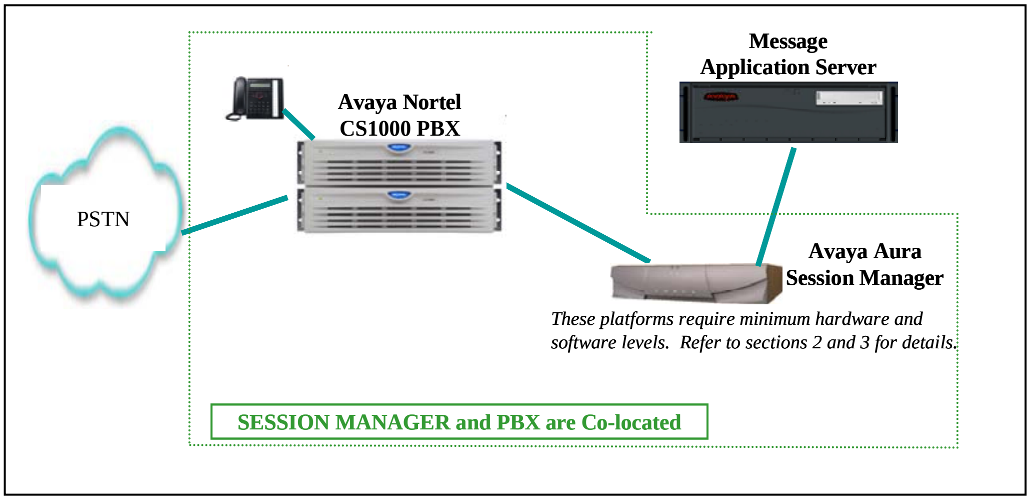
Avaya™
Modular Messaging

Configuration Note 88070 – Version A (3/11)

Avaya CS1000

SIP Integration w/ Avaya Aura Session Manager



Note: Integrating **MM with multiple Avaya CMs** requires special consideration regarding Session Manager administration to ensure call handling and MWI delivery. It is advisable to consult with your ATAC or Sales Engineer representative.

Overview

This Configuration Note is intended for Avaya certified technicians/engineers who are familiar with Modular Messaging procedures and terminology. It also assumes that you are Avaya certified or very familiar with the features and functionality of the Avaya PBXs supported in this Configuration Note and the SIP protocol.

Use this document in conjunction with *Modular Messaging Installation Guide* and the appropriate *Nortel PBX Guides* mentioned throughout this Config Note.

Please read the entire document before attempting any configuration.

SIP Trunks allows the Avaya CS1000 PBX and the Avaya Message Application Server to communicate over a LAN.

1.0 METHOD OF INTEGRATION

The Session Initiation Protocol (SIP) integration provides connectivity with the Avaya PBX CS1000 over a Local Area Network (LAN). The connectivity between the Avaya Message Application Server (MAS) and the PBX is achieved over an IP-connected SIP trunk via the Avaya Aura Session Manager proxy. This integration passes call information and MWI using SIP packets.

2.0 AVAYA MESSAGE APPLICATION SERVER REQUIREMENTS

Avaya MAS Requirements

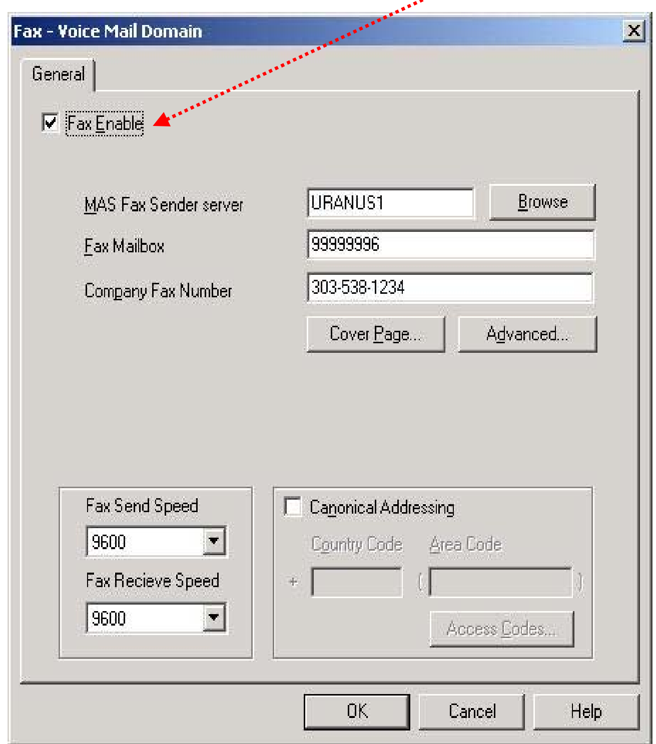
[1]**Release Note**: Should features of the integration not function optimally when integrated to a PBX or MM that may be operating on an unsupported software release as defined Section 2.0 and 3.1, customers will need to upgrade their PBX and/or MM to a supported software release.

- **Minimum releases required [1]:**
  - **MM 5.2 SP5**
- **MM license***

***Note**: A license must be obtained prior to installing the SIP integration and must be imported prior to testing/operation of the system.

Important: **Without this license SIP will not function.** The 10 user licenses that come with a new MM system will not work with the SIP integration.

- **Fax: To enable FAX over SIP** you must check the Fax_Enable box found on the General Tab on the Fax – Voice Mail Domain screen.



PBX hardware requirements

3.0 PBX HARDWARE REQUIREMENTS

Before performing the installation ensure the customer site has had an Avaya Network Assessment and the customer has implemented the recommendations.

- Avaya CS1000E CP+PM Call Serve 6.0.18 (with Software as detailed below in Section 3.1)
- Avaya CS1000E Signaling Server 6.0 (Linux-based)

PBX/SESSION MANAGER software requirements

3.1 PBX SOFTWARE REQUIREMENTS

Minimum Software [1] (see pg 2):

- **Avaya CS1000E** updated to the current DEPLIST
- **CS1000 R6 SIP GW** with nortel-cs1000-vtrk-6.00.18.65-61.i386 or higher
- **VTRUNK Application Software** with nortel-cs1000-vtrk-6.00.18.65-61.i386 or higher
- **VTRUNK SU** installed with the following activator patches are required (**Note**: You do not need both MPLR30222 and MPLR25529, just either one depending on your configuration)
  - **MPLR30222** (activates Diversion Header and supports History Info)

    - or -

  - **MPLR25529** (activates Diversion Header and removes History Info. May be used in stand-alone CS1000 environments where CS1000 to CS1000 SIP Peering is not used.)
  - **MPLR29593** (activates support for UPDATE of p-assert after call answer)

- continued on next page -

3.2 SESSION MANAGER SOFTWARE/HARDWARE REQUIREMENTS

Minimum Supported Software and Hardware:

- Avaya Aura Session Manager 5.2

Hardware Required:

- Avaya S8xxx with SM100 card (*acts as gateway to SM*)
- Customer responsible for:
  - Monitor, Keyboard, and Mouse
  - Cat 5 Ethernet Cables
  - Blank DVDs for burning ISO images if needed

Please refer to *Installing and Administering Session Manager* for more details.

3.3 CONNECTIVITY

- Ethernet LAN connectivity - TCP/IP

3.4 CUSTOMER-PROVIDED EQUIPMENT

- Wiring/equipment necessary to support the physical LAN (CAT 5 minimum)

- continued on next page -

Supported integration features

4.0 SUPPORTED INTEGRATION FEATURES

[✓] Items are supported

System Forward to Personal Greeting	
All Calls	[✓]
Ring/no answer	[✓]
Busy	[✓]
Busy/No Answer	[✓]
Station Forward to Personal Greeting	
All Calls	[✓]
Ring/no answer	[✓]
Busy	[✓]
Auto Attendant	[✓]
Call Me	[✓]
Direct Call	[✓]
External Call ID (ANI)	[✓]
Fax	[✓]
Find Me	[✓]
Internal Call ID	[✓]
Message Waiting Indication (MWI)	[✓]
Multiple Call Forward	[✓]
Multiple Greetings	[✓]
N+1	[✓]
Outcalling	[✓]
Queuing	[✓]
Return to Operator	[✓]

IMPORTANT: PBX options or features not described in this Configuration Note are not supported with this integration. To implement options/features not described in this document, please contact the Avaya Switch Integration product manager.

- continued on next page -

5.0 CONFIGURING THE AVAYA CS1000E

Note: This Configuration Note assumes basic configuration of telephones and SIP trunking to Session Manager has been completed.

For information on basic configuration please refer to *Communication Server 1000E Installation and Commissioning.* Release 6.0, rev 3.02. Nortel Doc#NN43041-310.

PBX Configuration

The following tasks must be completed in the following order when programming the PBX to integrate. PBX programming is intended for certified PBX technicians/engineers.

- Log in to CS1000E Element Manager
- Add a **Distant Steering Code** (DSC) for coverage and access to Modular Messaging
- Configure phones to cover* to the MM 'pilot' extension
- Log in to the Network Routing Service (NRS)
- Add a route for the MM 'pilot' extension

***Note**: Avaya uses the term "cover" while Nortel uses the term "forward."
For purposes of this document they are one in the same.

Configuring Session Manager with Avaya CS1000 and Modular Messaging

The diagram below is an example illustrating traffic engineering and load balancing used with Session Manager "Diamond Configuration."

- The Avaya CS1000 is configured so that users (stations) are divided up for load balancing by assigning users one of two cover paths and routing preferences.

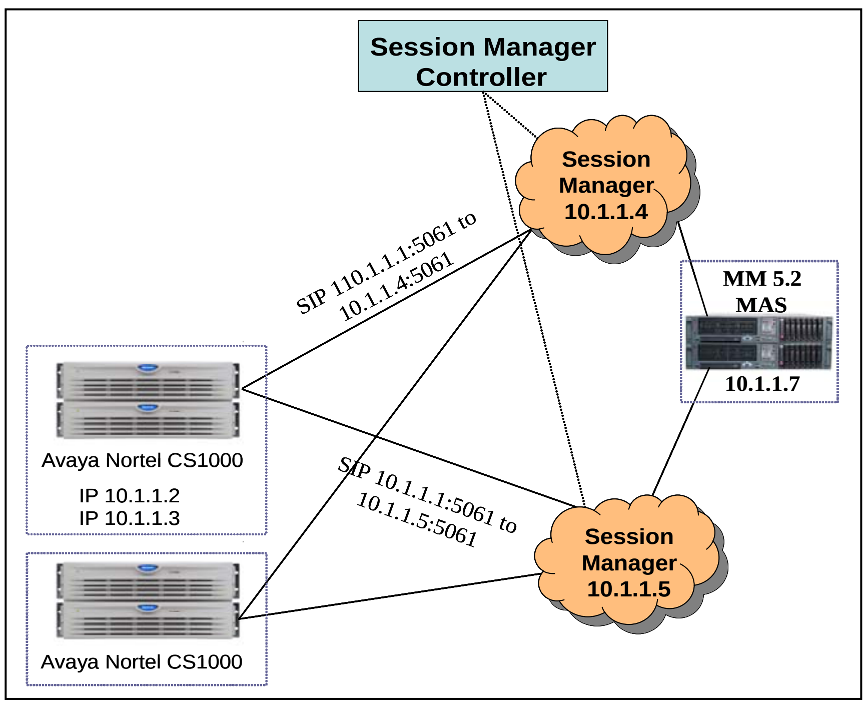
  Users can use either one of two pilot numbers for voicemail retrieval. In this way traffic is engineered so some sip traffic will use trunk x, y as the 1st and 2nd choice and others will use trunk y, x as the 1st and 2nd choice.

  All users can be served by either SM server should one go out of service for maintenance or any other reason. This provides for redundancy and provisioned load balancing.

- The Modular Messaging System is configured so that the PBX Site has two entries: 10.1.1.4 and 10.1.1.5.

  For originations from MM (i.e., MWI, Call Me, Find Me, Transfers, etc.), the MM will load balance between the two PBX (Session Manager) IP addresses. Should one become unavailable MM will automatically route all originations to the second IP address in the PBX administration.

  If using Session Manager in a Diamond Configuration you will to provision two SIP trunk groups, two route patterns, two routing entries, two SIP pilot numbers (Hunt Groups) and two cover paths.

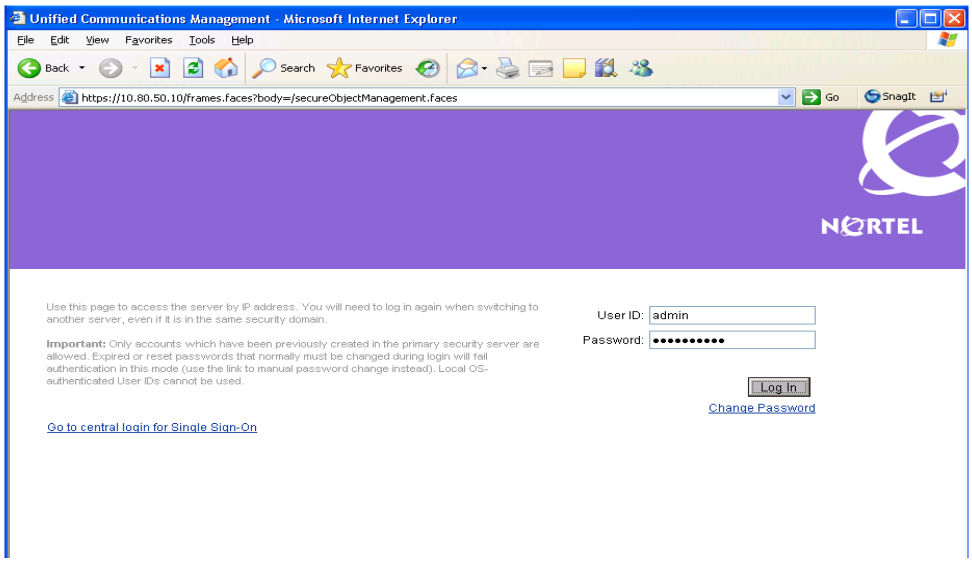


5.1 Configuring the Avaya CS1000E using the IE Browser

- Open Internet Explorer and enter the IP Address of the CS1000E call server. In the example image below the URL to login is **https://10.80.50.10/**

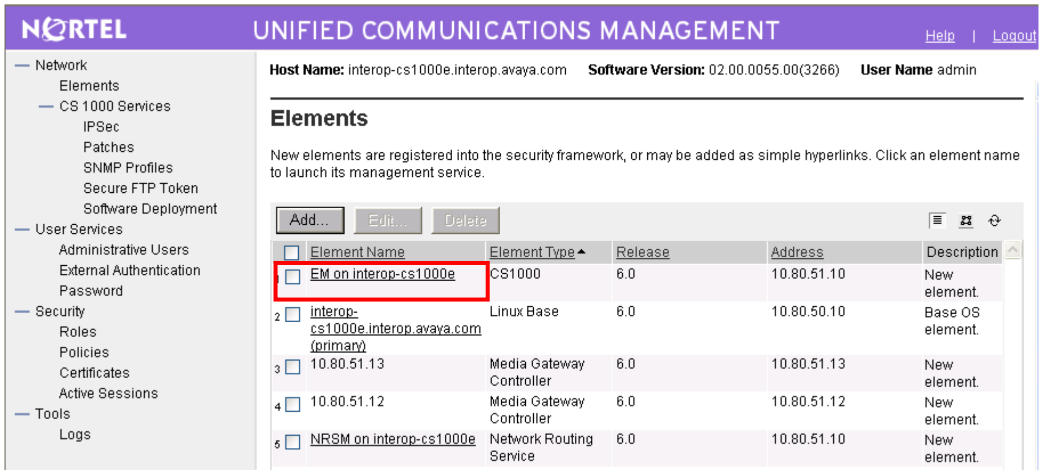
Note: IE is the only browser supported for CS1000E UCM

- This should bring you to the CS1000E Communications Management page.
- Log in using the appropriate Username and Password.



- continued on next page -

- Once logged in the first screen you will see is the Elements screen. Select the element of type **CS1000**.



- **ADD A DISTANT STEERING CODE (DSC)**

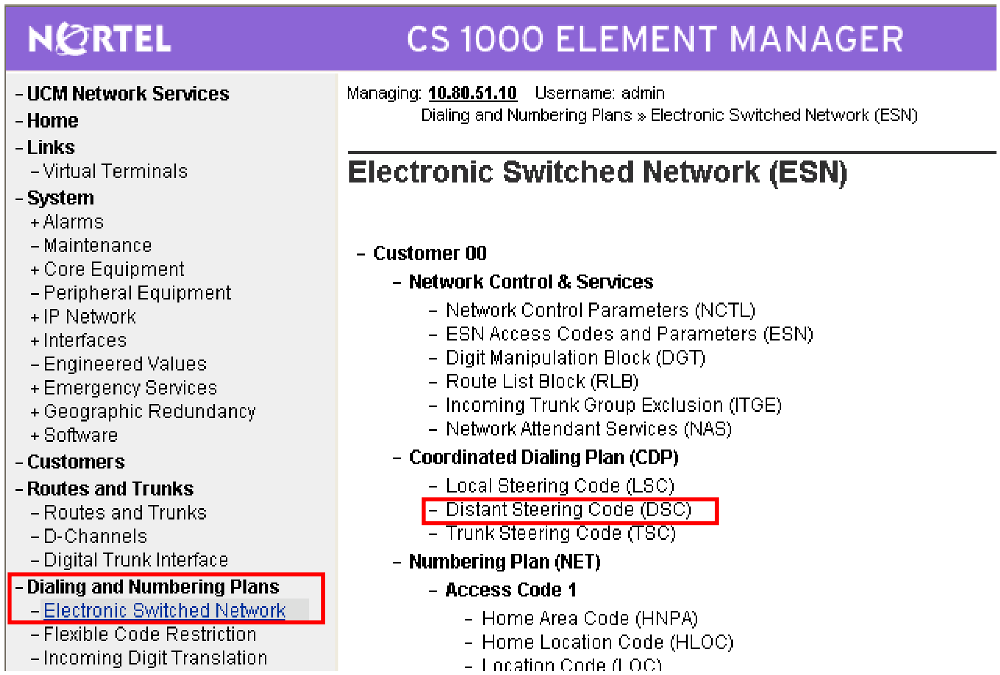
The CS1000E will router callers and subscribers to Modular Messaging using an Distant Steering Code, or DSC. In our example configuration the CS1000E only needs to route calls to Session Manager, which will route the calls to Modular Messaging.

In this configuration, extension **6665001** is our pilot number. This is the number used by subscribers to call to retrieve messages, and also the number that the CS1000E will use to cover to voice mail.

To do this we need to add a **Distant Steering Code (DSC)** for any number that starts with 666 and is 7-digits in length.

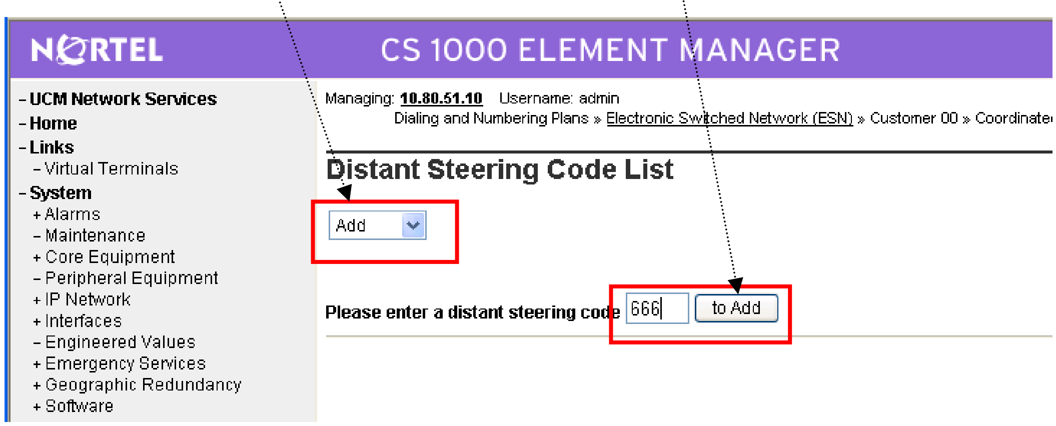
- continued on next page -

- To add a **DSC**, from the left-pane select **Electronic Switched Network**. Then, from the newly displayed right-panel select Distant Steering Code as indicated below.



- The screen below should now appear. Using the drop-down menu select **Add,** then enter **666** in the field next to *Please enter a distant steering code*. Then click on "**to Add**"

NOTE: It's not necessary to differentiate all numbers that begin with **666.** It's only necessary to get those calls that have a number beginning with **666** to the Avaya Aura Session Manager.

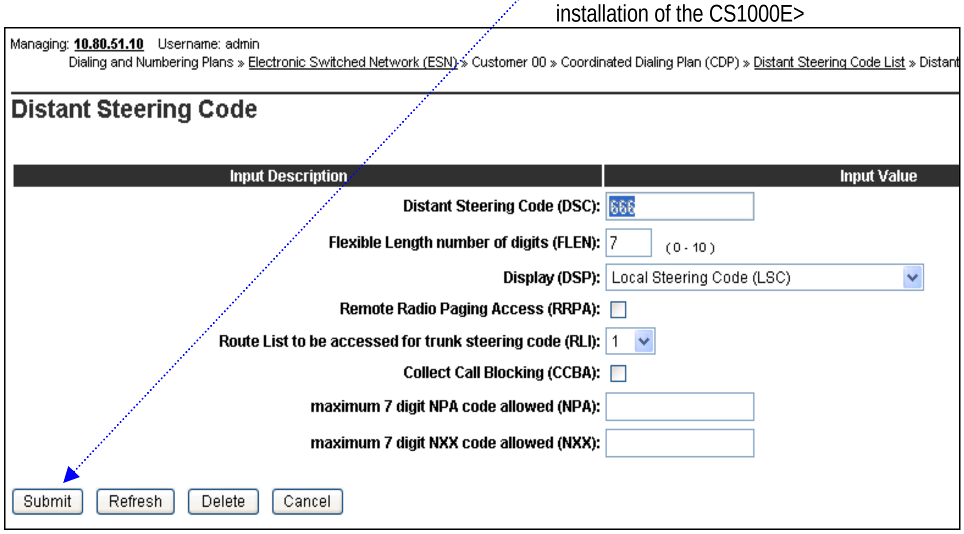


- The **Distant Steering Code** screen should now appear with **666** in the field adjacent **Distant Steering Code (DSC)**.
- Enter the following values and then click on **Submit**:

Flexible Length Number of digits (FLEN): 7 <*Maximum length of number starting with 666*>

Display (DSP): Local Steering Code (LSC)

Route List accessed for trunk steering code (RLI): 1 <this is the Route List built between the CS1000E Call Server and Signaling Server. In our example, RLI 1 was configured during the installation of the CS1000E>

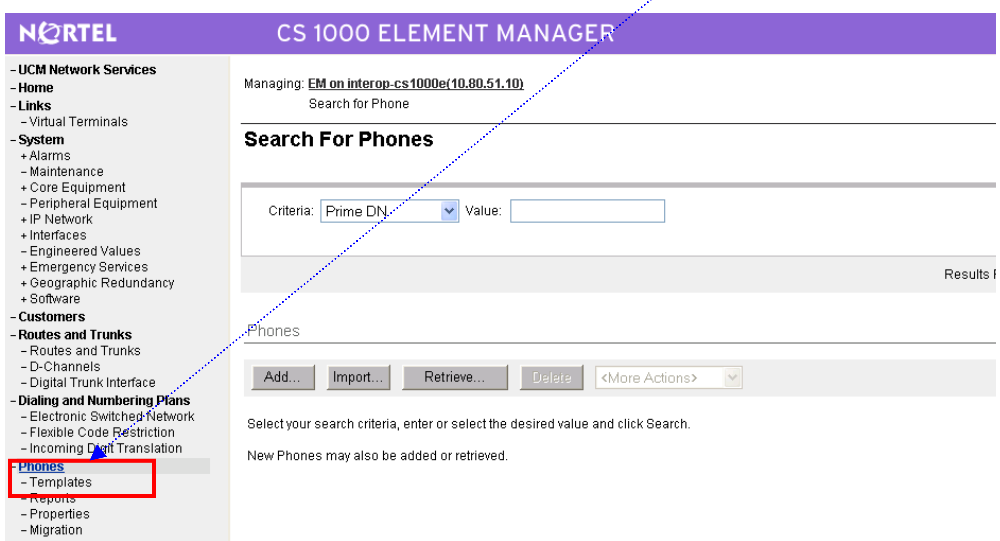


- continued on next page -

5.2 SUBSCRIBER ADMINISTRATION

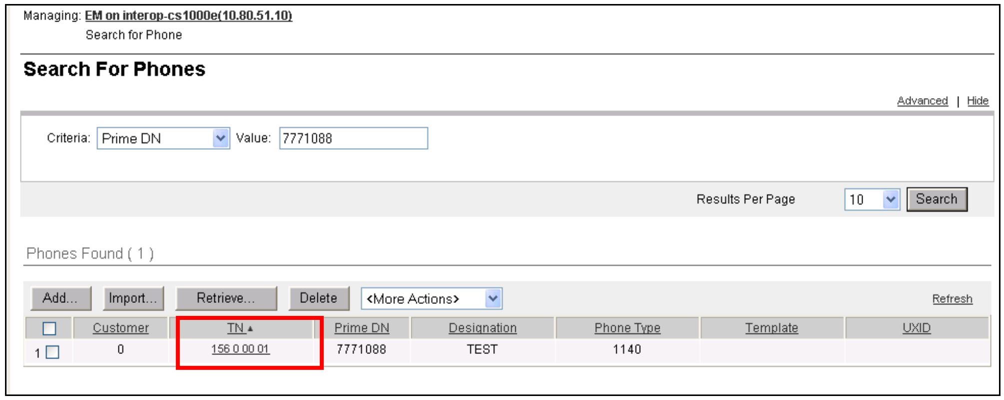
Subscriber administration includes:

- Configure Phones to Cover to the MM 'pilot' extension
- Every MM subscriber's station/phone on the CS1000E will need to be configured with the 'pilot' number of 6665001 so that **busy** and **no-answer** calls will route to MM. Although there are a number of tools that for telephone administration on the CS1000E (*i.e, Element Manager, Telephony Manager, and the command-line overlay terminal*) for this document we will continue to use Element Manager to administer the telephones.
- From the left-pane of Element Manager select **Phones**. You will now see the following screen.



- continued on next page -

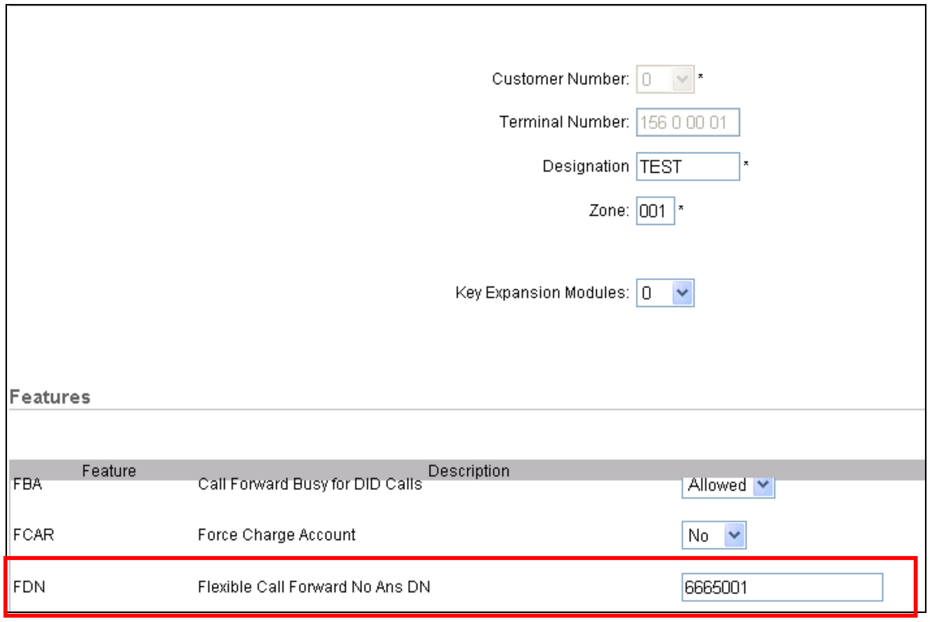
- For each existing subscriber's station, enter the Primary DN (Dialed Number) in the **Value** field and then select Search. The following screen appears. Select the value under the column **TN** to begin editing the station.

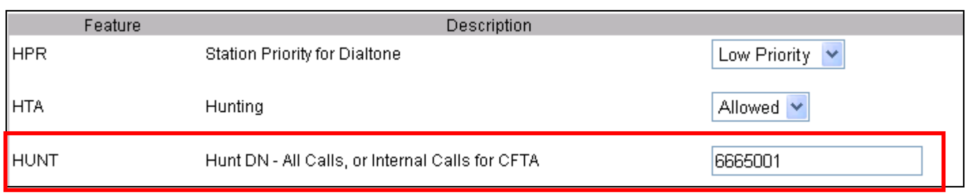


- In order for the station 7771088 to cover to Modular Messaging on **busy** and **no-answer** calls, the station must be configured with the MM pilot number. This is done using the following two Features (also referred to as Class of Service):
  - Flexible Call Forward No answer DN (FDN)
  - Hunt DN - All Calls, or Internal Calls for CFTA (HUNT)
- Once you have selected the station's TN *(A TN is the Terminal Number, or basically the port number on the switch. i.e., 156 0 00 01 is 156=Loop 0=Shelf 00=Card 01=Unit)* as described in Step 2 above, the following screen appears.

- continued on next page -

- In the **Feature**s section, scroll down the list of features and find the two previously mentioned, (FDN and HUNT).
- Enter **6665001** in each as shown below

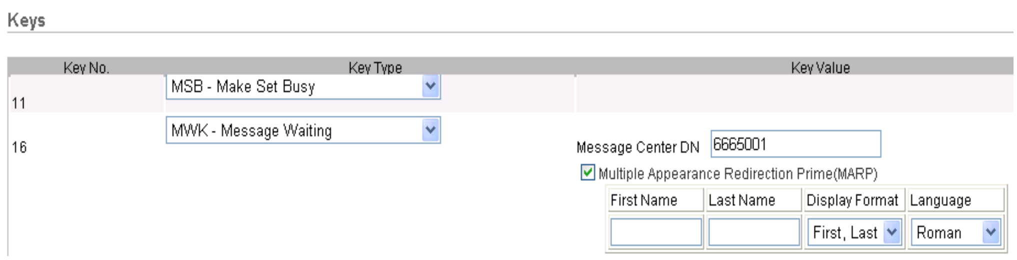




- continued on next page -

- It is also necessary to program a **MWK-Messaging** button on each station. This is found in the **Keys** section of the Phone Details screen.
- Scroll down in the **Keys** section and select an unused button. Select the following values from the pull down choices:

Key Type:	MWK – Message Waiting
Message Center DN:	6665001 <this is *the MM Pilot number*>.
MARP checkbox:	Check the box.



- Once all these changes have been completed, select **Save** (not shown) to save your changes.

- continued on next page -

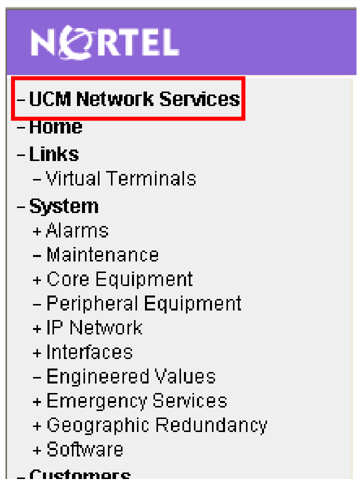
5.3 CONFIGURING NRS TO ROUTE CALLS TO MM

The last step to complete to route calls to MM (via Session Manager) is to configure a '**route**' on the Network Routing Service (NRS). The NRS can also be referred to as the SIP Proxy Server (SPS).

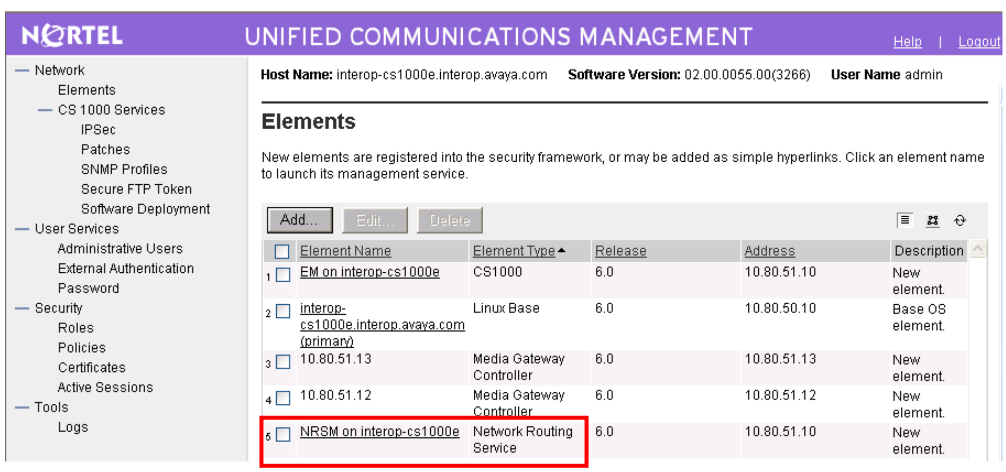
The test system used to create this configuration note, administered the NRS as a SIP Proxy to the CS1000 Signaling Server.

(For further information on configuring the CS1000 Signaling Server and NRS please refer to *Network Routing Service Fundamentals. Release 6.0, rev. 01.03. Nortel Doc # NN43001-130).*

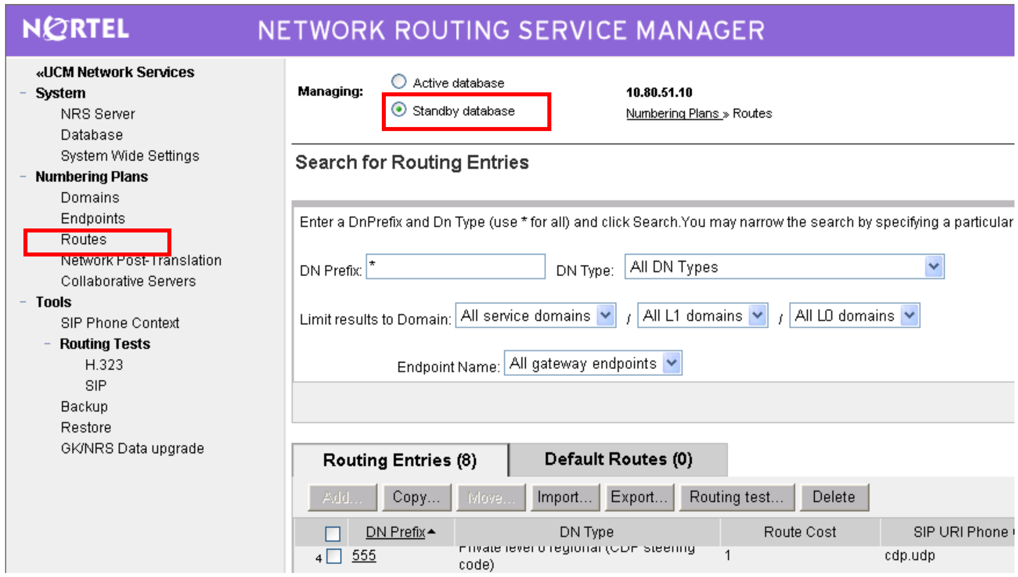
- To administer NRS, select **UCM Network Services** from the left-pane as shown below.



- Next select the element of type **Network Routing Service**:

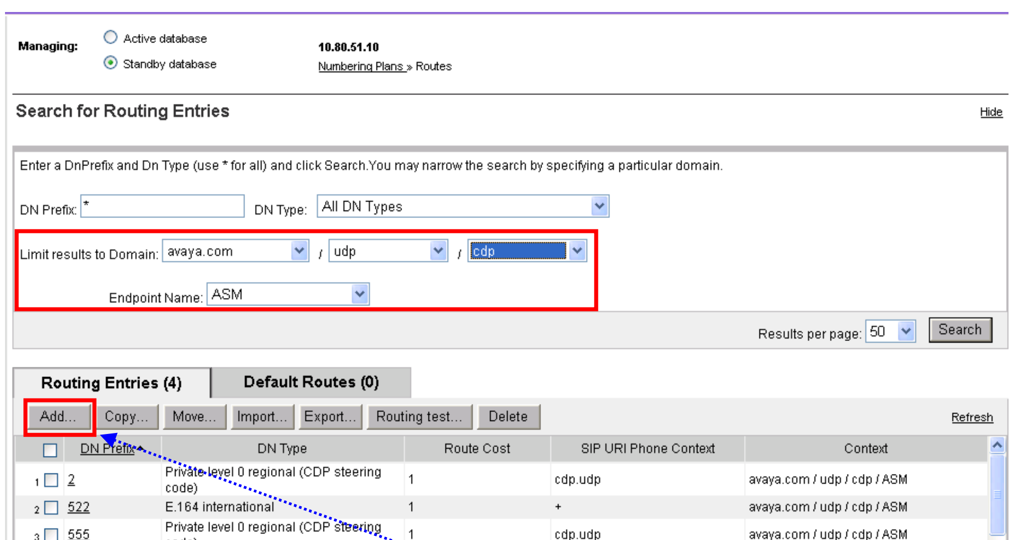


- Select Standby Database and Routes as shown below.



- To add a route for **666xxxx,** you will need to first select the appropriate context and endpoint. In our example below, the service Domain is **avaya.com**, **Level 1 (UDP)** domain is named **UDP** and **Level 0 (CDP)** domain is named **CDP**.

  The endpoint is the Avaya Aura Session Manager (**ASM**).



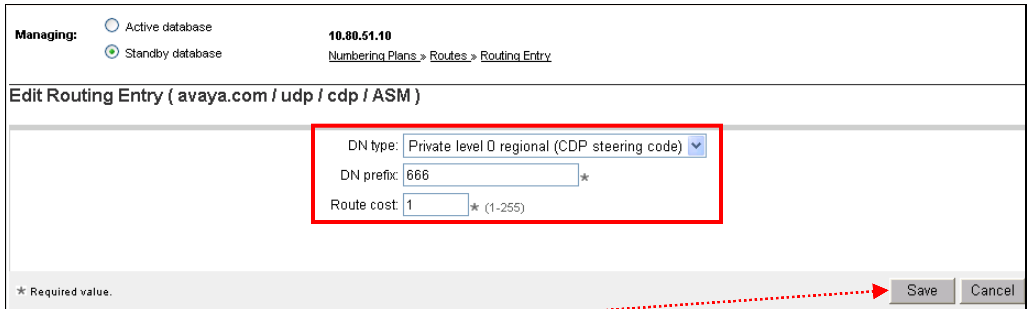
- Once these are selected as shown below, the **Add** button becomes available, now click on **Add** to add this entry.

- Enter the following values for the 666xxxx route:

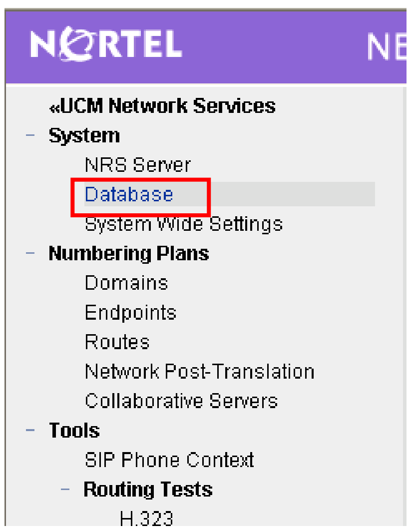
  DN Type: Private level 0 regional (CDP Steering Code)

  DN Prefix: 666 <The dialed digits or string>.

  Route Cost: 1 <enter the appropriate route cost if known>

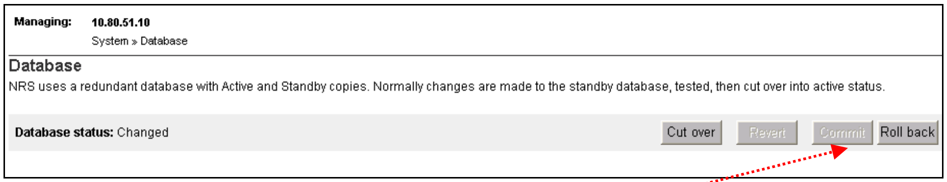


- Click **Save** when complete to save your entries.
- Your changes need to be saved in the NRS database to take effect. On the left side select **Database.**



- continued on next page -

At this point you should see the following screen.



Now click on **Cut Over**.

Then click on **Commit** (Commit should no longer be dimmed).

- continued on next page -

> **PLEASE NOTE**
>
> The screens and information provided in this section serve only as examples.
>
> The information you enter in each screen when administering your own system may be different that shown here.

5.4 CONFIGURING THE AVAYA AURA SESSION MANAGER

This section provides the procedures for adding Modular Messaging as a SIP Entity to the Avaya Aura Session Manager.

For further information on Avaya Aura Session Manager, please see *Administering Avaya Aura™ Session Manager*, Doc # 03-603324, Issue 2

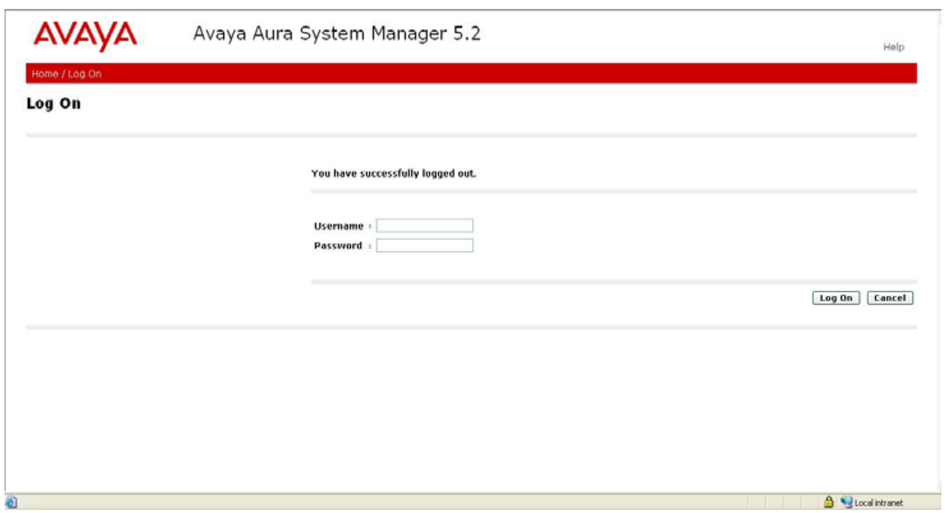
Steps:

- Log in to Avaya Aura™ Session Manager
- Administer MM as a SIP Entity
- Administer Entity Link
- Administer Time Ranges
- Administer Routing Policies
- Administer Dial Patterns
- Administer Regular Expression

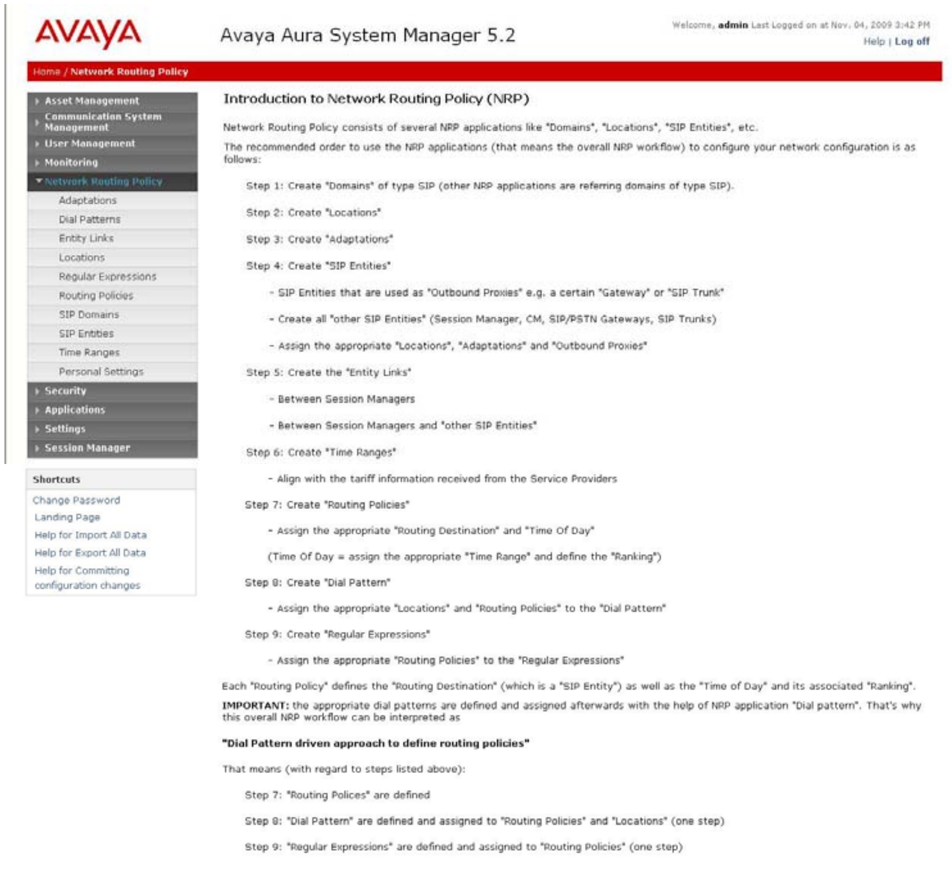
5.4.1 LOG IN TO AVAYA AURA™ SESSION MANAGER

Log into your Avaya Aura™ System Manager screen using IE or another Web Browser.

Note: You will need the IP address of the server, and a username and password



- Select **Network Routing Policy** from the left panel. You will see an Introduction to Network Routing Policy (NRP) in the right panel. This is the recommended order to use/configure NRP.

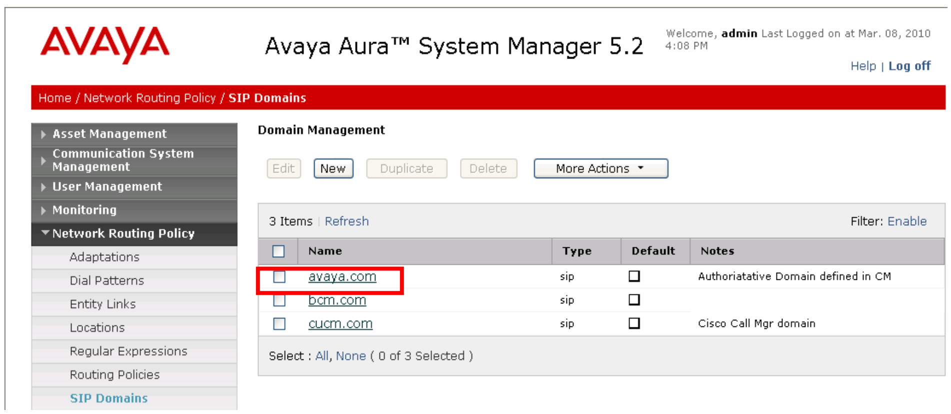


- **STEP 1: CREATE SIP DOMAIN**

Add the Authoritative SIP domain by selecting **SIP Domains** in the left panel and then clicking the **New** button (not shown) to create a new SIP domain entry.
You will need to complete the following options:

Name:	The Authoritative domain name. For example, **avaya.com**
Notes:	Optional description for the domain. (Sometimes it is best to add notes to help other administrators in your absence)

Click on **Commit** to save changes. You can verify if the domain was created by reviewing the information as shown in our example screen below.



Note: Since our example network does not interact with any foreign domains, no additional entries to SIP Domains is needed.

- ## STEP 2: CREATE LOCATIONS

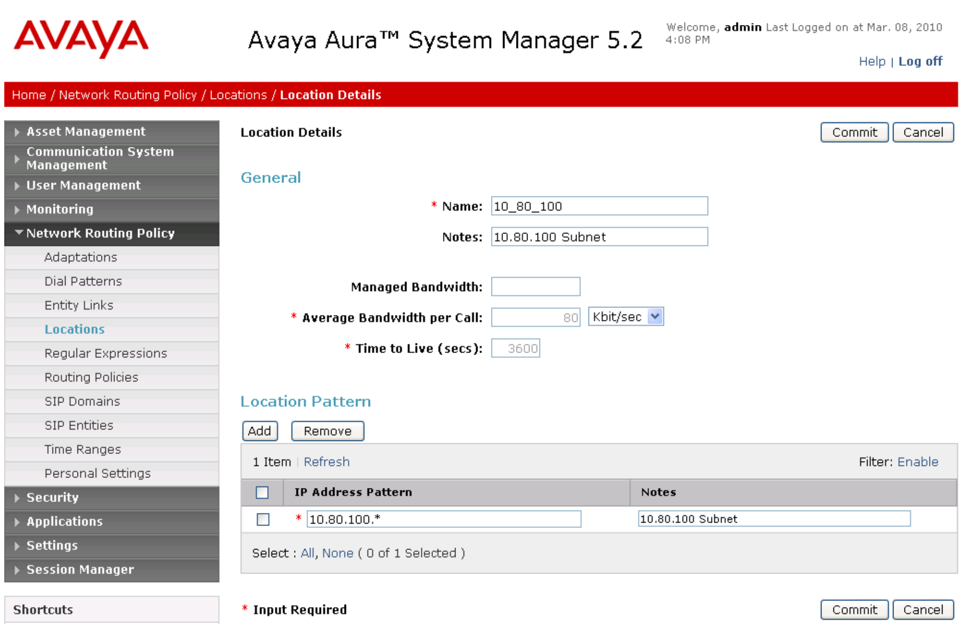
Locations in Session Manager are created to assist with call routing and to measure, monitor, and limit bandwidth usage among different locations. This is optional but recommended parameter to configure.

Locations are defined by an IP address or address pattern. The Locations screen may contain one or several IP addresses. Each SIP entity has an associated IP address.

Depending on the physical and geographic location of each SIP entity, some of the SIP Entities may be grouped into a single location. For example, if there are two Communication Managers located in Denver, they may form one location named Denver.

In our example configuration, our Modular Messaging server is in the **10.80.100.x/24** subnet. To add this subnet as a ***Location*** you would select **Locations** in the NRP. Then click **New**. The screen below will appear. Enter the following information:

Name:	Descriptive name for the Location
Notes:	Additional noted to further describe the location
Managed BW:	Enter a value (**optional**) that Session Manager will use to limit to entities in this location
Avg BW per Call:	Enter the amount that Session Manager should use on a per call basis in order to calculate total bandwidth usage.
Time to Live (secs):	default (change only if necessary)
Location Pattern:	Enter an IP address pattern (10.80.100.*), or host address, for entities that comprise this location. Multiple subnets or hosts can be defined under a single location.



- ## STEP 3: CREATE ADAPTATIONS (IF USED)

Note: Our example configuration has no Adaptation; all entries for Adaptations where therefore left as default.

- ## STEP 4: CREATE SIP ENTITIES

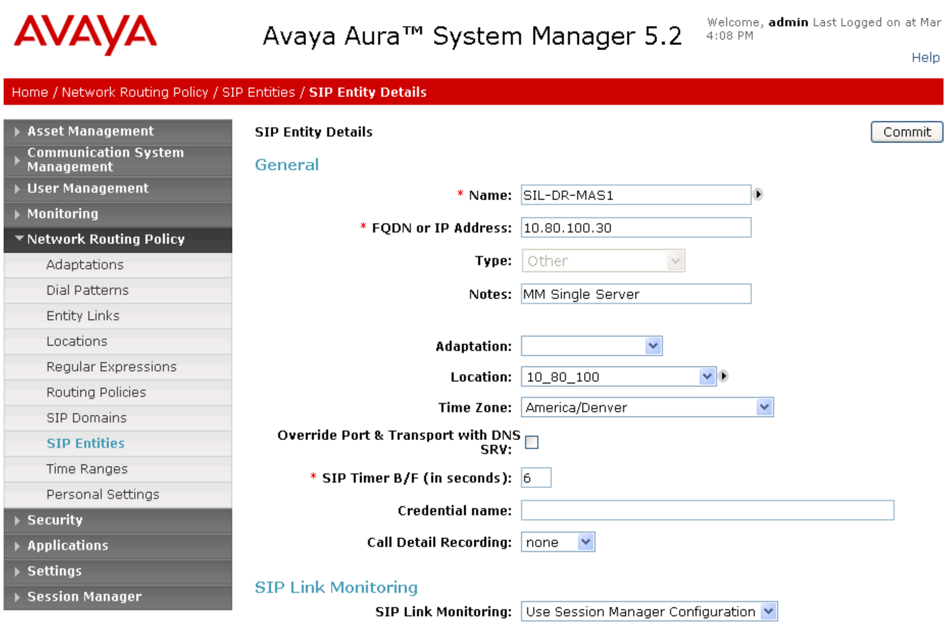
Create a SIP Entity for MM. A SIP Entities is a SIP-based telephony system that uses a SIP Trunk.
Select **SIP Entities** in the left panel, then click on the **New** button (not shown). The screen below will appear. You will then enter the following for each SIP Entity, or in this case MM.

GENERAL

Name:	Descriptive name for the SIP Entity
Name:	An informative name (e.g., SIL-DR-MAS1)
FQDN or IP Address:	IP address or hostname of the **MAS** server in the MM solution.
Location (optional):	The location name used in Step 2
Type:	**Other**. (Choices are **Session Manager, CM, or Other** for anything else such as our CS1000E and Modular Messaging)
Time Zone:	Time zone for this location

SIP Link Monitoring

SIP Link Monitoring:	Leave as default, shown below



- **STEP 5: CREATE ENTITY LINKS**

The SIP trunk between a Session Manager and a telephony/messaging system is defined by an Entity Link.

To add an Entity Link, select **Entity Links** on the left panel menu and click on the **New** button (not shown). Fill in the following fields in the new row that is displayed.

Name:	Descriptive name for the Entity Link
SIP Entity 1:	Select the Session Manager you will use
Protocol:	Transport protocol to be used to send SIP requests. (See Note on Protocol in sidebar)
Port:	Port number on MM that sends SIP requests
SIP Entity 2:	The other SIP Entity for this link (SIL-DR-MAS1)
Port:	Port number on MM that receives SIP requests
Trusted:	Trusted system (Yes if checked)
Notes:	Optional description for the Entity Link

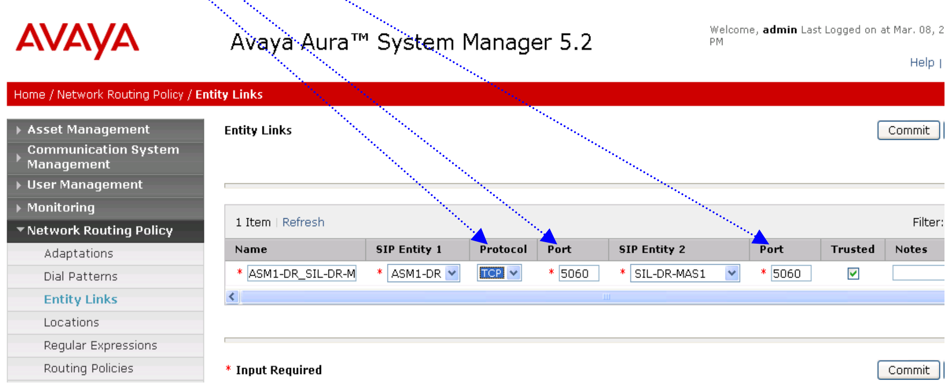
Note on Protocol:

Modular Messaging supports both TCP (unencrypted SIP signaling) and TLS (encrypted SIP signaling

For TCP MM uses port 5060.

For TLS MM uses port 5061.

Once all your information is entered, click on **Commit** to save changes.



- **NOTE:** The screen above serves only as an example. Your entity links and other information may be different than shown above.

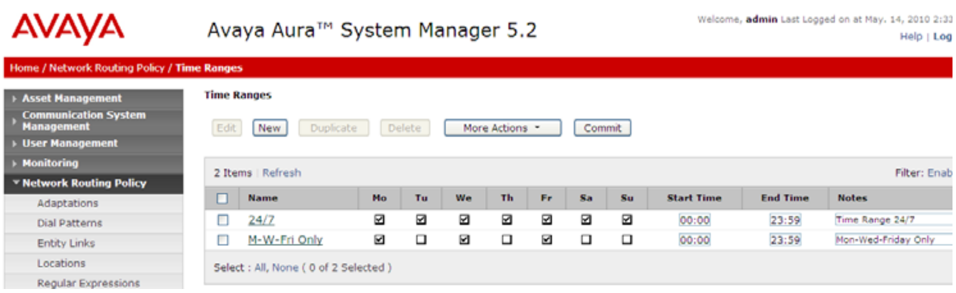
STEP 6: CREATE TIME RANGES

Time Ranges defined here are used to determine when the Routing Policies (Step 7) are active.

Session Manager uses a default time range of 24/7. To add another time range, select **Time Ranges** in the left panel, then click **New** on the right.

Enter the following information:

Name:	Descriptive name for the Time Range
Mo Tu We … Su:	Check the box under each day of the week included in the Time Range
Start Time	Start time. *This is a 24-hour clock, so our example of* ***00:00*** *for start of day is 12:00AM*
End Time	End time. *This is a 24-hour clock, so our example of* ***23:59*** *end of day is 11:59PM*
Notes:	Optional description for the Time Range



- **NOTE:** The screen above serves only as an example. Your entity links and other information may be different than shown above.

STEP 6: CREATE ROUTING POLICIES

Routing policies direct how calls will be routed to a system. A routing policy must be added for calls destined for Modular Messaging. In this scenario the pilot number to MM from the CS1000E is 6665001.

Select **Routing Policies** in the left panel, then click on **New** (not shown). The screen below will appear. Enter the following:

General

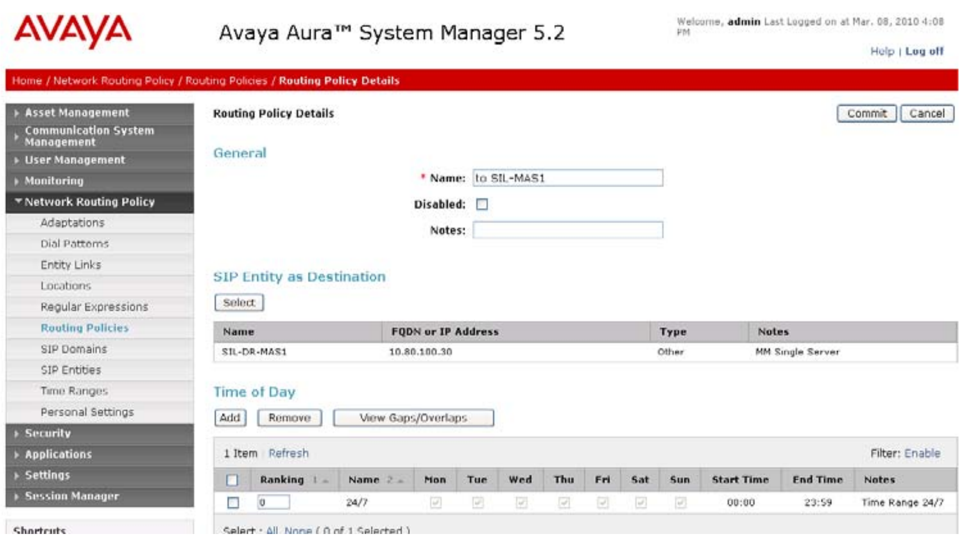
Name:	Descriptive name for the Routing Policies
Notes:	Optional description for the Routing Policy

SIP Entity as Destination

Click **Select**, then chose the SIP entity that you will apply this routing policy to.

Time of Day

Click **Add**, and then select a time range configured in Step 5



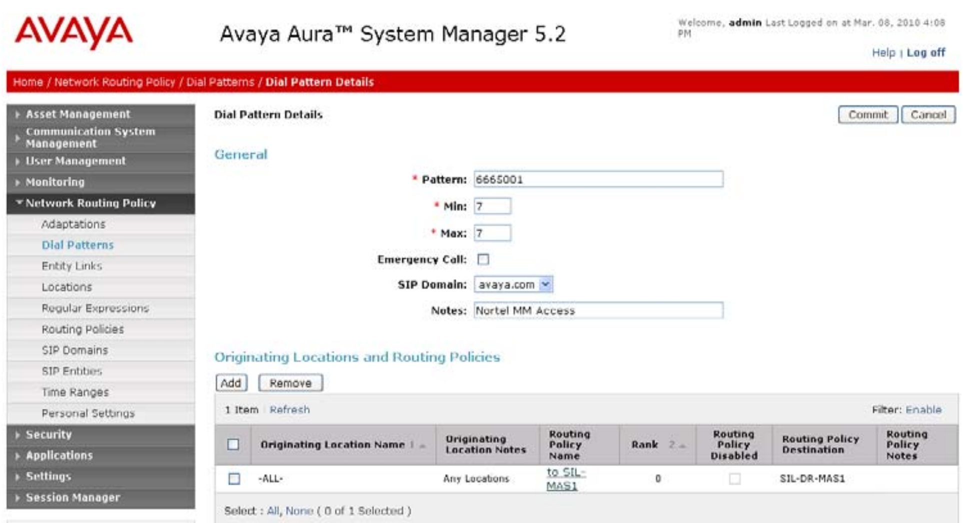
- <u>**NOTE:**</u> The screen above serves only as an example. Your entity links and other information may be different than shown above.

STEP 8: CREATE DIAL PATTERNS

Create a Dial Pattern(s) that will use the Routing Policy you created in Step 6. Select **Dial Patterns** on the left panel menu and then click on the **New** button (not shown).

General

Pattern:	Dialed number (this is the MM Pilot #)
Min	Minimum length of dialed number
Max	Maximum length of dialed number
SIP Domain	Usually the Authoritative domain. i.e., **avaya.com**
Notes	Optional description for this Dial Pattern

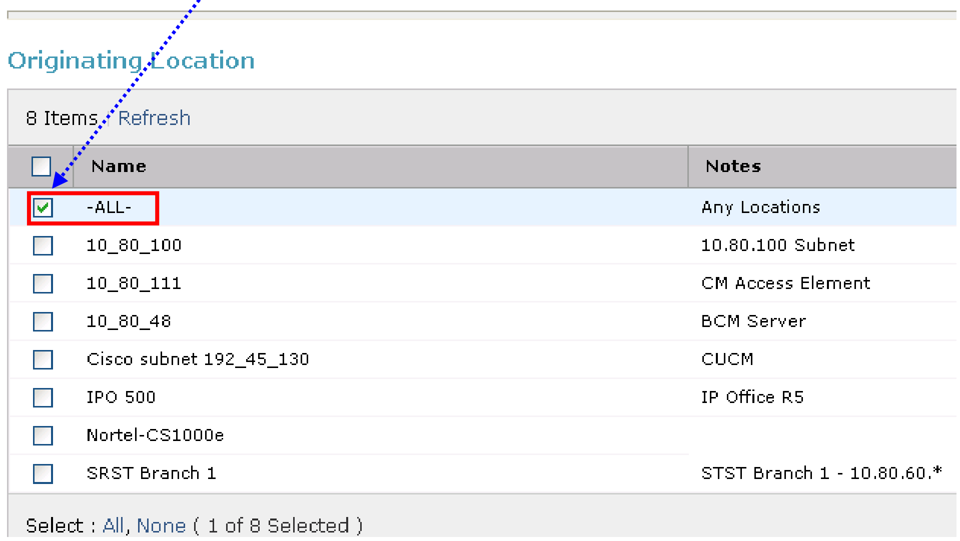


Originating Locations and Routing Policies

Select **Add**.

-continued on next page -

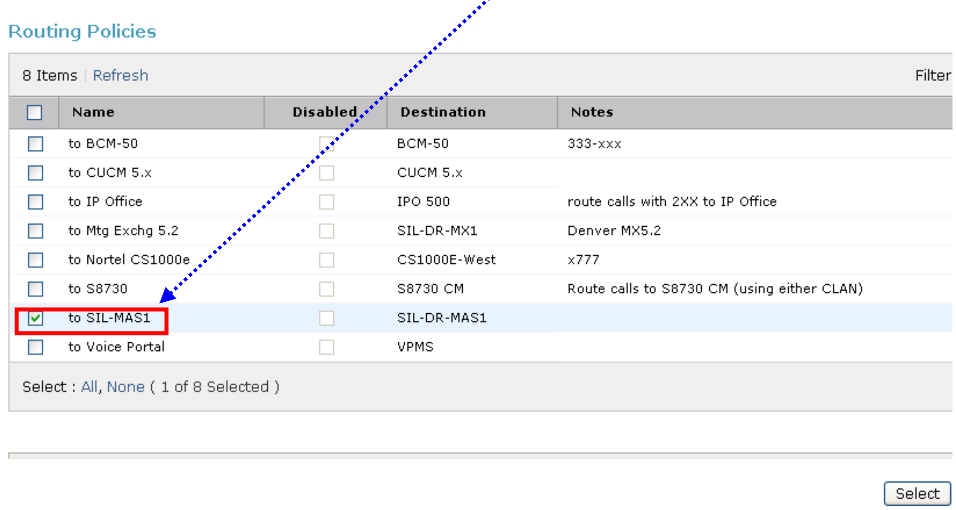
Select (check) **- ALL -** under **Originating Location** (shown in screen below)



☐	Name	Notes
☑	-ALL-	Any Locations
☐	10_80_100	10.80.100 Subnet
☐	10_80_111	CM Access Element
☐	10_80_48	BCM Server
☐	Cisco subnet 192_45_130	CUCM
☐	IPO 500	IP Office R5
☐	Nortel-CS1000e	
☐	SRST Branch 1	STST Branch 1 - 10.80.60.*

Scroll down and under **Routing Policies** select (check) the Routing Policy Name as defined in Step 6.

Note: In our example configuration we used "**to_SIL-MAS1**" as the name for our Routing Policy. Your Routing Policies names may be different.

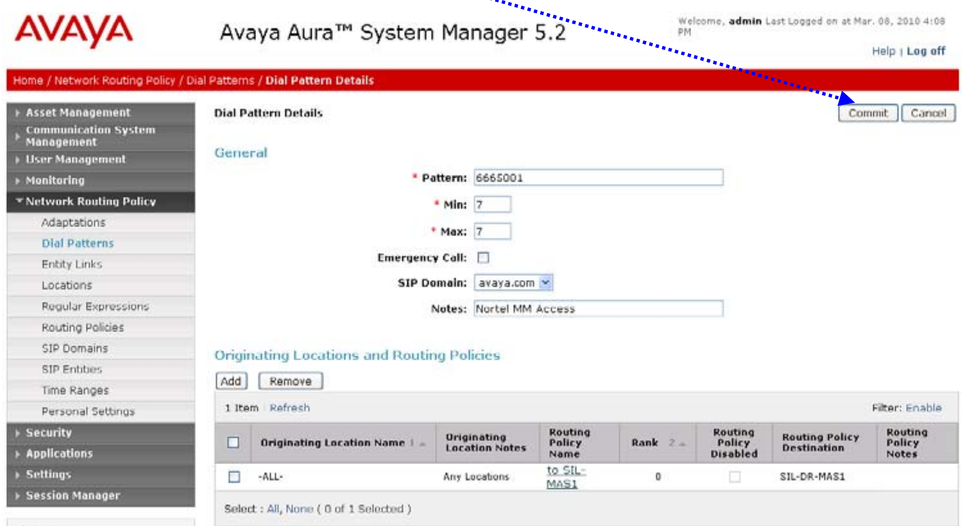


☐	Name	Disabled	Destination	Notes
☐	to BCM-50	☐	BCM-50	333-xxx
☐	to CUCM 5.x	☐	CUCM 5.x	
☐	to IP Office	☐	IPO 500	route calls with 2XX to IP Office
☐	to Mtg Exchg 5.2	☐	SIL-DR-MX1	Denver MX5.2
☐	to Nortel CS1000e	☐	CS1000E-West	x777
☐	to S8730	☐	S8730 CM	Route calls to S8730 CM (using either CLAN)
☑	to SIL-MAS1	☐	SIL-DR-MAS1	
☐	to Voice Portal	☐	VPMS	

Click **Select** button to confirm your selected options.

You should be returned to the Dial Pattern screen as shown below. This is the same screen you first used in STEP 8: CREATE DIAL PATTERNS.

Click on **Commit** to save your changes.



Step 9: Create "Regular Expressions"

Regular Expressions are defined assign to Routing Policies. The Routing policies can function without a regular expression. Regular expressions allow routing of Alpha Numeric addressed SIP Messages.

Note: For this integration we did not create any Regular Expressions, they were left as default.

- continued on next page -

6.0 Configuring the Messaging Application Server

Configuring the Message Application Server

Configuring the MAS platform for proper PBX integration requires configuring several menus accessed within the **Voice Mail System Configuration** application, and a certified MM engineer. This must be performed for each MAS Voice Mail Domain (VMD).

- Access the **Voice Mail System Configuration** application from the MAS program group. Expand all fields so all-applicable options are visible.

Ensure the new PBX is added as instructed by the Modular Messaging Installation guide. The new PBX should be:
Avaya CM (IP SIP)

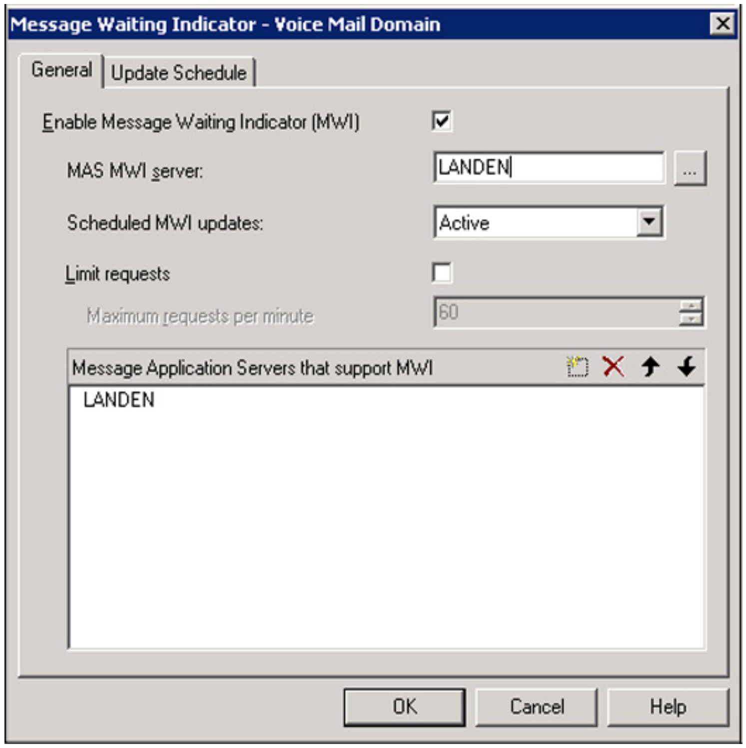
1. Select **Voice Mail Domains**
2. Expand **PBXs**
3. Select (double click) the **Avaya CM (IP SIP)**
4. Access the **Transfer/Outcall** tab
5. **Transfer Mode** = Full

NOTE: Administer transfers as FULL (Supervised transfer) to prevent callers from being disconnected when calls are re-routed back to the Message Server. Transfers should only be administered as blind or partial when the transferred to numbers will not be re-routed to the Message Server.

- continued on next page –

- The following programming is a continuation from the Modular Messaging (MAS section) Installation Guide:

▪ Next access the **Message Waiting Indicator (MWI)** tab



Note: **When using Operational History Viewer, MWI on/off commands will appear to be sent on Port 0.**

1. **Enable Message Waiting Indicator (MWI)** = Enable by checking the box
2. **MAS MWI Server** = Enter the name of the MWI server created during the installation procedure.
3. **Scheduled MWI updates: Active or Inactive** = Configure as per customer requirements.*
4. **Limit requests** = Leave Unchecked
5. **Maximum Requests per Minute** = <grayed out>
6. **Message Application Servers that Support MWI** = This box should contain a list of MAS servers capable of placing MWI requests.
7. Select **OK** to save changes

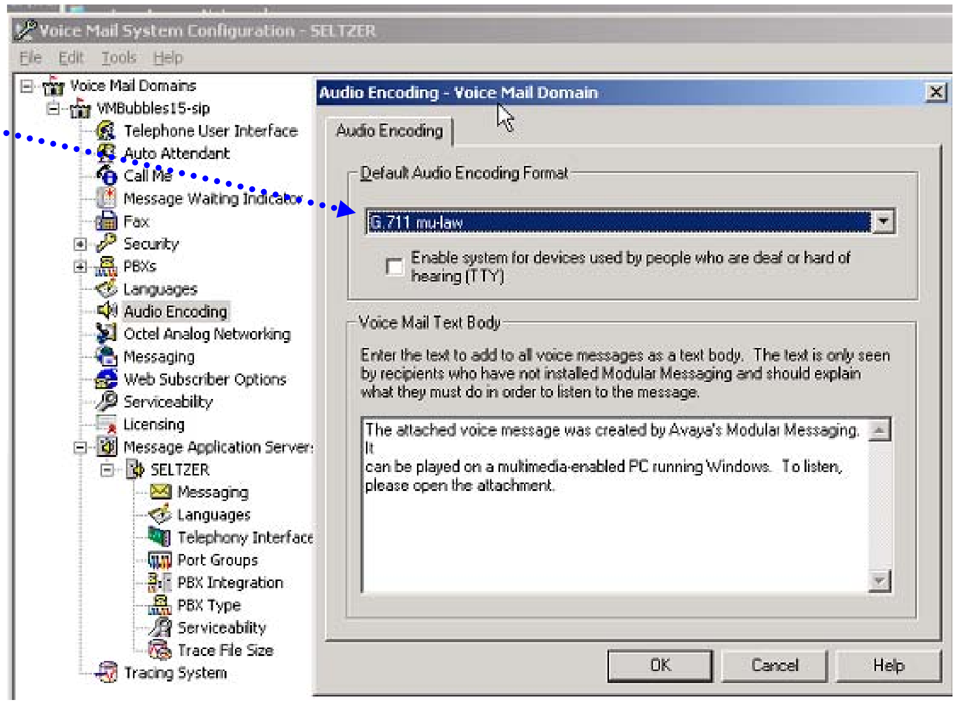
*Note: The Scheduled MWI updates parameter is only available on MM 3.x

Note 2: The MAS will prompt to restart the services. Wait until instructed below.

- Next double click to access **Audio Encoding** *(see below)*

1. Select the pull down for **Default Audio Encoding Format**
2. Chose **GSM or G.711** mu-law or a-law depending on your storage needs. (GSM is the default encoding method for MM)

Note: The **Default Audio Code Format** you select determines the encoding for the messages stored. This setting may be different than the codec you defined in the CM configuration for the *transport* of audio data. Avaya recommends use of G.711 for superior quality compared to GSM and/or if you need to support TTY. GSM encoding will yield greater message storage but at reduced audio quality and no support for TTY.



- Next double click to access the **Telephony Interface (IP SIP)**

1. **Playback Volume** = 2 (Default)
2. **Number of Ports** = **20** (if MAS is *S3400*)*****
   -or- **48** (if MAS is S3500)
   -or- **96** (if MAS is S8730/S8800).

Note: The Ports are enabled by default. The MAS service must be restarted to allow port enabling/disabling.

3. Select **OK** to save changes
4. Restart the MAS Service and then continue with the step below.

* **Important**: S3400 is not supported with MM 5.x

Special note for MM 5.x: Administering the **Corporate IP Address** is now done automatically at the system level.

The value you enter here should match the packet size sent by the PBX.

Only a packet size of 20 msecs is currently supported.

See Consideration 8.20

IMPORTANT

QOS values may not take effect unless a specific Registry Key is present. Check to see if the Registry Key **DisableUserTOSSetting** is in the following location:

HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\

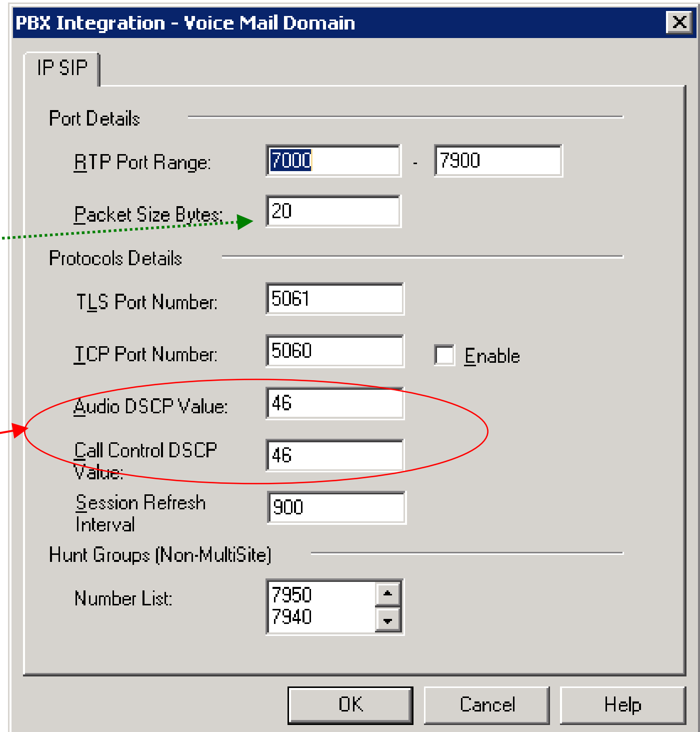
If the registry key is not there, add it with a DWord value of 0.

Then Restart the MAS. QOS values will now be in effect.
This issue will be corrected in MM 5.2SP8

The DSCP value of 46 denotes the packet(s) as "Expedited Forwarding." What this means is that it has the highest priority when it is received and forwarded by each node in a network.

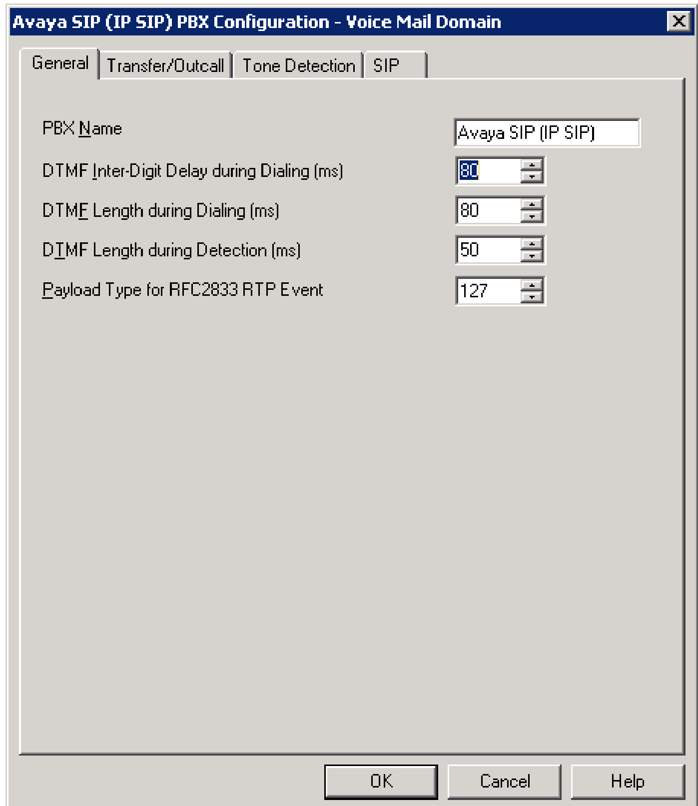
- Next double click on **PBX Integration** to see the following screen. This is the IP connectivity information between the PBX and MAS.

Note: The following screens show additional settings and values that were introduced beginning with MM 5.2 SP5.



1. **RTP Port Range** – default is 7000 – 7900
2. **Packet Size** – should match the packet size sent by the PBX
3. **TLS Port Number - 5061**
4. **TCP Port Number – 5060 (Enable** sets TCP listening port to value enter in adjacent field [5060]. Note: Most configurations will use TLS; leave this disabled. Typically TCP will be use by certified Avaya technicians)
5. **Audio DSCP Value** – 46 (default value)
6. **Call Control DSCP Value** – 46 (default value)
7. **Session Refresh Interval** – 900 (value is in seconds and defines duration before SIP session is refreshed (using INVITE) by MM. Value is used only for outgoing calls from MM.
8. **Hunt Group [Non-Multisite]** - Enter one or more hunt group numbers. These number(s) are used to reach/dial the MAS (pilot #). This list is also used to determine whether an outcall to the personal operator goes to coverage. Required for the Zero-Out feature on non-multisite MM systems.
9. Select **OK** to save changes

- Next expand **PBXs** then double-click on the PBX you want to configure. The screen below should appear. Access the **General** tab.



1. **PBX Name** - Default is **Avaya SIP (IP SIP)**. *(The default name is acceptable to use when administering a single site, but for Multi-Site use unique names to distinguish between PBXs in the list when they appear in the VMSC)*
2. **DTMF Inter-Digit Delay during Dialing (ms)** – 80 *(leave as default of 80)*
3. **DTMF Length during Dialing (ms)** – 80 *(leave as default of 80)*
4. **DTMF Length during Detection (ms)** – 50 *(leave as default of 50)*
5. **Payload Type for RFC2833 RTP Event** – 127 *(leave as default of 127)*
6. Select **OK** to save changes

- continued on next page –

- Next access the **Transfer/Outcall** tab.

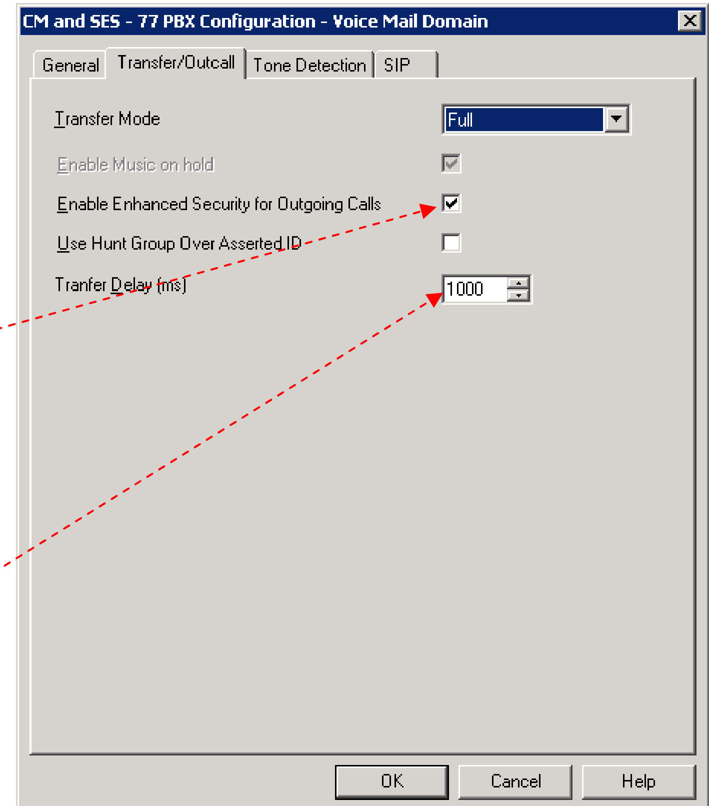
FIND ME Failures

Some transfers, particularly when the initial call is from an external number, may fail when this feature is enabled (checked)

Clearing (uncheck) this option will allow the transfer to proceed.

***Transfer Delay**

When shuffling is enabled, SIP messages for shuffling and transfer may collide forcing transfer messages to be resent after a short delay. This delay value prevents the potential of multiple collisions resulting in a long delay.



1. **Transfer Mode** - Full
2. **Enable Music on Hold DTMF Inter-Digit Delay during Dialing (ms)** – *This option is applicable only when the Transfer Mode selected is Blind. For other transfer modes, music on hold is always played.*
3. **Enable Enhanced Security for Outgoing Calls –** *when checked (enabled) the Avaya CM does an authorization check before making an outcall.*
4. **Use Hunt Group Over Asserted ID** – *when checked the value in the Hunt Group field (configured under Sites for multisite or under PBX Integration for non-Multisite) will be used instead of the value in the "Asserted ID" field for outcalls.*
5. **Transfer Delay (ms)*** - *When shuffling is enabled, this value allows 1 second (1000 msecs) for shuffling to complete and the talk path established.*
6. Select **OK** to save changes

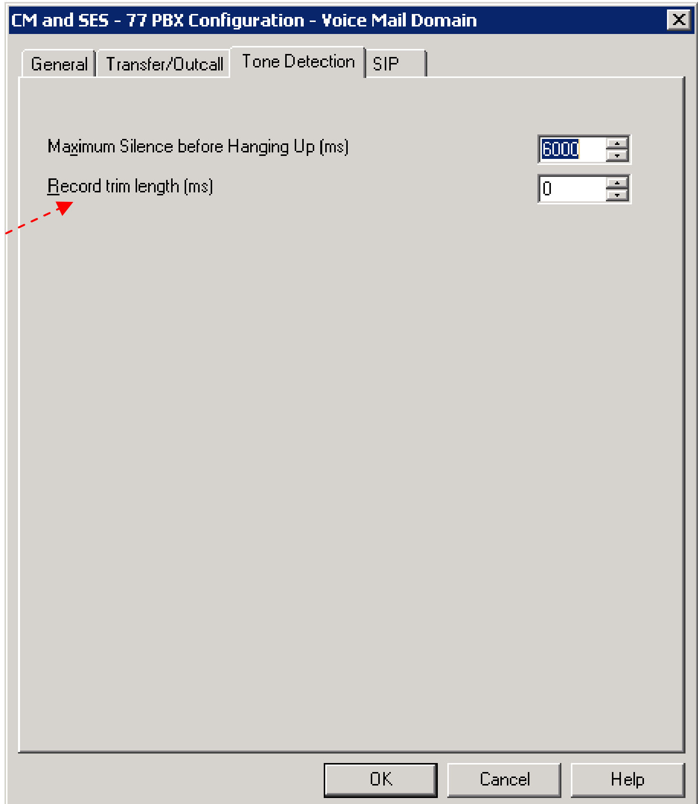
- continued on next page –

- Next access the **Tone Detection** tab.

***Recorded Trim Length**

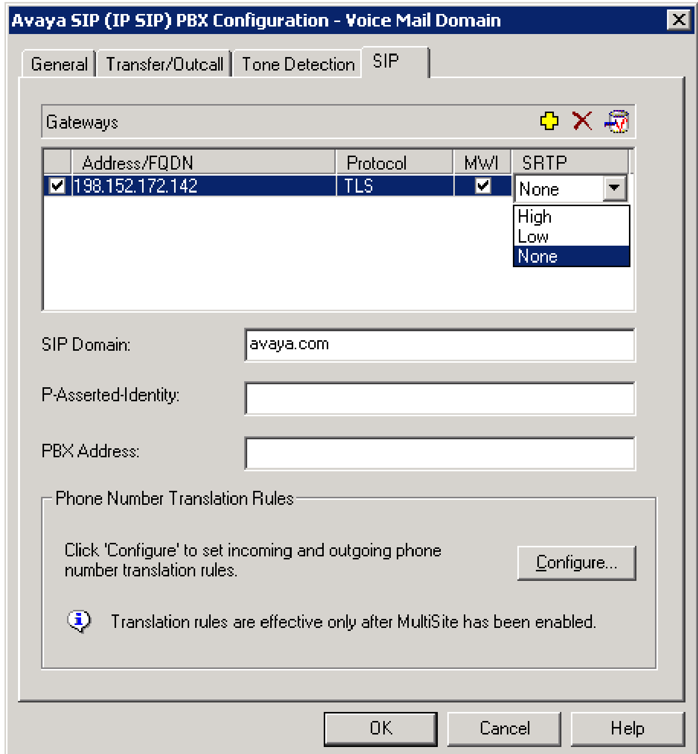
When leaving a message, callers can end the recording by pressing a key on the telephone key pad. However, in some circumstances a small portion of the tone that is heard when the DTMF key being pressed is recorded in the message.

This value can be used to remove this recorded tone by trimming a small amount from the end of the message.



1. **Maximum Silence before Hanging Up (ms)** – 6000
2. **Recorded trim length* (ms)** – 0
3. Select **OK** to save changes

- Now access the **SIP** tab



1. **Address/FQDN** - Select the checkbox and enter the IP Address or Domain Name of the PBX.
2. **Protocol -** Enter either TCP or TLS, depending on which protocol the gateway uses to communicate with the MAS. The default is TLS. Avaya recommends TLS because it is secure, but the gateway must be configured to use it.
3. **MWI -** Select to enable the Message Waiting Indicator feature for the PBX. The checkbox is checked by default.
4. **SRTP**[1] - Specifies the security level for communication between the gateway and the PBX. Double-click the entry and select **High**, **Low**, or **None**. Below are the corresponding Avaya CM encryption types:

SRTP **High** = 1-srtp-aescm128-hmac80 on the CM SRTP **Low** = 2-srtp-aescm128-hmac32 on the CM

5. **SIP Domain** = domain assigned in IP Network Region on PBX
6. **P-Asserted Identity**[2] –This should be the main number for MM. This extension number is used by the PBX to identify and grant appropriate permissions to Modular Messaging.
7. **PBX Address –** Enter the PBX IP address.

8. Select **OK** to save changes

[1] SRTP is a feature supported in MM 5.x
[2] This field is optional and is only applicable if your PBX is an Avaya CM.

After making these changes, return to “Configuring the voicemail system” within the Message Server Installation guide. Ensure you RESTART the Message Application Server services to apply these changes.

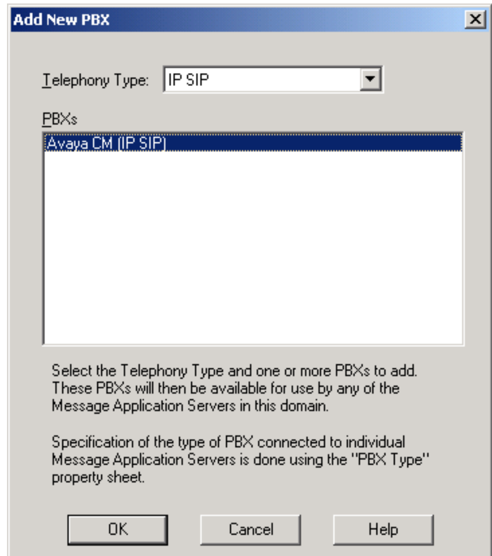
- continued on next page –

Important notes regarding this integration

8.0 CONSIDERATIONS / ALTERNATIVES

8.1 When converting from one integration type (i.e., H.323) to SIP, perform the following steps using VMSC.

Step 1. Right click the PBXs item under the voicemail domain and click on Add a New PBX Type to open the following form. Select the Telephony Type of IP SIP and highlight Avaya CM (IP SIP) then select OK.



Step 2. For each MAS in VMSC right click the MAS and select Run the Telephony Configuration Wizard.

Step 3. Run the wizard and configure the SIP settings as per Section 6.

Step 4. For each MAS open the Port Groups item and verify that there are no MWI Port Groups defined and that the number of ports in the Default Group equals the maximum allowed for the hardware.

Step 5. Restart MASs when complete.

8.2 Known Issues:

a. **Call diversion interoperability between QSIG and SIP (QSIG/SIP Interworking) is not supported in the CS1000.**

b. **ISSUE**: In the Event Viewer "An error occurred logging in to the MSS server to provide the MAS heartbeat (error cod:1)"

ISSUE: After a Voice Message is left for a user the MWI does not appear.

Solution: If you are using an MSS, follow instructions as noted under "***Verifying network adapters and bindings***" in the "Modular Messaging for the Avaya Message Storage Server (MSS) Configuration – Installation and Upgrades" guide. To save time the steps are shown below. Please be advised that we have added Step 7 in the list below to ensure the necessary services are restarted.

Verifying network adapters and bindings

You must complete the following steps to verify the search order in which private and corporate LANs are ordered on an CPE MAS.

1. On Windows desktop, select **My Network Places.**
2. Right-click and select **Properties.** The system opens the **Network Connections** window.
3. From the **Advanced** menu, click **Advanced Settings.**
4. In the **Adapters and Bindings** tab, from the list of connections, ensure that the connection to the private LAN (Local Area Connection) appears above the connection to the corporate LAN (Local Area Connection 2). This is to ensure that MAS accesses private LAN before the corporate LAN.

   Note: If the **Local Area Connection** is *not* the first entry, select **Local Area Connection.** Use the up arrow key to move the item to the first position. Click **OK.**
5. Click **OK.**
6. Close all open Windows.
7. Restart the MM **Mailbox Monitor**, which in turn will restart MM **Message Waiting Indicator Server** and MM **Call** Me **Server.**

8.3 **SIP integrations may not be reliable for TTY** if the IP network is unable to support uncompressed audio with no packet loss. For this reason we currently do not support TTY with this SIP integration.

8.4 Although **G.711 is recommended as the codec type for use with MM,** to avoid potential issues with voice quality, consideration should be given to networks using other types of codecs such as G.729. For example, if the entire network is using high compression codecs, when the information is converted and passed to MM (which uses a lower compression codec, i.e., G.711, voice quality may suffer.)

Note: MM does not support G.729. Should G.729 calls terminate on MM the ports will hang and the MAS Service will need to be restarted.

P-Asserted Identity

P-Asserted Identity is administered as extension only. The optional domain name added to the extension, for example: extension@domain-name.com is not supported and cannot be administered as part of the P-Assserted Identity.

Avaya recommends using the VMSC to administer P-Asserted Identity. (*see PBX Configuration / SIP tab settings in Section 6.0*) Settings for P-Asserted Identity as administered in the VMSC will override registry key settings used for P-Asserted Identity.

8.5 **Implementing P-Asserted Identity functionality**. MM has the capability of sending a P-Asserted Identity in SIP originations which allows finer control of MM calling permissions. Persons implementing this functionality should have an in-depth understanding of communication manager toll fraud related administration. Without this implementation MM calling permissions and transfer capabilities will depend on the features and subsequent administration of PBX.

a. On each MAS that takes calls open the registry and create a new string in the key named “P-Asserted-Identity” HKEY_LOCAL_MACHINE\SOFTWARE\Octel\Geneva\Vcm_TelephonyServiceMgr\SIP Set the string value to match the administered PBX extension. MM will then use this value and the SIP domain configured in the VMSC to generate a PAI of the format extension@administeredsipdomain.com.

Alternately you can specify the extension and domain in the registry string: *extension@specifieddomain.com*. In this case MM will not use the administered SIP domain to build and send a PAI; it will use the string entry. For example, if you set the registry string value to 7925 and the VMSC is configured to use a SIP domain of avaya.com then MM will create a PAI of 7925@avaya.com. If you populate the registry string with 7925@sv.avaya.com MM will use this as the PAI regardless of the VMSC SIP domain setting.

8.6 **If your integration is set to use TLS as the transport method/link type and calls are not completing but they do complete using TCP,** then the cause is usually a license issue. Check the MAS directory:

C:\Program Files\Avaya Modular Messaging\OpenSSL\AVA

Make certain the following 3 files are present:

- certchain.crt
- certchain.key
- dh1024.pem

If any one or all of these files are not present, reload the licenses. Once complete the 3 files should be present enabling calls to complete using TLS.

8.7 **When using SRTP –** If an MM is connected to a single SESSION MANAGER that is networked to more than one PBX for voice messaging, all PBXs communicating with that SESSION MANAGER should be enabled for SRTP or loss of connectivity may occur.

8.8 **When installing a patch or Service Pack on an MAS** it is advisable to stop calls from being placed to that MAS. You can do this by busying out the SIP Messaging signaling group, just remember to release the signaling group once completed to put it back in service. Alternately, you can unplug the Ethernet cable on the back of the MAS. Once complete plug the Ethernet cable back into the MAS.

8.9 **When MM transfers a call** the calling and called parties may experience a 1 second delay before the talk path is established.

8.10 **Outcalls** will display a calling party name of “Modular Messaging.”

8.11 **P-Asserted Identity** and outcalls - If you are experiencing failed outcalls, this may be a result of changes in newer MM releases to handle P-Asserted-Identity. Please update your MM5.2 system with the latest SP. Once completed, you will need to **add the following registry key** (unless someone has already added it) and use a DWORD value of 12 decimal (0xC hexadecimal):

HKEY_LOCAL_MACHINE\SOFTWARE\Octel\Geneva\Vcm_TelephonyServiceMgr\SIP\P-Asserted-Identity-Mode

8.12 In a **multi-PBX** network certain call scenarios such as FIND ME may have the originating leg on one PBX and the terminating leg on a different PBX. If calls drop or in some cases end up with a talk path, one workaround is to have the terminating call routed to the same PBX that originated the call. If this resolves the issue, the Dial Plan and Network Routing in the network should be reviewed for possible errors and omissions.

8.13 If a called party transfers a call to another extension, the **calling party may hear dead air** and no personal greeting played. This may be caused by an intermittent issue with shuffling. The current solution is to turn off shuffling on the MM signaling group for the SIP trunk to MM. This issue was corrected in MM 5.2 Service Pack 5.

8.14 In a **network consisting of an Avaya CM and CS1000** with a Session Manager, if a call originates from a station on CM to a station on the CS1000, and subsequently gets transferred to another station on the same CS1000 (for example in a zero out scenario) the caller may experience **no talk path**. The workaround for this issue is to disable a feature in the CM SIP trunk-group called Network Call Redirection (NCR).

8.15 **When transferring calls in a MultiSite** configuration, the administered Site Name will be displayed to the Called Party.

8.16 **MAS QOS values may not take effect** unless a Registry is present. Check to see if the Registry Key DisableUserTOSSetting is in the following location:

HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\

If the registry key is not there, add it with a DWord value of 0. Then Restart the MAS. QOS values will now be in effect. This issue will be corrected in MM 5.2SP8. Please refer to Avaya PSN #003151 for more details.

8.17 Voice messaging recorded have pops and parts are missing.

Check to ensure 20 msecs is used for the RTP Packet size. Any other setting on the PBX or MM for this integration is currently not supported and is known to causes audio issues.

Note: Dialogic DSE Gateways used for integration that use SRTP require the MM to have a setting of 30 msecs. This is the only exception supported.

CHANGE HISTORY		
Revision	**Issue Date**	**Reason for Change**
Version A	3/25/2011	Initial release

AVAYA Inc.
4655 Great America Parkway
Santa Clara CA 95054
+1-866-Go-Avaya
From Outside the US: +1 (908) 953-6000
http://www.avaya.com

ADDENDUM FOR AUDIOCODES GATEWAY INTEGRATIONS

This section contains information regarding Issues and Solutions found with AudioCodes Gateways integrations.

Note for MM: Only AudioCodes firmware version 5.60A.xxx.xxx is supported.

1. Issue: FIND ME: On a Find Me call when the called party answers they hear four DTMF digits (A, B, C, D) are played followed by about 1 second of silence, followed by the normal prompt with the first little bit missing).

SOLUTION: In the AudioCodes .ini file Add the *RxDTMFHangOverTime* parameter with a value of 100 instead of the default value of 1000ms.

2. Issue: *DTMF* - *User presses the # key in a recording which is translated to a slight "bleep" when the recording is listened to.*

SOLUTION: Although you can reduce the length of the DTMF chirp it is still heard. So the best option is to trim the recording in MM by adding the registry key *TrimRecordedAudioMS* location show below, and set a Dword value from the default of 0 (zero) to a value of say 500 (please note this is in milliseconds). Then adjust it up/down from there as needed.

KEY_LOCAL_MACHINE\SOFTWARE\Octel\Geneva\Vcm_TelephonyServiceMgr\SIP

Note: As of MM 5.2 SP5 this value can be set in the VMSC on the Tone Tab for a selected PBX as “Record Trim Length”. See Tone Detection Tab in Section 6.0 of this document.

3. Issue: *Transfer/FINDME Fails* - Calls originating through one Mediant Gateway to MM, that have a new independent call established from the MM through Mediant B will ring the end user but when call is answered user hears a tone and call is disconnected and a SIP 481 error is generated in the logs. Call is split and cannot be bridged as GWs do not know each has a leg of the same call.

SOLUTION: Use one Gateway. A solution to using Multiple Gateway configurations was added to MM SP4Patch3 and SP6

4. Issue: *Beep tone* - A beep tone is heard when on a transfer just before the Personal Greeting is played. On a RNA no tone is heard.

SOLUTION: This occurs because MM sends an sdp with (audio) “a=inactive.” This then causes the Mediant gateway to play a HELP_TONE because it assumes that MoH (Music on Hold) will have to be played locally since there is no audio stream expected (a=inactive). The only way around this is to remove the tone from the CPT file in the Gateway. A CPT with this tone removed is available from Integrations Support.

5. Issue: *E1 calls fail on upper half of span* - If calls on E1 channels above 16 (the D-Channel for an E-1) have no talk path (dead air) it may be a setting in the AudioCodes Gateway causing it.

SOLUTION: In the AudioCodes ini file, check the ISDNGeneralCCBehavior parameter to see if it is set to 32. If so change it to 0, which is the default value. Then reload/burn the INI and calls should complete properly.