
Name: Test Lab		
MEDIA PARAMETERS		
Codec Set: 1	Intra-region IP-IP Direct Audio: yes	
	Inter-region IP-IP Direct Audio: yes	
UDP Port Min: 2048	IP Audio Hairpinning? n	
UDP Port Max: 3329		

4.6. Administer SIP Trunks with Avaya Aura™ Session Manager

Two SIP trunks are needed for the configuration presented in these notes: one for the inbound calls from Passport 4000 Fax Server and a second one outbound to the Fax Server, the outbound signaling group requires to have the IP address of the Passport 4000 Fax Server in **Far-end Domain** field. To administer a SIP Trunk on Communication Manger, two intermediate steps are required, creation of a signaling group and trunk group.

4.6.1. Add SIP Signaling Group (inbound calls)

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

- **Group Type:** sip
- **Transport Method:** tcp
- **Near-end Node Name:** C-LAN node name from **Section 4.2** (i.e., **clan**).
- **Far-end Node Name:** Session Manager node name from **Section 4.2** (i.e., **SM100**).
- **Near-end Listen Port:** 5061
- **Far-end Listen Port:** 5061
- **Far-end Domain:** Leave blank.
- **DTMF over IP:** rtp-payload

```
add signaling-group 2                                     Page 1 of 1
                                                         SIGNALING GROUP

Group Number: 2                      Group Type: sip
                                   Transport Method: tls

IMS Enabled? n
IP Video? n

Near-end Node Name: clan              Far-end Node Name: SM100
Near-end Listen Port: 5061            Far-end Listen Port: 5061
Far-end Domain:                      Far-end Network Region: 1

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? n                 IP Audio Hairpinning? n
H.323 Station Outgoing Direct Media? n Direct IP-IP Early Media? n
                                         Alternate Route Timer(sec): 6
```

4.6.2. Configure a SIP Trunk Group (inbound calls)

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

- **Group Type:** **sip**
- **Group Name:** A descriptive name (i.e., **to AuraSM**).
- **TAC:** An available trunk access code (i.e., **802**).
- **Service Type:** **tie**
- **Signaling Group:** Number of the signaling group added in **Section 4.6.1** (i.e. **2**).
- **Number of Members:** The number of SIP trunks to be allocated to calls routed to **Session Manager** (must be within the limits of the total trunks available from licensed verified in **Section 4.1**).

Note: The number of members determines how many simultaneous calls can be processed by the trunk through Session Manager.

add trunk-group 2		Page 1 of 21	
TRUNK GROUP			
Group Number: 2	Group Type: sip	CDR Reports: y	
Group Name: To AuraSM	COR: 1	TN: 1	TAC: 802
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
Service Type: tie	Auth Code? n		
Signaling Group: 2			
Number of Members: 30			

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

add trunk-group 2		Page 3 of 21	
TRUNK FEATURES			
ACA Assignment? n	Measured: none	Maintenance Tests? y	
Numbering Format: public			
UII Treatment: service-provider			
Replace Restricted Numbers? n			
Replace Unavailable Numbers? n			

4.6.3. Add SIP Signaling Group (outbound calls)

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

- **Group Type:** **sip**
- **Transport Method:** **tcp**
- **Near-end Node Name:** C-LAN node name from **Section 4.2** (i.e., **clan**).
- **Far-end Node Name:** Session Manager node name from **Section 4.2** (i.e., **SM100**).
- **Near-end Listen Port:** **5061**
- **Far-end Listen Port:** **5061**
- **Far-end Domain:** The IP address configured on Passport 4000 Fax Server in **Section 6.3** (i.e. **193.120.221.160**).
- **DTMF over IP:** **rtp-payload**

```
add signaling-group 3                                     Page 1 of 1
                                     SIGNALING GROUP

Group Number: 3                      Group Type: sip
                                     Transport Method: tls

IMS Enabled? n
IP Video? n

Near-end Node Name: clan              Far-end Node Name: SM100
Near-end Listen Port: 5061            Far-end Listen Port: 5061
Far-end Network Region: 1
Far-end Domain: 193.120.221.160

Incoming Dialog Loopbacks: eliminate Bypass If IP Threshold Exceeded? n
                                     RFC 3389 Comfort Noise? n
DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3   IP Audio Hairpinning? n
Enable Layer 3 Test? n               Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n Alternate Route Timer(sec): 6
```

4.6.4. Configure a SIP Trunk Group (outbound calls)

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

- **Group Type:** sip
- **Group Name:** A descriptive name (i.e., to **AuraSM**).
- **TAC:** An available trunk access code (i.e., **803**).
- **Service Type:** tie
- **Signaling Group:** The number of the signaling for outbound calls (i.e. **3**).
- **Number of Members:** The number of SIP trunks to be allocated to calls routed to **Session Manager** (must be within the limits of the total **trunks available** from licensed verified in **Section 4.1**).

add trunk-group 3		Page 1 of 21	
TRUNK GROUP			
Group Number: 3	Group Type: sip	CDR Reports: y	
Group Name: To AuraSM	COR: 1	TN: 1	TAC: 803
Direction: two-way	Outgoing Display? n		
Dial Access? n	Night Service:		
Queue Length: 0			
Service Type: tie	Auth Code? n		
Signaling Group: 3			
Number of Members: 30			

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

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

Navigate to **Page 4** and change **Telephone Event Payload Type** to **101**. Use default values for all other fields. Submit these changes.

add trunk-group 3		Page 4 of 21	
PROTOCOL VARIATIONS			
Mark Users as Phone? n			
Prepend '+' to Calling Number? n			
Send Transferring Party Information? n			
Network Call Redirection? n			
Send Diversion Header? n			
Support Request History? n			
Telephone Event Payload Type: 101			

4.7. Configure Route Pattern

Configure a route pattern to correspond to the newly added SIP trunk group for outbound calls. Use **change route pattern n** command, where **n** is an available route pattern. Enter the following values for the specified fields, and retain the default values for the remaining fields. Submit these changes.

- **Pattern Name:** A descriptive name (i.e., **to AuraSM**).
- **Grp No:** The trunk group number from **Section 4.6.4**.
- **FRL:** Enter a level that allows access to this trunk, with **0** being least restrictive.

change route-pattern 2										Page	1 of	3						
Pattern Number: 2										Pattern Name: to AuraSM								
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:	3	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					

4.8. Configure Location and Public Unknown Numbering

Use the **change locations** command to assign the SIP route pattern for Avaya SIP endpoints to a location corresponding to the **Main** site. Add an entry for the Main site if one does not exist already. Enter the following values for the specified fields, and retain default values for the remaining fields. Submit these changes.

- **Name:** A descriptive name to denote the Main site.
- **Timezone:** An appropriate time zone offset.
- **Rule:** An appropriate daylight savings rule (i.e., **0**).
- **Proxy Sel. Rte. Pat.:** The route pattern number from **Section 4.7** (i.e., **2**).

change locations										Page	1 of	1
LOCATIONS												
ARS Prefix 1 Required For 10-Digit NANP Calls? y												
Loc	Name	Timezone		Rule	NPA				Proxy Sel			
No		Offset							Rte Pat			
1:	Main	+ 00:00		0					2			

Use the **change public-unknown-numbering 0** command, to define the calling party number to be sent to Passport 4000 Fax Server. Add an entry for the trunk group defined in **Section 4.6.4**. In the example shown below, all calls originating from a **4-digit** extension beginning with **30** and routed to trunk group **3** will result in a **11-digit calling number**. The calling party number will be in the SIP “From” header. Submit these changes.

change public-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext	Ext	Trk	CPN	Total	
Len	Code	Grp(s)	Prefix	CPN	
				Len	
4	30	1	0044208123	14	Total Administered: 1
4	30	2	0044208123	14	Maximum Entries: 9999
4	30	3	0208123	11	

4.9. Administer AAR Analysis

This section provides sample Automatic Alternate Routing (AAR) used for routing calls with dialed digits **50xx** to Passport 4000 Fax Server. Note that other methods of routing may be used. Use the **change aar analysis 0** command and add an entry to specify how to route the calls to **50xx** (Passport 4000 Fax Server through Session Manager). Enter the following values for the specified fields and retain the default values for the remaining fields. Submit these changes.

- **Dialed String:** Dialed prefix digits to match on, in this case **50**.
- **Total Min:** Minimum number of digits, in this case **4**.
- **Total Max:** Maximum number of digits, in this case **4**.
- **Route Pattern:** The route pattern number from **Section 4.7** i.e. **2**.
- **Call Type:** **aar**

change aar analysis 0							Page 1 of 2
AAR DIGIT ANALYSIS TABLE							
Location: all							Percent Full: 1
Dialed	Total	Route	Call	Node	ANI		
String	Min Max	Pattern	Type	Num	Reqd		
50	4 4	2	aar				

4.10. Save Translations

Configuration of Communication Manager is complete. Use the **save translations** command to save these changes.

5. Configure Avaya Aura™ Session Manager

This section provides the procedures for configuring Session Manager, assuming it has been installed and licensed as described in **Reference [3]**. The procedures include adding the following items:

- Specify SIP Domain.
- Logical/physical Locations that can be occupied by SIP Entities.
- SIP Entities corresponding to the SIP telephony systems and Session Manager.
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities.
- Routing Policies, which control call routing between the SIP Entities.
- Dial Patterns, which govern to which SIP Entity a call is routed.
- Session Manager, corresponding to the Session Manager Server to be managed by System Manager.

Configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL **http://<ip-address>/SMGR**, where **<ip-address>** is the IP address of System Manager. Log in with the appropriate credentials and accept the Copyright Notice. The menu shown below is displayed. Expand the **Network Routing Policy** Link on the left side as shown.

The screenshot displays the Avaya Aura™ System Manager 5.2 web interface. At the top, the Avaya logo is on the left, the title "Avaya Aura™ System Manager 5.2" is in the center, and the user status "Welcome, admin Last Logged on at Jan. 29, 2010 9:52 AM" with "Help | Log off" links is on the right. A red navigation bar below the header contains the text "Home / Network Routing Policy". On the left, a vertical menu lists various system management categories: Asset Management, Communication System Management, User Management, Monitoring, Network Routing Policy (highlighted with a red box), Adaptations, Dial Patterns, Entity Links, Locations, Regular Expressions, Routing Policies, SIP Domains, SIP Entities, Time Ranges, Personal Settings, Security, Applications, Settings, and Session Manager. Below this menu is a "Shortcuts" section with links for "Change Password", "Landing Page", "Help for Import All Data", "Help for Export All Data", and "Help for Committing configuration changes". The main content area is titled "Introduction to Network Routing Policy (NRP)" and contains the following text: "Network Routing Policy consists of several NRP applications like 'Domains', 'Locations', 'SIP Entities', etc. The recommended order to use the NRP applications (that means the overall NRP workflow) to configure your network configuration is as follows:" followed by a list of nine steps: Step 1: Create "Domains" of type SIP (other NRP applications are referring domains of type SIP). Step 2: Create "Locations". Step 3: Create "Adaptations". Step 4: Create "SIP Entities" with sub-points: "SIP Entities that are used as 'Outbound Proxies' e.g. a certain 'Gateway' or 'SIP Trunk'", "Create all 'other SIP Entities' (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)", and "Assign the appropriate 'Locations', 'Adaptations' and 'Outbound Proxies'". Step 5: Create the "Entity Links" with sub-points: "Between Session Managers" and "Between Session Managers and 'other SIP Entities'". Step 6: Create "Time Ranges" with sub-point: "Align with the tariff information received from the Service Providers". Step 7: Create "Routing Policies" with sub-points: "Assign the appropriate 'Routing Destination' and 'Time Of Day'" and "(Time Of Day = assign the appropriate 'Time Range' and define the 'Ranking')". Step 8: Create "Dial Pattern" with sub-point: "Assign the appropriate 'Locations' and 'Routing Policies' to the 'Dial Pattern'". Step 9: Create "Regular Expressions" with sub-point: "Assign the appropriate 'Routing Policies' to the 'Regular Expressions'". The page concludes with the statement: "Each 'Routing Policy' defines the 'Routing Destination' (which is a 'SIP Entity') as well as the 'Time of Day' and its associated 'Ranking'."

5.1. Specify SIP Domain

Add the SIP domain for which the communications infrastructure will be authoritative. Do this by selecting **SIP Domains** on the left and clicking the **New** button on the right. The following screen will then be shown. Fill in the following fields and click **Commit**.

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

The screenshot shows the Avaya Aura System Manager 5.2 interface. The top header includes the Avaya logo, the title 'Avaya Aura™ System Manager 5.2', and a welcome message for 'admin' last logged on at Jan. 29, 2010 9:52 AM. A red breadcrumb trail shows 'Home / Network Routing Policy / SIP Domains'. The left sidebar contains a navigation menu with 'SIP Domains' selected. The main content area is titled 'Domain Management' and shows a table with one item, 'avaya.com', with type 'sip'. The 'Commit' button is highlighted.

Name	Type	Default	Notes
* avaya.com	sip	<input type="checkbox"/>	

* Input Required

5.2. Add Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside, for purposes of bandwidth management. A single location is added to the configuration for Communication Manager and the Passport 4000 Fax Server. To add a location, select **Locations** on the left and click on the **New** button on the right. The following screen will then be shown. Fill in the following:

Under **General**:

- **Name:** A descriptive name.
- **Notes:** Descriptive text (optional).
- **Managed Bandwidth:** Leave the default or customize as described in [5].

Under **Location Pattern**:

- **IP Address Pattern:** A pattern used to logically identify the location. In these Application Notes, the pattern selected defined the networks involved. Other patterns can be used.
- **Notes:** Descriptive text (optional).

The screen below shows addition of the **testlab** location, which includes all the components of the compliance test lab. Click **Commit** to save.

The screenshot displays the Avaya Aura™ System Manager 5.2 web interface. The top navigation bar includes the Avaya logo, the product name and version, a user status message ('Welcome, admin Last Logged on at Jan. 29, 2010 9:52 AM'), and links for 'Help' and 'Log off'. Below this is a red breadcrumb trail: 'Home / Network Routing Policy / Locations / Location Details'. On the left, a sidebar menu lists various management categories, with 'Locations' highlighted under 'Network Routing Policy'. The main content area is titled 'Location Details' and contains two sections: 'General' and 'Location Pattern'. In the 'General' section, the 'Name' field is populated with 'testlab' and is circled in red. Other fields include 'Notes', 'Managed Bandwidth', 'Average Bandwidth per Call' (set to 80 Kbit/sec), and 'Time to Live (secs)' (set to 3600). The 'Location Pattern' section has an 'Add' button and a table with one item. The table has columns for 'IP Address Pattern' and 'Notes'. The first row shows the pattern '*193.120.221.*' circled in red. At the bottom of the table, it says 'Select : All, None (0 of 1 Selected)'. In the top right corner of the form area, there are 'Commit' and 'Cancel' buttons, with 'Commit' circled in red.

IP Address Pattern	Notes
193.120.221.	

5.3. Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP-based telephony system supported by it using SIP trunks. In the sample configuration, a SIP Entity is added for the Session Manager, the C-LAN board in the Avaya G650 Media Gateway and the Passport 4000 Fax Server.

5.3.1. Adding Communication Manager SIP Entity

To add a SIP Entity, navigate **Network Routing Policy** → **SIP Entities** on the left and click on the **New** button on the right.

Under **General**:

- **Name:** A descriptive name (i.e. **AvayaCM**).
- **FQDN or IP Address:** IP address of the signaling interface of CLAN board in the G650 Media gateway, i.e. **193.120.221.132**.
- **Type:** Select **CM**.
- **Location:** Select one of the locations defined previously i.e. **testlab**.
- **Time Zone:** Time zone for this entity.

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

AVAYA Avaya Aura™ System Manager 5.2 Welcome, **admin** Last Logged on at Feb. 08, 2010 8:38 AM [Help](#) | [Log off](#)

Home / Network Routing Policy / SIP Entities / **SIP Entity Details**

SIP Entity Details Commit Cancel

General

* Name:

* FQDN or IP Address:

Type:

Notes:

Adaptation:

Location:

Time Zone:

Override Port & Transport with DNS SRV: ☐

* SIP Timer B/F (in seconds):

Credential name:

Call Detail Recording:

SIP Link Monitoring

SIP Link Monitoring:

5.3.2. Adding Passport 4000 Fax Server SIP Entity

Navigate **Network Routing Policy** → **SIP Entities** on the left and click on the **New** button on the right.

Under **General**:

- **Name:** A descriptive name (i.e. **Passport4000**).
- **FQDN or IP Address:** IP address of the signaling interface on the Fax Server, i.e. **193.120.221.160**.
- **Type:** Select **other**.
- **Location:** Select one of the locations defined previously i.e. **testlab**.
- **Time Zone:** Time zone for this entity.

Under **SIP Link Monitoring**, in the drop down menu, select **Link Monitoring Disabled**. Defaults can be used for the remaining fields. Click **Commit** to save SIP Entity definition. The picture below shows the configuration of the SIP Entity related to the Passport 4000 Fax Server.

The screenshot displays the Avaya Aura System Manager 5.2 web interface. The left-hand navigation pane shows the 'Network Routing Policy' section expanded, with 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and contains two sections: 'General' and 'SIP Link Monitoring'. In the 'General' section, the following fields are configured: Name is 'Passport4000', FQDN or IP Address is '193.120.221.160', Type is 'Other', Location is 'testlab', and Time Zone is 'Europe/Dublin'. The 'SIP Link Monitoring' section shows 'SIP Link Monitoring' set to 'Link Monitoring Disabled'. A 'Commit' button is visible in the top right corner of the configuration area.

AVAYA Avaya Aura™ System Manager 5.2 Welcome, admin Last Logged on at Feb. 08, 2010 8:38 AM Help | Log off

Home / Network Routing Policy / SIP Entities / SIP Entity Details

SIP Entity Details [Commit] [Cancel]

General

* Name: Passport4000

* FQDN or IP Address: 193.120.221.160

Type: Other

Notes:

Adaptation:

Location: testlab

Time Zone: Europe/Dublin

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Link Monitoring Disabled

5.3.3. Adding Avaya Aura™ Session Manager SIP Entity

Navigate **Network Routing Policy** → **SIP Entities** on the left and click on the **New** button on the right.

Under **General**:

- **Name:** A descriptive name, i.e. **SessionManager**.
- **FQDN or IP Address:** IP address of the Session Manager i.e. **193.120.221.154**, the SM-100 Security Module.
- **Type:** Select **Session Manager**.
- **Location:** Select one of the locations defined previously.
- **Time Zone:** Time zone for this entity.

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

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

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

AVAYA Avaya Aura™ System Manager 5.2
Welcome, **admin** Last Logged on at Feb. 08, 2010 8:38 AM [Help](#) | [Log off](#)

Home / Network Routing Policy / SIP Entities / SIP Entity Details

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

General

* Name:

* FQDN or IP Address:

Type:

Notes:

Location:

Outbound Proxy:

Time Zone:

Credential name:

SIP Link Monitoring

SIP Link Monitoring:

Entity Links

Entity Links can be modified after SIP Entity is committed.

Port

[Add](#) [Remove](#)

2 Items | [Refresh](#) Filter: [Enable](#)

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

Select : All, None (0 of 2 Selected)

5.4. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity link. To add an Entity Link, select **Entity Links** on the left and click on the **New** button on the right. Fill in the following fields in the new row that is displayed:

- **Name:** A descriptive name.
- **SIP Entity 1:** Select the Session Manager entity.
- **Port:** Port number to which the other system sends SIP requests.
- **SIP Entity 2:** Select the name of the other system.
- **Port:** Port number on which the other system receives SIP requests.
- **Trusted:** Check this box, otherwise calls from the associated SIP Entity specified will be denied.
- **Protocol:** Select the transport protocol between **UDP/TCP/TLS** to align with the definition on the **other end** of the link. In these application notes **TLS** was used for **Communication Manager** and **UDP** for **Passport 4000 Fax Server**.

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

The screenshot shows the Avaya Aura System Manager 5.2 interface. The left sidebar has a tree view with 'Entity Links' selected under 'Network Routing Policy'. The main area shows a table with one row for an entity link. The fields are: Name (*SessionManager-C), SIP Entity 1 (*SessionManager), Protocol (TLS), Port (*5061), SIP Entity 2 (*AvayaCM), Port (*5061), Trusted (checked), and Notes. There are 'Commit' and 'Cancel' buttons at the top right and bottom right of the table area.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
*SessionManager-C	*SessionManager	TLS	*5061	*AvayaCM	*5061	<input checked="" type="checkbox"/>	

The screen below illustrate adding the Entity Link for Passport 4000 Fax Server.

The screenshot shows the Avaya Aura System Manager 5.2 interface. The left sidebar has a tree view with 'Entity Links' selected under 'Network Routing Policy'. The main area shows a table with one row for an entity link. The fields are: Name (*SessionManager-C), SIP Entity 1 (*SessionManager), Protocol (UDP), Port (*5060), SIP Entity 2 (*Passport4000), Port (*5060), Trusted (checked), and Notes. There are 'Commit' and 'Cancel' buttons at the top right and bottom right of the table area.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
*SessionManager-C	*SessionManager	UDP	*5060	*Passport4000	*5060	<input checked="" type="checkbox"/>	

5.5. Add Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 5.3**. Two routing policies must be added: one for Communication Manager and one for Passport 4000. To add a routing policy, select **Routing Policies** on the left and click on the **New** button on the right. The following screen is displayed. Fill in the following:

Under **General**:

- Enter a descriptive name in **Name**.

Under **SIP Entity as Destination**:

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

Under **Time of Day**:

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

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

The screenshot displays the Avaya Aura System Manager interface. The left sidebar shows the navigation menu with 'Routing Policies' highlighted. The main content area is titled 'Routing Policy Details' and includes a 'Commit' button. The 'General' section shows the policy name 'RP2CM' and a note 'Routes to CM'. The 'SIP Entity as Destination' section shows a 'Select' button and a table with one entry: 'AvayaCM' with FQDN '193.120.221.132' and Type 'CM'. The 'Time of Day' section shows an 'Add' button and a table with one entry: '24/7' with a time range of '00:00' to '23:59' and a note 'Always Active'.

Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Feb. 09, 2010 5:30 PM

Home / Network Routing Policy / Routing Policies / Routing Policy Details

Routing Policy Details [Commit] [Cancel]

General

* Name: **RP2CM**

Disabled: ☐

Notes: **Routes to CM**

SIP Entity as Destination

[Select]

Name	FQDN or IP Address	Type	Notes
AvayaCM	193.120.221.132	CM	

Time of Day

[Add] [Remove] [View Gaps/Overlaps]

1 Item | Refresh Filter: Enable

	Ranking 1 ▲	Name 2 ▲	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	Always Active

Select : All, None (0 of 1 Selected)

The following picture shows the Routing Policy for Passport 4000 Fax Server.

AVAYA Avaya Aura™ System Manager 5.2

Welcome, admin Last Logged on at Feb. 09, 2010 5:30 PM

Help | Log off

Home / Network Routing Policy / Routing Policies / Routing Policy Details

Routing Policy Details [Commit] [Cancel]

General

* Name: RP2Passport4000

Disabled: ☐

Notes: route to Passport 4000

SIP Entity as Destination

[Select]

Name	FQDN or IP Address	Type	Notes
Passport4000	193.120.221.160	Other	

Time of Day

[Add] [Remove] [View Gaps/Overlaps]

1 Item | Refresh Filter: Enable

	Ranking 1 ▲	Name 2 ▲	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	Always Active

Select : All, None (0 of 1 Selected)

5.6. Add Dial Patterns

Dial patterns must be defined that will direct calls to the appropriate SIP Entity. In the sample configuration, 4-digit extensions beginning with **30** reside on Communication Manager and 4-digit beginning with **50** reside on Passport 4000. In the sample application, international (14 digits) and national (11 digits) numbers are also used, requiring additional Dial Patterns to be specified. The table below illustrates the possible combinations of dial pattern used.

Prefix / Pattern	Length	Destination Entity	Remark
00442081233	14	AvayaCM	International for CM extensions
02081233	11	AvayaCM	National numbering
30	4	AvayaCM	Local extension
00442012335	14	Passport 4000	International for Passport 4000 Fax
02081235	11	Passport 4000	National numbering
50	4	Passport 4000	Local extensions
00442081234	14	AvayaCM (to be forwarded to PSTN)	International to reach test fax on PSTN
02081234	11	AvayaCM (to be forwarded to PSTN)	National to reach test fax on PSTN

To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button on the right. Fill in the following, as shown in the screen below, which corresponds to the dial pattern for routing calls to Communication Manager:

Under **General**:

- **Pattern:** Dialed number or prefix.
- **Min** Minimum length of dialed number.
- **Max** Maximum length of dialed number.
- **Notes** Comment on purpose of dial pattern.

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

AVAYA Avaya Aura™ System Manager 5.2 Welcome, admin Last Logged on at Feb. 09, 2010 5:30 PM Help | Log off

Home / Network Routing Policy / Dial Patterns / Dial Pattern Details

Dial Pattern Details Commit Cancel

General

* Pattern: 30

* Min: 4

* Max: 4

Emergency Call: ☐

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item | Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	RP2CM	0	<input type="checkbox"/>	AvayaCM	Routes to CM

Select : All, None (0 of 1 Selected)

The following screen shows a sample dial pattern definition for Passport 4000 Fax Server.

AVAYA Avaya Aura™ System Manager 5.2 Welcome, **admin** Last Logged on at Feb. 09, 2010 5:30 PM Help | Log off

Home / Network Routing Policy / Dial Patterns / Dial Pattern Details

Dial Pattern Details Commit Cancel

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	RP2Passport4000	0	<input type="checkbox"/>	Passport4000	route to Passport 4000

Select : All, None (0 of 1 Selected)

The following screen summarizes all the dial pattern definitions for the sample application.

AVAYA Avaya Aura™ System Manager 5.2 Welcome, **admin** Last Logged on at Feb. 09, 2010 5:30 PM Help | Log off

Home / Network Routing Policy / Dial Patterns

Dial Patterns Edit New Duplicate Delete More Actions Commit

8 Items Refresh Filter: Enable

<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	SIP Domain	Notes
<input type="checkbox"/>	00442081233	14	14	<input type="checkbox"/>	-ALL-	
<input type="checkbox"/>	00442081234	14	14	<input type="checkbox"/>	-ALL-	
<input type="checkbox"/>	00442081235	14	14	<input type="checkbox"/>	-ALL-	
<input type="checkbox"/>	02081233	11	11	<input type="checkbox"/>	-ALL-	
<input type="checkbox"/>	02081234	11	11	<input type="checkbox"/>	-ALL-	
<input type="checkbox"/>	02081235	11	11	<input type="checkbox"/>	-ALL-	
<input type="checkbox"/>	30	4	4	<input type="checkbox"/>	-ALL-	
<input type="checkbox"/>	50	4	4	<input type="checkbox"/>	-ALL-	

Select : All, None (0 of 8 Selected)

5.7. Add Avaya Aura™ Session Manager

To complete the configuration, adding the Session Manager will provide the linkage between System Manager and Session Manager. Expand the **Session Manager** menu on the left and select **Session Manager Administration**. Then click **Add**, and fill in the fields as described below and shown in the following screen:

Under **General**:

- **SIP Entity Name:** Select the name of the SIP Entity added for Session Manager.
- **Description:** Descriptive comment (optional).
- **Management Access Point Host Name/IP**
Enter the IP address of the Session Manager management interface.

Under **Security Module**:

- **Network Mask:** Enter the network mask corresponding to the IP address of the SM100 interface (i.e., **255.255.255.128**).
- **Default Gateway:** Enter the IP address of the default gateway for SM100 interface (i.e., **193.120.221.129**).

Use default values for the remaining fields. Click **Save** to add this Session Manager.

AVAYA Avaya Aura™ System Manager 5.2 Welcome, **admin** Last Logged on at Feb. 09, 2010 5:30 PM [Help](#) [Log off](#)

Home / Session Manager / Session Manager Administration / **Edit Session Manager**

Add Session Manager [Commit](#) [Cancel](#)

General | Security Module | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server |
Expand All | Collapse All

General

SIP Entity Name

Description

*Management Access Point Host Name/IP

*Direct Routing to Endpoints

Security Module

SIP Entity IP Address

*Network Mask

*Default Gateway

*Call Control PHB

*QoS Priority

*Speed & Duplex

VLAN ID

6. Lane Telecommunications Passport 4000 Configuration

This section provides the procedures for configuring the Passport 4000 Fax Server. It's assumed that the product has been successfully installed as per Reference [5], [6] and [7]. The configuration procedure requires the following steps:

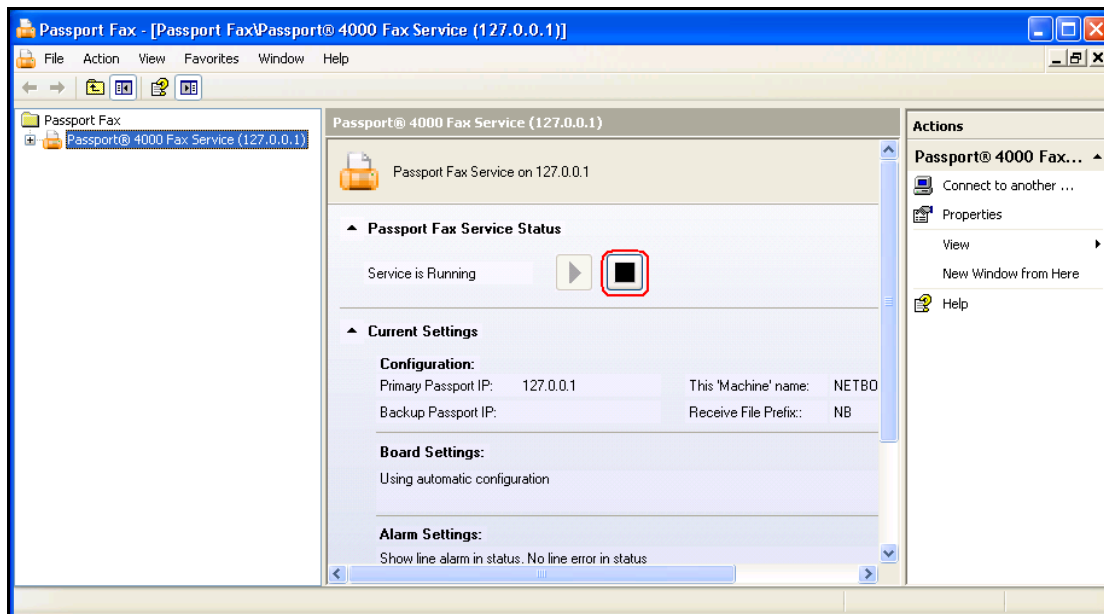
- Stopping the running Fax Service.
- Verify the SIP License.
- Configuring the SIP Interface.
- Restarting the Fax Service.
- Configure the Fax Lines.

6.1. Stopping the Running Fax Service

The management of the Passport 4000 service is carried with a dedicated snap-in that can be activated by clicking on the Passport 4000 Fax Service icon:



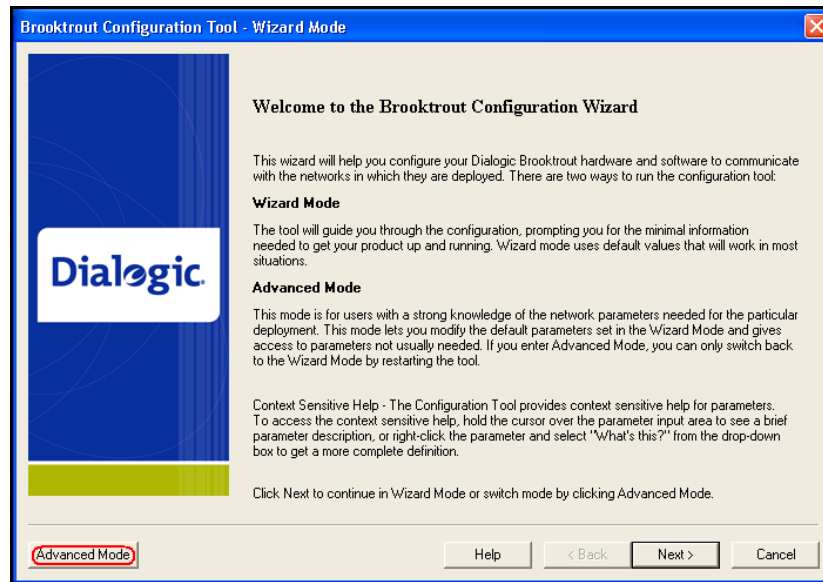
A new window will open to manage the service. Click on the **stop** button, the picture below illustrates the management snap-in window.



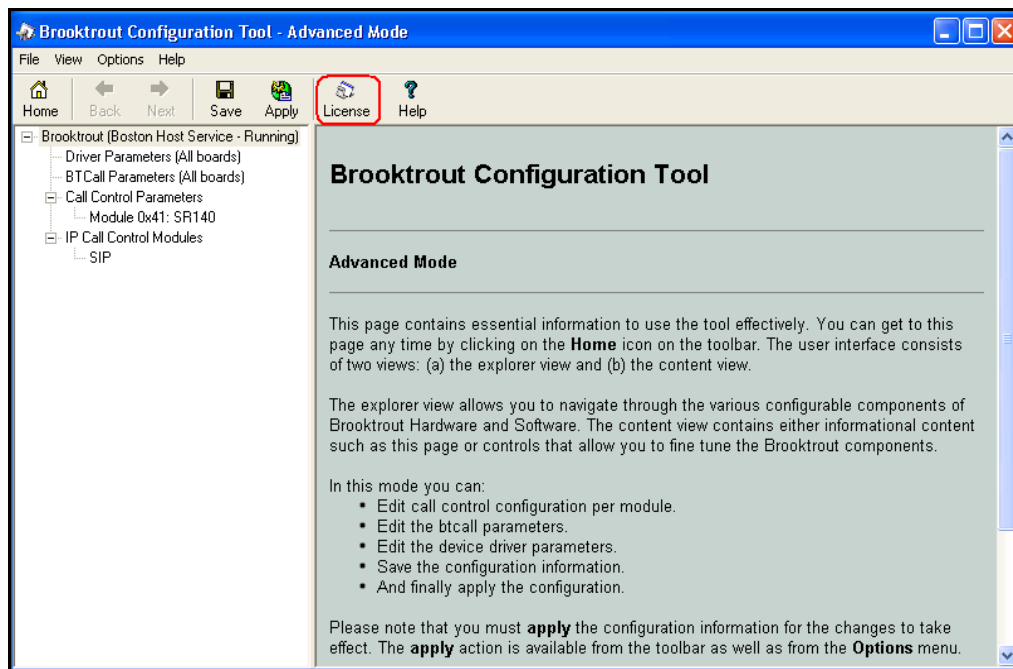
6.2. Verify the SIP License

To verify the SIP license activate the Dialogic Brooktrout configuration tool, usually located under the path: **C:\Program Files\Passport4000\FaxService\Brooktrout\configtool.exe**.

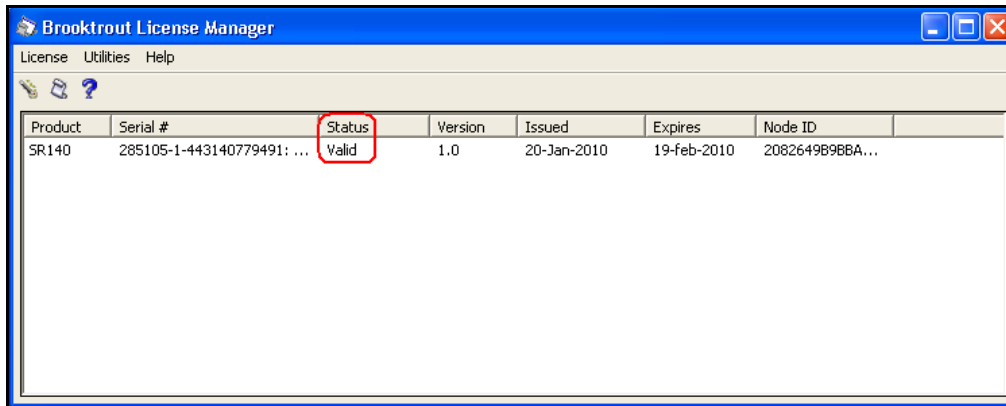
A welcome screen is presented, click on the **Advance Mode** button. The figure below illustrates the activation of the **configtool.exe** program.



The **Brooktrout Configuration Tool – Advance Mode** window is displayed. Click on the **License** icon as shown in the picture below.

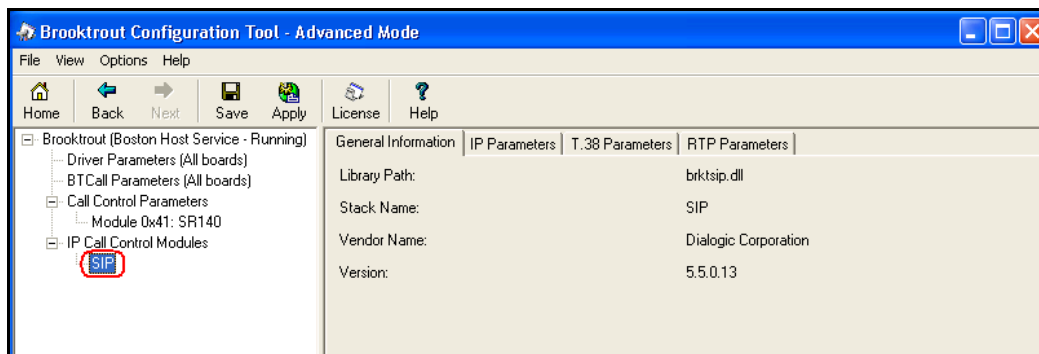


The **Brooktrout License Manager** window opens showing the status of the current installation. Verify that under the **Status** column it is reported as **Valid**. If this is not the case contact Lane Telecommunications support. Close the **Brooktrout License Manager** window when finished. The figure below shows the license used for the sample Application Notes.



6.3. Configure the SIP Interface

To configure the telephony network interfaces of the Passport 4000, use the **Brooktrout Configuration – Advance Mode** window. Navigate the menu on the left hand side pane **Brooktrout (Boston Host Service – Running) → IP Call Control Modules → SIP**.



On the right hand pane select the **IP Parameters** tab and configure the following fields:

- **Primary Gateway:** The IP address and the port of the SM100 (**193.120.221.154** port **5060** in these sample application notes).
- **From Value:** The SIP from value inserted by Passport 4000 when dialing out (in these notes: **00442081235000@193.120.221.160**).
- **Contact Address:** The IP address and port on which the SIP stack is listening into (i.e. **193.120.221.160** port **5060**).

The screenshot shows the 'IP Parameters' tab in the 'Brooktrout Configuration - Advance Mode' window. The 'Maximum SIP Sessions' is set to 1. The 'Primary Gateway' is configured with IP address 193.120.221.154 and port 5060. The 'From Value' is set to 00442081235000@193.120.221.160. The 'Contact Address' is set to 193.120.221.160 and port 5060. Other fields like 'Primary Proxy Server', 'Additional Proxy Server #2-4', 'Primary Registrar Server URL', 'Additional Registrar Server #2-4', 'Username' (PassportFAX), 'Session Name' (Passport), 'Session Description', 'Description URL', 'Email Address', and 'Phone Number' are empty. A 'Show Advanced >>' button is at the bottom right.

Select the **RTP Parameters** tab and configure the following fields:

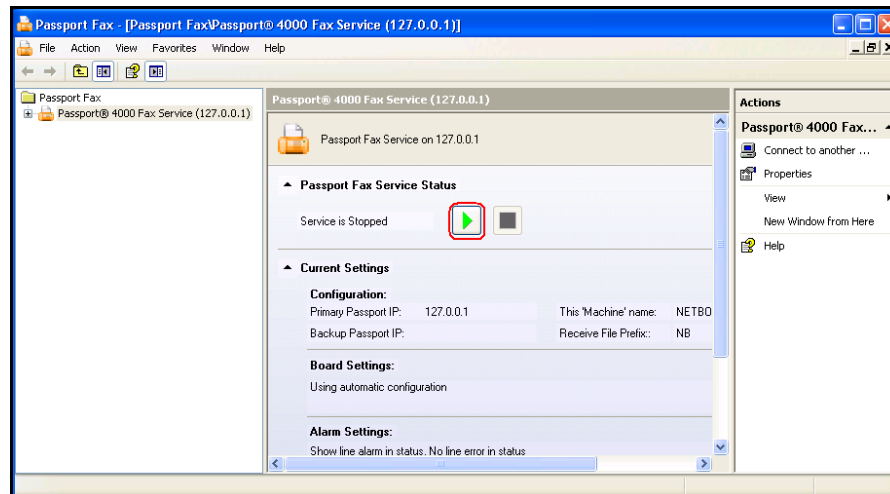
- **RTP codec list** The codec used when sending receiving sip calls (**pcma** in these sample Application Notes).

The screenshot shows the 'RTP Parameters' tab in the 'Brooktrout Configuration - Advance Mode' window. The 'RTP codec list' is set to 'pcma'. The 'Silence Control' is set to 'inband'. A 'Show Advanced >>' button is at the bottom right.

The **Brooktrout Configuration – Advance Mode** window can be closed.

6.4. Restarting the Fax Service

To reactivate the Passport 4000 service, re-activate the management snap in as detailed in **Section 6.1**. Click on the start icon to reactivate the service. The picture below illustrates the management snap-in window.

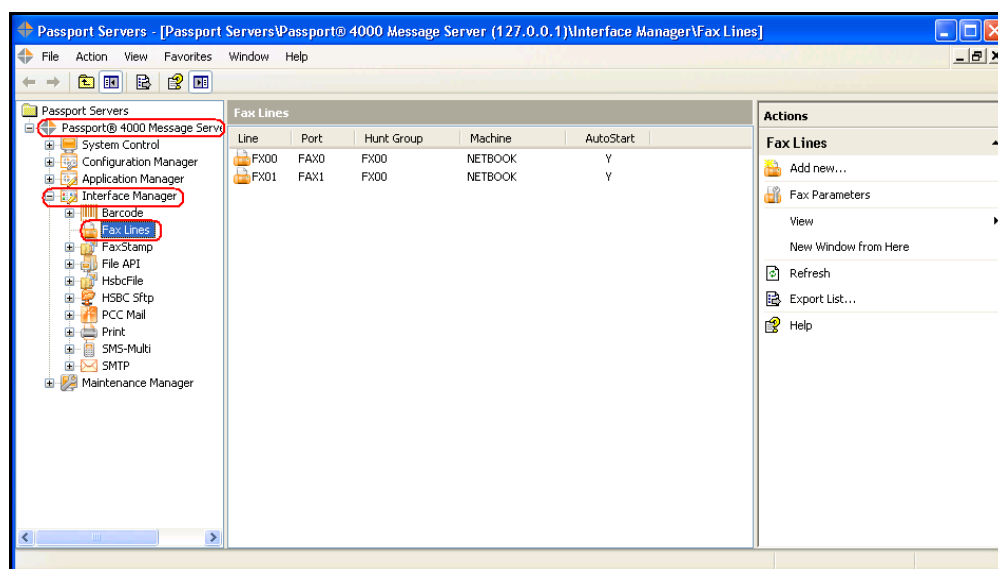


6.5. Configure Fax Lines

To configure Fax Line activate the configuration program by clicking on the Passport 4000 Services icon:



A new window will open; on the left hand side expand **Passport 4000 Message Server** → **Interface Manager** → **Fax lines**, as displayed by the figure below.



Ensure that there are configured sufficient numbers of fax lines, and the proper settings are enabled. Refer to [5], [6] and [7] for additional details. In the following pictures are presented the properties of a FAX line used in the sample notes.

FX00 Properties

General Fax Options Caller ID/TSI Batching

Fax Line Configuration

Line Name:

Port Name:

Machine Name:

Hunt Group:

Line Queue:

Printer Selections

Transmit:

Receive:

☒ Auto Start

OK Cancel Apply Help

FX00 Properties

General Fax Options Caller ID/TSI Batching

☐ Enable Secondary DTMF

☒ Archive Transmissions Graphically

Limit DID Digits:

Add DID Prefix:

☒ Use DID Digits as Originator Code

☐ Discard Partial Received Faxes

☐ Use Rec'd Filename as Reference

Banner Information

Fax ID:

Company Name:

Phone Access Code

OK Cancel Apply Help

FX00 Properties

General Fax Options Caller ID/TSI Batching

Incoming Calls show Correspondent ID as:

☐ Calling Fax Machine's Transmitting Subscriber Identification (TSI)

☐ Calling Fax Machines Telephone Number (Caller ID)

☒ Caller ID/TSI

☐ TSI/Caller ID

OK Cancel Apply Help

FX00 Properties

General Fax Options Caller ID/TSI Batching

Batching/Gang Sending

☐ No Batching, Allow Gang Sending

☒ No Batching, Disallow Gang Sending

☐ Batching, Disallow Gang Sending

OK Cancel Apply Help

7. Verification Steps

This section provides the verification steps that may be performed to verify that the Passport 4000 Fax Server can establish calls to Communication Manager and PSTN through Session Manager.

7.1. SIP Monitoring on Avaya Aura™ Session Manager

Expand the menu on the left and navigate **Session Manager**→**System Status**→**SIP Entity Monitoring**. Verify that none of the links to the defined SIP entities are down, indicating that they are all reachable for call routing.

The screenshot displays the Avaya Aura™ System Manager 5.2 web interface. The left-hand navigation menu is expanded, showing the following hierarchy: **Session Manager** (highlighted with a red box) → **System Status** (highlighted with a red box) → **SIP Entity Monitoring** (highlighted with a red box). The main content area is titled "SIP Entity Link Monitoring Status Summary" and includes a "Refresh" button. Below this is a table showing the status of SIP entity links for the "SessionManager" instance. The table has five columns: "Session Manager Name", "Entity Links Down/Total", "Entity Links Partially Down", "SIP Entities - Monitoring Not Started", and "SIP Entities - Not Monitored". The "SessionManager" row shows 0/2 entity links down, 0 partially down, 0 not started, and 1 not monitored. Below the table is a section titled "All Monitored SIP Entities" with another "Refresh" button and a list of monitored entities. The list shows 1 item, "AvayaCM", with a "Filter: Enable" button.

Session Manager Name	Entity Links Down/Total	Entity Links Partially Down	SIP Entities - Monitoring Not Started	SIP Entities - Not Monitored
SessionManager	0/2	0	0	1

SIP Entity Name
AvayaCM

7.2. Verify Avaya Aura™ Communication Manager Trunk Status

On Communication Manager, ensure that all the signalling groups are in-service status, by issuing the command **status signaling-group n** where **n** is the signalling group number.

```
status signaling-group 2
```

```
STATUS SIGNALING GROUP
```

```
Group ID: 2                               Active NCA-TSC Count: 0
Group Type: sip                           Active CA-TSC Count: 0
Signaling Type: facility associated signaling
Group State: in-service
```

```
status signaling-group 3
```

```
STATUS SIGNALING GROUP
```

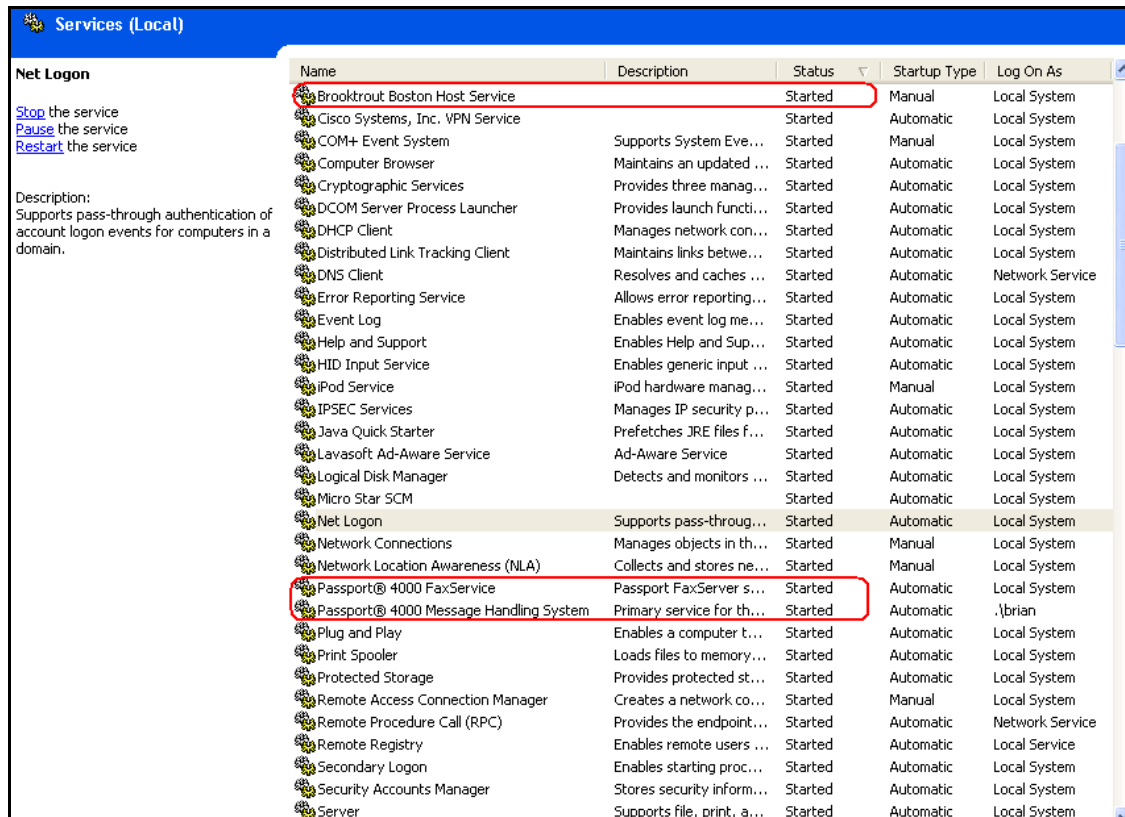
```
Group ID: 3                               Active NCA-TSC Count: 0
Group Type: sip                           Active CA-TSC Count: 0
Signaling Type: facility associated signaling
Group State: in-service
```

7.3. Passport 4000 Fax Server Services Status

Using the operating system **services.msc** snap-in, verify that the following services are in **Started** status:

- **Brooktrout Boston Host Service**
- **Passport 4000 FaxService**
- **Passport 4000 Message Handling System**

The figure below shows the services status test installation of the Passport 4000 Fax Server.



7.4. Passport 4000 SIP Listener Verification

To ensure that the SIP listener configured in **Section 6.3** is properly configured and operative, run from the command line of the Passport 4000 Fax Server the command **netstat -an -p UDP** ensure that there is an instance of port **5060** for the ip address configured on the server. The figure below shows the output of the command on the server used in the sample application.

```
C:\Documents and Settings\Brian>netstat -an -p UDP
```

Active Connections

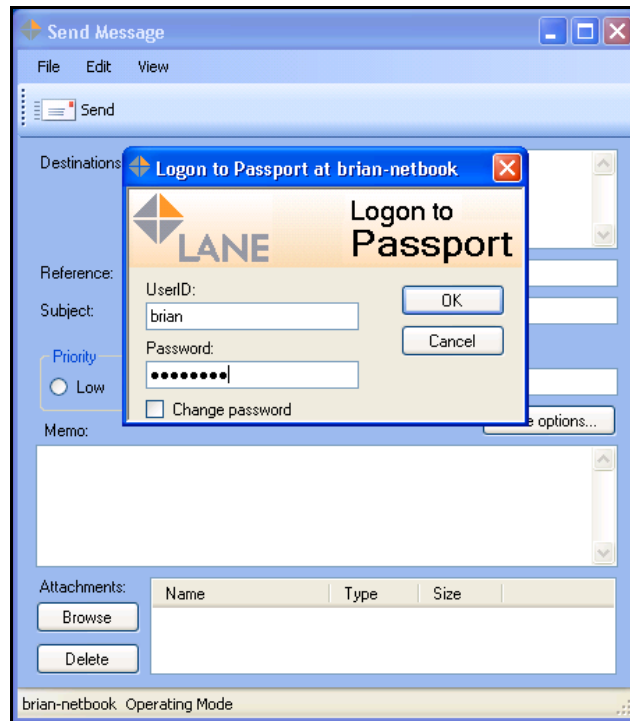
Proto	Local Address	Foreign Address	State
UDP	0.0.0.0:445	*:*	
UDP	0.0.0.0:500	*:*	
UDP	0.0.0.0:1025	*:*	
UDP	0.0.0.0:1434	*:*	
UDP	0.0.0.0:4500	*:*	
UDP	0.0.0.0:59097	*:*	
UDP	127.0.0.1:123	*:*	
UDP	127.0.0.1:1900	*:*	
UDP	127.0.0.1:62514	*:*	
UDP	193.120.221.160:123	*:*	
UDP	193.120.221.160:137	*:*	
UDP	193.120.221.160:138	*:*	
UDP	193.120.221.160:1900	*:*	
UDP	193.120.221.160:5060	*:*	
UDP	193.120.221.160:5353	*:*	

7.5. Functional Verification

Ensure system functionality with sending and receiving faxes from and to the Passport 4000 Fax Server.

7.5.1. Sending Faxes from Passport 4000

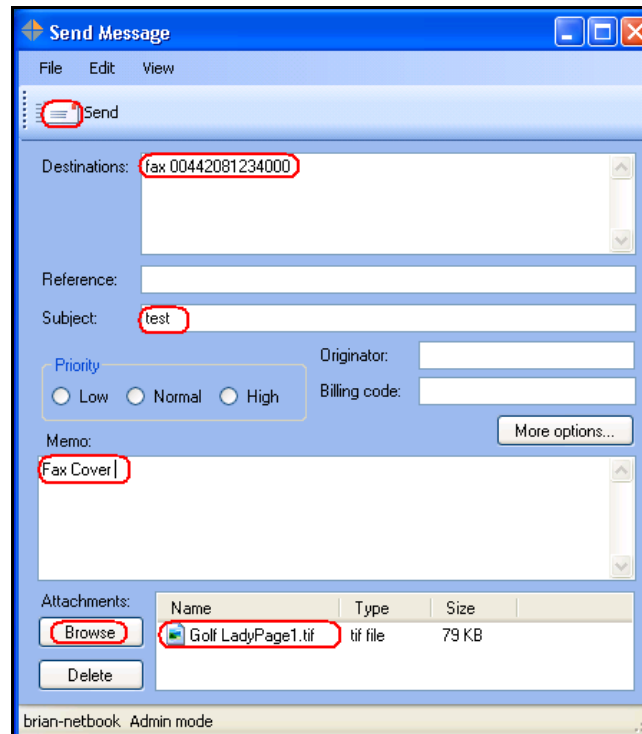
Activate the Send Message application **Start menu→Passport 4000→Client Applications DLL Version→SendMsg**; log in to the application with the credential defined at installation time. The figure below displays the logon in the **Send Message** application.



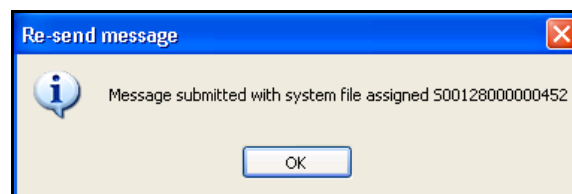
After log on, in the **Send Message** window fill the following fields:

- **Destinations:** the word **fax** followed by the number of the recipient (i.e. **fax 00442081234000**).
- **Subject:** a subject title.
- **Memo:** some test string that **will appear on the Fax Cover** with the **Subject** entered above.

Under **Attachments**, click on the **Browse** button and select a **tif** file to be attached as fax document, select a sample graphic image (in our notes **GolfLadyPage1.tif**). Click on the **Send** button to activate the fax sending. The figure below illustrates the **Send Message** window.



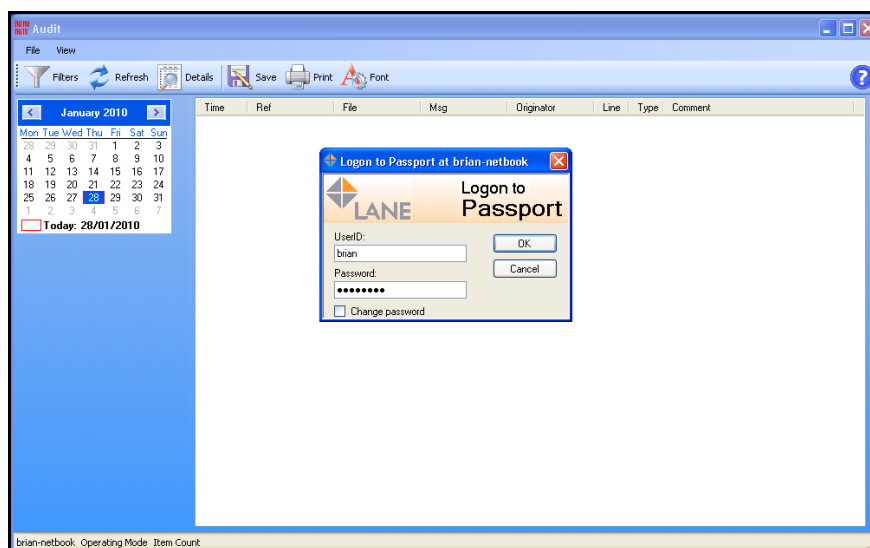
The system will display a notification window with a system file name as shown below.



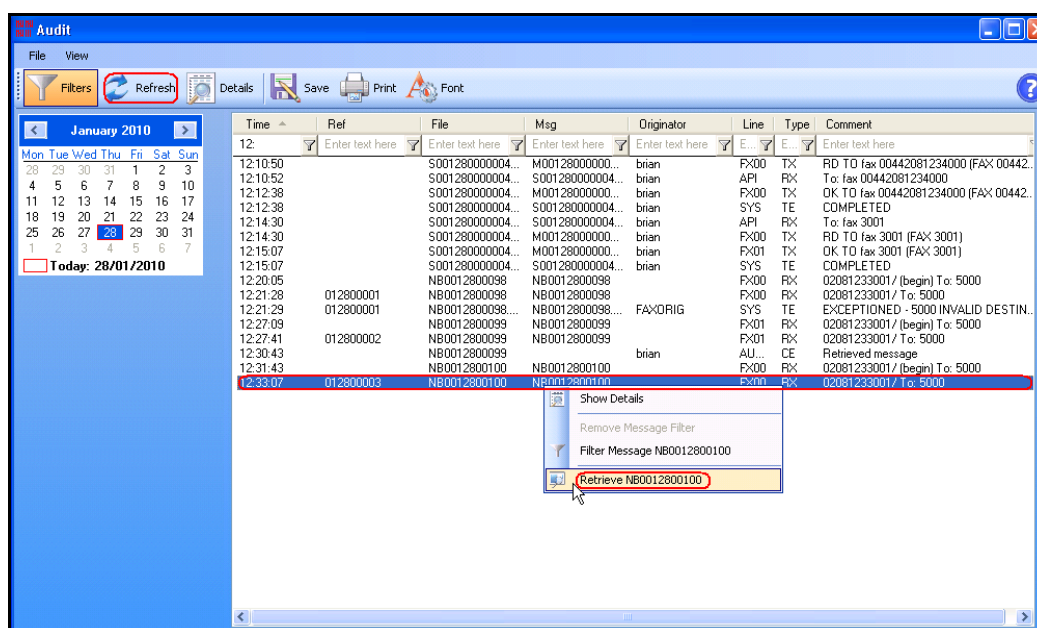
Verify reception and the quality of the fax on the analog fax machine connected to the PSTN line. Repeat sending a fax to a local fax machine connected to Communication Manger (ext. 3001)

7.5.2. Receiving Fax on Passport 4000

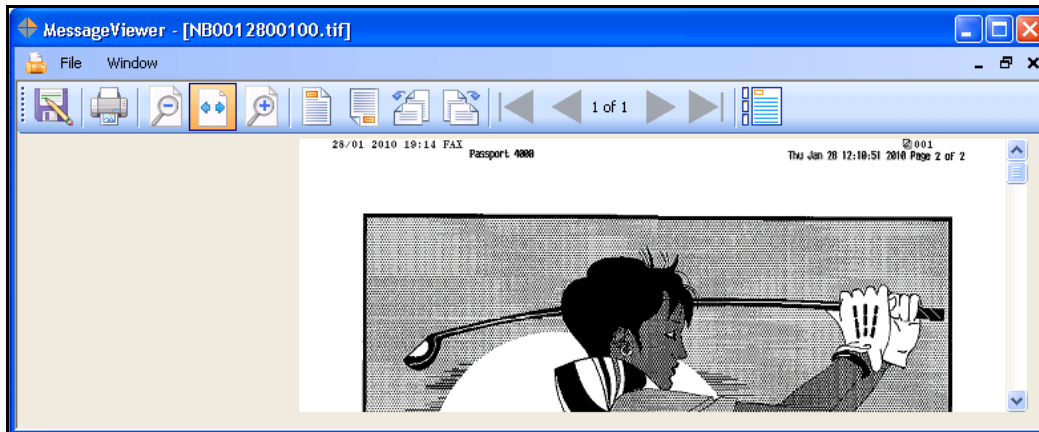
In order to analyze the incoming faxes, activate the Passport 4000 **Audit** program from **Start menu→Passport 4000→Client Applications DLL Version→Audit**; log in to the application with the credential defined at installation time. The figure below displays the logon in the **Audit** application.



From the local fax machine (ext. 3001) send a test page to the number configured for accessing the Passport 4000 (ext. 5000). In the **Audit** application click on **Refresh** icon to update the log, and new entries are inserted in the log to report successful fax reception. **Right** click on the **log line** and select **Retrieve** to retrieve and visualize the fax. The figure below illustrates the process.



The **MessageViewer** application is launched by the system showing the contents of the fax, as in the example illustrated below.



Repeat the steps above from a fax machine connected to the PSTN

8. General Test Approach

The interoperability compliance test included feature and serviceability. The feature testing focused on verifying the following:

- Sending Fax from the PSTN Fax to Passport 4000.
- Sending Fax from Communication Manager to Passport 4000.
- Sending Fax from Passport 4000 to a fax machine on PSTN.
- Sending Fax from Passport 4000 to a fax machine on Communication Manager.
- Sending concurrent Faxes to Passport 4000.
- All the fax transmissions were tested with single and multiple pages.
- Verifying G.711A and G.711MU on Communication Manager and Passport 4000.

The serviceability testing focused on verifying the ability of the Passport 4000 Fax Server to recover from adverse conditions, such as network failures.

8.1. Test Results

All test cases passed. Lane Telecommunication Passport 4000 Fax Server successfully sent and received faxes from PSTN as well from local analog fax connected to Communication Manager, by using SIP infrastructure provided by Avaya Aura™ Session Manager.

9. Conclusion

As illustrated in these Application Notes, Lane Telecommunications Passport 4000 Fax Server interoperates with Avaya Aura™ Session Manager and Avaya Aura™ Communication Manager using SIP trunks. The test used G711A and G711MU codecs for media encoding.

10. Additional References

Reference documentation can be found on the Avaya support site at: <http://support.avaya.com>

- [1] *Administering Avaya Aura™ Communication Manager; Doc # 03-300509, May 2009*
- [2] *Avaya Aura™ Communication Manager Feature Description and Implementation Doc # 555-245-205, May 2009*
- [3] *Administering Avaya Aura Session Manager; Doc # 03-603324; Nov-2009*

Lane Telecommunications' references available at <http://www.lanetelecom.com>

- [4] *P4000 System Control*
- [5] *P4000 Configuration Manager*
- [6] *P4000 Interface Manager*
- [7] *P4000 Maintenance Manager*

Prerequisite and Installation manuals are available directly from Lane Telecommunications.

APPENDIX

In this section are presented the relevant configuration files for the devices used in the DevConnect compliance testing.

Brooktrout SIP stack configuration file

Here follows the sample configuration file for the Brooktrout SR140 SIP stack in used by Passport 4000 Fax Server.

```
# callctrl.cfg
#
# Sample Call Control configuration file for Boston Bfv API.
#
# This is an all-in-one file that contains examples for several
# different types of configurations. All of the configuration lines have
# been commented out. You should uncomment the lines that are
# appropriate for your configuration.
#
# NOTE: Ensure that you use an absolute path for all the parameters that
# accept
# file names.
#
# Default installation location
#-----
--
# OS | default [INSTALL_LOCATION]
#-----+-----
--
# Windows BSS (boston.msi) | "C:/Program Files/Brooktrout"
# Windows SDK (sdk_windows.exe) | C:/Brooktrout/Boston
# Linux | /usr/sys/brooktrout/boston
# Solaris | /usr/sys/brooktrout/boston
#-----
#
# Parameters that accept file names
#-----
# Parameter | OS | Location
#-----+-----+-----
# trace_file | All | [INSTALL_LOCATION]/config/ecc.log
#-----+-----+-----
# country | All | [INSTALL_LOCATION]/config/us600.qslac
#-----+-----+-----
# protocol_file | All |
# [INSTALL_LOCATION]/config/analog_loopstart_us.lec
#-----+-----+-----
# module_library | Windows BSS | C:/Windows/System32/brktsip.dll
# | Windows SDK | [INSTALL_LOCATION]/bin/brktsip.dll
# | Linux | /usr/lib/brktsip_mt.so
# | Solaris | /usr/lib/brktsip_mt.so
#-----+-----+-----
# vb_firm | Windows BSS | [INSTALL_LOCATION]/bin/bostvb.dll
# | Windows SDK | [INSTALL_LOCATION]/fw/bostvb.dll
# | Linux | [INSTALL_LOCATION]/fw/bostvb.so
#-----+-----+-----
#
```

```

#
# Refer to the Call Control Configuration File section in the Brooktrout Fax
# and Voice API Programmer's Reference Manual for more information.

1314_trace=verbose
1413_trace=verbose
api_trace=verbose
internal_trace=verbose
host_module_trace=verbose
ip_stack_trace=verbose
# Most of the time a path should be used for this file name.
trace_file=ecc.log
max_trace_files=1
max_trace_file_size=10
[host_module.1]
module_library=brktsip.dll
enabled=true
[host_module.1/t38parameters]
t38_fax_rate_management=transferredTCF
fax_transport_protocol=t38_only
t38_fax_udp_ec=t38UDPRedundancy
rtp_ced_enable=true
t38_max_bit_rate=33600
t38_fax_version=3
media_renegotiate_delay_inbound=4000
media_renegotiate_delay_outbound=-1
t38_fax_fill_bit_removal=false
t38_fax_transcoding_jbig=false
t38_fax_transcoding_mmr=false
t38_t30_fastnotify=false
t38_UDPTL_redundancy_depth_control=5
t38_UDPTL_redundancy_depth_image=2
media_passthrough_timeout_inbound=1000
media_passthrough_timeout_outbound=4000
t38_type_of_service=0
[host_module.1/parameters]
sip_max_sessions=254
sip_default_gateway=193.120.221.154:5060
sip_proxy_server1=
sip_proxy_server2=
sip_proxy_server3=
sip_proxy_server4=
sip_registration_server1=
sip_registration_server1_aor=
sip_registration_server1_username=
sip_registration_server1_password=
sip_registration_server1_expires=3600
sip_registration_server2=
sip_registration_server2_aor=
sip_registration_server2_username=
sip_registration_server2_password=
sip_registration_server2_expires=3600
sip_registration_server3=
sip_registration_server3_aor=
sip_registration_server3_username=

```

```

sip_registration_server3_password=
sip_registration_server3_expires=3600
sip_registration_server4=
sip_registration_server4_aor=
sip_registration_server4_username=
sip_registration_server4_password=
sip_registration_server4_expires=3600
sip_registration_interval=60
sip_Max-Forwards=70
sip_From=5000@193.120.221.160
sip_Contact=193.120.221.160:5060
sip_username=PassportFAX
sip_session_name=Passport
sip_session_description=
sip_description_URI=
sip_email=
sip_phone=
sip_Route=
sip_session_timer_session_expires=0
sip_session_timer_minse=-1
sip_session_timer_refresh_method=0
sip_ip_interface=
sip_ip_interface_port=5060
sip_redirect_as_calling_party=0
sip_redirect_as_called_party=0
sip_user_agent=Brktsip/6.2.0B5 (Dialogic)
[host_module.1/rtp]
rtp_codec=pcma
rtp_frame_duration=20
rtp_jitter_buffer_depth=100
rtp_silence_control=inband
rtp_type_of_service=0
rtp_voice_frame_replacement=0
[module.41]
model=SR140
virtual=1
exists=1
vb_firm=C:\Program Files\Passport4000\FaxService\Brooktrout\bostvb.dll
channels=2
[module.41/ethernet.1]
ip_interface={16814059-C4B1-41DC-89EF-DE047D8FAAD8}:0
media_port_min=56000
media_port_max=57000
[module.41/host_cc.1]
host_module=1
number_of_channels=2

```

©2010 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.