Avaya Solution & Interoperability Test Lab

Application Notes for Acme Packet® Net-Net® Interactive Session Recorder with Avaya Aura® Session Manager and Avaya Aura® Communication Manager - Issue 1.0

Abstract

These Application Notes describe a compliance-tested configuration consisting of Acme Packet® Net-Net® Interactive Session Recorder with Avaya Aura® Session Manager and Avaya Aura® Communication Manager.

Acme Packet® Net-Net® Interactive Session Recorder provides a SIP trunk-side audio recording solution which leverages the routing capabilities of Avaya Aura® Session Manager and Avaya Aura® Communication Manager.

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 a compliance-tested configuration consisting of Acme Packet® Net-Net® Interactive Session Recorder with Avaya Aura® Session Manager and Avaya Aura® Communication Manager.

The purpose of this integration is to provide a scalable audio recording solution for enterprises requiring conversations with external parties be recorded for compliance or training purposes. Unlike many recording solutions, this integration enables capture of audio calls at the network core using SIP methods. This approach has the advantage of being less taxing on communication system resources. Similar to TDM trunk-side recording solutions, the internal call segments between parties within the enterprise, including consultative legs of conference or transfer calls cannot be captured using the tested method.

In order for the application to be able to identify recorded calls, SIP header information was retained for each recorded session. For the tested configuration, PSTN calls were routed from Communication Manager via SIP trunks to Session Manager, and then to the recorders. The recorders, upon receipt of a call would launch a second call through Session Manager to Communication Manager and upon successful completion of the second call, would bridge the audio between the two calls while capturing the audio for later playback.

As the recorders act as a back-to-back user agent in the tested configuration, several steps were implemented to ensure reliability of calls in the event of failures of components. These included the ability to load balance calls to the two servers, and routing schemes that ensured that upon failure of one or both servers, calls would route back to Communication Manager.

2. General Test Approach and Test Results

The compliance test focused on routing and media interoperability between Acme Packet® Net-Net® Interactive Session Recorder and Avaya Aura® Session Manager and Avaya Aura® Communication Manager.

The tested configuration used standard configurations of SIP, H.323, Digital and Analog Endpoints registered with Communication Manager, or Session Manager. Details regarding the configuration of these elements were not directly related to the interoperability of the tested solution and are not covered in detail in these notes.

2.1. Interoperability Compliance Testing

The focus of the compliance test was to confirm inbound and outbound SIP calls could be successfully recorded. Additional test conditions were included to verify the functionality of typical call scenarios such as conference and transfer, bridged call appearances, and EC500. Serviceability testing included disconnecting Communication Manager as well as the recorders from the network, rebooting the recorder servers as well as rebooting Session Manager to confirm that the application was capable of recovering from typical outages.

2.2. Test Results

The objectives of the test were verified. It should be understood that with this solution, call integrity relies upon the availability of the Interactive Session Recorder servers. In most use scenarios, server failure mid-call will result in calls being terminated unexpectedly. With proper care in the configuration, failures can be minimized for subsequent calls by implementing robust routing schemes.

As is expected with trunk-side recording solutions, internal call segments, including the temporary legs of consultative conference and transfer calls resulted in silence as these audio streams do not pass through the recorders. Calls to deskphones with EC500 activated to alert a mapped external phone (typically a cell phone) were successfully recorded whether picked up on either the desk or cell phone, as well as when handed off in both directions.

2.3. Support

Technical support for Acme Packet products can be obtained at:

- Phone: 1-781-756-6920 or 1-866-ACME PKT (226-3758)
- Email: support@acmepacket.com
- Web: http://www.acmepacket.com/support.htm

3. Reference Configuration

The compliance test configuration included a single site consisting of Avaya Aura® Communication Manager and Avaya Aura® Session Manager with several SIP, H.323 and TDM endpoints. SIP trunks were used for signaling and call routing to and from Communication Manager and Session Manager, as well as a PRI trunk for outside calls to the public network.

The Acme Packet® Net-Net® Interactive Session Recorder solution was installed on a pair of Windows 2008R2 Servers which follows common deployment strategies for scalability and high availability design considerations.

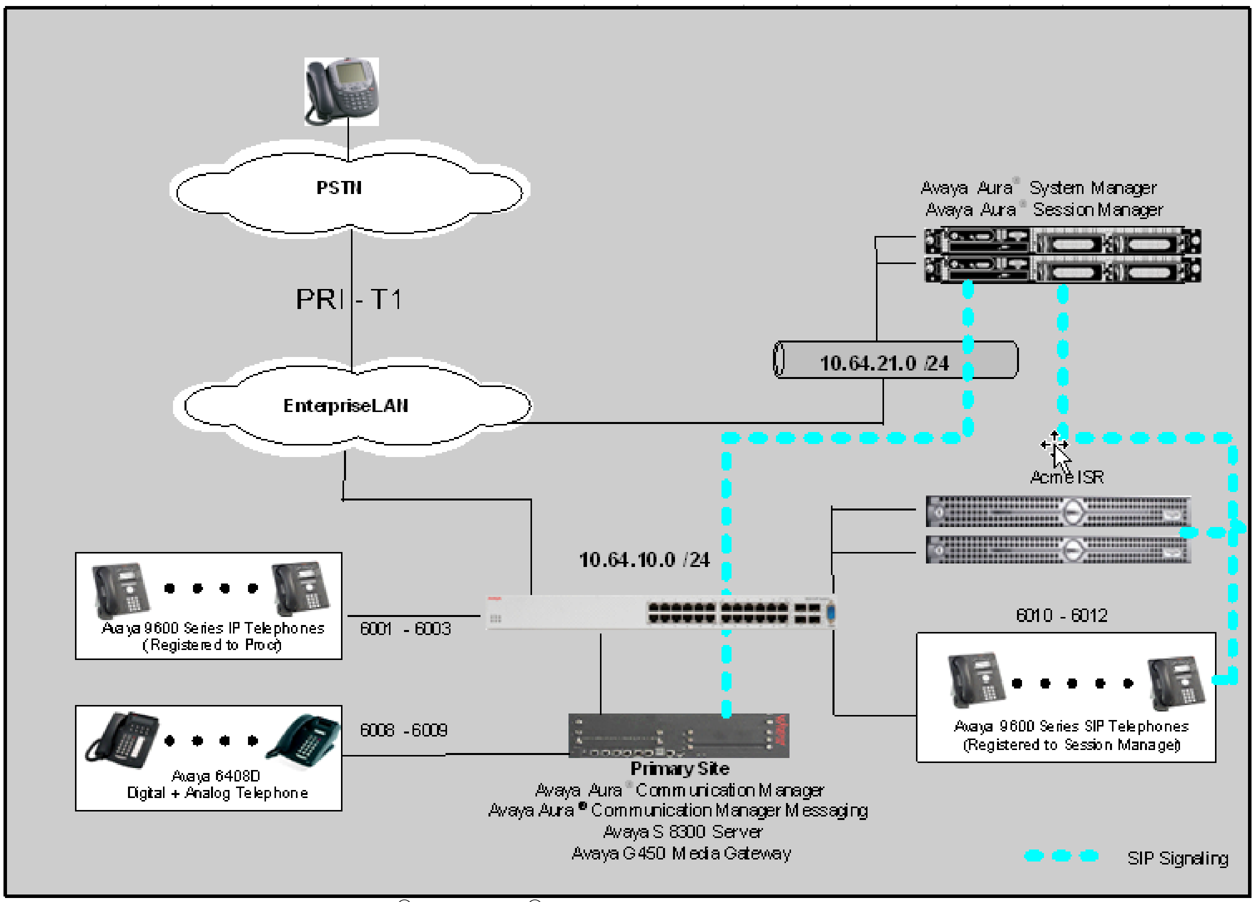


Figure 1 – Acme Packet® Net-Net® Interactive Session Recorder Compliance Test Configuration

4. Equipment and Software Validated

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

Equipment	Version
Avaya Aura® System Manager On Dell™ PowerEdge™ R610 Server	6.1 (Build No. - 6.1.0.4.5072-6.1.4.11) Avaya System Platform 6.0.2.1.5
Avaya Aura® Session Manager On HP ProLiant DL360 G7 Server	6.1 (Build No. - 6.1.04.0.610023)
Avaya Aura® Communication Manager On Avaya S8300D Server	6.1 (R016x.00.1.510.1 - 18621) Avaya System Platform 6.0.2.1.5
Avaya 9600 Series SIP Phones	SIP 2.6
Avaya 9600 Series H.323 Phones	H.323 3.11
Analog Phone	-
Acme Packet® Net-Net® Interactive Session Recorder on Microsoft Windows 2008R2 Server	2.2

5. Configure Avaya Aura® Communication Manager

Communication Manager used an existing configuration with SIP trunks to connect to Avaya Aura® Session Manager. Configuration of this aspect of the integration was standard. The primary focus of these Application Notes will be to describe the routing used to ensure high availability of resources to minimize the risks of failed calls.

5.1. Communication Manager Configuration Details

All the configuration changes in this section for Communication Manager are performed through the System Access Terminal (SAT) interface. For more information on configuring Communication Manager, refer to the Avaya product documentation, Reference [2] and [3].

This section provides the procedures for configuring Communication Manager. The procedures are as follows:

- Verify Feature and License are adequate for the integration
- Administer Routing for Calls
- Administer Media Properties

1.	**Verify Feature and License are adequate for the integration** The solution used SIP trunks to facilitate communications with the recorders. Two trunk ports were required for each concurrent call that was recorded. Verify that there are an adequate number of trunk port licenses using the **display system-parameters customer-options** command. Consult with your Avaya sales, or Authorized Reseller if more licenses are required. In addition, standard Call Center features (not shown) were required to enable the call center functionality used in the test.

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

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 4000  106
           Maximum Concurrently Registered IP Stations: 2400  4
             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  1
                   Maximum Video Capable IP Softphones: 2400  2
                       Maximum Administered SIP Trunks: 4000  72
  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    1
           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
```

2. **Administer Routing for Calls**

All Inbound PSTN calls routed to VDN 6500 used Vector 5 for routing calls to Session Manager. The vector used a round robin method to route to the two recorders, thus load balancing inbound traffic.

The recorders routed all inbound calls back to the ACD queue via VDN 6000 which used standard ACD queuing (details not shown).

On-Demand recording was implemented by calling VDN 6502, which routed all calls to one of the recorders using a ***route-to 6103*** command in Vector 6 (not shown).

Full details of creating the VDNs and Vectors followed standard administration practices, so these notes will not describe all of the details. Use the ***list vdn*** command to view the existing vdns:

```
list vdn

                          VECTOR DIRECTORY NUMBERS
                                                                          Evnt
                                            VDN          Vec          Orig    Noti
Name (22 characters)   Ext/Skills     Ovr COR TN   PRT Num  Meas Annc    Adj

ACD                    6000            n   1   1    V   3    none

From PSTN Gateway      6500            n   1   1    V   5    none

On Demand Recording    6502            n   1   1    V   6    none
```

Variable A was defined as a ***collect*** variable **Type** using the **change variables** command as shown below:

```
change variables                                                 Page   1 of  39
                              VARIABLES FOR VECTORS

Var Description                     Type    Scope Length Start Assignment       VAC
A   Route Switch                    collect G     1      1     0
B
```

VDN **6500** used **Vector 5** with **Variable A** to alternately route calls to each recorder. Vector 5 was created using the ***change vector 5*** command.

```
                                  CALL VECTOR

    Number: 5                    Name: Route Switch
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n           Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 wait-time    0   secs hearing silence
02 goto step    5            if A                <>     0
03 set          A      = A      ADD   1
04 route-to     number 6101             with cov n if unconditionally
05 set          A      = A      SUB   1
06 route-to     number 6102             with cov n if unconditionally
07 stop
```

Administer Routing for Calls (Continued)

Calls to 61xx used AAR to route to Session Manager. Using the **change dialplan analysis** command, an entry was created as follows to define the pattern ***61xx*** as an ***AAR* call type**:

```
                            DIAL PLAN ANALYSIS TABLE
                                  Location: all            Percent Full: 2

    Dialed   Total  Call      Dialed   Total  Call      Dialed   Total  Call
    String   Length Type      String   Length Type      String   Length Type
   20          5   ext
   4           5   udp
   5           4   udp
   6           4   ext
   61          4   aar
   63          4   ext
   8           1   fac
   9           1   fac
   *           3   fac
   *           4   dac
   #           3   fac
```

An AAR entry was created using the **change aar analysis** command to route calls with the dialed string pattern ***61*** to Session Manager using the existing ***Route Pattern 30*** (details not shown) via existing Trunk Group 30 (details not shown). Agents initiated outbound calls using the AAR feature access code 8 which routed all outbound calls through Session Manager in order to put the recorders in the call path. For purposes of the testing, all outbound PSTN calls were to area code 303 numbers.

```
                        AAR DIGIT ANALYSIS TABLE
                             Location: all            Percent Full: 0

         Dialed           Total     Route    Call   Node  ANI
         String          Min  Max  Pattern   Type   Num   Reqd
    1303                  11   11   30       aar          n
    601                    4    4   30       aar          n
    605                    4    4   30       aar          n
    61                     4    4   30       aar          n
```

In turn, the recorders initiated a second outbound call back to Communication Manager by appending the ARS feature access code 9 to the dialed number. Existing ARS entries were used to route calls to the PRI trunk to the PSTN using the 11 digit pattern starting with ***130***.

```
                            ARS DIGIT ANALYSIS TABLE
                                  Location: all            Percent Full: 0

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd

    130                   11   11    2       hnpa         n
    17                    11   11    2       hnpa         n
    1800                  11   11    deny    fnpa         n
    1900                  11   11    deny    fnpa         n
```

3.	**Administer Media Properties**

The Interactive Session Recorders require the following media properties:

- Audio Codec G.711, 20ms packets
- Silence Suppression disabled
- Media shuffling disabled
- DTMF In-Band (rtp-payload)

Use the **change ip-codec-set** command to confirm ***G.711MU*** is an option for the network region where the SIP trunk to Session Manager is connected. Also confirm the **Silence Suppression** is set to ***n***.

```
                         IP Codec Set

    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.722.1-32K                  1        20
 2: G.711MU           n          2        20
 3: G.729             n          2        20
```

Use the ***change signaling-group 30*** command and disable shuffling (**Direct IP-IP Connections**) by setting the entry to (***n***), and set **DTMF over IP** to ***rtp-payload***.

```
                               SIGNALING GROUP

 Group Number: 30             Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n                                             SIP Enabled LSP? n
     IP Video? y          Priority Video? n        Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM



   Near-end Node Name: procr                 Far-end Node Name: AuraSM
 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): 6
```

In the tested configuration, a second SIP trunk (not shown), using different Listen Ports was configured in order to facilitate a return route for calls that could not reach a recorder either due to lack of capacity or a server outage.

6. Configure Avaya Aura® Session Manager

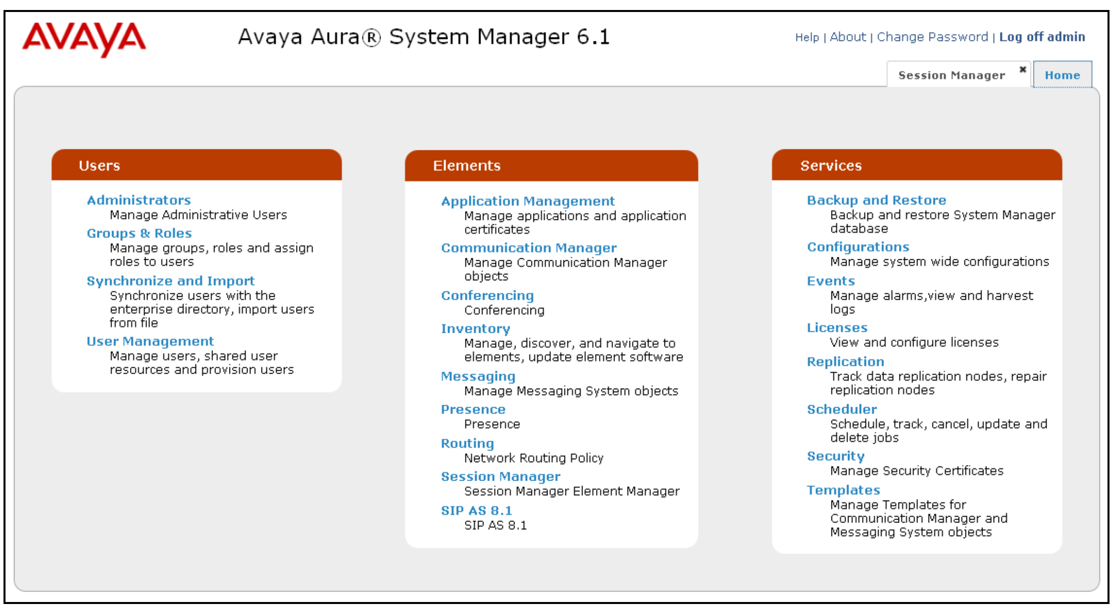
The test configuration used an existing environment with Communication Manager and Session Manager links/trunks already configured. Some of the existing settings will be highlighted to facilitate an understanding of the test environment; however details of many configuration steps will be omitted unless they have specific implications for the tested solutions. More information on these topics can be found in [1].

This section provides the procedures for configuring Session Manager. The procedures fall into the following areas:

- Administer SIP Entities and Entity Links
- Review Entity Links
- Create SIP Adaptations
- Create Routing Policies

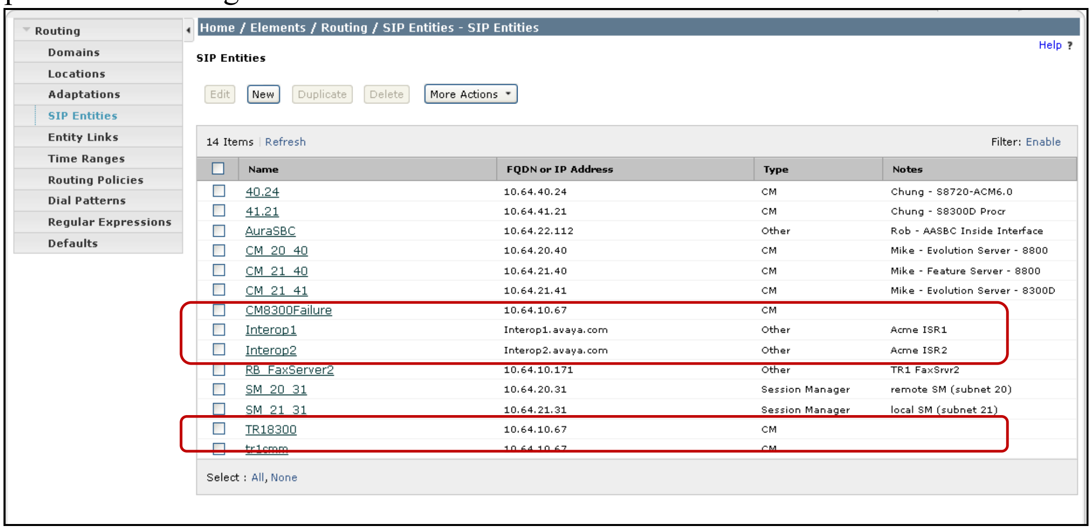
Session Manager is configured through Avaya Aura® System Manager. Access the web-based administration interface using **https://<host>/SMGR** in a browser where **<host>** is the IP Address or Fully Qualified Domain Name of the System Manager server. Login using appropriate credentials.

The landing page shown below is the base for navigating to the various administrative functions. For the tested configuration, the **Routing** and **Session Manager** objects were used to make all of the changes necessary to prepare the existing environment for the application. Clicking on these links, a tab opens up like shown below with the Session Manager tab (which is in the background in this screenshot).

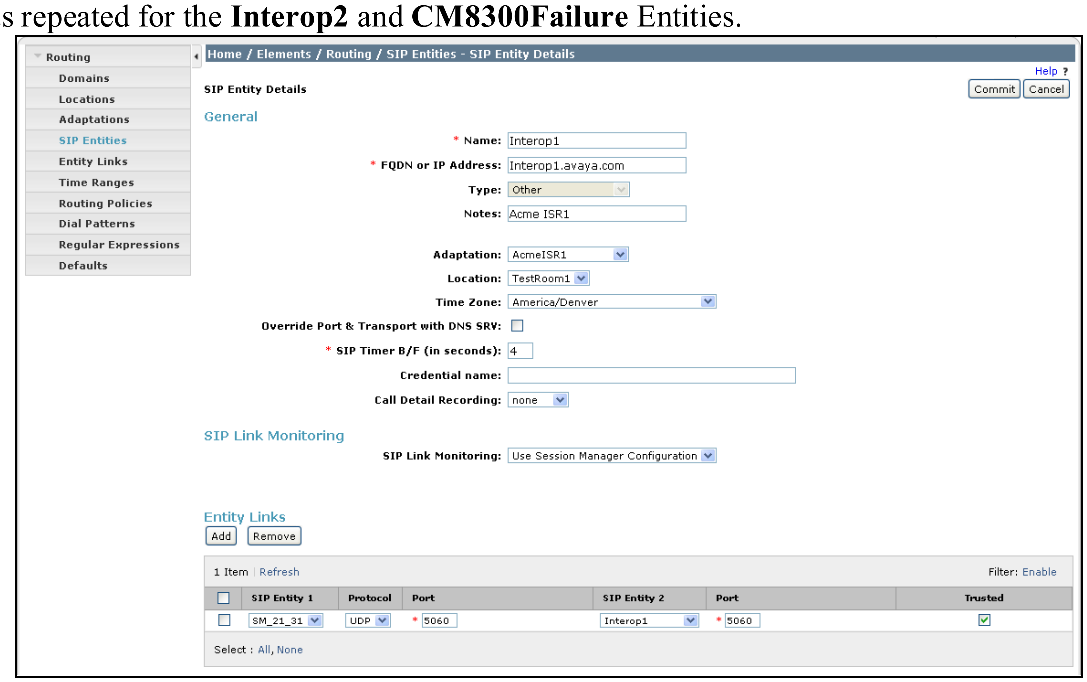


1. **Administer SIP Entities and Entity Links**

On the **Routing** tab, select the SIP Entities link and click **New** to add SIP Entity information for each recorder. For the tested configuration, existing CM entity **TR18300** was used for SIP links to Communication Manager. **Interop1** and **Interop2** were created for the two recording servers, and **CM8300Failure** was created to enable a unique adaptation for routing calls when no recorders were available.

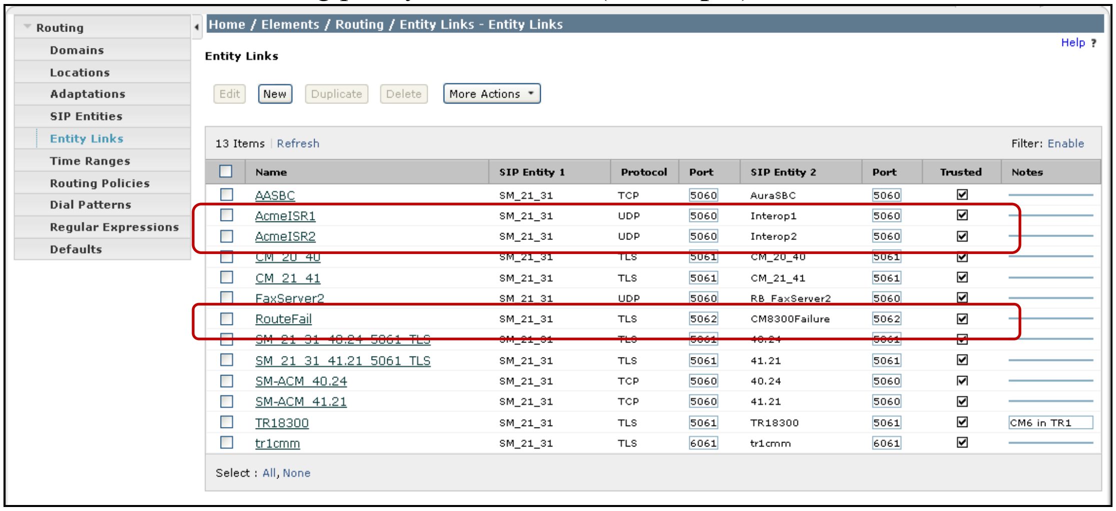


Details for the SIP Entity were added for each new Entity. The **Entity Name** can be any meaningful name. Enter the **FQDN or IP Address** of the recorder. Note that the Adaptation shown in this screenshot is described in **Step 3**. The **Entity Link** was created using the **Add** button and providing the information shown below (details not shown). Note that Interactive Session Recorders currently supports UDP messaging only. This step was repeated for the **Interop2** and **CM8300Failure** Entities.



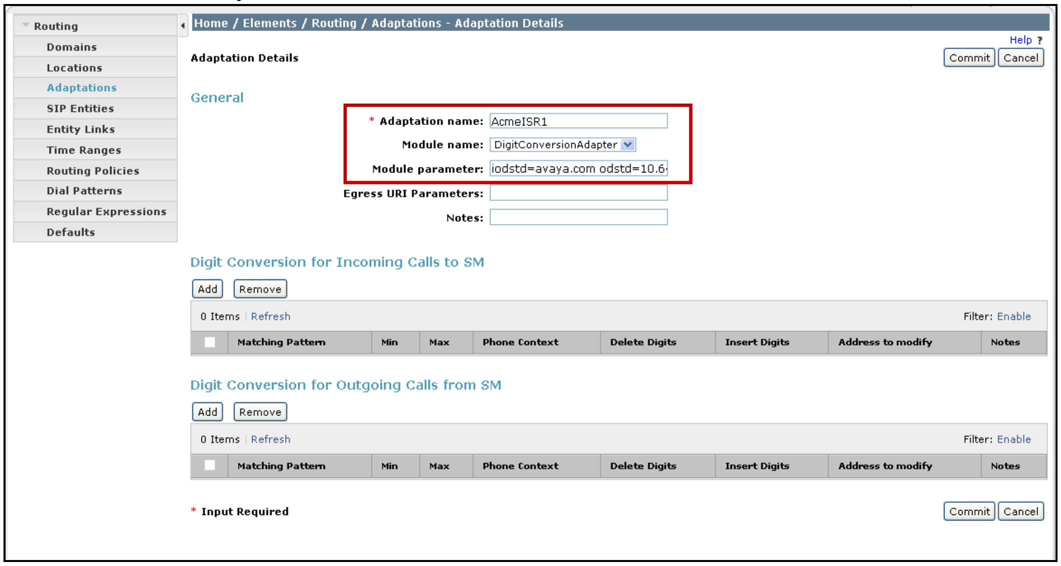
2. **Review SIP Entity Links**

The screenshot below highlights the four Entity Links used in the tested configuration. Note that the **RouteFail** Entity and Entity Link were created using a different IP Port in order to differentiate the Entity Link from the primary SIP trunk between Communication Manager and Session Manager. This allowed the unique Adaptation rules to be applied when the **RouteFail** routing policy was invoked (see **Step 5**).

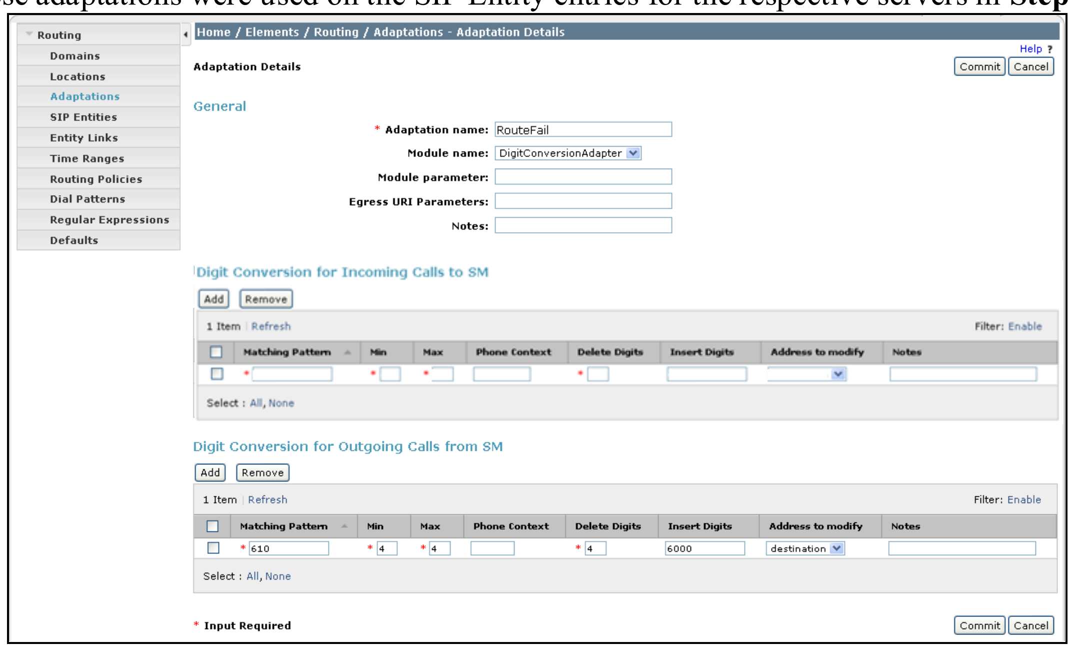


3. **Create SIP Adaptations**

Session Manager uses Adaptation rules to manipulate SIP Headers. For the tested configuration, the recorders sent all requests from their own IP Address domains, and Session Manager and Communication Manager used the avaya.com domain. An Adaptation was created for each recorder to reconcile the domain names using the **Module parameter** ***iodstd=avaya.com odstd=10.64.10.1170/140***.



An Adaptation was created for conditions when both recorders were unable to handle an inbound call. By replacing the ***610x*** dialed digits with ***6000***, calls were routed to VDN 6000 and queued to agents. An Adaptation could similarly be created adding a ***9*** to the 11 digit dialed number for outbound calls for a bypass route for outbound calls (not tested). These adaptations were used on the SIP Entity entries for the respective servers in **Step 2**.



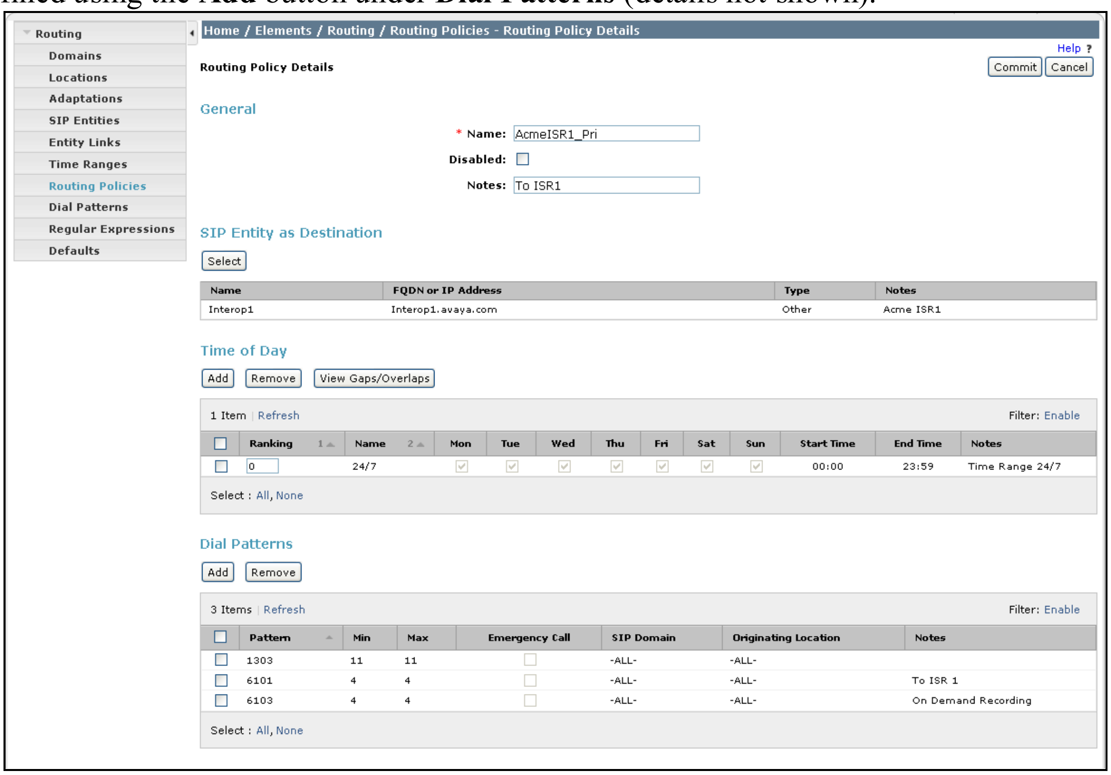
4. **Create Routing Policies**

Session Manager Routing Policies are created in a two-step process. A **Routing Policy** is created, and **Dial Patterns** are defined for use in one or more policies.

The following table describes the **Routing Policies** used in the tested configuration:

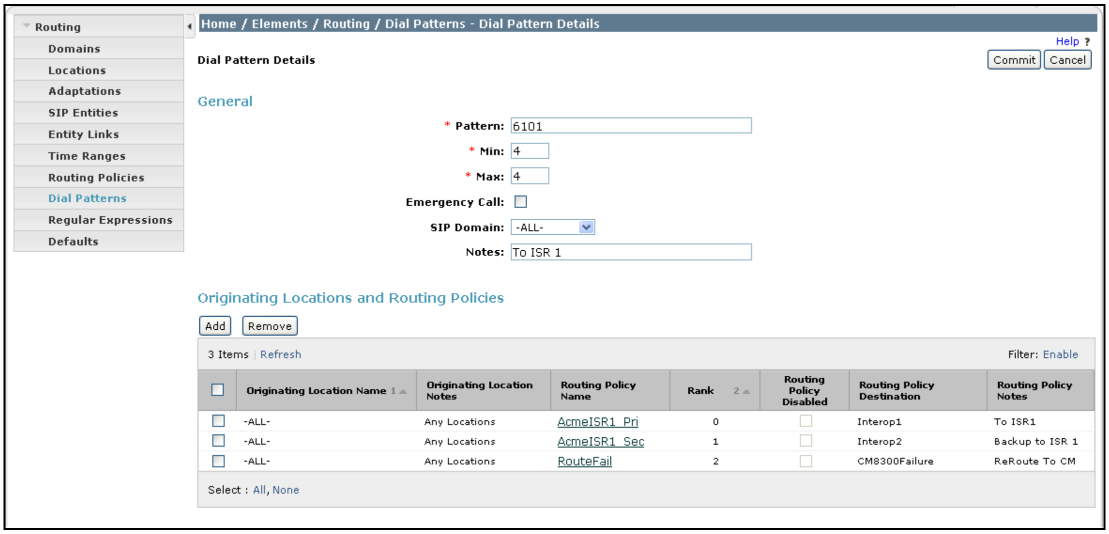
Route-To Digits (Dial Pattern)	Primary Server	Secondary Server	Routing Policy	Description
1303 (11 Digits)	Interop1	Interop2	AcmeISR1_Pri AcmeISR1_Sec	Outbound Calls to Server 1 Failover to Server 2
6101 (4 Digits)	Interop1	Interop2	AcmeISR1_Pri AcmeISR1_Sec RouteFail	Inbound ACD to Server 1 Failover to Server 2 Failover to CM
6102 (4 Digits)	Interop2	Interop1	AcmeISR2_Pri AcmeISR2_Sec RouteFail	Inbound ACD to Server 2 Failover to Server 1 Failover to CM
6103 (4 Digits)	Interop1	Interop2	AcmeISR1_Pri	On-Demand Recording

Each Routing Policy was administered similar to the following screenshot. The **Time of Day Ranking** for each Primary policy was ***0***. For Secondary policies, a **Ranking** of ***1*** was used, and for the **RouteFail** policy, a **Ranking** of ***2*** was used. This instructs Session Manager in what order to consider each policy for a given Dial Pattern. Dial Patterns were defined using the **Add** button under **Dial Patterns** (details not shown).



Create Routing Policies (Continued)

Another way of looking at the Routing Policies is to review policies assigned to each of the Dial Patterns. For the **Dial Pattern *6101***, calls routed to Server 1 using the ***AcmeISR1_Pri*** routing policy first (due to the 0 rank), then to Server 2 if there were no ports or if the server was out of service using the ***AcmeISR1_Sec*** routing policy, then finally back to CM using the ***RouteFail*** routing policy.

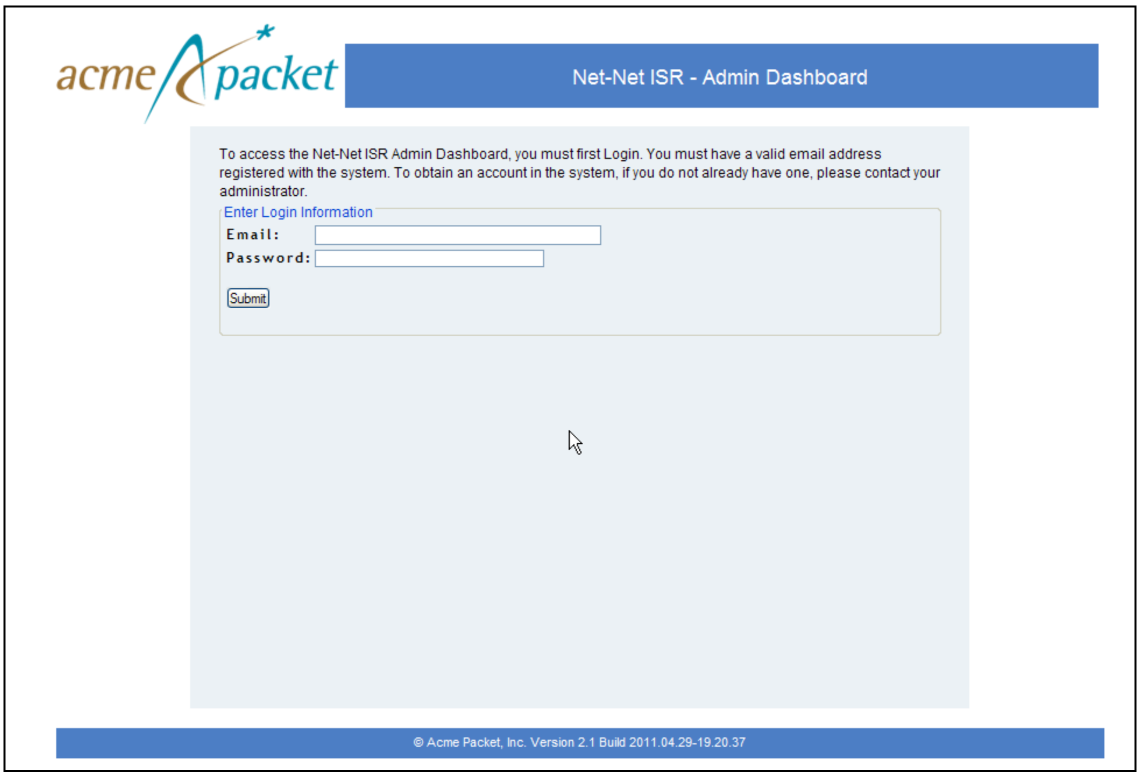


7. Acme Packet® Net-Net® Interactive Session Recorder

This section provides the steps for configuring the Acme Packet® Net-Net® Interactive Session Recorder. Each server was independently configured, only one server configuration is described as the entries on each server were similar.

7.1. Interactive Session Recorder Configuration Details

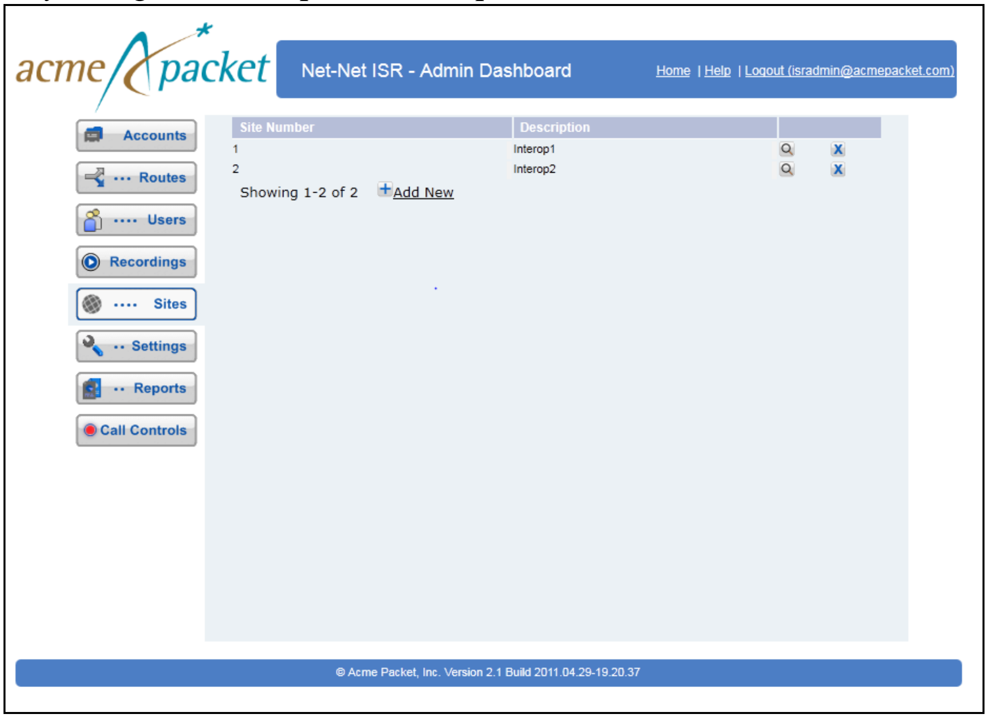
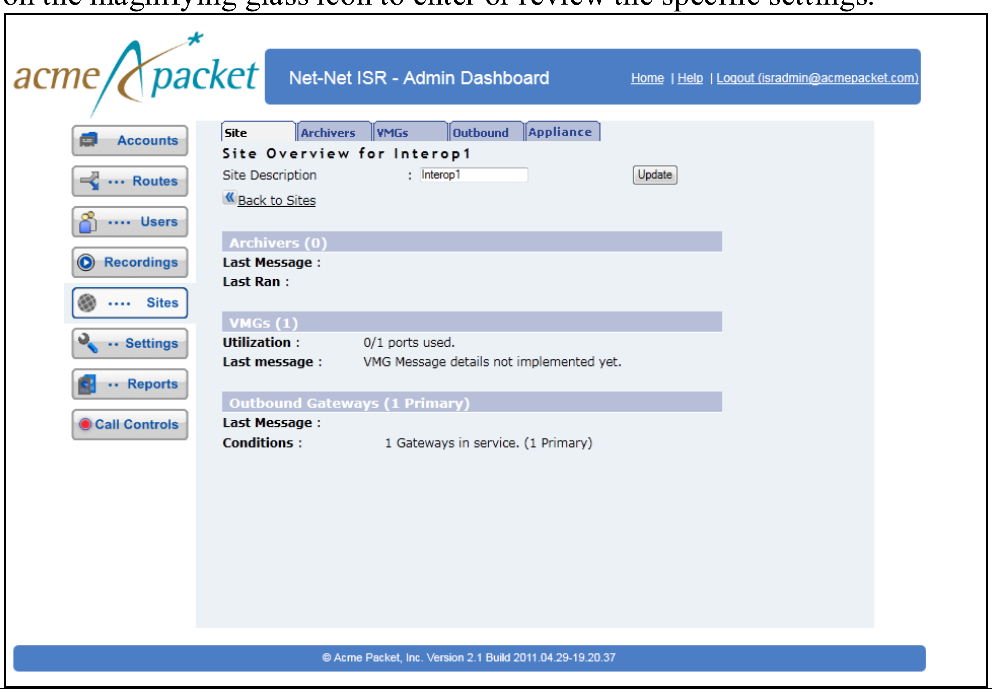
The Interactive Session Recorder is configured using a web browser. Enter the URL of the server such as **http://<host>:9000/AdminDashboard** where <host> is the ip address or fully qualified domain name of the server. Login using appropriate credentials.



In general, the steps were as follows:

- Configure the Site(s)
- Configure Routing

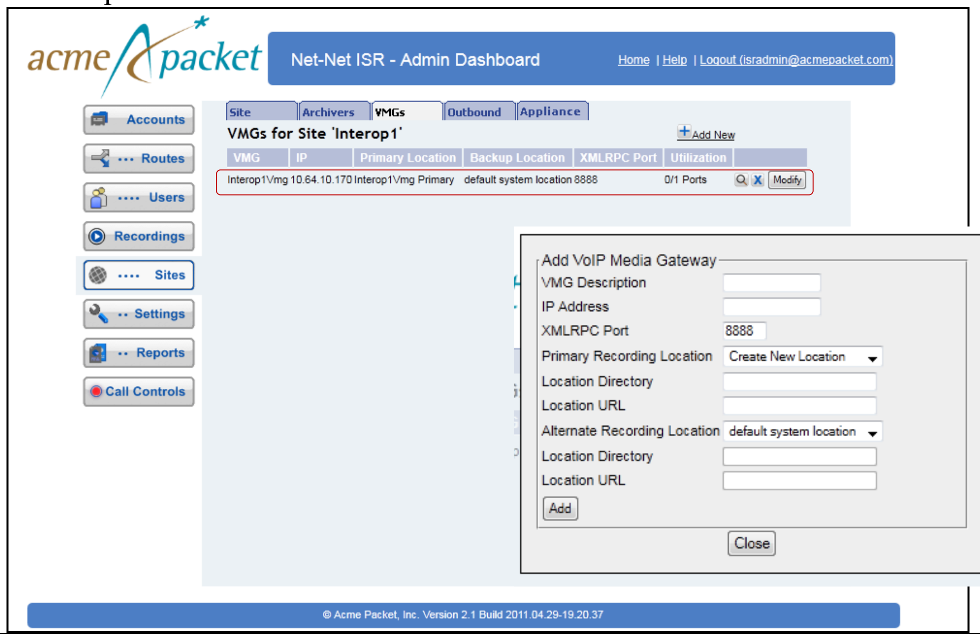
Note that some of these steps require several subtasks, the illustrations of these subtasks cover several pages to complete each task.

Step	Description
1.	**Configure the Site** Each server is configured as a Site. Click the **Sites** button to navigate to the **Sites** form, and click **Add New** to create a new Site. In the illustration below, two servers were previously configured, ***Interop1*** and ***Interop2***.  Click on the magnifying glass icon to enter or review the specific settings. 

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td></td><td>

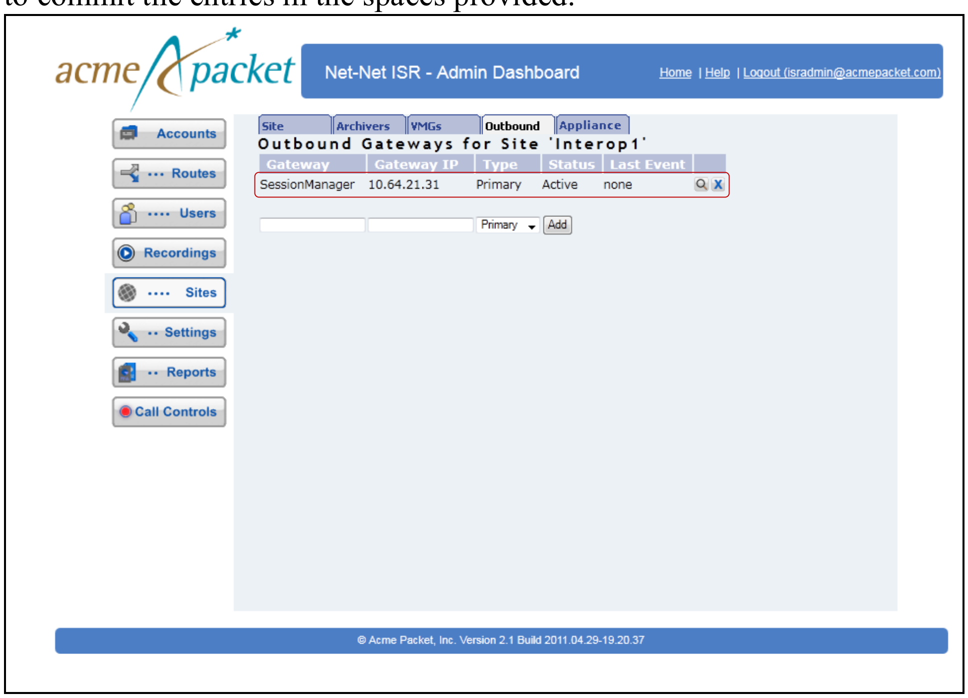
Configure the Site (continued)

Click on the **VMGs** Tab (Voice Media Gateway is the internal name of the recording service). The entry below illustrates the settings previously configured for Interop1 and the inset illustrates the dialog used to create an entry when the **Add New** link is clicked. Repeat this step for each server.



</td></tr>
<tr><td></td><td>

Click the **Outbound** tab to configure the Session Manager interface. Use the **Add** button to commit the entries in the spaces provided.



</td></tr>
</table>

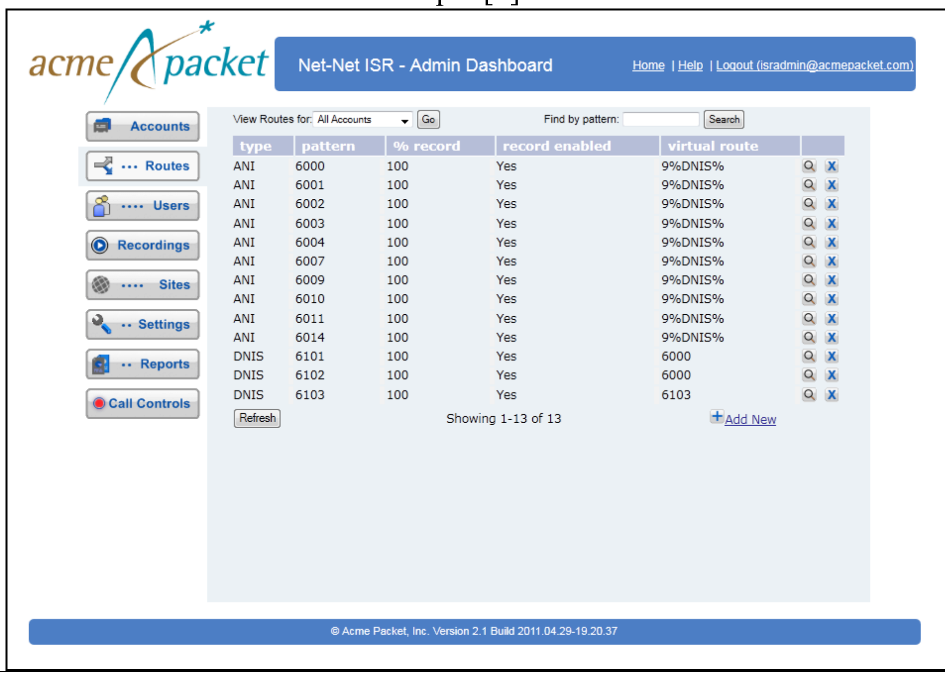
<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>2.</td><td>

Configure Routing

The Interactive Session Recorder uses routes to define recording and routing rules. Rules are based on ANI or DNIS patterns or a combination of the two.

Click on the **Routes** tab to review rules, or click the **Add New** link to configure new rules. In the illustration below, ANI rules were used for outbound calls, to record 100% of the calls from defined internal extensions, and to add 9 to the DNIS (to inform Session Manager to route the call to Communication Manager, and to inform Communication Manager to route to the PSTN using ARS).

Wildcards can be used in defining ANI or DNIS for these rules, but defining each specific ANI permits a more granular use of permissions within the application. See the documentation for more details on this topic [3].



</td></tr>
</table>

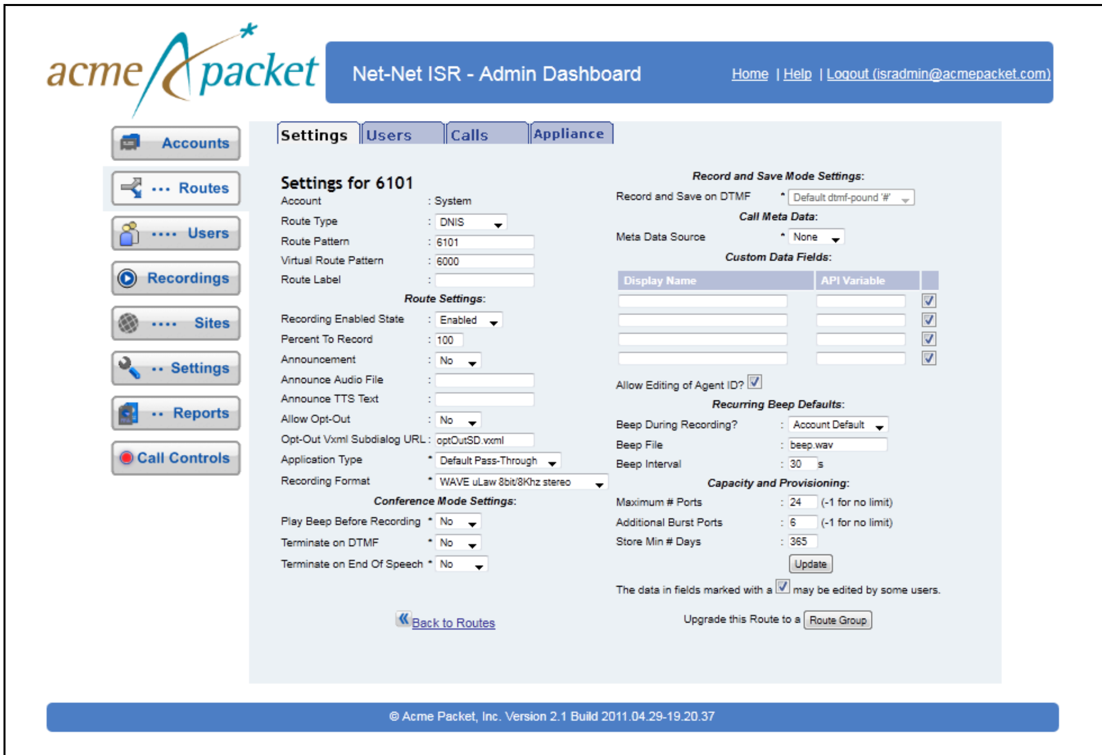
<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td></td><td>

Configure Routing (continued)

Below is an illustration of the details of the existing settings for the 6101 DNIS (Inbound) route rules. This screen appears when the **Add New** link is clicked on the main **Routes** page.

Specific entries include **Route Pattern** (***6101*** in this case, which is the pattern used to route inbound calls to Interop1 as described in Session Manager **Section 6, Step 5**). The **Virtual Route Pattern** is the entry which creates the destination address for calls using this pattern, in this case ***6000*** which is a VDN on Communication Manager that routes calls to ACD agents. Details of the options for the other entries shown below can be found in [3].

This step was repeated for the ***6102*** and ***6103*** route patterns. Route Pattern 6103 differed in the **Application Type** setting which was set to ***Conference*** (not shown). The ***Default Pass Through*** **Application Type** used for all other call types resulted in two call legs (one in to the recorder, and one out of the recorder) where the ***Conference*** **Application Type** simply answers and thus records the call. To activate this type of recording, users simply conferenced extension 6103 to any existing call from the phone or softphone application.

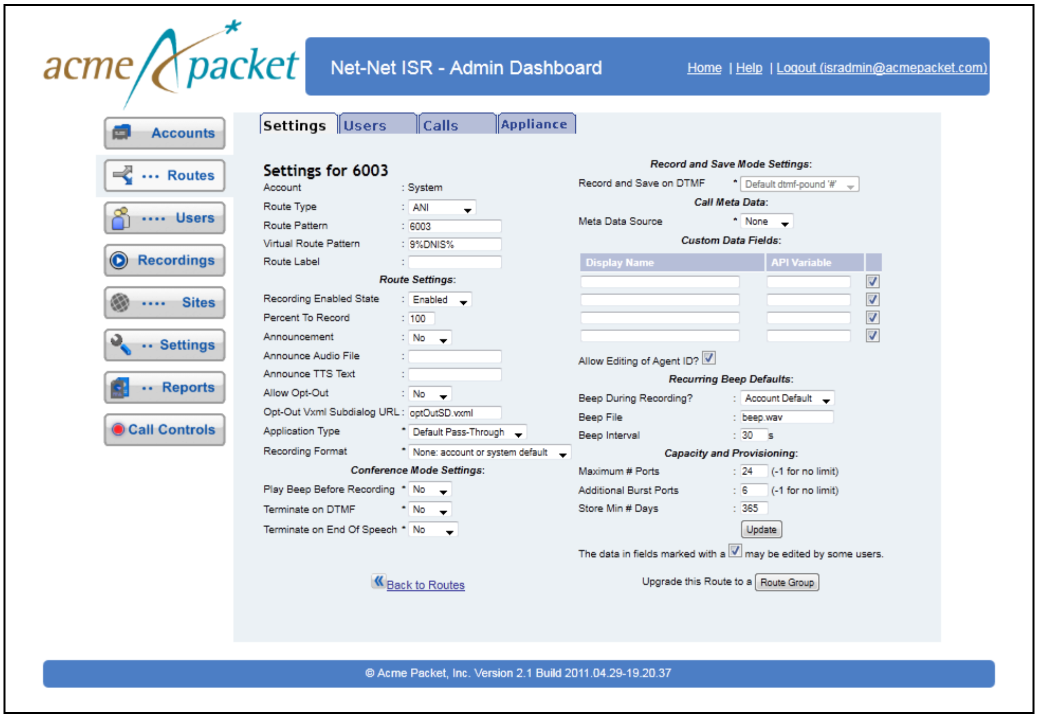


</td></tr>
</table>

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td></td><td>

Configure Routing (continued)

Outbound dialing rules were created for each extension used in the test environment using the ***ANI*** **Route Type**. For the **Virtual Route Pattern**, ***9%DNIS%*** was used to instruct the application to append a 9 to the number the user dialed for proper routing in Session Manager and Communication Manager. This step was repeated for each station with the Route Pattern definition matching each configured station on Communication Manager and Session Manager.

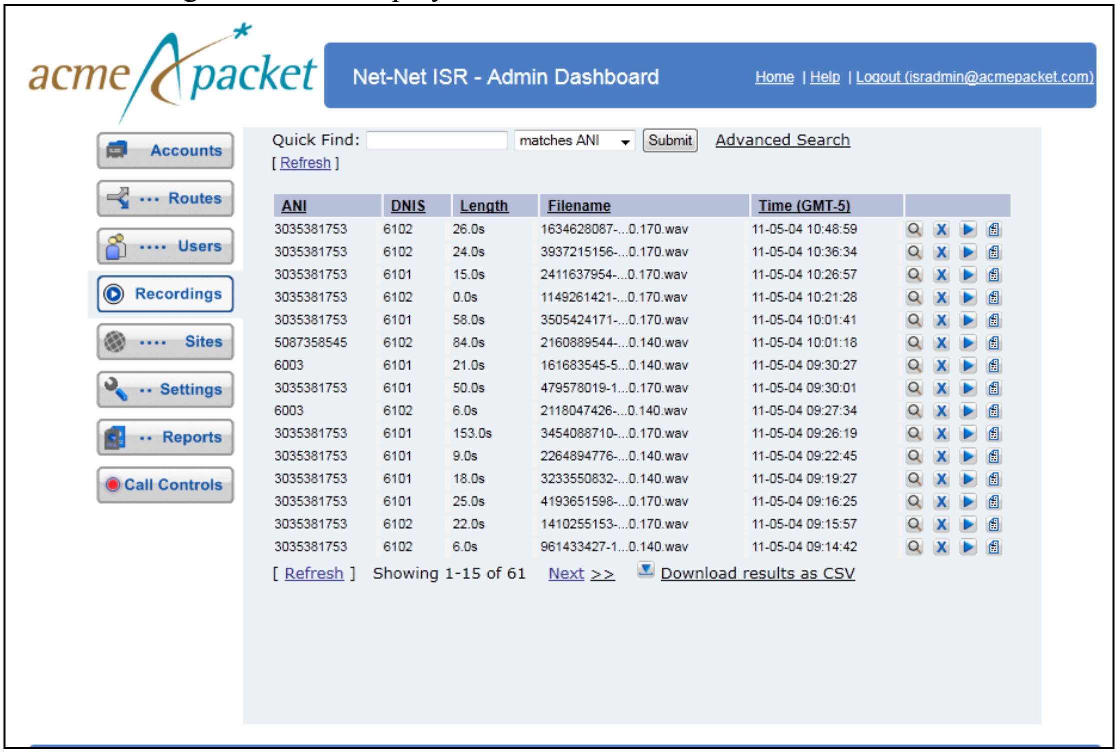


Configuration changes are read by the application every 60 seconds. Alternately, the Newfound VoIP Media Gateway service can be restarted from the Windows Services utility.

</td></tr>
</table>

8. Verification Steps

Following each completed test case, the Recordings list was used to query for the recently completed recordings and initiate a playback.



The log file is at D:\Newfound\VoIPMediaGateway\log\NewfoundVMG.log and, at startup, will look like this:

```
05/04/2011 16:42:23[NOTICE] mixMaster:
>>>>>>Logger properties file(C:\Newfound\VoIPMediaGateway/vmgLog.properties) loaded<<<<<<
05/04/2011 16:42:23[  WARN] mixMaster: Unable to read license file VoIPMediaGateway.lic. Starting two(2) ports service instance...
05/04/2011 16:42:23[NOTICE] mixMaster: Using two(2) ports license for VoIPMediaGateway
05/04/2011 16:42:23[NOTICE] mixMaster: VoIP Media Gateway v2.2.0 (REL1 built on 20110223.155714) starting.
05/04/2011 16:42:23[NOTICE] mixMaster: Fetching configuration from C:\Newfound\VoIPMediaGateway/vmgConfig.xml:
05/04/2011 16:42:23[  INFO] mixMaster: Got host IP address: 10.64.10.170
```

After outputting all of the default configuration settings, the recorder will load all of the routes and outbound gateways that have been created into its Local Route Cache.

```
05/04/2011 16:42:23[  INFO]  RouteMap: Get Account List returned 1 accounts last update @ 2011-05-04 16:42:23.0.
05/04/2011 16:42:23[  INFO]  RouteMap: RouteMap cache is being created...
05/04/2011 16:42:23[  INFO]  RouteMap: XmlRpc method 'getRouteMap' return ACK
05/04/2011 16:42:23[  INFO]  RouteMap: ENLIST route with rout_id: 1,routePattern: 6101
05/04/2011 16:42:23[  INFO]  RouteMap: route with rout_id: 1,routePattern: 6101 added
.
05/04/2011 16:42:23[  INFO]  RouteMap: ENLIST route with rout_id: 15,routePattern: 6103
05/04/2011 16:42:23[  INFO]  RouteMap: route with rout_id: 15,routePattern: 6103 added
05/04/2011 16:42:23[  INFO]  RouteMap: RouteMap cache creation process finished.
05/04/2011 16:42:23[  INFO]  RouteMap: Get RouteMap returned 13 routes last update @ 2011-05-04 16:42:23.0.
```

Any errors in this section will mean that the route map was not created.

Then it will also create an outbound gateway list:

```
05/04/2011 16:42:23[  INFO]  RouteMap: Outbound Gateway list is being created...
05/04/2011 16:42:23[  INFO]  RouteMap: XmlRpc method 'getOutboundGateway' return ACK
05/04/2011 16:42:23[  INFO]  RouteMap: ENLIST Outbound Gateway with gateway_id: 1, gateway_address: 10.64.21.31
05/04/2011 16:42:23[  INFO]  RouteMap: Outbound Gateway entry with gateway_id: 1,gateway_address: 10.64.21.31 added
05/04/2011 16:42:23[  INFO]  RouteMap: Outbound Gateway list creation process finished.
05/04/2011 16:42:23[  INFO]  RouteMap: Get Outbound Gateway returned 1 gateways last update @ 2011-05-04 16:42:23.0.
```

Once the route cache and the outbound gateway lists are created, calls can be made. From here, every minute the RouteMap will be refreshed – meaning that changes made through the AdminDashboard can take up to 1 minute to take effect.

Common errors include:

1. Outbound Gateway (Session Manager) unable to process call.

```
05/04/2011 10:37:07[NOTICE]  sipProxy: Refusing Call As Unavailable (sc=0x00000000028CA3E0)
05/04/2011 10:37:07[  INFO]  sipProxy: (SIP Event - BYE received, Reason: Service Unavailable [cid = 27, did = 28])
```

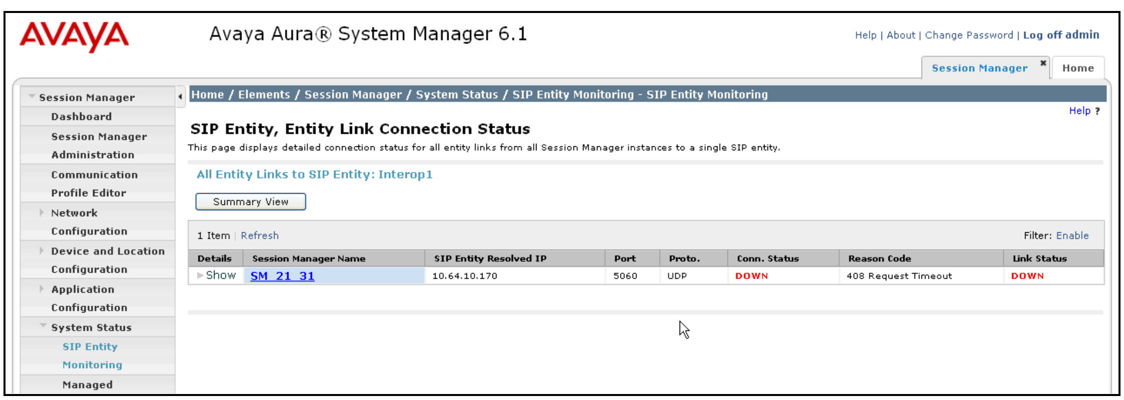
2. Server at capacity

```
05/04/2011 15:02:01[  INFO]  sipProxy: (SIP INVITE received - new call!!! [cid = 11, did = 12])
05/04/2011 15:02:01[  CRIT]channelMap: error: no channels available to take this call!!!!
05/04/2011 15:02:01[ ERROR]  sipProxy: No more channel resource is available for 6102
05/04/2011 15:02:01[NOTICE]  sipProxy: Refusing Call (sc=0x00000000006FE7F0)
```

3. No Route found for incoming ANI/DNIS – call being forwarded to Interactive Session Recorder for which no routing rule has been created

```
05/04/2011 15:26:39[  INFO]callManager: [Channel 1] Looking up call w/ ANI: 3035381753 DNIS: 6101
05/04/2011 15:26:39[NOTICE]  RouteMap: Call route with ANI: 3035381753 DNIS: 6101 returned CALL_TYPE_NOTFOUND.
05/04/2011 15:26:39[NOTICE]  sipProxy: Refusing Call (sc=0x0000000000690B70) as NOT FOUND
05/04/2011 15:26:39[NOTICE]  sipProxy: [Channel 1] Returning SIP Channel to IDLE List.
05/04/2011 15:26:39[  INFO]  sipProxy: (SIP Event - BYE received, Reason: Not Found [cid = 1, did = 2])
```

Additionally, from Avaya Aura® Session Manager, confirm the status of the Entity Link by navigating to **Elements > Session Manager > System Status > SIP Entity Monitoring** and clicking on the Entity Link to the server:



9. Conclusion

Acme Packet® Net-Net® Interactive Session Recorder successfully demonstrated the ability to record calls that passed through the Avaya Aura® Session Manager. Further, the application demonstrated the ability to successfully recover from network and server outages with minimal delay in recovering to full functionality.

10. Additional References

Product documentation for Avaya products may be found at http://support.avaya.com.

[1] *Administering Avaya Aura™ Session Manager*, Document ID 03-603324, Issue 1, Release 6.1, November, 2010.

[2] *Administering Avaya Aura™ Communication Manager Server Options,* Document ID 03-603479, Issue 2.2, Release 6.0.1, April, 2011.

[3] *Administering Avaya Aura™ Communication Manager,* Document ID 03-300509, Issue 6.0, Release 6.0, June, 2010.

[4] *Net-Net® Interactive Session Recorder Administrator Guide,* Version 2.1, January, 2011

[5] *Net-Net® Interactive Session Recorder Installation Guide,* Version 2.1, April 2011

Product information for Acme Packet products may be found online at www.acmepacket.com.

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.