Abstract

These Application Notes describe the steps to configure the Open Web Services and Inova IT SIP Objects.NET (SO.NET) Third Party Call Control sample applications to work with an environment comprised of Avaya SIP Application Server (SIP A/S), Avaya Communication Manager, and Avaya SIP Enablement Services.

The Third Party Call Control applications are amongst several sample applications available with Avaya SIP A/S and with Inova IT SO.NET. The Third Party Call Control applications establish a call between two endpoints. For these Application Notes, two third party call control applications are included in the sample configuration described in these Application Notes. One application is installed with the Open Web Services Add Pack and the other application is installed with the SIP Objects.NET Framework.
1. Introduction

These Application Notes describe the steps to configure the Open Web Services (OWS) and Inova IT SIP Objects.NET (SO.NET) Third Party Call Control (3PCC) sample applications to work with an environment comprised of Avaya SIP Application Server (SIP A/S), Avaya Communication Manager, and Avaya SIP Enablement Services (SES).

1.1. Background

In the sample configuration, there are several components that are installed on Avaya SIP A/S platform. The Service Oriented Object Framework (SOOF), also known as SIP Service Oriented Architecture (SOA), is a SOA-based application development and deployment framework that is deployed on top of Avaya SIP A/S. SOOF/SIP SOA includes a suite of re-usable SIP Service Components including OWS. OWS exposes some of the underlying Service Component functionality as web services according to the Parlay X 2.0 API [12].

OWS provides a Third Party Call Control service that uses the Parlay X 2.0 3PCC API. The Third Party Call Control service allows applications to establish calls between two endpoints.

Several sample applications are available to demonstrate the types of applications and services that can be created using the services provided with Avaya SIP A/S. Additionally, the development of these applications is supported using different development environments such as the Eclipse Integrated Development Environment and Microsoft Visual Studio.

For development on Microsoft Visual Studio, Inova IT SO.NET provides a framework that is built on top of OWS. This provides a .NET centric view of the call control functionality exposed by OWS and defined in the Parlay X 2.0 specifications.

The Third Party Call Control applications are amongst the sample applications that are available for use with Avaya SIP A/S. For these Application Notes, two third party call control applications are included in the sample configuration described in these Application Notes. One application is installed with the Open Web Services Add Pack [9] and the other set is installed with the Inova IT SIP Objects.NET Framework [13].

These Application Notes focus on the following:

- The configuration of the SIP trunks between Avaya Communication Manager and Avaya SES to support calls from Avaya SIP A/S.
- The configuration of the SIP trunks between Avaya SIP A/S and Avaya SES.
- The configuration of Avaya SIP A/S to support the OWS Third Party Call Control service.
- The configuration of the Third Party Call Control applications to work with Avaya Communication Manager endpoints.

For administration of endpoint telephones and general administration of Avaya Communication Manager and Avaya SES, refer to the appropriate documentation listed in Section 10.
1.2. Network Configuration

These Application Notes present a sample configuration for the network shown in Figure 1. For the sample configuration, Avaya Communication Manager is running on the Avaya S8300 Server with an Avaya G700 Media Gateway. Avaya SIP A/S is configured in a single-box deployment where all of the cluster elements (one Management Server, one Service Director, and one Service Host) are on a single hardware platform. Oracle Database 10g Express Edition is used as the database for Avaya SIP A/S and is installed on the same server PC as Avaya SIP A/S.

SIP trunks are used to connect Avaya Communication Manager and Avaya SIP A/S via Avaya SES. All calls established by the Third Party Call Control service running on Avaya SIP A/S are carried over these SIP trunks.

As shown in Figure 1 and listed in Table 1, there are several Avaya Digital, H.323, and SIP telephones that are connected to or registered with Avaya Communication Manager or Avaya SES. Additionally, there is a Public Switch Telephone Network (PSTN) connection from Avaya Communication Manager to establish calls with PSTN telephones. With the exception of the Digital and the PSTN telephones, all components are connected to a single Avaya C364T-PWR Converged Stackable Switch.
Figure 1: Network Configuration Diagram
2. Equipment and Software Validated

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

<table>
<thead>
<tr>
<th>Equipment</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avaya S8300 Server with Avaya G700 Media Gateway</td>
<td>Avaya Communication Manager 5.0 R015x.00.0.825.4</td>
</tr>
<tr>
<td>Avaya SIP Enablement Services</td>
<td>5.0, SES-5.0.0.0-825.31</td>
</tr>
<tr>
<td>Avaya SIP Application Server</td>
<td>7.2.11</td>
</tr>
<tr>
<td>Service Oriented Object Framework</td>
<td>1.1.5</td>
</tr>
<tr>
<td>Service Components</td>
<td>1.5.2</td>
</tr>
<tr>
<td>Open Web Services</td>
<td>1.1.0</td>
</tr>
<tr>
<td>Sun Microsystems Java</td>
<td>1.5.0</td>
</tr>
<tr>
<td>on Dell Precision 380</td>
<td>Microsoft Windows 2003 Server, Service Pack 2</td>
</tr>
<tr>
<td>Avaya 4610SW IP Telephone</td>
<td>2.8 (H.323)</td>
</tr>
<tr>
<td></td>
<td>3.1.0 (Avaya Quick Edition)</td>
</tr>
<tr>
<td>Avaya 4621SW IP Telephone</td>
<td>2.8 (H.323)</td>
</tr>
<tr>
<td></td>
<td>2.2.2 (SIP)</td>
</tr>
<tr>
<td></td>
<td>3.1.0 (Avaya Quick Edition)</td>
</tr>
<tr>
<td>Avaya 9620 IP Telephone</td>
<td>2.0.1.34 (Avaya one-X™ Deskphone SIP)</td>
</tr>
<tr>
<td>Avaya 9630 IP Telephone</td>
<td>2.0.1.34 (Avaya one-X™ Deskphone SIP)</td>
</tr>
<tr>
<td>Avaya 6408D+ Digital Telephone</td>
<td>N/A</td>
</tr>
<tr>
<td>Avaya C364T-PWR Converged Stackable Switch</td>
<td>4.5.14</td>
</tr>
<tr>
<td>Inova IT SIP Objects.NET Framework</td>
<td>1.1.5</td>
</tr>
<tr>
<td>Microsoft Internet Explorer</td>
<td>7.0.5730.13</td>
</tr>
<tr>
<td>Microsoft Internet Information Services</td>
<td>5.1</td>
</tr>
<tr>
<td>Microsoft Visual Studio</td>
<td>2005 Professional 8.0.50727.762 (SP.050727-7600)</td>
</tr>
<tr>
<td>Oracle Database 10g Express Edition on Dell Precision 380</td>
<td>2 Microsoft Windows 2003 Server, Service Pack 2</td>
</tr>
<tr>
<td>Management PC on Dell PowerEdge 850</td>
<td>Microsoft Windows 2003 Server Enterprise Edition with Service Pack 2</td>
</tr>
</tbody>
</table>

Table 1: Configuration Equipment and Version
3. Avaya Communication Manager Configuration

The configuration of Avaya Communication Manager and the endpoints that connect to Avaya Communication Manager is not the focus of these Application Notes. This configuration information is provided in References [1-3]. For these Application Notes, it is assumed that SIP connectivity to Avaya SES, that all of the endpoints shown in Figure 1, and that the PSTN trunk have been configured.

In this sample configuration, the Third Party Call Control applications initiate calls to Avaya endpoints and to the PSTN. A five digit Uniform Dial Plan (UDP) was used for internal calls (25xxx for Avaya Quick Edition endpoints, 26xxx for SIP endpoints, 300xx for H.323 endpoints, and 301xx for Digital endpoints). For external calls to the PSTN, an 11-digit dial plan was used (1 732 852 1xxx).

These Application Notes assume that the following procedures have already taken place:

- All Digital, H.323, and SIP stations have been configured.
- The SIP trunk between Avaya Communication Manager and Avaya SES has been configured to support trunking between the two systems and to support the SIP endpoints registered with Avaya SES (see Section 3.4).
- The PSTN trunk has been configured.
- Routing to the PSTN has been configured. For this sample configuration, Automatic Route Selection (ARS) was used to route calls to the PSTN trunk.

This section focuses on the configuration of the SIP trunk used for the calls generated by Avaya SIP A/S on behalf of the Third Party Call Control applications. For ease of configuration, all components are configured to use IP network region “1” and IP codec set “1”. Media shuffling (direct IP-IP media) is enabled. Codec set “1” has “G.711MU” and “G.729AB” codecs configured.

To configure the SIP trunk, the following procedures were used:

- Display IP node names
- Display IP codec sets and network regions
- Configure SIP trunk group and signaling group

The following configuration of Avaya Communication Manager was performed using the System Access Terminal (SAT). After completion of the configuration in this section, use the “save translation” command to make the changes permanent.
3.1. Display IP Node Names

Use the “display node-names ip” command to view the entries for the system processor and for Avaya SES. In this case, “procr” and “150.1.1.100” are listed under Name and IP Address for the system processor and “sesisv” and “150.1.1.150” are listed under Name and IP Address for Avaya SES. The actual node names and IP addresses may vary.

```
display node-names ip
Name          IP Address
default       0.0.0.0
procr         150.1.1.100
sesisv        150.1.1.150
```

3.2. Display IP Codec Set

In the sample configuration, codec set “1” was used for all components. Use the “display ip-codec-set n” command, where “n” is an existing codec set number. For this configuration, G.711MU (µ-law) and G.729AB are supported. The actual codecs may vary.

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

3.3. Display IP Network Region

In the sample configuration, network region “1” was used for all components. Use the “display ip-network-region n” command, where “n” is an existing network region number. Note that Authoritative Domain is set to “isvabc.com” which is the SIP domain for Avaya SES as shown in Section 4.1.

```
display ip-network-region 1
IP NETWORK REGION
Region: 1
Location: 1 Authoritative Domain: isvabc.com
Name: Network Region 1
MEDIA PARAMETERS
Intra-region IP-IP Direct Audio: yes
Inter-region IP-IP Direct Audio: yes
Codec Set: 1
IP Audio Hairpinning? n
UDP Port Min: 2048
UDP Port Max: 3329
```
3.4. Configure SIP Trunk Group and Signaling Group

In the sample configuration, trunk group “1” and signaling group “1” were used to reach SIP endpoints registered with Avaya SES. A separate trunk group “3” and signaling group “3” were added to reach Avaya SIP A/S.

3.4.1. Display SIP Trunk and Signaling Groups for Avaya SES Endpoints

Use the “display trunk-group n” command, where “n” is the trunk group number. Trunk group “1” uses signaling group “1” as shown below.

```
+-----------------------------------+-----------+-----------+----------+-----+----------+-----+-------------+-----------------+
| Group Number: 1                   | Group Type: sip | CDR Reports: y |
| Group Name: Avaya SES isvabc.com | COR: 1       | TN: 1      | TAC: #01 |
| Direction: two-way                | Outgoing Display? n |
| Dial Access? n                    | Night Service: |
| Queue Length: 0                   |               |
| Service Type: tie                 | Auth Code? n  |
+-----------------------------------+-----------+-----------+----------+-----+----------+-----+-------------+-----------------+
| TRUNK GROUP                        | Signaling Group: 1 |
| Number of Members: 20             |               |
```

Use the “display signaling-group n” command, where “n” is an available signaling group number.

```
+-----------------------------------+----------+-----------------+-------------------+----------+----------+---------------+
| Group Number: 1                   | Group Type: sip | Transport Method: tls |
| Near-end Node Name: procr         | Far-end Node Name: sesisv |
| Near-end Listen Port: 5061        | Far-end Listen Port: 5061 |
| Far-end Domain: isvabc.com        | Far-end Network Region: 1 |
| Bypass If IP Threshold Exceeded? n|
| DTMF over IP: rtp-payload         | Direct IP-IP Audio Connections? y |
| Enable Layer 3 Test? n            | IP Audio Hairpinning? n |
| Session Establishment Timer(min): 3 |
+-----------------------------------+----------+-----------------+-------------------+----------+----------+---------------+
```

Use the “display signaling-group n” command, where “n” is an available signaling group number.
3.4.2. Configure SIP Trunk and Signaling Groups for Avaya SIP A/S

In the sample configuration, trunk group “3” and signaling group “3” were used to reach Avaya SIP A/S.

Administer a SIP signaling group to use for signaling. Use the “add signaling-group n” command, where “n” is an available signaling group number. Enter the following values for the specified fields and retain the default values for all remaining fields. Submit these changes.

- **Group Type:** “sip”
- **Transport Method:** “tls”
- **Near-end Node Name:** System processor node name from Section 3.1.
- **Far-end Node Name:** Avaya SIP A/S domain name from Section 3.1.
- **Near-end Listen Port:** “5061”
- **Far-end Listen Port:** “5061”
- **Far-end Network Region:** Avaya network region number “1” from Section 3.3.
- **Far-end Domain:** SIP domain name of Avaya SIP A/S from Section 5.1.
- **DTMF over IP:** “rtp-payload”

```
add signaling-group 3
```

<table>
<thead>
<tr>
<th>SIGNALING GROUP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Number: 3</td>
</tr>
<tr>
<td>Transport Method: tls</td>
</tr>
<tr>
<td>Near-end Node Name: procr</td>
</tr>
<tr>
<td>Near-end Listen Port: 5061</td>
</tr>
<tr>
<td>Far-end Network Region: 1</td>
</tr>
<tr>
<td>Far-end Domain: isvsipas.com</td>
</tr>
<tr>
<td>Bypass If IP Threshold Exceeded? n</td>
</tr>
<tr>
<td>DTMF over IP: rtp-payload</td>
</tr>
<tr>
<td>Direct IP-IP Audio Connections? y</td>
</tr>
<tr>
<td>IP Audio Hairpinning? n</td>
</tr>
<tr>
<td>Enable Layer 3 Test? n</td>
</tr>
<tr>
<td>Session Establishment Timer(min): 3</td>
</tr>
</tbody>
</table>
Use the “add trunk-group n” command, where “n” is an available trunk group number. Enter the following values for the specified fields and retain the default values for the remaining fields. Submit these changes.

- **Group Type:** “sip”
- **Group Name:** A descriptive name.
- **TAC:** An available trunk access code.
- **Service Type:** “tie”
- **Signaling Group:** Signaling group number for newly created signaling group.
- **Number of Members:** Desired number of trunk group members.

```
add trunk-group 3

<table>
<thead>
<tr>
<th>TRUNK GROUP</th>
<th>Page 1 of 21</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Number: 3</td>
<td></td>
</tr>
<tr>
<td>Group Name: SIP A/S 150.1.1.161</td>
<td></td>
</tr>
<tr>
<td>Direction: two-way</td>
<td></td>
</tr>
<tr>
<td>Dial Access? n</td>
<td></td>
</tr>
<tr>
<td>Queue Length: 0</td>
<td></td>
</tr>
<tr>
<td>Service Type: tie</td>
<td></td>
</tr>
<tr>
<td>CDR Reports: y</td>
<td></td>
</tr>
<tr>
<td>COR: 1</td>
<td></td>
</tr>
<tr>
<td>TN: 1</td>
<td></td>
</tr>
<tr>
<td>TAC: #03</td>
<td></td>
</tr>
<tr>
<td>Outgoing Display? n</td>
<td></td>
</tr>
<tr>
<td>Night Service:</td>
<td></td>
</tr>
<tr>
<td>Queue Length: 0</td>
<td></td>
</tr>
<tr>
<td>Signaling Group: 3</td>
<td></td>
</tr>
<tr>
<td>Number of Members: 10</td>
<td></td>
</tr>
</tbody>
</table>
```
4. Avaya SIP Enablement Services Configuration

This section provides the procedures for configuring SIP trunking between Avaya SES and Avaya SIP A/S. Other standard configuration information is covered in Reference [1].

The procedures in this section are used to configure the SIP trunk between Avaya SES and Avaya SIP A/S to allow the calls initiated by the Third Party Call Control applications to reach Avaya SES and to terminate on Avaya Communication Manager. As all SIP endpoints are registered with Avaya SES, Avaya SES knows how to handle calls to the SIP endpoints. As the Digital, H.323, and PSTN endpoints do not register with Avaya SES, additional configuration is needed to instruct Avaya SES to deliver the SIP INVITE messages for these endpoints to Avaya Communication Manager.

The procedures include the following areas:

- Display SIP domain
- Configure media server address map
- Configure trusted host

4.1. Display SIP Domain

Access the Avaya SES administration web interface by using the URL “http://<ip-address>/admin” in an Internet browser window, where “<ip-address>” is the IP address of Avaya SES. The IP address for Avaya SES may vary. In the sample configuration, “150.1.1.150” was used, as shown in Figure 1. Log in with the appropriate credentials and click the Launch SES Administration Interface link.

![Launch SES Administration Interface](image)
Select Server Configuration → System Properties from the left-hand pane to display the View System Properties window. Use the value in the SIP Domain field (in this case “isvabc.com”) for configuring Authoritative Domain in Section 3.3 and for configuring Far-end Domain in Section 3.4.1.
4.2. Configure Media Server Address Map

To ensure that calls to non-SIP endpoints (Digital, H.323, and PSTN) are routed to Avaya Communication Manager, create a media server address map. For this sample configuration, calls to Digital endpoints (301xx), H.323 endpoints (300xx), and PSTN endpoints (917321xxx) were routed to Avaya Communication Manager using a media server address map.

From the Top window, select Media Servers → List from the left-hand pane to display the List Media Servers window. Click the Map link in the right-hand pane.

In the List Media Server Address Map window, click the Add Map In New Group link in the right-hand pane.
The **Add Media Server Address Map** window is displayed next. This window is used to specify which calls are to be routed to Avaya Communication Manager. For the **Name** field, enter a descriptive name to denote the routing. For the **Pattern** field, enter an appropriate syntax for address mapping. For calls to Digital and H.323 endpoints, a pattern of “^sip:30[0-9]{3}” was used to match to any extensions in the range of 30000-30999. Retain the check in **Replace URI** and click **Add**.

Click **Continue** on the **Continue** window that confirms that the address map was added (not shown). An updated **List Media Server Address Map** window is displayed. The address map that was just added is shown. Also, a contact that matches the address of the media server is also automatically created. In this sample configuration, the contact is “sip:$\text{(user)}@150.1.1.100:5061;transport=tls”. “150.1.1.100” is the IP address of the Avaya Communication Manager system processor as shown in **Section 3.1**. Avaya SES will substitute “$\text{(user)}” with the user portion of the request URI before sending the message.

One more address map is needed to match calls to PSTN endpoints. Click **Add Another Map**.
The **Add Media Server Address Map** window is displayed again. For the **Name** field, enter a descriptive name to denote the routing. For the **Pattern** field, enter an appropriate syntax for address mapping, in this case “PSTN”. For calls to PSTN endpoints, a pattern of “^sip:917328521.*” was used to match to any number starting with “917328521”. Retain the check in **Replace URI** and click **Add**. Click **Continue** on the **Continue** window that confirms that the address map was added. An updated **List Media Server Address Map** window is displayed with the two address maps that were added and the associated contact address.
4.3. Configure Trusted Host

Administer Avaya SIP A/S as a trusted host so that Avaya SES will not challenge the SIP messages from Avaya SIP A/S. From the Top window, select Trusted Hosts → Add from the left-hand pane to display the List Trusted Hosts window.

![List Trusted Hosts Window](image1)

The Add Trusted Host window is displayed next. For the IP Address field, enter the IP Address of Avaya SIP A/S (shown in Figure 1). For the Comment field, enter a descriptive name. Click Add.

![Add Trusted Host Window](image2)
Click **Continue** on the **Continue** window that confirms that the trusted host entry was added (not shown). An updated **List Trusted Hosts** window is displayed.
5. Avaya SIP Application Server Configuration

The installation and configuration of Avaya SIP A/S are covered in References [5] and [6], respectively. For this sample configuration, Avaya SIP A/S was installed on a system running the Microsoft Windows operating system. It is assumed that Avaya SIP A/S has been installed and licensed. The Avaya SIP A/S used in this configuration is on a single-box deployment where all of the cluster elements (one Management Server, one Service Director, and one Service Host) are on a single hardware platform.

In addition to the Avaya SIP A/S platform, the following components are all assumed to be installed.

- SIP Service Oriented Architecture 1.1 [5]
- Service Components Start-up Pack 1.5 [7]
- Open Web Services Add Pack 1.1 [9]
- SIP A/S Element Manager [5]
- Oracle Database 10g Express Edition [16]

**NOTE**: Oracle Database 10g Express Edition is the database that was used in this sample configuration. Other databases are supported by Avaya SIP A/S and can be used. The installation and configuration of Oracle Database 10g Express Edition are not the focus of these Application Notes and are not covered.

This section focuses on the procedures to configure Avaya SIP A/S to support the Third Party Call Control service, which is required by the Third Party Call Control sample applications. The Third Party Call Control service is included in Open Web Services. The procedures are as follows:

- Display initial configuration parameters
- Deploy extension and services
  - Deploy Distributed State Management (DSM)
  - Deploy Service Components
  - Deploy Open Web Services
- Configure SOOF aliases
  - Configure Service Components aliases
  - Configure Open Web Services aliases
The configuration of Avaya SIP A/S was performed using the SIP A/S Element Manager application. As Avaya SIP A/S is installed on a Microsoft Windows platform for this sample configuration, access the SIP A/S Element Manager by selecting Start → Programs → Ubiquity → Ubiquity Element Manager → Ubiquity Element Manager. The SIP A/S Element Manager window is displayed.

For the procedures covered in this section, it is assumed that a cluster has been configured and connected to the Management Server, a Service Director is connected, a Service Host has been connected, and a channel has been connected to the Service Host. The Management Server “Ubiquity Services” and the cluster “SIP_AS_72” were both used in this sample configuration. For more information on the configuration and management of Avaya SIP A/S, see Reference [6].
5.1. Display Initial Configuration Parameters

This section summarizes the parameters configured during the Avaya SIP A/S installation procedures that are used for configuring the SIP trunk with Avaya SES (see Sections 3.4.2 and 4.3) and for configuring the DSM extension (see Section 5.2.1). Navigate to the Service Host Collection Configuration tab by selecting Ubiquity Services → SIP_AS_72 → Connected to SIP A/S Management Server → Service Host Collection and then clicking the Configuration tab. Controlled Domains contains the SIP domain that is controlled by Avaya SIP A/S.

**NOTE:** The IP address for Avaya SIP A/S is also used for the SIP domain.

The other fields in this screen were populated as part of the initial installation and configuration. The RDMBS Connection String and RDMBS Driver fields are specific for the connection to the Oracle database. The RDMBS Connection String value is used in the configuration in Section 5.2.1. These values will vary depending on the database that is used.
5.2. Deploy Extension and Services

To support the Third Party Call Control sample applications, the DSM extension and two Avaya SIP A/S services must be deployed. The extension and the services are installed with Avaya SIP A/S, Service Components, and Open Web Services, respectively.

5.2.1. Deploy Distributed State Management Extension

Access the Extensions tab for the Service Host Collection in the SIP A/S Element Manager window. From left-hand pane for the SIP A/S Element Manager window shown in Section 5.1, select Ubiquity Services → SIP_AS_72 → Connected to SIP A/S Management Server → Service Host Collection. Click the Extensions tab and then click Configure. Select “dsm_database.jar” in the Installed Extensions frame. Click the button between the Installed Extensions and Deployed Extensions frames.

The Enter binding name dialogue box is displayed. Retain the value for the field. Click OK.

The Extension Management dialogue box is displayed. Click Yes to continue with the deployment of the extension.
The \texttt{dsm\_database.jar} dialogue box is displayed. Enter the parameters as described below and retain the default values for the remaining fields. Click \textbf{Apply}.

- \textbf{RDMBS Connection String}: “jdbc:oracle:thin:UserName/PassWord@localhost:1521:XE” (see Section 5.1)
- \textbf{User ID}: “UserName” (the user name in the \textbf{RDBMS Connection String} in Section 5.1).
- \textbf{Password}: “PassWord” (the password in the \textbf{RDBMS Connection String} in Section 5.1).

![dsm\_database.jar](image)

A confirmation dialogue (\textbf{Important Information}) is then displayed indicating that configuration changes have been applied to the cluster (not shown). Click \textbf{OK}.

\subsection*{5.2.2. Deploy Service Components}

Based on the recommendation from References [8], the “bundled” Service Components service file (“service\_components.sar”) was used for this sample configuration. If necessary, the Service Components can be deployed as individual services using individual files for each service (e.g., “call.sar”, “incoming\_dialog.sar”, etc.).
Access the Applications tab for the Service Host Collection in the SIP A/S Element Manager window. From left-hand pane for the SIP A/S Element Manager window shown in Section 5.1, select Ubiquity Services → SIP_AS_72 → Connected to SIP A/S Management Server → Service Host Collection. Click the Applications tab and then click Configure. Scroll down the list in the Application Repository frame and select “service_components.sar”. Click the button between the Application Repository and Deployed Applications frames and click Apply.

A confirmation dialogue (Deploy service_components.sar) is then displayed indicating that the service is being provisioned (not shown). Then the Configuration for service_components.sar dialogue is displayed. Retain the default values for the fields and click Apply.
A confirmation dialogue (Deploy service_components.sar) is then displayed indicating that the service is being deployed (not shown). A confirmation dialogue (Important Information) is then displayed indicating that configuration changes have been applied to the cluster (not shown). Click OK. The “service_components.sar” service is then displayed in the Deployed Applications frame (see Section 5.2.3).

### 5.2.3. Deploy Open Web Services

Based on the recommendation from Reference [10], the “bundled” Open Web Services service file (“parlayx_components.sar”) was used for this sample configuration. If necessary, Open Web Services can be deployed as individual services using individual files for each service (e.g., “parlayx_threepcc.sar”, “parlayx_audiocall.sar”, etc.).

Access the Applications tab for the Service Host Collection in the SIP A/S Element Manager window. From left-hand pane for the SIP A/S Element Manager window shown in Section 5.1, select Ubiquity Services → SIP_AS_72 → Connected to SIP A/S Management Server → Service Host Collection. Click the Applications tab and then click Configure. Scroll down the list in the Application Repository frame and select “parlayx_components.sar”. Click the button between the Application Repository and Deployed Applications frames and click Apply.

A confirmation dialogue (Deploy parlayx_components.sar) is then displayed indicating that the service is being provisioned (not shown).
Then the Configuration for `parlayx_components.sar` dialogue is displayed. The parameters listed below were used for the sample configuration. Retain the default values for the remaining fields. Click **Apply**.

- **SIP From Address**: “sip:FromAddr@isvsipas.com”
- **SIP From Address For Calling Party**: “sip:CallingPartyFromAddr@isvsipas.com”
- **The ‘From Address’ to appear in all outgoing SIP dialogs**: “sip:OutgoingFromAddr@isvsipas.com”
- **Rule Management Component Alias**: “parlayx_call_handling_RuleManagement”
- **SIP From Address For Called Party**: “sip:CalledPartyFromAddr@isvsipas.com”
The SIP URIs shown in the above configuration include “isvipsas.com” which represent the domain name of Avaya SIP A/S as shown in Section 5.1. These values were used for demonstration purposes to clearly identify the type of SIP “From” address being used. **NOTE:** The SIP “From” headers in this configuration do not include a “display name” as “display name” is not supported for the Open Web Services configuration. Usually, the SIP “From” header is in the form of “‘User Name’ <sip:User@domain-name>’, where “User Name” is the “display name”.

A confirmation dialogue (Deploy parlayx_components.sar) is then displayed indicating that the service is being deployed (not shown). A confirmation dialogue (Important Information) is then displayed indicating that configuration changes have been applied to the cluster (not shown). Click OK.

### 5.3. Configure SOOF Servlet Aliases

Once the services listed in Section 5.2 have been deployed, SOOF Servlet aliases must be configured for the deployed services.

#### 5.3.1. Configure Service Components Aliases

Access the SOOF tab for the Service Host Collection in the SIP A/S Element Manager window. From left-hand pane for the SIP A/S Element Manager window shown in Section 5.1, select Ubiquity Services → SIP_AS_72 → Connected to SIP A/S Management Server → Service Host Collection. Click the SOOF tab. Click Alias (on the left-hand side within the SOOF tab). In the SOOF Components frame, select “service_components” and click Configure. Then click Import.
The **Open** dialogue is displayed. For this sample configuration, the bundled “services_components.sar” service is used. Therefore, per Reference [8], the alias file that must be used is the “single_sar_service_components.alias” file. This file is placed in the “alias” sub-folder where the Service Components files were installed. In this sample configuration, the alias file is located in the “C:\USCL\ServiceComponents-1.5.2\alias\” folder. If the Service Components were deployed as individual services, a different alias file would be used. Browse to the above alias file and click **Open**.

The aliases that were imported from the alias file are now displayed in the **Aliases** frame in the **SOOF** tab. Click **Apply**.
5.3.2. Configure Open Web Services Aliases

Repeat the steps in Section 5.3.1 to configure the aliases for Open Web Services. Select “parlayx_components” in the SOOF Components frame instead of “service_components”. For this sample configuration, the bundled Open Web Services service file is used. Therefore, per Reference [10], the alias file that must be used is the “components.alias” file. This file is placed in the “alias” sub-folder where the OWS files were installed. In this sample configuration, the alias file is located in the “C:\ USCL\OpenWebServices-AddPack-1.1.0\alias\” folder. If the Open Web Services were deployed as individual services, a different alias file would be used.

6. Third Party Call Control Service Configuration

Once the Avaya SIP A/S Open Web Services in Section 5 have been deployed and configured, client applications can use the following web service URL to invoke methods on the Third Party Call Control web service supported by Open Web Services:

- http://<Avaya SIP A/S-IP-address>:6060/parlayx_components/ThirdPartyCall

In this sample configuration, “<Avaya SIP A/S address>” was replaced with the domain of Avaya SIP A/S as shown in Section 5.1. The web service URL was as follows. This URL was used by the sample applications as shown in Sections 7 and 7.2.

- http://isvsipas.com:6060/parlayx_components/ThirdPartyCall

Note that “parlayx_components” was used as the parlayx_components.sar service that was deployed in Section 5.2.3.
7. Third Party Call Control Application Configuration

This section focuses on the configuration of the Third Party Call Control sample applications.

7.1. Configure Open Web Services Add Pack Sample Application

A sample application for the Third Party Call Control service is included in the installation of the Open Web Services Add Pack (see Reference [9]). Two applications are provided: one application supports Microsoft .NET and the other supports BEA Weblogic. For this sample configuration, the Microsoft .NET sample application was used. This application was installed in the following folder. The folder will vary based on where Avaya SIP A/S and OWS were installed.

- C:\Ubiquity\USCL\OpenWebServices-AddPack-1.1.0\sample\

The application must be deployed on a web server. For this sample configuration, Microsoft Internet Information Services (IIS) was used to host these web services. A different web server can be used. As the focus is not on the web server, detailed instructions on deploying the web services on Microsoft IIS is not provided.

Per the instructions that are provided in the “readme.txt” file that accompanies the sample application (see Reference [11]), copy the contents of the application files to a virtual directory on the web server. In this sample configuration, the directory that was used is “C:\inetpub\wwwroot\<virtual-directory>”, where <virtual-directory> is the name of the virtual directory on the web server. Once deployed, the application can be accessed using the following URL:


For this sample configuration, the web server was hosted on the system shown in Figure 1 (IP address “150.1.1.170”). The “<virtual-directory>” where the files were placed on this system was “SIP-AS-3PCC”. Therefore, the URL to access the application was as follows:

Start the .NET Third Party Call Control sample application by entering the URL “http://150.1.1.170/SIP-AS-3PCC/Default.aspx” into an Internet browser on any PC within the network.
7.2. Configure SIP Objects.NET Sample Application

To support SIP Objects.NET and deploy sample applications that are installed with SIP Objects.NET, the components listed below are assumed to be installed.

- SIP Objects.NET Framework (see Reference [13])
- Microsoft Visual Studio

A sample application for the Third Party Call Control service is included with the installation of the SIP Objects.NET Framework. Configuration files are provided to compile either a web client or a Windows client. For this sample configuration, a Windows client application was compiled and used. This sample application was installed in the following folder. The folder will vary based on where SIP Objects.NET was installed.

- C:\Program Files\Inova IT\SIP Objects.NET\Samples\Components\

The application must be compiled with Microsoft Visual Studio. A “Readme.txt” file (see Reference [15]) is included with instructions on the changes needed to the configuration files and how to build the Windows client executable file. As the focus is not on the use of Microsoft Visual Studio, detailed instructions on building the executable file are not provided.

The Third Party Call Control sample application files are installed in the “ThirdPartyCall” folder under the folder listed above. Open the “Readme.txt” file installed in this folder and follow the directions to compile the Windows executable file. Per the instructions, the gateway string must be changed. Replace the string “http://owsserver” with the web service URL from Section 6.

For this sample configuration, the Windows executable file “ThirdPartyCall.exe” was compiled and stored in the “ThirdPartyCall\ThirdPartyCall\bin\Debug” folder.
8. Verification Steps

This section provides the tests that can be performed on Avaya Communication Manager and on Avaya SIP A/S to verify proper configuration of Avaya Communication Manager, Avaya SES, and Avaya SIP A/S.

8.1. Verify Avaya Communication Manager

8.1.1. Verify Idle Trunk and Signaling Groups

Verify the status of the SIP trunk group by using the “status trunk n” command, where “n” is the trunk group number administered in Section 3.4.2. Verify that all trunks are in the “in-service” state as shown below. For this sample configuration, as no calls were present on this trunk, the state of all of the trunk members was “in-service/idle”.

```
status trunk 3

TRUNK GROUP STATUS

<table>
<thead>
<tr>
<th>Member</th>
<th>Port</th>
<th>Service State</th>
<th>Mtce Connected Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>0003/001</td>
<td>T00101</td>
<td>in-service/idle</td>
<td>no</td>
</tr>
<tr>
<td>0003/002</td>
<td>T00102</td>
<td>in-service/idle</td>
<td>no</td>
</tr>
<tr>
<td>0003/003</td>
<td>T00103</td>
<td>in-service/idle</td>
<td>no</td>
</tr>
<tr>
<td>0003/004</td>
<td>T00104</td>
<td>in-service/idle</td>
<td>no</td>
</tr>
<tr>
<td>0003/005</td>
<td>T00105</td>
<td>in-service/idle</td>
<td>no</td>
</tr>
<tr>
<td>0003/006</td>
<td>T00106</td>
<td>in-service/idle</td>
<td>no</td>
</tr>
<tr>
<td>0003/007</td>
<td>T00107</td>
<td>in-service/idle</td>
<td>no</td>
</tr>
<tr>
<td>0003/008</td>
<td>T00108</td>
<td>in-service/idle</td>
<td>no</td>
</tr>
<tr>
<td>0003/009</td>
<td>T00109</td>
<td>in-service/idle</td>
<td>no</td>
</tr>
<tr>
<td>0003/010</td>
<td>T00110</td>
<td>in-service/idle</td>
<td>no</td>
</tr>
</tbody>
</table>
```

Verify the status of the SIP signaling group by using the “status signaling-group n” command, where “n” is the signaling group number administered in Section 3.4.2. Verify that the signaling group is “in-service” as indicated in the Group State field shown below.

```
status signaling-group 3

STATUS SIGNALING GROUP

<table>
<thead>
<tr>
<th>Group ID:</th>
<th>3</th>
<th>Active NCA-TSC Count: 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Type:</td>
<td>sip</td>
<td>Active CA-TSC Count: 0</td>
</tr>
<tr>
<td>Signaling Type: facility associated signaling</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Group State: in-service</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
8.1.2. Verify Active Trunk Group

Using the SIP Objects.NET Third Party Call client, make a call originating from SIP endpoint “26003” to H.323 endpoint “30001”. Start the application by browsing to the location of the “ThirdPartyCall.exe” file (see Section 7.2) and double-click on the file. The Third Party Call dialogue is displayed.

- In the **Caller** field, the URI of the calling party was entered. In this example, “sip:26003@isvabc.com” was entered for the originating SIP endpoint.
- In the **Callee** field, the URI of the called party was entered. In this example, “sip:30001@isvabc.com” was entered for the called H.323 endpoint.

Verify that there are two trunk group members that are in the “in-service/active” state as shown below.

<table>
<thead>
<tr>
<th>Status trunk 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRUNK GROUP STATUS</td>
</tr>
<tr>
<td>Member</td>
</tr>
<tr>
<td>--------</td>
</tr>
<tr>
<td>0003/001 T00101</td>
</tr>
<tr>
<td>0003/002 T00102</td>
</tr>
<tr>
<td>0003/003 T00103</td>
</tr>
<tr>
<td>0003/004 T00104</td>
</tr>
<tr>
<td>0003/005 T00105</td>
</tr>
<tr>
<td>0003/006 T00106</td>
</tr>
<tr>
<td>0003/007 T00107</td>
</tr>
<tr>
<td>0003/008 T00108</td>
</tr>
<tr>
<td>0003/009 T00109</td>
</tr>
<tr>
<td>0003/010 T00110</td>
</tr>
</tbody>
</table>
Verify the status of one of the connected SIP trunks by using the command “status trunk x/y”, where “x” is the number of the SIP trunk group from Section 3.4.2 for calls from Avaya SIP A/S, and “y” is the member number of a connected trunk. Verify that the Service State is “in-service/active” and that Audio Connection Type displays “ip-direct” which indicates that media shuffling is enabled.

```
status trunk 3/1

TRUNK STATUS

Trunk Group/Member: 0003/001  Service State: in-service/active
Port: T00101  Maintenance Busy? no
Signaling Group ID:
IGAR Connection? no
Connected Ports: T00011

  Port  Near-end IP Addr : Port  Far-end IP Addr : Port
Signaling: 01A0017  150.1.1.100 : 5061  150.1.1.150 : 5061
G.711MU Audio:  150.1.1.207 : 5004  150.1.1.231 : 2970
Video:
Video Codec:
Authentication Type: None

Audio Connection Type: ip-direct
```

### 8.2. Verify Avaya SIP A/S

Verify that Avaya SIP A/S has been configured properly to support the Third Party Call Control service.

As shown in Section 8.1.2, use the SO.NET Third Party Call client to make a call. This time make a call from SIP endpoint “26003” (this is an Avaya 9630 IP Telephone) to SIP endpoint “26005” (this is an Avaya 4621SW IP Telephone). Verify that the name displayed on endpoint “26005” is “FromAddr” for calling party name and “FromAddr@isvubi.com” for calling party number. **NOTE:** The calling party name shown on the display for endpoint “26003” is the name of the trunk used in Section 3.4.2 (“Avaya SIP A/S 150.1.1.161”).

Repeat the scenario above with “26005” as the calling party and “26003” as the called party. Verify that the name shown on the display for endpoint “26005” is “CallingPartyFromAddr” for calling party name and “CallingPartyFromAddr@isvubi.com” for calling party number. The calling party name on endpoint “26003” still shows the name of the trunk.

Only the Avaya 4600 Series IP Telephones running the SIP software show the proper calling party or called party information as defined in Section 5.2.3. This telephone gathers the information from the SIP “From” header. In the case of the other telephones, including the Avaya 9600 Series IP Telephones running the SIP software, Avaya Communication Manager determines the information that is displayed on the endpoint display. Avaya Communication Manager expects that the SIP “From” header includes both a **display name** in addition to the SIP URI, e.g., “**John Doe**” <sip:FromAddr@isvsipas.com>”. If the display name does not exist, Avaya Communication Manager uses the name of the trunk used for calls from Avaya SIP A/S (see Section 3.4.2) for the calling party and called party information (in this case, “Avaya SIP A/S 150.1.1.161”).
8.3. Verification Scenarios
Verification scenarios for the Third Party Call Control sample applications included the scenarios listed below.

- Using G.711 μ-law and G.729 media codecs, calls can be made using the Open Web Services Start-Pack Third Party Call Control sample application using each type of endpoint (Digital, H.323, SIP, and PSTN) as the calling party endpoint and each type of endpoint as the called party.
- Using G.711 μ-law and G.729 media codecs, calls can be made using the SIP Objects.NET Framework Third Party Call Control sample application using each type of endpoint (Digital, H.323, SIP, and PSTN) as the calling party endpoint and each type of endpoint as the called party.
- Proper display of the calling party name information was verified for only the Avaya 4600 Series IP Telephones running the SIP software. As a result of the limitation stated in Section 8.2, all other endpoints displayed the name of the trunk administered in Avaya Communication Manager. In this case, the calling party name is “Avaya SIP A/S 150.1.1.161”, the name of the trunk used for calls to endpoints from Avaya SIP A/S (see Section 3.4.2).

9. Conclusion
As illustrated in these Application Notes, through the use of the Open Web Services Third Party Call Control service deployed on Avaya SIP A/S, the Open Web Services and Inova IT SIP Objects.NET Third Party Call Control sample applications can interoperate with Avaya Communication Manager using SIP trunks via Avaya SES. The only interoperability issue to note is that when calls are made by the sample applications, the proper calling party information is only displayed by the Avaya 4600 Series IP Telephones running the SIP software. For all other endpoints, the trunk group name is displayed as the calling party name. This is due to the limitation covered in Section 8.2.
10. Additional References

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


©2008 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 Solution & Interoperability Test Lab at interoplabnotes@list.avaya.com.