ADDENDUM: Avaya Communication Manager Survivable SIP Gateway Solution using the AudioCodes MP-114 in a Centralized Trunking Configuration – v1.1

1. Overview

This application note is an addendum to the '*Avaya Communication Manager Survivable SIP Gateway Solution using the AudioCodes MP-114 in a Centralized Trunking Configuration*'.

The two items covered in this addendum are

- Required Firmware Upgrade
- Use of Scenario Files to simplify administration
- Enhanced routing during both regular and emergency modes
- IP Security settings on the Audio Codes gateway

Figure 1 illustrates the routing during a normal (Sunny) day scenario.
An off-net call will come into the Audio Codes MP-11x gateway via one of the local FXO trunks. The MP-11x gateway will reroute the call to a Phantom Extension via the Avaya SES. The SES will map the destination extension to an Avaya Communication Manager Server and forward the call via this trunk. The Phantom Station on Avaya Communication Manager will cover to a Coverage Answer Group containing up to 8 local branch stations. The call is then forwarded to the local MP-11x gateway stations. The local branch stations that are a member of the Coverage Answer Group will ring on their first available Call Appearance.

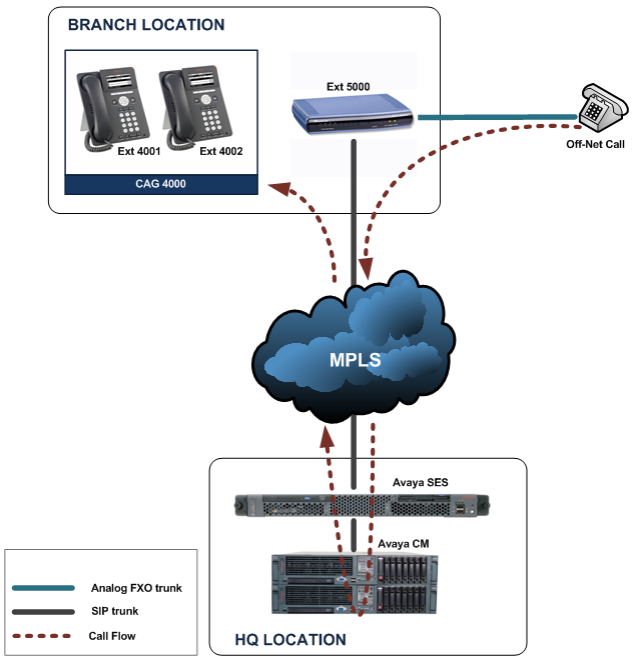
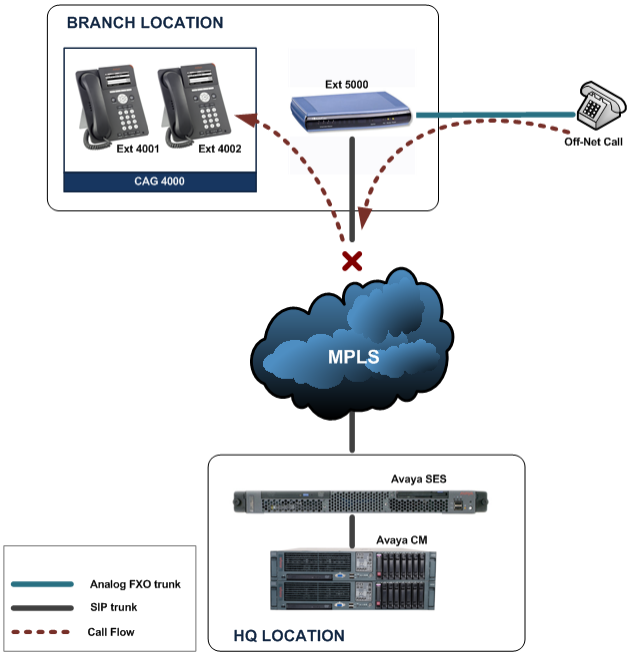


Figure 1 - Sunny Day Scenario



In Emergency (Rainy Day) scenario where network failure to the Core is detected, all calls will failover to a single local endpoint rather than to a group of endpoints. This is shown in Figure 2.

Figure 2 - Emergency (Rainy) Day Scenario

2. Administration

2.1 Require Firmware Upgrade

The original application note was built around firmware 5.40. The rest of this document requires and assumes that the Audio Codes MP-114 / 118 is updated to firmware 5.60A or newer. This firmware can be downloaded from support.avaya.com.

2.2 Enhanced Routing

This application note makes use of features at the Core (Avaya Communication Manager) to ring multiple branch endpoints at the same time. The specific feature utilized is called 'Coverage Answer Groups'.

In the event of network failure or branch isolation, a local failover point is administered on the MP-11x.

To begin, you will need to login to your Avaya Communication Manager and create a 'Coverage Answer Group' as shown in Figure 1. You will name this group and enter up to 8 Branch extensions that you wish to ring simultaneously.

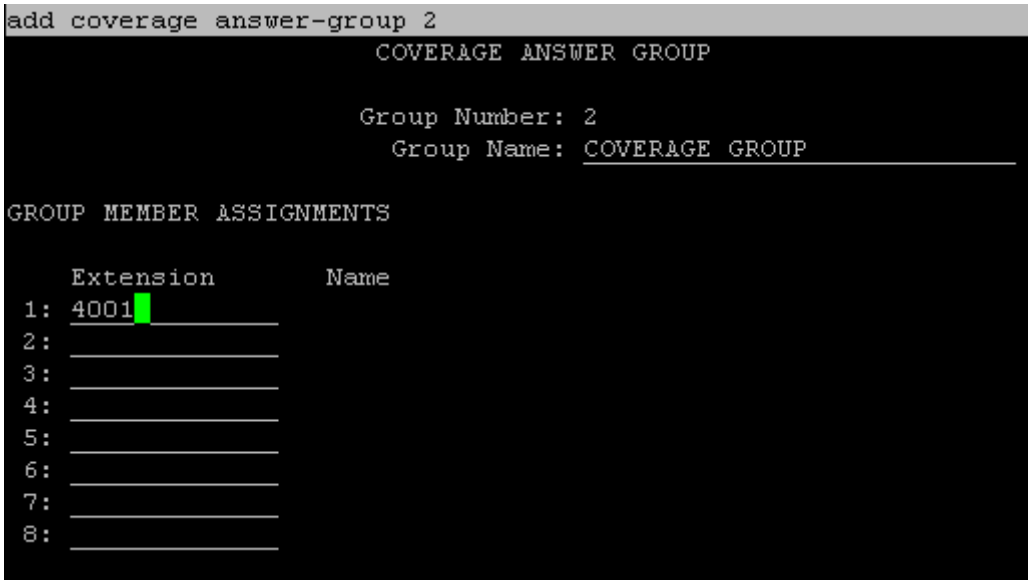


Figure 3 - Coverage Answer Group

The next step is to create a Coverage Path that points to the Coverage Answer Group just created. Add a new Coverage Path as shown in Figure 2. At the bottom of the page at Point1, enter the Coverage Answer Group number created previously. If you created Coverage Answer Group 1 then enter c1.

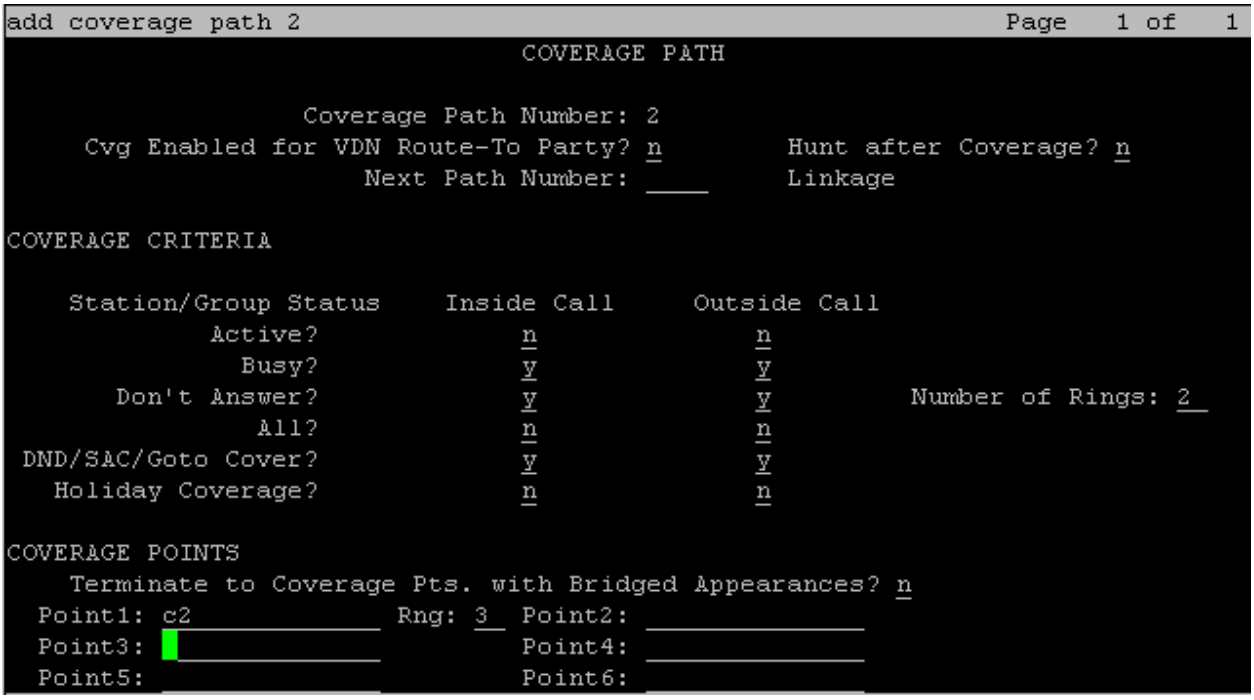


Figure 4 - Coverage Path

The final step of administration on Communication Manager is to create a Phantom Station as shown in Figure 3. Create a station as shown below and add the Coverage Path number created in Figure 2 to the Coverage Path 1 field for this Phantom Station.


```
change station 4004                                          Page   1 of   5
                                    STATION

Extension: 4004                       Lock Messages? n                BCC: 0
     Type: 6408D+                     Security Code:                   TN: 1
     Port: X                    Coverage Path 1: 1                    COR: 1
     Name: Phantom              Coverage Path 2:                      COS: 1
                                Hunt-to Station:
STATION OPTIONS
                                     Time of Day Lock Table:
             Loss Group: 2         Personalized Ringing Pattern: 1
           Data Module? n                    Message Lamp Ext: 40004
        Speakerphone: 2-way               Mute Button Enabled? y
     Display Language: english

       Survivable COR: internal              Media Complex Ext:
  Survivable Trunk Dest? y                        IP SoftPhone? n
```

Figure 5 - Phantom Station

The only administration required on the Sip Enablement Server (SES) is shown in Figure 4. Select the Map link on the Communication Manager Server Entry for the Communication Manager in the previous steps. Add a new Map similar to that shown below that will capture the Phantom Station Extension and route it to the Avaya Communication Manager.

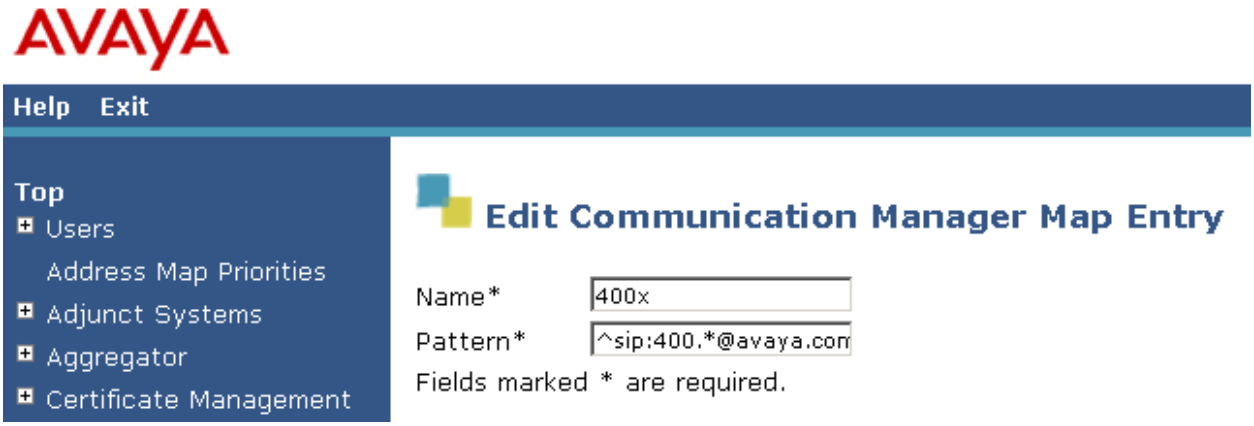


Figure 6 - SES Map Entry

2.3 Scenario Files

Scenario files are loaded on the MP-11x Gateway web interface similar to configuration files. They are used to direct an administrator to the specific fields that are required to customize a site.

To begin, download the SCENARIO.dat file from support.avaya.com. Login to the MP-11x gateway. Select the Scenarios button from the administration menu as shown in figure 1.

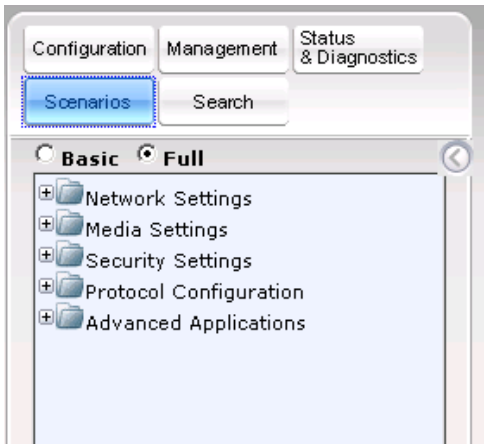


Figure 7 - Scenarios Button

Scroll down and select the 'Get/Send Scenario File' button. Select the browse button on locate the SCENARIO.dat file. Select 'Send File' button as shown in Figure 2.

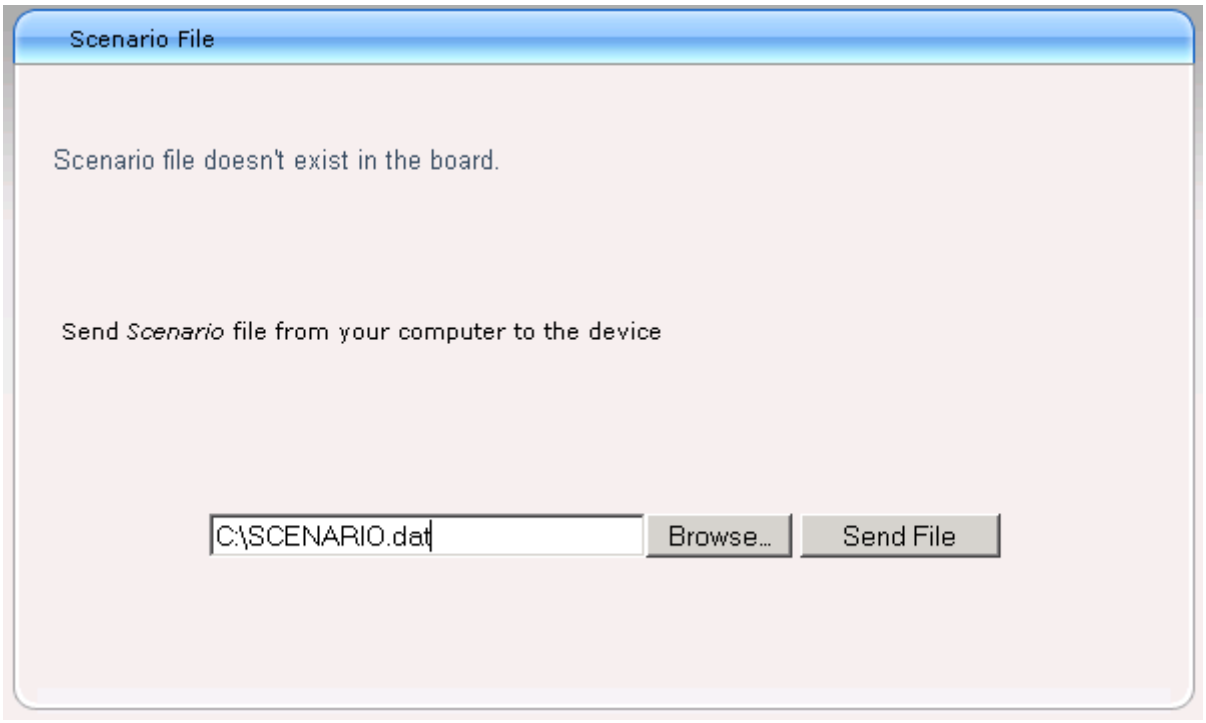
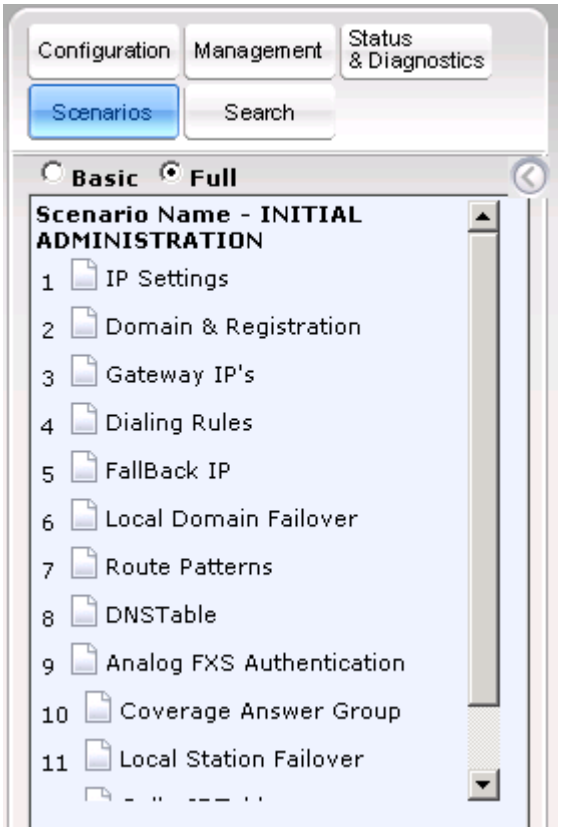


Figure 8 - Loading Scenario File



Once loaded, the scenario steps will show up left side of the page. You can proceed through the steps by either selecting a step from the list or selecting the 'Next' button within each step. See Figure 3.

In each step, only the relevant fields are available for administration. All preset fields are non-administrable and grayed out.

Many of the pages in each step are already detailed in the '*Avaya Communication Manager Survivable SIP Gateway Solution using the AudioCodes MP-114 in a Centralized Trunking Configuration*' application note. Only those administration steps that are new will be detailed in this addendum.

Figure 9 - Scenario Steps Loaded

Step 2 – Domain and Registration: Set the Proxy name and Gateway name to your SIP domain.

Step 3 – Gateway IP's: Select page '0' from the Proxy Set ID list. Enter the IP of the MP-11x Gateway in the Proxy Address followed by ':5060' as shown in Figure 4.

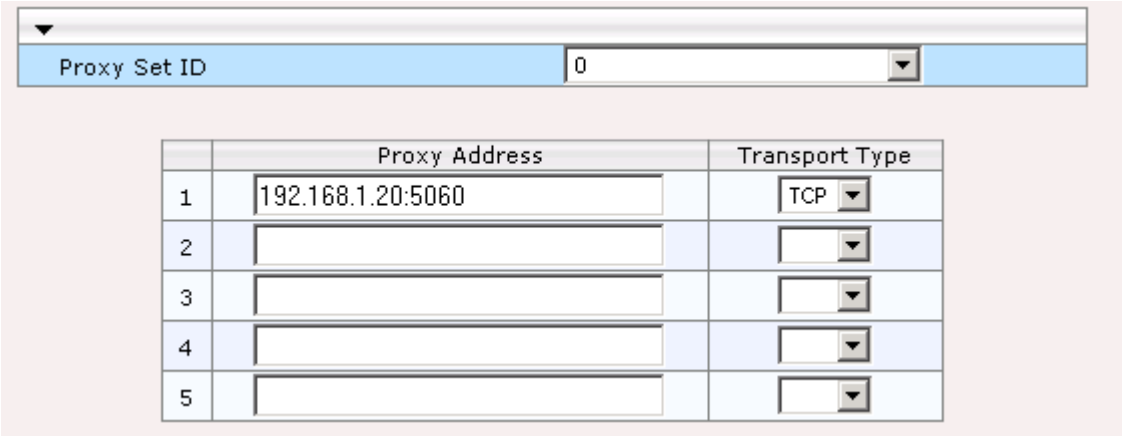


Figure 10 - First Gateway IP

Select page '1' from the Proxy Sett ID list. Enter the IP of your SES Home in the Proxy Address field.

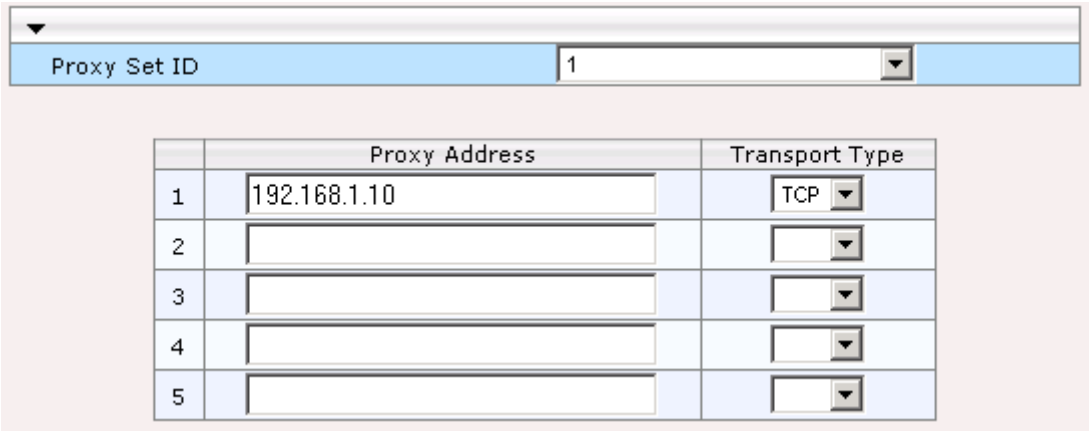


Figure 11 - Second Gateway IP

Step 6 – Local Domain Failover: Replace both of the 'avaya.com' names with your local SIP domain. This domain will be resolved by the DNS table at step 8.

Figure 12 - Failover Domain

Step 7 – Route Patterns: ONLY replace the '4004' entry with the Coverage Answer Group extension on your Avaya Communication Manager. Replace the '500' entry with the leading digits of any local extension that you wish to dial on your Avaya Communication Manager. Add other relevant entries as detailed in the original application note.

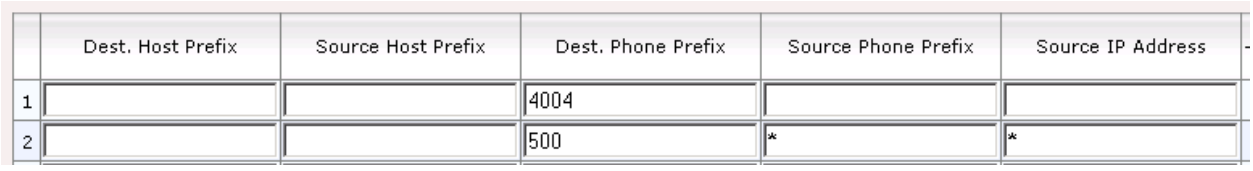


Figure 13 - Route Patterns

Step 8 – DNS Table: Enter your SIP domain in place of 'avaya.com' and the IP address of your MP-11x gateway in the 'First IP Address' field.

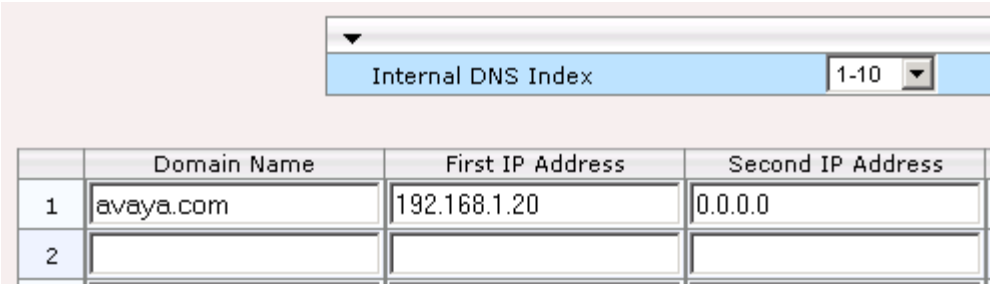


Figure 14 - Internal DNS

Step 10 – Coverage Answer Group: Replace the '4004' with the Extension of the Coverage Answer Group on your Avaya Communication Manager. This is the same extension set in step 7. Place this extension in any additional FXO ports that you wish to route to this CAG. See Figure 9.

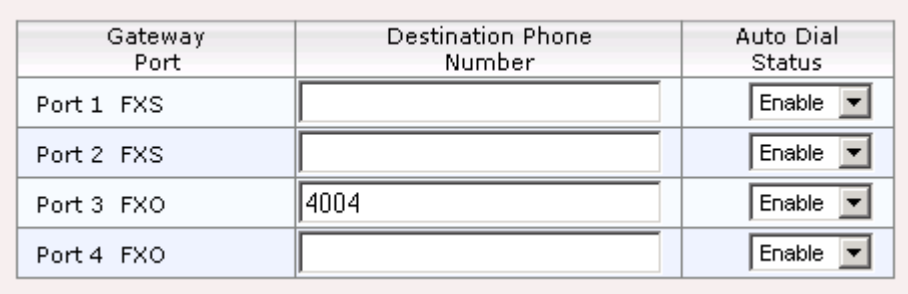


Figure 15 - Coverage Answer Group

Step 11 – local station failover: First replace the Destination Prefix with the Extension of your Coverage Answer Group. Second, replace the Prefix to Add field with the local Extension that you wish to failover to. Third, replace the Stripped Digits From Right with the number of digits in your Coverage Answer Group extension. See Figure 10.

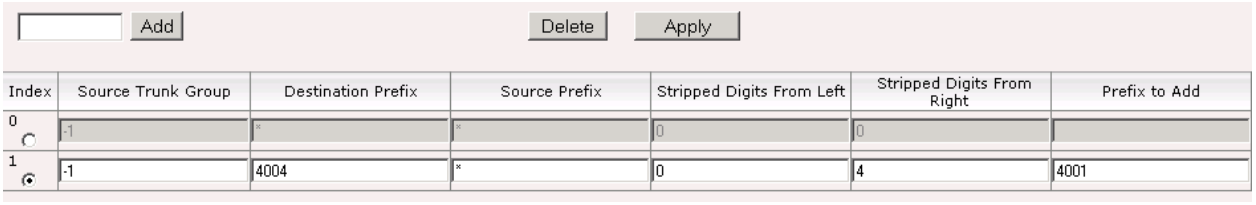


Figure 16 - Coverage Answer Group Failover point

Once you have finished all 13 steps, you will need to select the 'Delete Scenario File' button*. The previous action is needed only in the current firmware release.

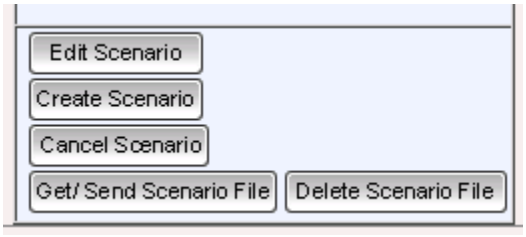


Figure 17 - Delete Scenario File button

3. IP Security Settings

By default HTTPS is not enabled in the default configuration file but can be enabled on a site by site basis. The reason that this is not enabled by default is because HTTPS forwarding is not yet supported by the current firmware on the Audio Codes MP-11x.

3.1 Enable HTTPS and Cipher Values

The first step is to open the 'General Security Settings' form and modify the 'Secured Web Connection (HTTPS)' field to 'HTTPS Only' as shown in Figure 18.

You will need to Burn and Reset the gateway before this setting will be effective.

****NOTE:** Administrators will now need to manually type in HTTPS in the browser URL as the gateway does not support HTTPS forwarding currently.

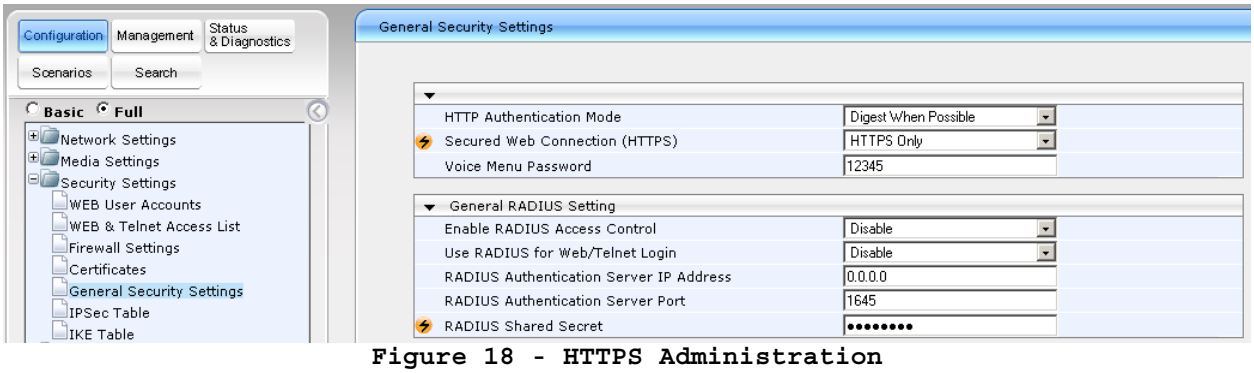


Figure 18 - HTTPS Administration

3.2 Certificates

There is also an option to install an SSL certificate purchased from a CA or generate or install a self-signed certificate. This is performed through the 'Certificates' form under 'Security Settings' menu option. See Figure 19.

Figure 19 - Certificate Administration

CONTENTS

