Avaya Solution & Interoperability Test Lab

Application Notes for Configuring FaxCore Evolution Fax Server with Avaya Aura® Communication Manager R6.2 and Avaya Aura® Session Manager R6.3 via SIP Trunk Interface - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring FaxCore Evolution Fax Server with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using a SIP trunk interface.

FaxCore Evolution (eV5) is a software based fax server that sends and receives fax calls over an IP network. In the configuration tested, FaxCore Evolution Fax Server interoperated with Avaya Aura® Session Manager to send/receive faxes using SIP trunks and the T.38 fax protocol.

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 procedures for configuring FaxCore Evolution Fax Server, herein referred to as FaxCore eV5, with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using a SIP trunk interface.

FaxCore Inc. is the next generation fax server built natively on the Microsoft .NET platform, which provides a secure manageable, flexible and efficient way to fax while leveraging internet technologies such as web and e-email. The award-winning FaxCore fax server makes it possible for companies to easily add electronic fax to MFPs, phone systems offering T.38 and other back-office applications.

FaxCore eV5 is a software based fax server that sends and receives fax calls over an IP network. FaxCore eV5 utilizes the Brooktrout SR140 T.38 Fax over Internet Protocol (FoIP) virtual fax software from Dialogic. In the configuration tested, FaxCore eV5 interoperated with Avaya Aura® Session Manager to send/receive faxes using SIP trunks and the T.38 protocol between FaxCore eV5 and the Avaya infrastructure.

2. General Test Approach and Test Results

This section describes the general test approach used to verify the interoperability of FaxCore eV5 with Avaya Communication Manager and Session Manager via SIP trunks

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 general test approach was to make intra-site and inter-site fax calls to and from the FaxCore eV5. The compliance tested configuration contained two sites. Site 2 served as the main enterprise site and Site 1 served as a simulated PSTN or a remote enterprise site. Inter-site calls and simulated PSTN calls were made using SIP trunks and ISDN-PRI trunks between the sites. Faxes were sent with various page lengths, resolutions, and at various fax data speeds. For capacity testing, 100 2-page faxes were continuously sent between the two FaxCore eV5 fax servers. Serviceability testing included verifying proper operation/recovery from network outages, unavailable resources, Communication Manager and FaxCore eV5 restarts. Fax calls were also tested with different Avaya Media Gateway media resources to process the fax data. This included 2 TN2302 MedPro circuit packs, 2 TN2602 MedPro circuit packs in the Avaya G650 Media Gateway; and the integrated VoIP engine of the Avaya G450 Media Gateway with 4 MP80s VoIP Modules.

Specifically, the following fax operations were tested during compliance testing:

- Faxes from/to a fax server to/from an analog fax machine at a local site
- Faxes from/to a fax server to/from an analog fax machine at a remote site
- Faxes from/to a fax server to/from a fax server at a remote site

2.2. Test Results

All test cases were executed and passed with the following exceptions/observations noted:

- During serviceability testing when the FaxCore eV5 servers were reset, faxes in the state of 'sending' would remain in a hung state until a force reset of that fax was issued. Faxes in queue or schedule state resumed with no issues observed.
- FaxCore software does not currently support media shuffling.

2.3. General Observation

Fax calls consume DSP (Digital Signal Processing) resources for processing fax data on the TN2302 IP Media Processor (MedPro) circuit pack and the TN2602 IP Media Processor circuit pack in the Avaya G650 Media Gateway and the integrated Voice over Internet Protocol (VoIP) engine of the Avaya G450 Media Gateway. To increase the capacity to support simultaneous fax calls, additional TN2302 and/or TN2602 MedPro circuit packs may need to be installed in the Avaya G650 Gateway, and additional Avaya MP80 VoIP Module or Modules need to be installed in the Avaya G450 Media Gateway. Customers should work with their Avaya sales representatives to ensure that their fax solutions have adequate licenses and DSP resources to match the intended Fax capacity/usage.

2.4. Support

For technical support on FaxCore eV5, contact FaxCore at:

- Web: http://www.faxcore.com/support.asp
- Phone: 1 (888) 905-4881
- Email: support@faxcore.com

3. Reference Configuration

The test configuration was designed to emulate two completely separate corporations/sites with multiple Port Networks at one site (Site 1), and modular Gateway resources at the other site (Site 2). **Figure 1** illustrates the configuration used in these Application Notes, with a focus on the configuration at Site 2. Communication Manager Servers and Gateways at the two sites were connected via SIP and ISDN-PRI trunks. Faxes were alternately sent between the two sites using these two facilities. The fax servers communicated directly with Session Manager via SIP. Each Session Manager was configured using a System Manager.

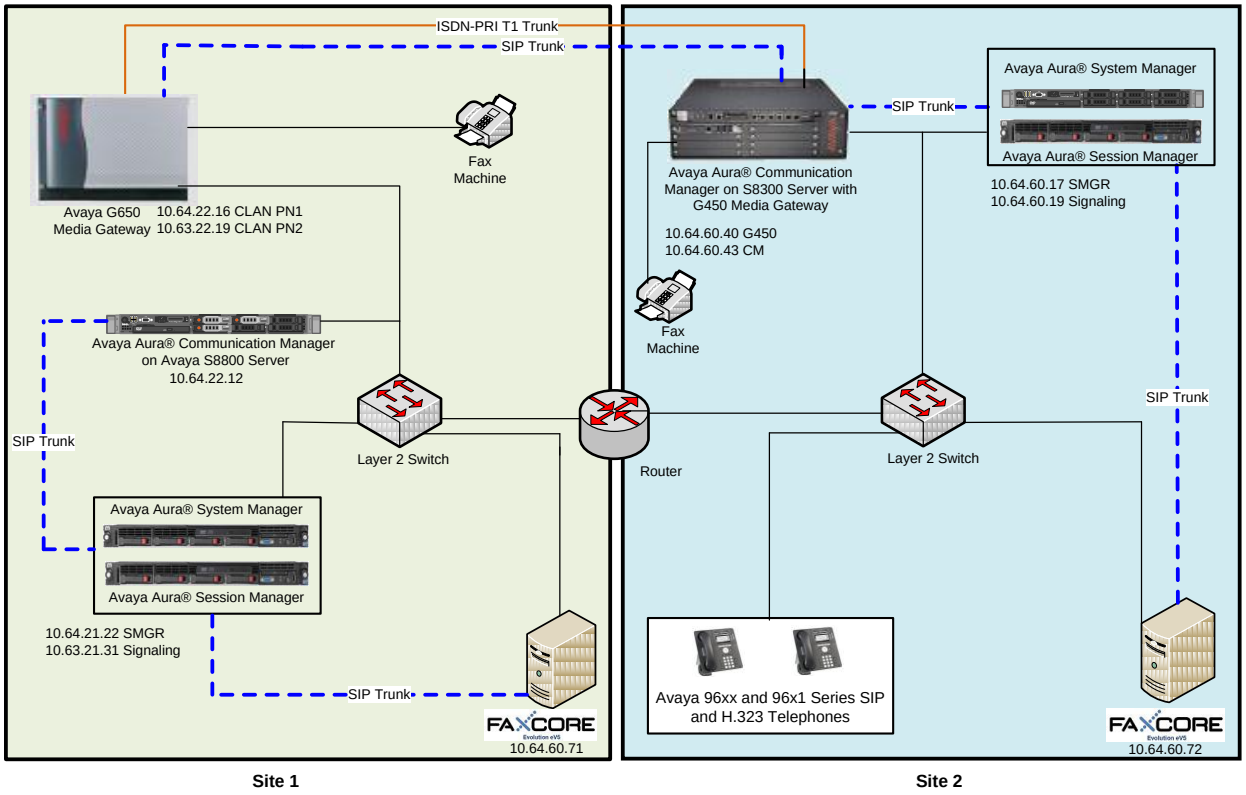


Figure 1: FaxCore eV5 Test Configuration

Site 1 consisted of an Avaya S8800 Server running Communication Manager with an Avaya G650 Media Gateway. The FaxCore eV5 running on a Windows 2008 Server at this site communicated with Session Manager via a SIP trunk. Session Manager communicated with Communication Manager via a SIP trunk which terminated on a CLAN circuit pack in port network 2.The media resources required are provided by the IP Media Processor (MedPro) circuit packs. Two versions of the IP MedPro circuit pack were tested in the configuration: the TN2302 and the TN2602. Various IP endpoints at this site included Avaya one-X® Deskphone 96xx and 96x1 (not all shown) series phones and an analog fax machine.

Site 2 consisted of an Avaya S8300D Server running Communication Manager in an Avaya G450 Media Gateway. The signaling and media resources needed to support SIP trunks are integrated directly on the media gateway processor with DSP childboards. The G450 for this test had 4 MP80 VoIP Modules installed. The FaxCore eV5 running on a Microsoft Windows 2008 Server at this site communicated with Session Manager via an SIP trunk. Various IP endpoints at this site included Avaya one-X® Deskphone 96xx and 96x1 (not all shown) series phones and an analog fax machine.

The IP phones (H.323 and SIP) at each site had no specific role in fax operations; therefore, this part of the configuration is not covered in these Application Notes. They were present in the configuration to verify VoIP telephone calls did not have an adverse impact on the FoIP faxing operations.

A fax call originating from a local fax server was sent to Session Manager via a SIP trunk. Based on the dialed digits, Session Manager and Communication Manager routed the fax call either to the local fax machine or to one of the trunks (ISDN-PRI or SIP) to reach the remote site. When the fax call reached the remote site, the Communication Manager at that site routed the call either to the local fax machine or to Session Manager for onward routing to the local fax server over the SIP trunk.

4. Equipment and Software Validated

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

Equipment	Software
Site 1	
Avaya S8800 Server	Avaya Aura® Communication Manager R6.2 (R016x.02.0.823.0, Patch 20199)
Dell™ PowerEdge™ R610	Avaya Aura ® System Manger 6.3.0 - GA (Build No. - 6.3.0.8.5682-6.3.8.818 Software Update Revision No: 6.3.0.8.923)
HP ProLiant DL360 G7 Server	Avaya Aura® Session Manger 6.3.0.0.630039
Avaya G650 Media Gateway - 2 CLANs - 2 MedPros – TN2302 - 2 MedPros – TN2602	 TN799DP - HW01 FW38 & HW13 FW 38 TN2302AP - HW20 FW120 TN2602AP - HW04 FW63
FaxCore Web Client	6.0.1.19
FaxCore eV5 - running on a Windows Server 2008 R2	eV5
Dialogic Brooktrout SR140 Fax Software – Boston Bfv API – Boston Driver	 v6.5.5 (Build 8) v6.5.2 (Build 2)

Analog Fax Machine	-
Avaya one-X® Deskphones **(**SIP)	6.2.1 (96xx) 2.6.9 (96x1)
Avaya one-X® Deskphones (H.323)	6.2.2 (96xx) 3.1.5 (96x1)
Site 2	
Avaya S8300D Server	Avaya Aura® Communication Manager R6.2 (R016x.02.0.823.0, Patch 20199)
Avaya G450 Media Gateway	32.24.0
HP ProLiant DL360 G7 Server	Avaya Aura ® System Manger 6.3.0 - GA (Build No. - 6.3.0.8.5682-6.3.8.818 Software Update Revision No: 6.3.0.8.923)
HP ProLiant DL360 G7 Server	Avaya Aura® Session Manger 6.3.0.0.630039
FaxCore eV5 - running on a Windows Server 2008 R2	eV5
Dialogic Brooktrout SR140 Fax Software – Boston Bfv API – Boston Driver	 v6.5.5 (Build 8) v6.5.2 (Build 2)
Analog Fax Machine	-
Avaya one-X® Deskphones **(**SIP)	6.2.1 (96xx) 2.6.9 (96x1)
Avaya one-X® Deskphones (H.323)	6.2.2 (96xx) 3.1.5 (96x1)

5. Configure Avaya Aura® Communication Manager

This section describes the Communication Manager configuration necessary to interoperate with the FaxCore eV5. It focuses on the configuration of the routing and SIP trunk between Communication Manager and Session Manager. All other components are assumed to be in place and previously configured, including the SIP and ISDN-PRI trunks that connect Sites 1 and 2 in **Figure 1**.

The examples shown in this section refer to Site 2. Similar steps also apply to Site 1 using values appropriate for that location.

The configuration of Communication Manager was performed using the System Access Terminal (SAT). After the completion of the configuration, perform a **save translation** command to make the changes permanent.

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

- Verify Communication Manager License
- IP Codec Set
- IP Network Region
- IP Node Names
- SIP Signaling Group
- SIP Trunk Group
- Private Numbering
- Route Pattern
- AAR Analysis

5.1. Verify Avaya Aura® Communication Manager

Use the **display system-parameters customer-options** command and on **Page 2,** verify that the **Maximum Administered SIP Trunks** have sufficient remaining capacity. The example shows that **4000** licenses are available and **75** are in use.

The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity.

```
display system-parameters customer-options                    Page   2 of  11
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 4000  80
          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  0
                   Maximum Video Capable IP Softphones: 2400  0
                      Maximum Administered SIP Trunks: 4000  75
  Maximum Administered Ad-hoc Video Conferencing Ports: 4000  0
   Maximum Number of DS1 Boards with Echo Cancellation: 80    0
                            Maximum TN2501 VAL Boards: 10    0
                    Maximum Media Gateway VAL Sources: 50    0
          Maximum TN2602 Boards with 80 VoIP Channels: 128   0
         Maximum TN2602 Boards with 320 VoIP Channels: 128   0
   Maximum Number of Expanded Meet-me Conference Ports: 300   0

       (NOTE: You must logoff & login to effect the permission changes.)
```

5.2. IP Codec Set

Use the **change ip-codec-set command** to administer an IP codec set. IP codec set **1** was used during compliance testing. Multiple codecs can be listed in priority order to allow the codec used by a specific call to be negotiated during call establishment. The example below shows the values used during compliance testing. IP codec sets are used in **Section 5.3** for configuring IP network regions to specify which codec sets may be used within and between network regions.

```
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:
```

On **Page 2**, set the **FAX Mode** field to ***t.38-standard***. The **Modem Mode** field should be set to ***off***.

Leave the **FAX Redundancy** setting at its default value of ***0.*** A packet redundancy level can be assigned to improve packet delivery and robustness of FAX transport over the network (with increased bandwidth as trade-off). Avaya uses IETF RFC-2198 and ITU-T T.38 specifications as redundancy standard. With this standard, each Fax over IP packet is sent with additional (redundant) 0 to 3 previous fax packets based on the redundancy setting. A setting of 0 (no redundancy) is suited for networks where packet loss is not a problem.

```
change ip-codec-set 1                                          Page   2 of   2

                         IP Codec Set

                             Allow Direct-IP Multimedia? n

     Maximum
                    Mode                Redundancy
    FAX             t.38-standard        0
    Modem           off                  0
    TDD/TTY         US                   3
    Clear-channel   n                    0
```

5.3. IP-Network-Region

Use the **change ip-network-region** command to administer the network region settings. The values shown below are the values used during compliance testing. Note that the **IP-IP Direct Audio** settings must be disabled for faxing to work correctly with FaxCore eV5.

- **Authoritative Domain**: ***avaya.com***
- **Name**: Any descriptive name may be used (if desired).
- **Intra-region IP-IP Direct Audio**: ***no***
  Inter-region IP-IP Direct Audio: ***no***
  IP-IP Direct Audio (media shuffling) can be further restricted at the trunk level on the **Signaling Group** form.
- **Codec Set**: ***1*** The codec set contains the list of codecs available for calls within this IP network region.

```
change ip-network-region 1                                    Page   1 of  20
                            IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain: avaya.com
    Name: PN1
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: no
      Codec Set: 1              Inter-region IP-IP Direct Audio: no
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
SIP IP ENDPOINTS                                    RSVP Enabled? n
  SIP Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

5.4. IP Node Names

Use the **change node-names ip** command to create a node name and enter the IP address of Session Manager. Enter a descriptive name in the **Name** column and the Session Manager IP address in the **IP Address** column. Also note the node name of the processor (***procr***) as it will be used later to configure the SIP trunk between Communication Manager and Session Manager.

```
change node-names ip                                          Page   1 of   2
                                  IP NODE NAMES
    Name                  IP Address
CM_650                  10.64.22.16
default                 0.0.0.0
msgserver_cm2           10.64.60.43
procr                   10.64.60.43
procr6                  ::
smd4f26                 10.64.60.19
```

5.5. SIP Signaling Group

During compliance testing, a SIP signaling group and the associated SIP trunk group were used for routing fax calls to/from the fax server via Session Manager. Use the **add signaling group** command to create a signaling group for use by the SIP trunk to the FaxCore eV5. Signaling group 1 was configured using the parameters highlighted below. Default values may be used for all other fields.

The following values for the specified fields and the default values may be used for the remaining fields.

- Set the **Group Type** to ***SIP***.
- The **Transport Method** was set to the recommended default value of ***tls*** (Transport Layer Security). As a result, the **Near-end Listen Port** and **Far-end Listen Port** are automatically set to ***5061***.
- Set the **Near-end Node Name** to the node name that maps to the IP address of the processor (e.g., ***procr***) used to connect to Session Manager (See **Section 5.4**).
- Set the **Far-end Node Name** to the node name that maps to the IP address of Session Manager (See **Section 5.4**).
- Set the **Far-end Network Region** was set to ***1***. This is the IP network region which contains Session Manager and the fax server.
- Set the **Direct IP-IP Audio Connections** field to **n**. This setting disables Media Shuffling on the trunk level.

```
add signaling-group 1                                          Page   1 of   5
                              SIGNALING GROUP

  Group Number: 1              Group Type: sip
  IMS Enabled? n         Transport Method: tls
       Q-SIP? n
     IP Video? n                                  Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM



   Near-end Node Name: procr                 Far-end Node Name: smd4f26
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                         Far-end Network Region: 1

Far-end Domain: avaya.com
                                              Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                 RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload           Direct IP-IP Audio Connections? n
Session Establishment Timer(min): 3                    IP Audio Hairpinning? n
         Enable Layer 3 Test? y
                                                   Alternate Route Timer(sec): 20
```

5.6. SIP Trunk Group

Trunk group ***1*** was configured with the **add trunk-group** command using the parameters highlighted below. Default values may be used for all other fields.

On **Page 1**:

- Set the **Group Type** field to ***sip***.
- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Service Type** field to ***tie***.
- Set the **Member Assignment Method** to ***auto***.
- Set the **Signaling Group** to the signaling group configured in the previous section.
- In **Number of Members** field, enter the number of members in the trunk group. This determines how many simultaneous calls can be supported by the configuration.

```
add trunk-group 1                                              Page   1 of  21
                                TRUNK GROUP

Group Number: 1                     Group Type: sip           CDR Reports: y
  Group Name: smd4f26                        COR: 1        TN: 1        TAC: *001
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                  Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 1
                                                     Number of Members: 50
```

On **Page 3**:

- Set the **Numbering Format** field to ***private***. This field specifies the format of the calling party number sent to the far-end.

```
add trunk-group 1                                              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
```

5.7. Private Numbering

Private numbering defines the calling party number to be sent to the far-end. Use the **change private-numbering** command to create an entry that will be used by the trunk group defined in the previous section. In the example shown below, all calls originating from a 5-digit extension beginning with 4 or 5 and routed across any trunk group (since the **Trk Grp(s)** entry is blank) will be sent as a 5-digit calling number.

```
change private-numbering 0                                      Page   1 of   2
                         NUMBERING - PRIVATE FORMAT

Ext  Ext            Trk        Private          Total
Len  Code           Grp(s)     Prefix           Len
 5   4                                          5     Total Administered: 2
 5   5                                          5        Maximum Entries: 540
```

5.8. Route Pattern

Use the **change route-pattern** command to create a route pattern that will route calls to the SIP trunk that connects to Session Manager.

A descriptive name was entered for the **Pattern Name** field. The **Grp No** field was set to the trunk group created in **Section 5.6**. The Facility Restriction Level (**FRL**) field was set to a level that allows access to this trunk for all users that require it. The value of ***0*** is the least restrictive level. The **Numbering Format** was set to ***lev0-pvt***. The default values were used for all other fields.

```
change route-pattern 1                                          Page   1 of   3
                  Pattern Number: 1   Pattern Name: smd4f26
                                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: 1    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                               lev0-pvt  none
 2: y y y y y n  n            rest                                         none
 3: y y y y y n  n            rest                                         none
 4: y y y y y n  n            rest                                         none
 5: y y y y y n  n            rest                                         none
 6: y y y y y n  n            rest                                         none
```

5.9. AAR Analysis

Automatic Alternate Routing (AAR) was used to route calls to FaxCore via Session Manager. Use the **change aar analysis** command to create an entry in the AAR Digit Analysis Table for this purpose. The highlighted entry specifies that if the dialed number is 50000 and is 5 digits long, to use route pattern 1. Route pattern 1 routes calls to Session Manager.

```
change aar analysis 5                                        Page   1 of   2
                          AAR DIGIT ANALYSIS TABLE
                                Location: all            Percent Full: 2

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    50000                 5    5    1         aar          n
```

6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager as shown in the reference configuration. All provisioning for Session Manager is performed via the System Manager web interface. System Manager delivers a set of shared, secure management services and a common console across multiple products in the Avaya Aura® network, including the central administration of routing policies, and a common format for logs and alarms. This section assumes that Session Manager and System Manager have been installed and that network connectivity exists between the two platforms.

This section summarizes the configuration steps that are necessary for interoperating with FaxCore eV5. The test environment was previously configured to enable Communication Manager and Session Manager at each site to communicate with each other. Details of this configuration and the SIP endpoints are not described in this document. Additional information can be obtained from **Reference [3]**.

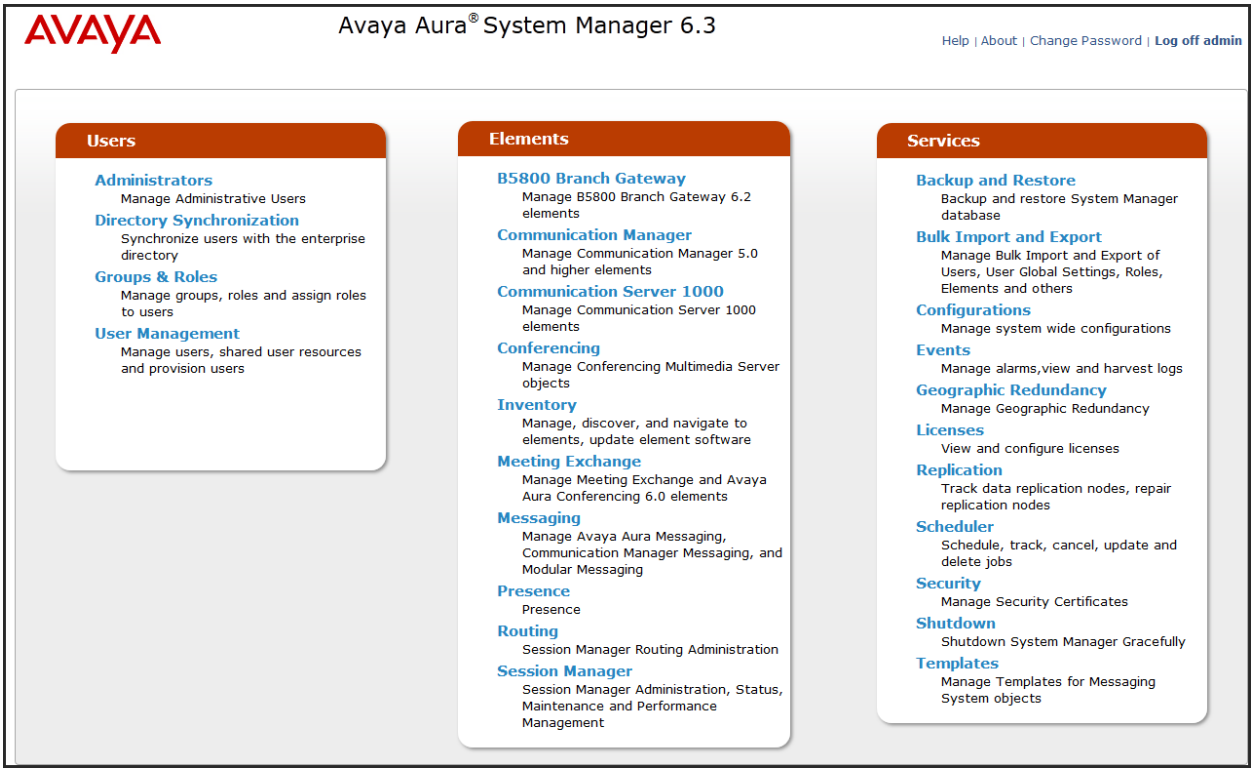
The examples shown in this section refer to Site 2. Similar steps also apply to Site 1 using values appropriate for that location.

The procedures described in this section include configurations for the following:

- **SIP Domains** - SIP Domains are the domains for which Session Manager is authoritative in routing SIP calls. In other words, for calls to such domains, Session Manager applies Network Routing Policies to route those calls to SIP Entities. For calls to other domains, Session Manager routes those calls to another SIP proxy (either a pre-defined default SIP proxy or one discovered through DNS).
- **SIP Entities** – Typically SIP Entities represent SIP network elements such as Session Manager instances, Communication Manager Systems, Session Border Controllers, SIP gateways, SIP trunks, and other SIP network devices.
- **Entity Links** – Connection information which define the SIP trunk parameters used by Session Manager when routing calls to/from other SIP Entities. (e.g., ports, protocol (UDP/TCP/TLS), and trust relationship).
- **Routing Policies** - Policies that determine which control call routing between the SIP Entities based on applicable Dial Patterns.
- **Dial Patterns** – Matching digit patterns which govern to which SIP Entity a call is routed.

Session Manager is managed via System Manager. Using a web browser, access ***https://<ip-addr of System Manager>/SMGR***.

Log in using appropriate credentials. The main page for the administrative interface is shown below.



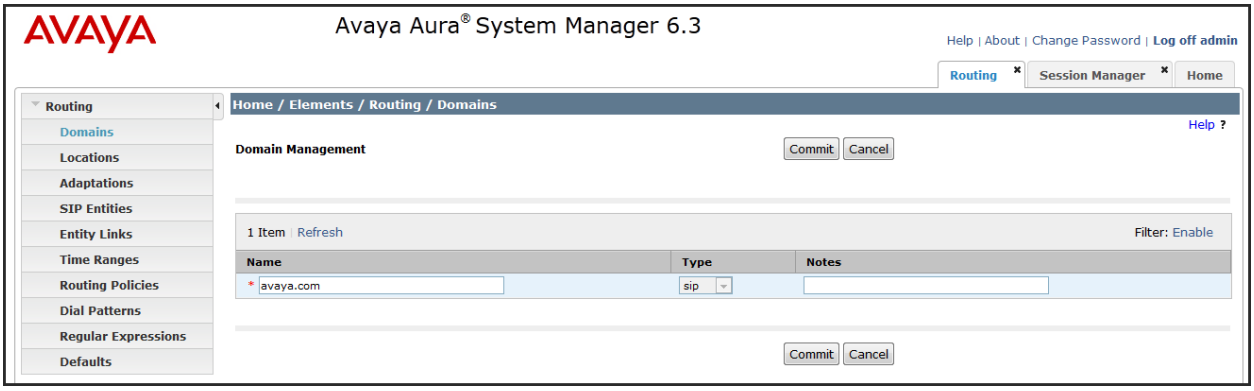
6.1. SIP Domains

In the reference configuration, one SIP domain was used; **avaya.com**.

Navigate to **Element → Routing → Domains** and click the **New** button (not shown) to add a new SIP domain with the following:

- **Name**: ***avaya.com***
- **Type** : ***sip***
- **Notes**: optional descriptive text

Click on the **Commit** button.



6.2. SIP Entity

A SIP Entity must be added for the Session Manager and for each SIP-based telephony system supported by it using SIP trunks. During compliance testing, a SIP Entity was added for Session Manager (not shown), Communication Manager (not shown), and the FaxCore eV5 server.

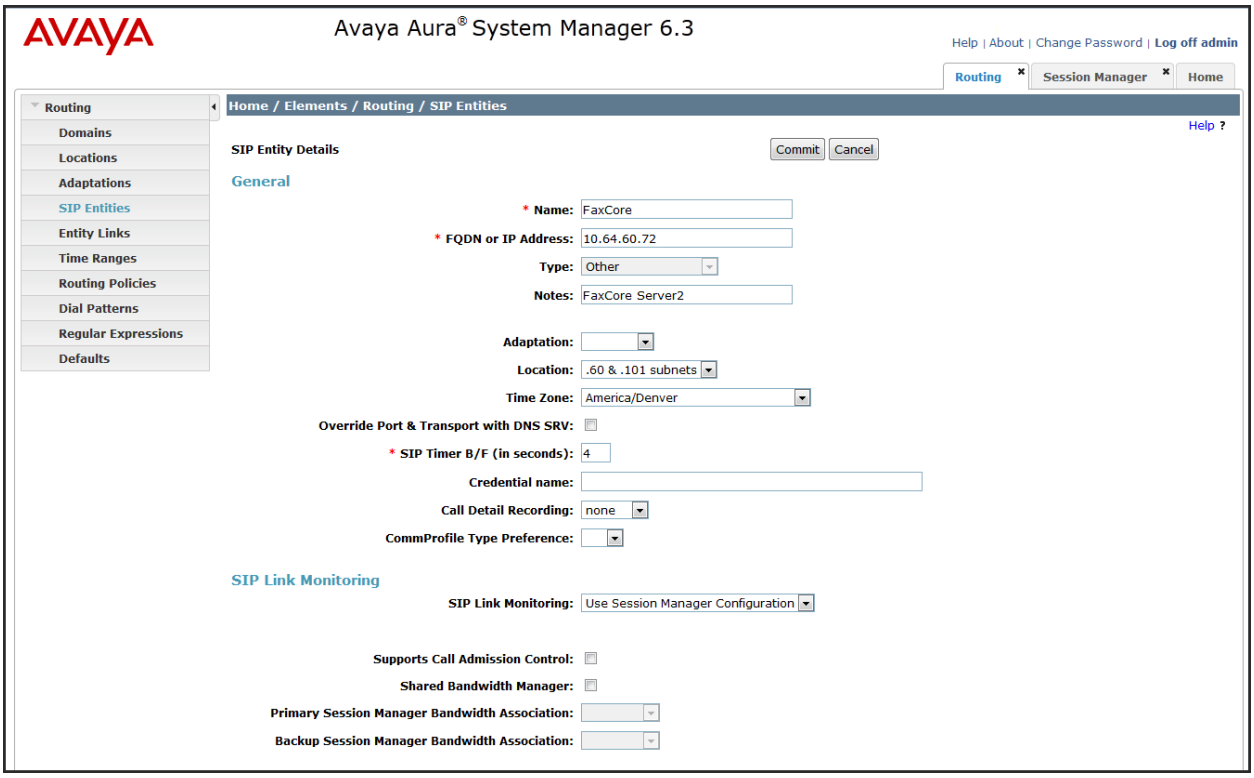
Navigate to **Routing → SIP Entities**, and click the **New** button (not shown) to add a SIP Entity. The configuration details for the SIP Entity defined for the fax server are as follows:

Under **General**

- **Name**: a descriptive name.
- **FQDN or IP Address**: ***10.64.60.72*** (FaxCore server in Site 2).
- **Type**: select ***Other***.
- **Location**: select a previously defined location (the definition of the location is not shown in this document). Selecting a location is optional.

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

The screen below shows the SIP Entity configuration details for the fax server.



6.3. Entity Link

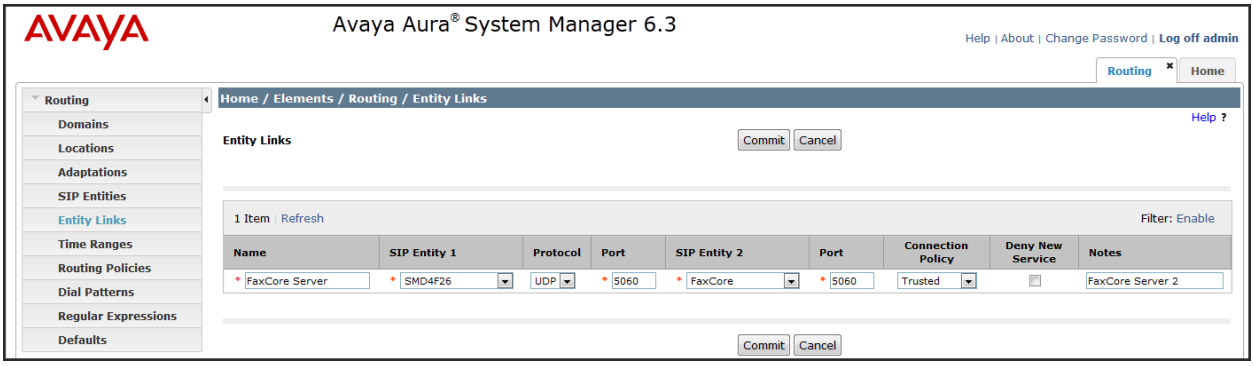
A SIP trunk between Session Manager and a telephony system is described by an Entity link. Two Entity Links were created:

- Session Manager ←→ Communication Manger (not shown)
- Session Manager ←→ FaxCore

Navigate to **Routing→Entity Links**, and click the **New** button (not shown) to add a new Entity Link. The screen below shows the configuration details for the Entity Link connecting Session Manager to the fax server.

- **Name**: a descriptive name.
- **SIP Entity 1**: select the Session Manager SIP Entity.
- **Protocol**: select ***UDP*** as the transport protocol to match the protocol used by the fax server.
- **Port**: ***5060***. This is the port number to which the other system sends SIP requests.
- **SIP Entity 2**: select the fax server SIP Entity.
- **Port:** ***5060***. This is the port number on which the other system receives SIP requests.
- **Connection Policy**: select ***Trusted***.
- **Notes**: optional descriptive text.

Click **Commit** to save the configuration.



6.4. Routing Policy

Routing Policies were added for routing fax calls to the fax server and calls from the fax server to other SIP entities (not shown).

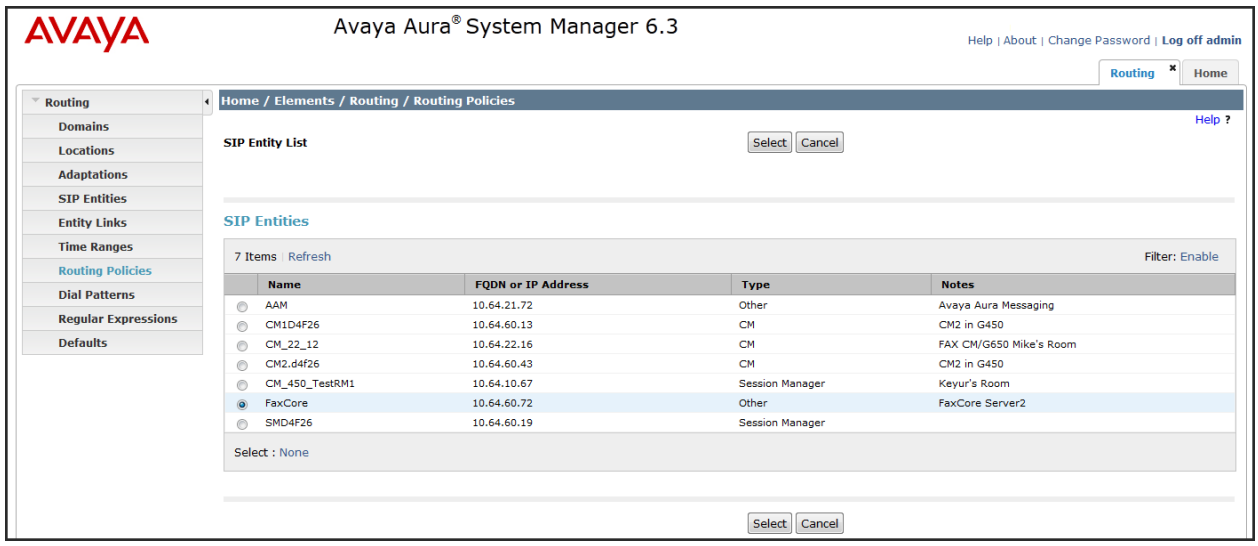
Navigate to **Routing→Routing Policies**, and click the New button (not shown) to add a new Routing Policy.

Under **General**

- **Name**: a descriptive name.
- **Notes**: optional descriptive text.

Under **SIP Entity as Destination**

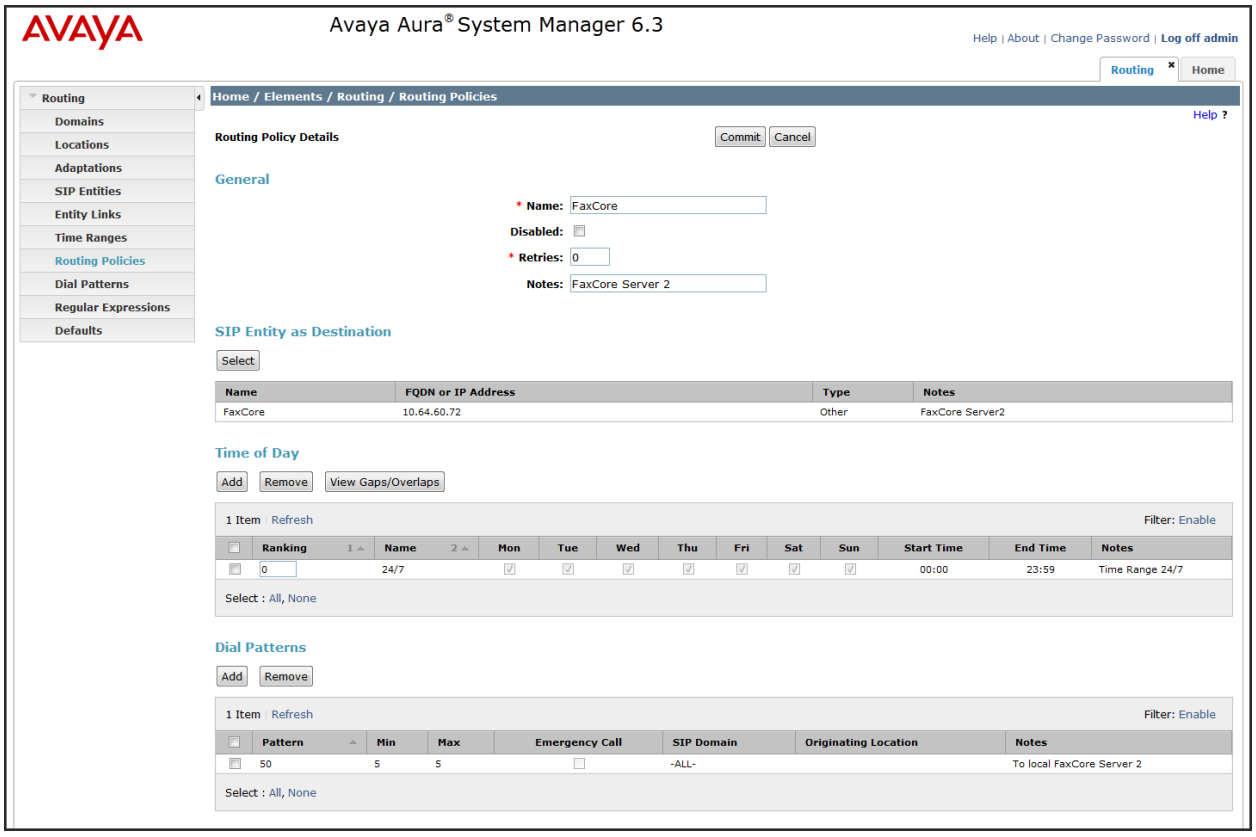
Click the **Select** button and the screen below is displayed. Select the **FaxCore** SIP Entity (defined in **Section 6.2**), to which the routing policy applies, and click the **Select** button to return to the previous screen.



Under **Time of Day**
Click **Add** to select a Time Range (not shown since the default time range of 24/7 was used during compliance testing).

Default settings can be used for the remaining fields. Click **Commit** to save the configuration.

The screen below shows the routing policy used during compliance testing.



6.5. Dial Pattern

Dial Patterns define digit strings to be matched against dialed numbers for directing calls to the appropriate SIP Entities. 5-digit numbers beginning with "50" were routed to the fax server.

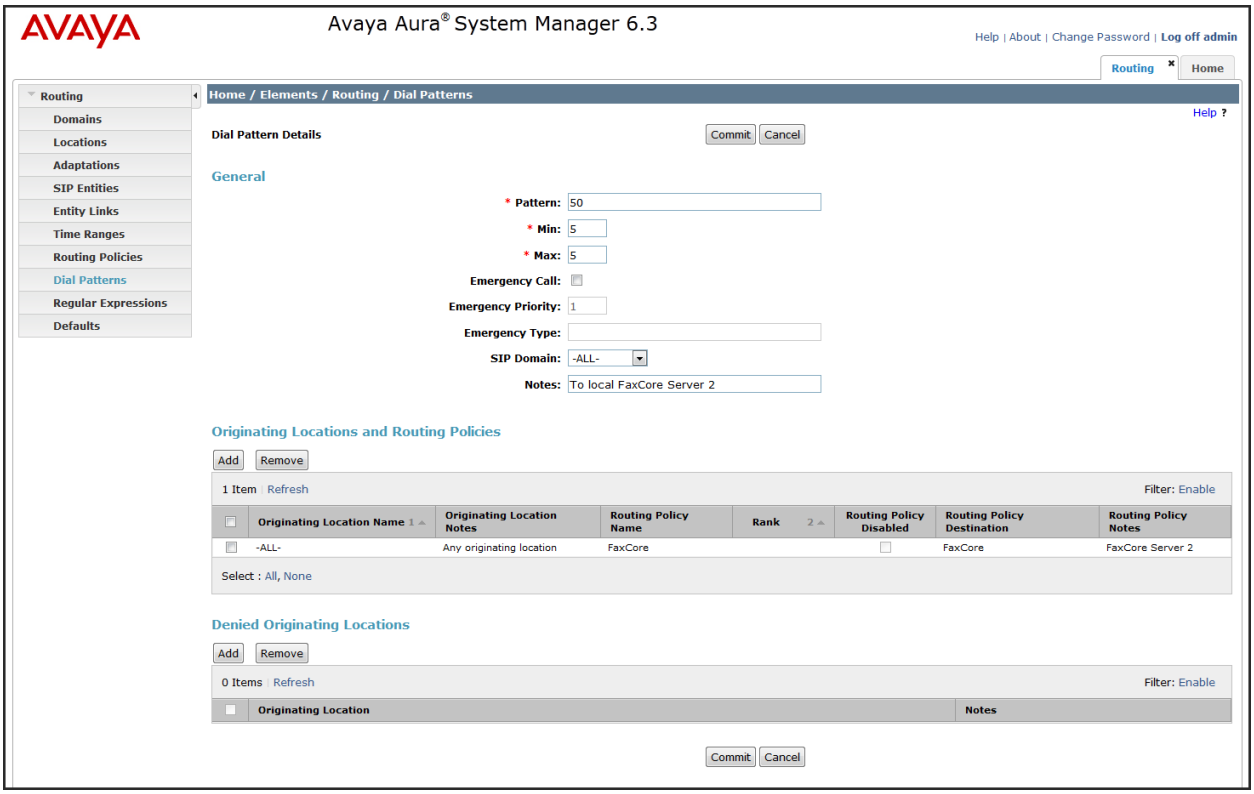
Navigate to **Routing→Dial Patterns**, click the **New** button (not shown) to add a new Dial Pattern.

Under **General**

- **Pattern**: dialed number or prefix.
- **Min**: minimum length of dialed number.
- **Max**: maximum length of dialed number.
- **SIP Domain**: select the SIP Domain created in **Section 6.1** (or select –ALL– to be less restrictive).
- **Notes**: optional descriptive text.

Under **Originating Locations and Routing Policies**
Click **Add** to select the appropriate originating Location (e.g., **–ALL–**) and Routing Policy (e.g., **FaxCore**) from the list (not shown).

Default settings can be used for the remaining fields. Click **Commit** to save the configuration.



7. Configure FaxCore eV5

This section describes the configuration of FaxCore eV5 Software. It assumes that the fax server application and all required software components, including Dialogic Brooktrout SR140 Fax Software, have been installed and properly licensed. For instructions on installing Dialogic Brooktrout SR140 Fax Software, consult the Dialogic Brooktrout SR140 Fax Software documentation (**Reference [4]**).

FaxCore eV5 uses the Brooktrout configuration tool. The configurations documented in this section pertain to interoperability between FaxCore Evolution and the Avaya SIP infrastructure. The standard configuration pertaining to the Dialogic Brooktrout SR140 (e.g., administering fax channels) are not covered; see Reference [4] for this information.

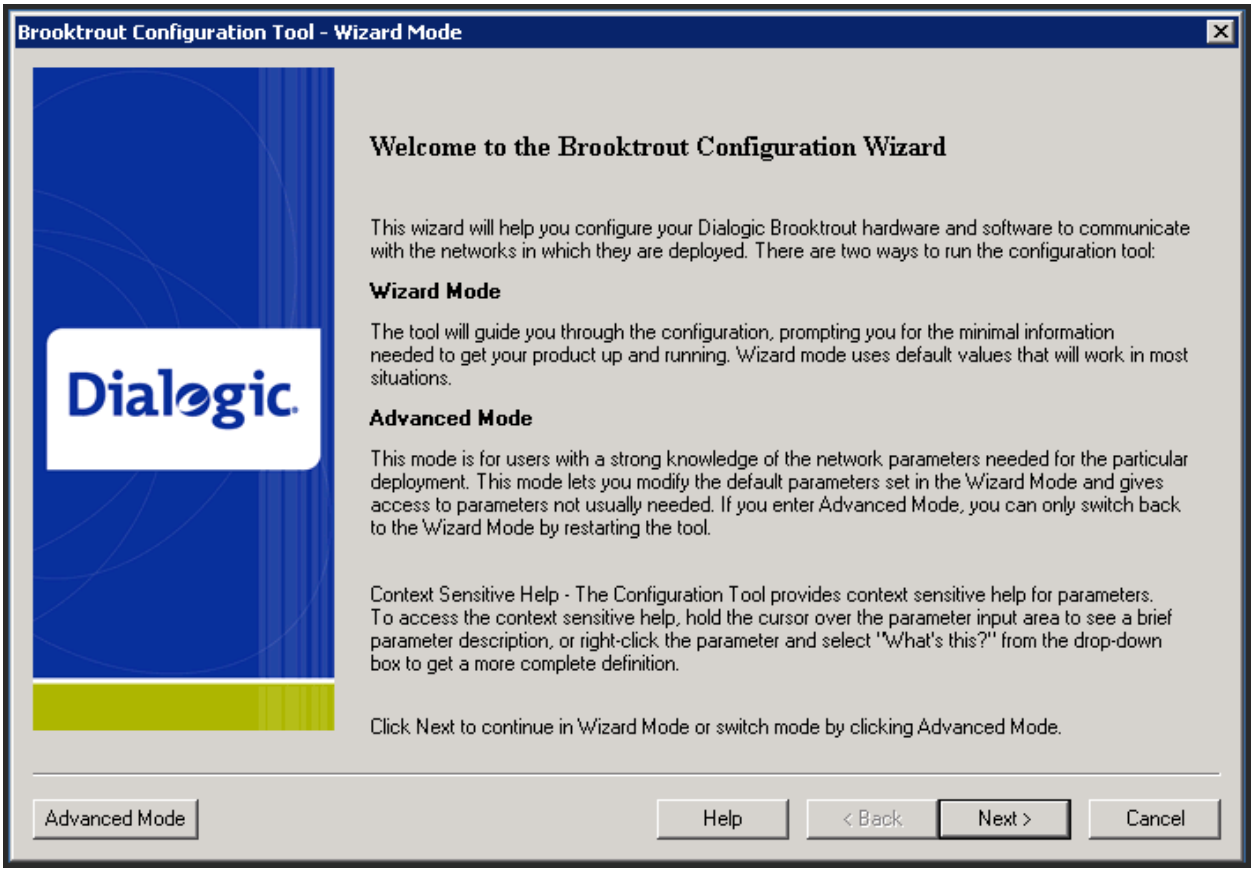
The examples shown in this section refer to Site 2 in **Figure 1**. Similar steps also apply to Site 1 using values appropriate for that location

The configuration procedures covered in this section include the following:

- Launch Brooktrout Configuration Tool
- Configure IP Stack
- Configure SIP IP Parameters
- Configure T.38 Parameters
- Configure RTP Parameters
- Configure RTP Port Range
- Complete Brooktrout SR140 Configuration

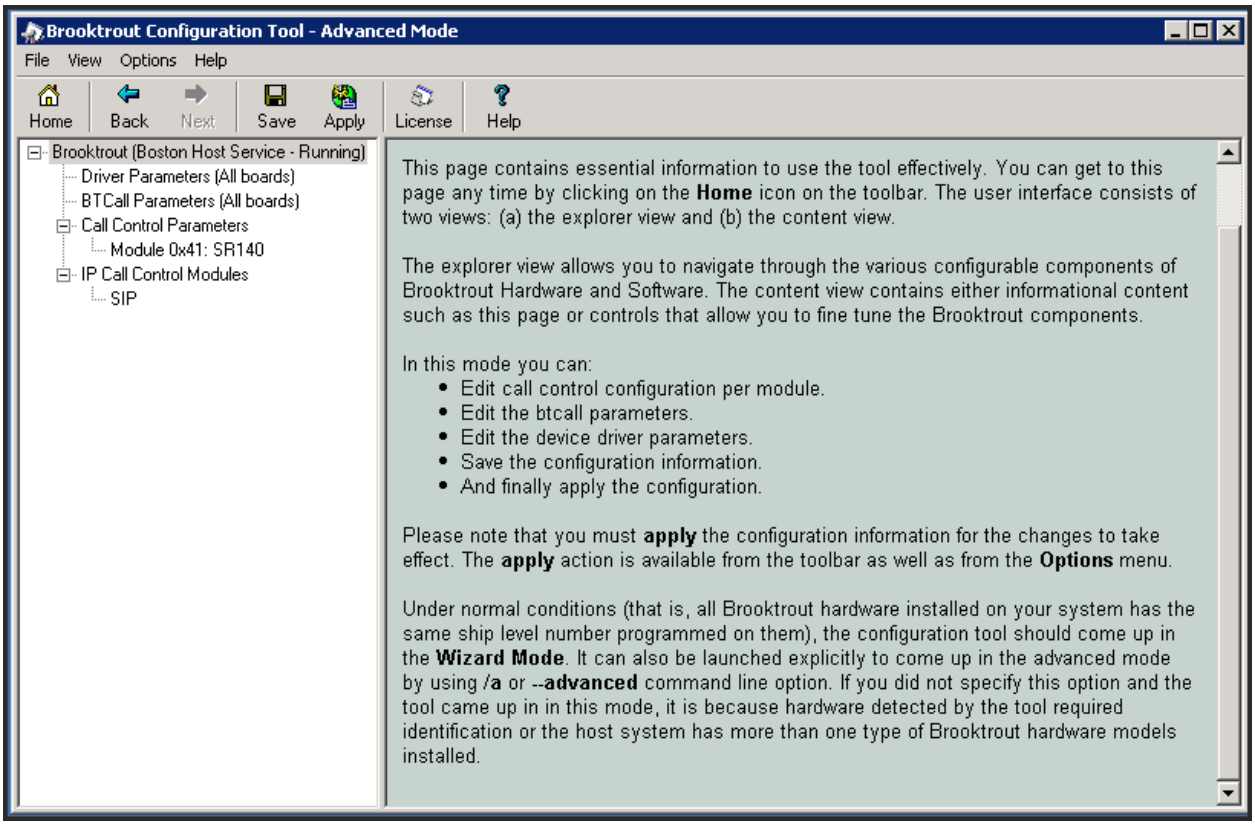
7.1. Launch Brooktrout Configuration Tool

Navigate to the path of the Brooktrout configuration tool (**configtool.exe**) and launch the tool. The **Brooktrout Configuration Tool – Wizard Mode** window gets displayed. Click the **Advanced Mode** button on the bottom left.

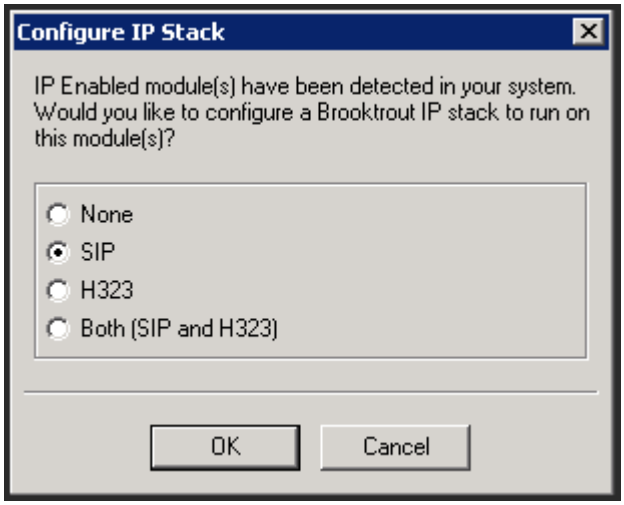


7.2. Configure IP Stack

The following configuration tool window is displayed.



Select **Options → Configure IP Stack** from the top menu. The screen below is displayed. Select **SIP** and click **OK**.



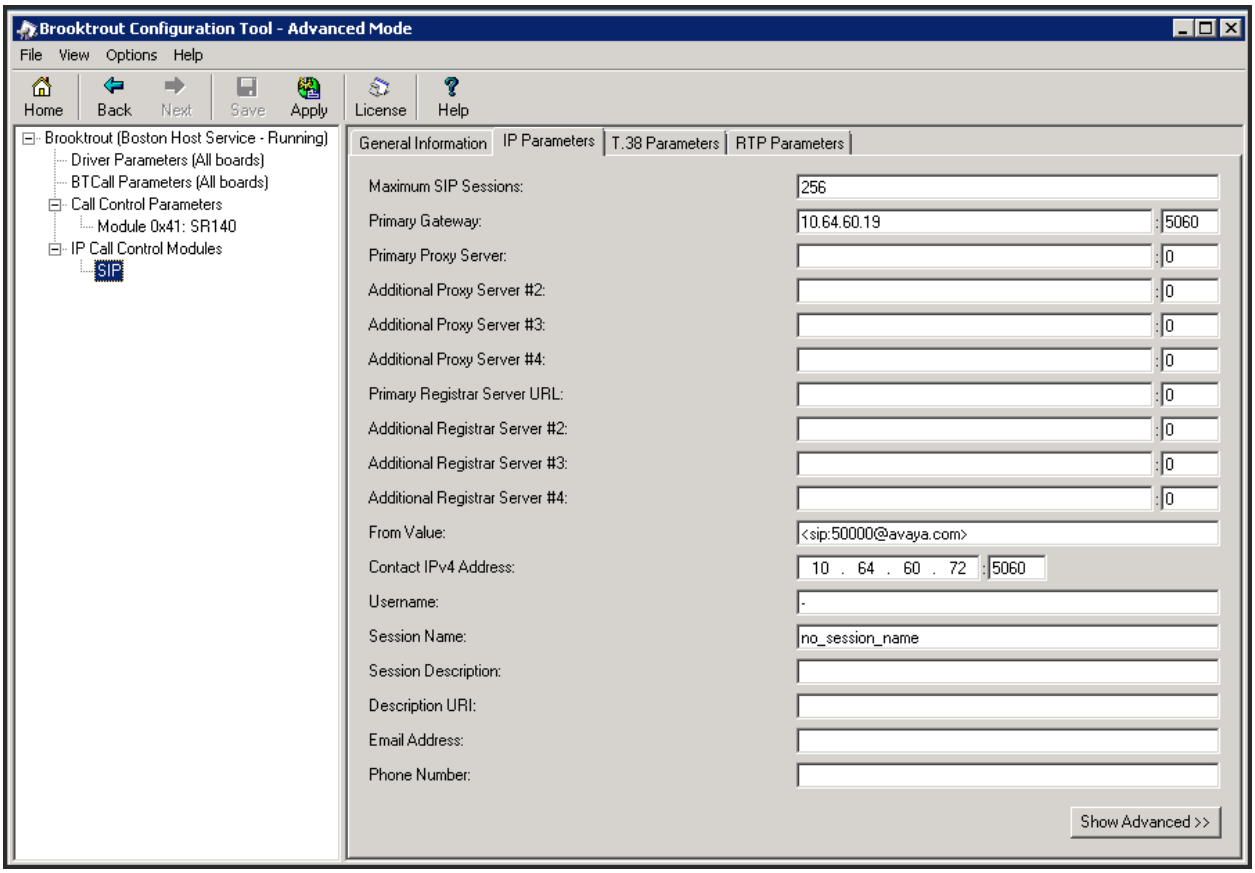
7.3. Configure SIP IP Parameters

Important: *This step describes configuring the SIP Primary Gateway address using the Brooktrout Configuration Tool. This method is sufficient if the fax server will communicate with a single SIP gateway. Refer to the Dialogic Brooktrout SR140 Fax Software documentation for configuration details if the fax server will communication with multiple SIP gateways*.

From the pane on the left, navigate to **Brooktrout → IP Call Control Modules → SIP** in the left navigation menu. Select the **IP Parameters** tab in the right pane. Configure the fields as follows:

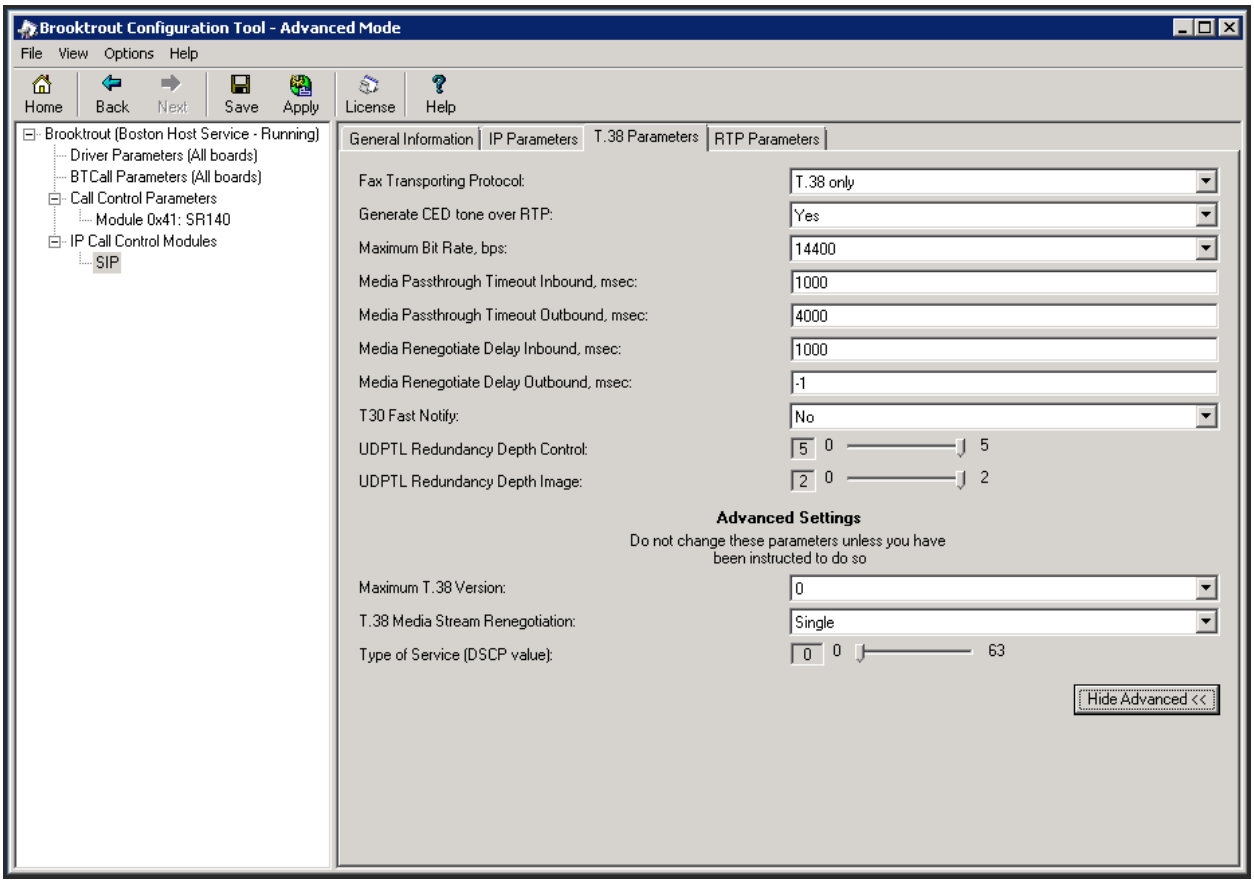
- **Primary Gateway** – set to the IP address of the Session Manager, and port number ***5060***.
- **From Value** – set to appropriate format of ***UserInfo@DomainName***. The *DomainName* should be set to the authoritative domain as configured in Session Manager.
- **Contact Address** – set to the IP address assigned to the FaxCore eV5 server and the port number ***5060***.
- Username – Required. Default value is a dash ("-") character.

Use default values for all other fields.



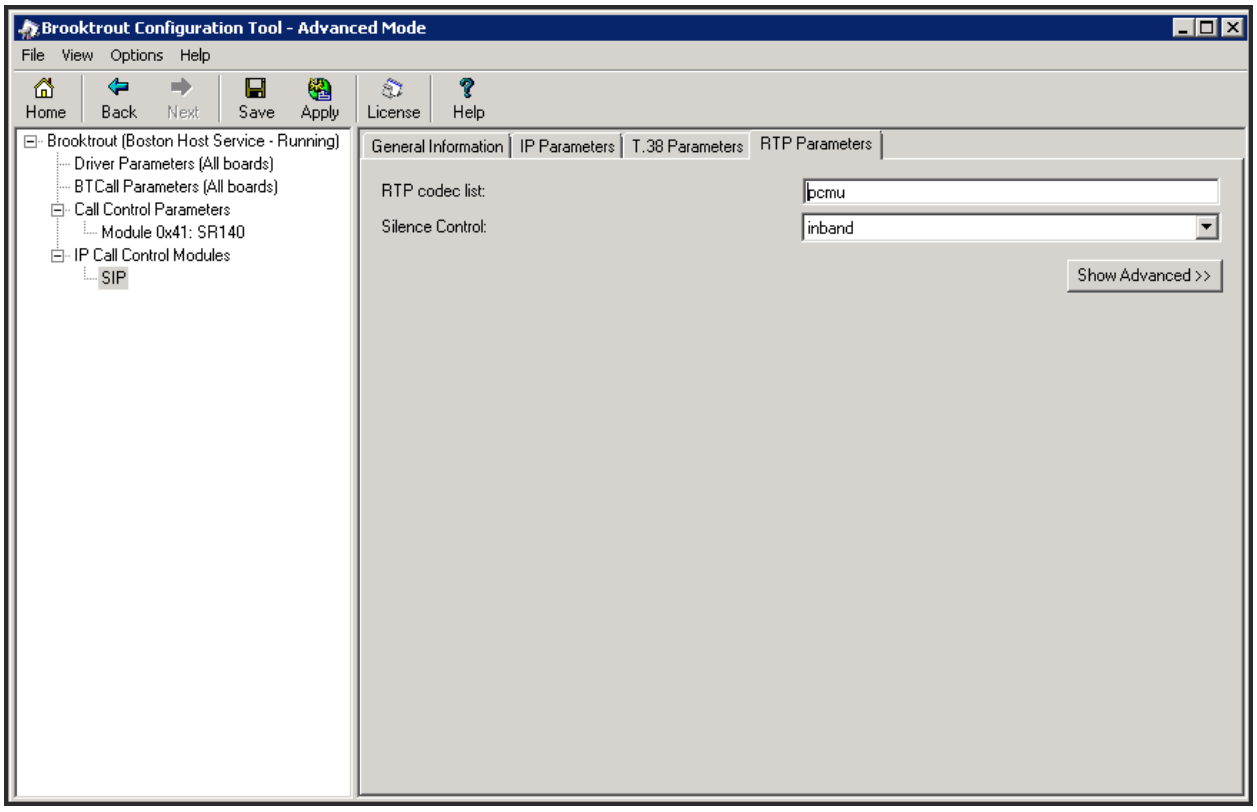
7.4. Configure T.38 Parameters

Select the **T.38 Parameters** tab. The screenshot below shows the values used during the compliance testing.



7.5. Configure RTP Parameters

Select the **RTP Parameters** tab. Set the **RTP codec list** value to use only a single codec, either ***pcmu*** or ***pcma*** to match the codec used in your region.

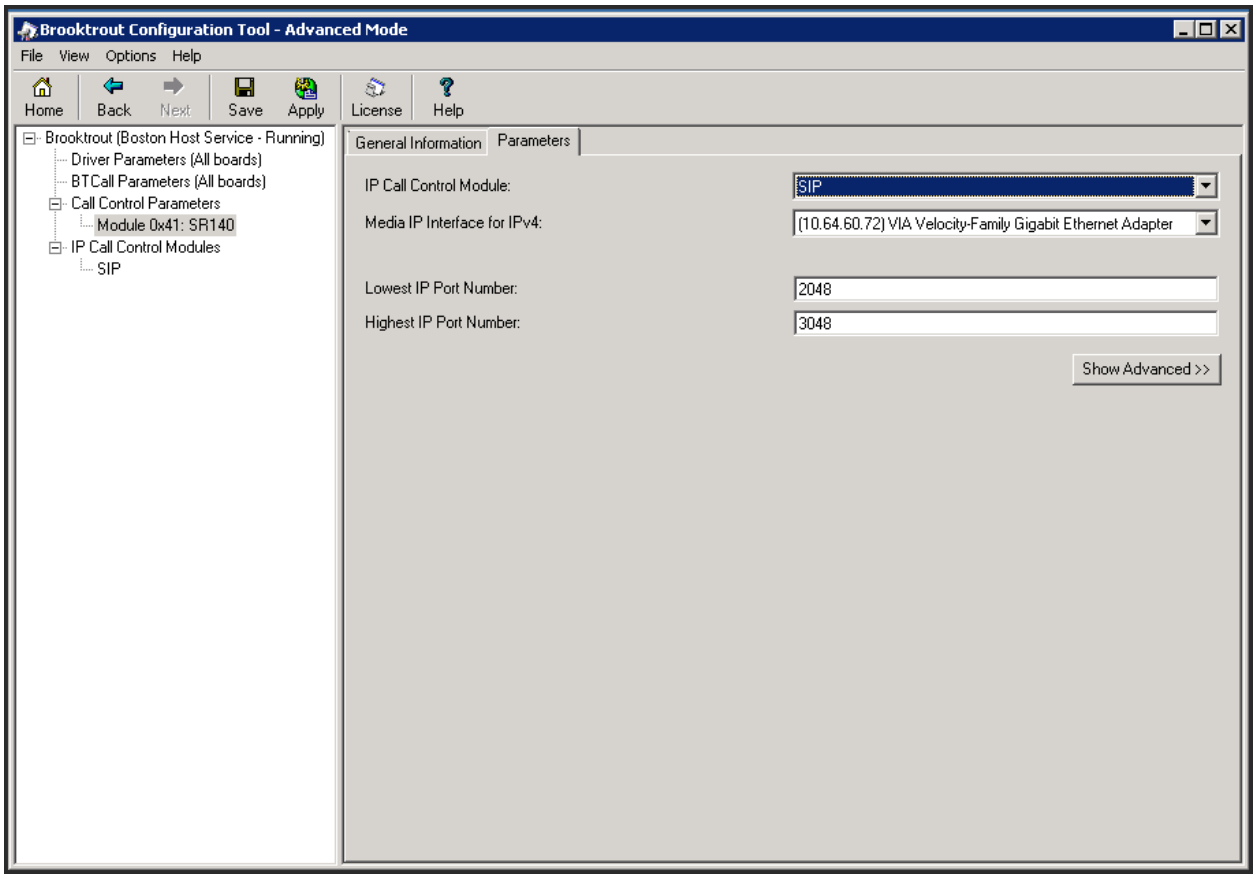


7.6. Configure RTP Port Range

From the pane on the left, navigate to **Call Control Parameters → Module 0x41: SR140**.

Select the **Parameters** tabs. Configure the **Lowest IP Port Number** and **Highest IP Port Number** values to match the **UDP Port Min** and **UDP Port Max** values in **the IP Network Region** configuration screen in Communication Manager.

Note: *The Communication Manager default port range is 2048 to 3329; however, the Brooktrout Configuration Tool range only spans 1000 ports. If Lowest IP Port Number is set to 2048, the Highest Port Number should automatically be set to 3048.*



7.7. Complete Configuration

After verifying all the above parameters are properly set, click **Save** in the button menu and exit the Brooktrout Configuration Tool.

From Windows explorer, navigate to the path of the Brooktrout call control configuration file (**callctrl.cfg**). Open the **callctrl.cfg file** and verify the following (making any edits as necessary):

- Verify that the following configuration segment is present; and that the **rtp_codec** value under the **[host_module.1/rtp]** header matches the value specified in **Section 7.5** above, either "pcmu" or "pcma". (Note, . . . below indicates other entries under the header).

```
[host_module.1/rtp]
 ...
rtp_codec=pcmu
 ...
```

- Verify that **rtp_ced_enable** is set to ***true*** under the **[host_module.1/t.38parameters]** header. (Note, . . . below indicates other entries under the header).

```
[host_module.1/t.38parameters]
 ...
 rtp_ced_enable=true
 ...
```

After making and saving any edits in the **callctrl.cfg** file, restart the fax server.

8. Verification Steps

The following steps may be used to verify the configuration:

- From Communication Manager SAT, use the following commands:
  - **status signaling-group** command to verify that the SIP signaling groups are in-service.
  - **status trunk-group** command to verify that the SIP trunk groups are in-service.
  - **list trace tac** command to verify that fax calls are routed over the expected trunks.
- From System Manager, confirm that the Entity Links between Session Manager and the FaxCore eV5 servers at both sites are in service.
- Verify that fax calls can be placed to/from the FaxCore eV5 at each site.
- Verify that fax calls can be placed to/from FaxCore eV5 servers and analog machines.

9. Conclusion

These Application Notes describe the procedures required to configure the FaxCore eV5 Software to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. FaxCore eV5 server successfully passed compliance testing. All test cases were completed and passed with the exceptions/observations noted in **Section 2.2**.

10. Additional References

The following Avaya product documentation can be found at http://support.avaya.com.

[1] *Avaya Aura® Communication Manager Feature Description and Implementation Release 6.2, Issue 9.0, December 2012, Document Number 555-245-205.*

[2] *Administering Avaya Aura® Communication Manager Release 6.2, Issue 7.0, December 2012, Document Number 03-300509.*

[3] *Administering Avaya Aura® Session Manager, Release 6.3, December 2012.*

[4] *Dialogic Brooktrout SR140 Fax Software documentation may be found at* http://www.dialogic.com/en/Products/fax-boards-and-software/foip/sr140.aspx.

[5] *FaxCore Administrators Manual* – provided by FaxCore

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.