Avaya Solution & Interoperability Test Lab

Application Notes for ATT AMX Alarm Management Server and Avaya Aura® Communication Manager and SIP Interface via Avaya Aura® SIP Enablement Services – Issue 1.0

Abstract

These Application Notes describe the compliance testing of ATT AMX Alarm Management Server with Avaya Aura® Communication Manager. The ATT AMX Alarm Management Server communicates with Communication Manager via a SIP trunk connected to Avaya Aura® SIP Enablement Services. The compliance testing tested the major functions of the ATT AMX Alarm Management Server product.

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.

Table of Contents

1. Introduction

These Application Notes describe the configuration steps required for ATT AMX Alarm Management Server to successfully interoperate with Communication Manager and the Avaya R4 DECT base station. The ATT AMX Alarm Management Server generates preconfigured or ad hoc alarms which were signaled to Communication Manager as calls via the SIP interface which are sent to Communication Manager via SIP Enablement Services. For the compliance tests described by these Application Notes, ATT AMX Alarm Management Server and Communication Manager were configured to operate as follows:

- Each alarm consisted of an audio message and a text message. The text message was sent as the calling party name (which can have a maximum length of fifteen characters) and was thus visible for alarms to local extensions and DECT endpoints (but not PSTN endpoints).
- All alarms were sent as "Priority" calls, and were thus not forwarded to coverage if unanswered by local extensions.
- Alarms were also configured such that the alarm recipient must acknowledge via telephone keypad input, thus preventing alarms which were answered by voicemail systems from being considered as delivered.

For alarms to extensions coupled to GSM endpoints via the Avaya EC500 facility, EC500 was configured to require acknowledgement for calls answered by the GSM endpoint, thus allowing GSM voicemail systems to be ignored.

The ATT AMX Alarm Management Server does not support the SIP re-invites used by Communication Manager to establish direct IP-IP audio connections.

1.1. Interoperability Compliance Testing

The compliance testing included the following test scenarios:

- Alarm creation via text-to-speech and via telephone input
- Alarm delivery to idle station
- Alarm to busy station
- Alarm to station, no answer
- Alarm to station with coverage enabled, no answer
- Alarm to station with call forwarding enabled
- Alarm to unavailable station
- Alarm to tandem station (both GSM and DECT as twin)
- Alarm to hunt group
- Alarm to multiple endpoints
- Automatic startup after power interruption
- Recovery from interruption to interface to PBX

Where appropriate, each of these tests was performed with local extension, DECT mobile endpoints, PSTN endpoints, and cellular endpoints.

1.2. Support

Support for ATT products is available at

▪ Web-based support:	only for accredited partners
▪ Email:	Support@attag.ch
▪ help desk:	+41 44 908 6004

2. Reference Configuration

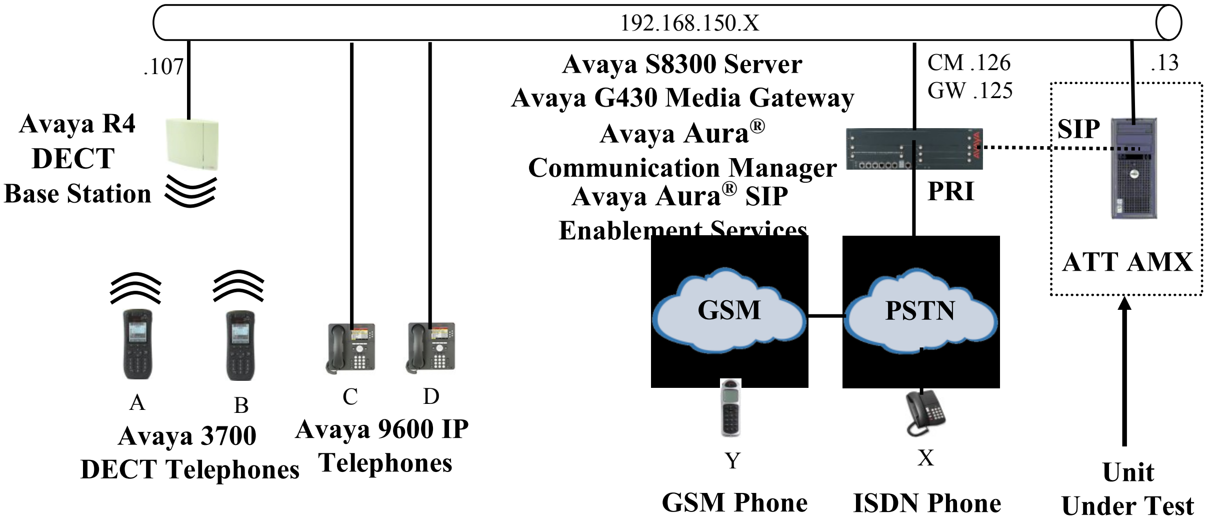


Figure 1: Reference Configuration

The ATT AMX Alarm Management Server in the above diagram interfaces to Communication Manager via SIP trunk. The ISDN endpoint is included in the configuration so that alarms can be sent to PSTN endpoints. The GSM endpoint is included in the configuration so that alarms can be sent to a local extension which is coupled to a GSM endpoint via EC500.

The following table contains additional information about how each of the telephones contained in the above diagram are configured in Communication Manager:

Diagram	Ext	Endpoint
A	10303	Avaya DECT 3720 Telephone
B	10304	Avaya DECT 3725 Telephone
C	10183	Avaya 9630G IP Telephone
D	10094	Avaya 9620 IP Telephone
X	06911111111	ISDN endpoint
Y	+492222222222	GSM endpoint
	20000	AMX Alarm Generation

Table 1: Extensions Used for Testing

3. Equipment and Software Validated

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

Software Component	Version
Avaya Aura® Communication Manager Avaya Aura® SIP Enablement Services	R015x.02.1.016.4 Update 18365
Avaya G430 Media Gateway	30.14.0
Avaya MM710AP DS1 (PRI) interface	HW05/FW021
Avaya 9600 Series Telephones	3.1.1
Avaya 3720 DECT Telephone	3.0.7
Avaya 3725 DECT Telephone	3.0.10
Avaya R4 DECT	Hardware: IPBS1-Y3/PB, IPBS: 3.2.8, Bootcode: 3.0.26
Pika SIP AllOnHost Stack	2.8.10
ATT AMX Alarm Management Server	Release 9.0

Table 2: Equipment and Versions Validated

4. Configure Avaya Aura® Communication Manager

The configuration and verification operations illustrated in this section were performed using the Communication Manager System Administration Terminal (SAT).

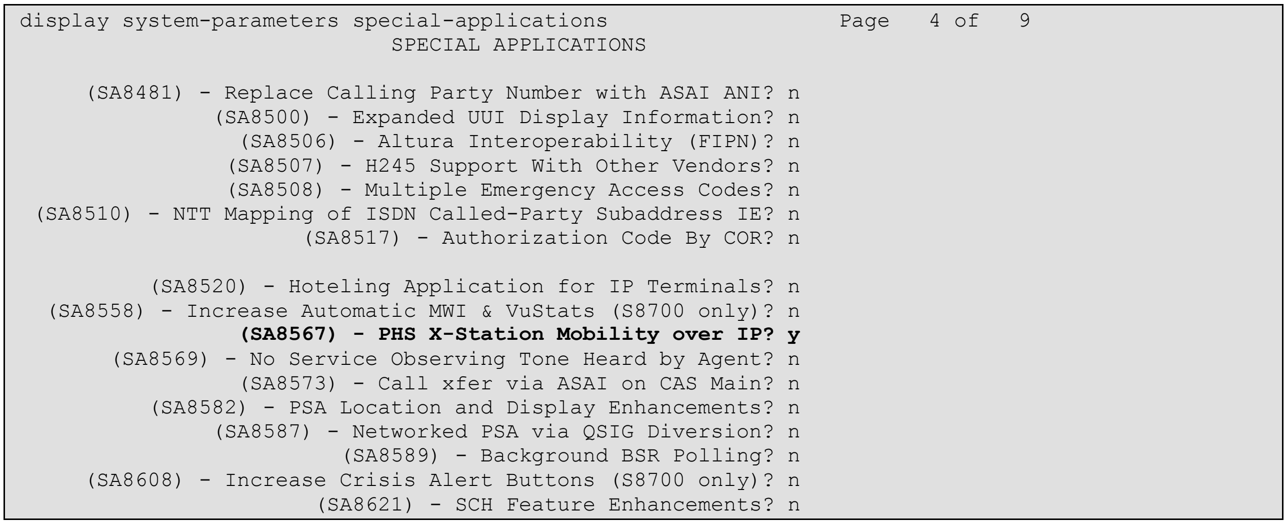
Note that the configuration of the interface to the PSTN is out of the scope of these application notes.

4.1. Verify System-Parameters Special-Applications

Use the **display system-parameters special-applications** command to verify that Communication Manager is configured to meet the minimum requirements to support the special applications used for these tests, as shown by the parameter values in **Table 3**. If these are not met in the configuration, please contact an Avaya representative for further assistance.

Parameter	Usage
(SA8567) - PHS X-Station Mobility over IP	The value must be set to “y”.

Table 3: Configuration Values for System-Parameters Special-Applications



```
display system-parameters special-applications                  Page   4 of   9
                             SPECIAL APPLICATIONS

     (SA8481) - Replace Calling Party Number with ASAI ANI? n
               (SA8500) - Expanded UUI Display Information? n
                 (SA8506) - Altura Interoperability (FIPN)? n
                (SA8507) - H245 Support With Other Vendors? n
                (SA8508) - Multiple Emergency Access Codes? n
 (SA8510) - NTT Mapping of ISDN Called-Party Subaddress IE? n
                      (SA8517) - Authorization Code By COR? n

          (SA8520) - Hoteling Application for IP Terminals? n
  (SA8558) - Increase Automatic MWI & VuStats (S8700 only)? n
                 (SA8567) - PHS X-Station Mobility over IP? y
       (SA8569) - No Service Observing Tone Heard by Agent? n
                 (SA8573) - Call xfer via ASAI on CAS Main? n
          (SA8582) - PSA Location and Display Enhancements? n
               (SA8587) - Networked PSA via QSIG Diversion? n
                         (SA8589) - Background BSR Polling? n
     (SA8608) - Increase Crisis Alert Buttons (S8700 only)? n
                       (SA8621) - SCH Feature Enhancements? n
```

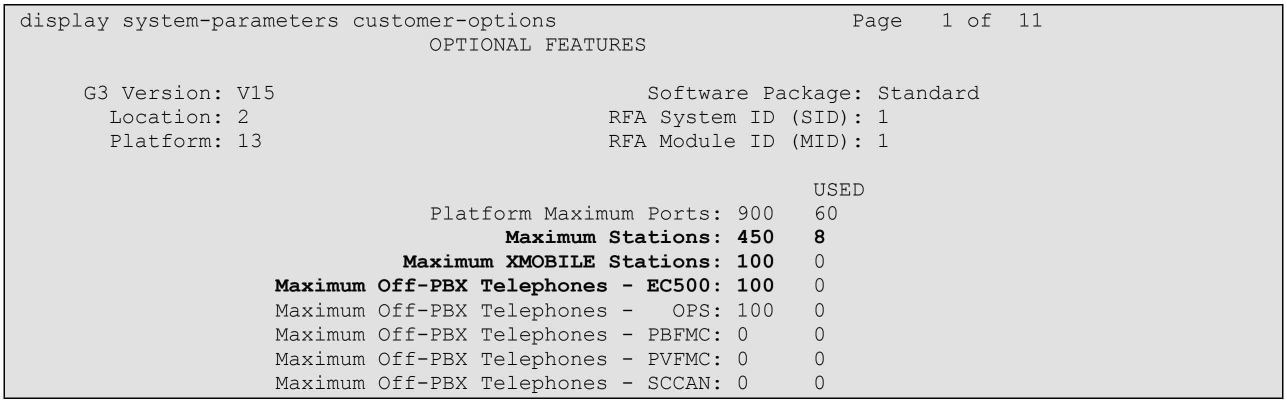
Figure 2: System-Parameters Special-Applications Form, Page 4

4.2. Verify System-Parameters Customer-Options

Use the **display system-parameters customer-options** command to verify that Communication Manager is configured to meet the minimum requirements to support the configuration used for these tests, as shown by the parameter values in **Table 4**. If these are not met in the configuration, please contact an Avaya representative for further assistance.

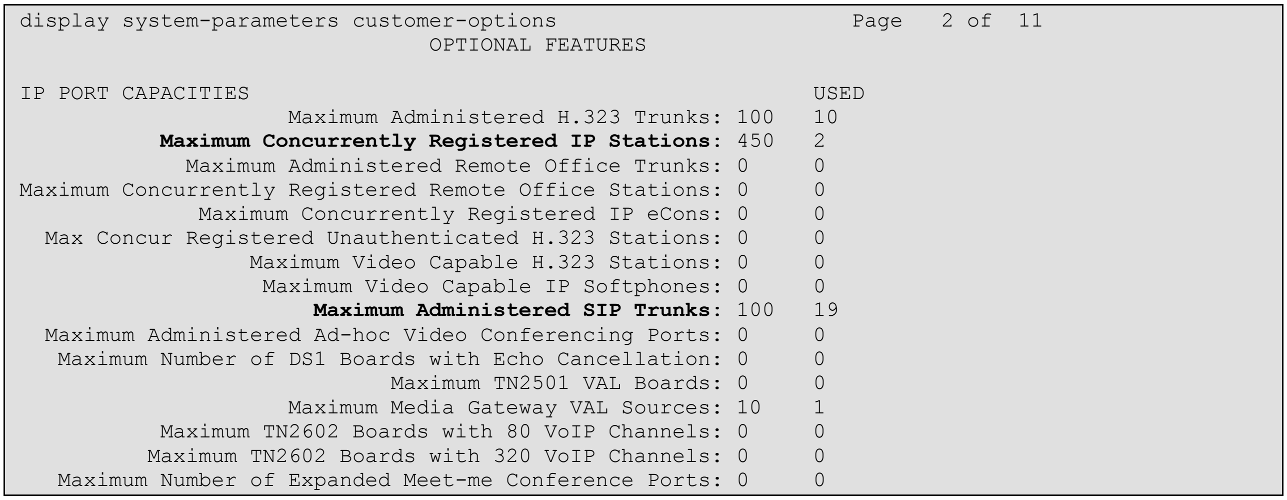
Parameter	Usage
Maximum Stations (Page 1)	The value must be sufficient to allow the number of stations, including the AMX, shown in **Table 1**.
Maximum XMOBILE Stations (Page 1)	The value must be sufficient to allow the number of DECT stations, including the AMX, shown in **Table 1**.
Maximum Off-PBX Telephones – EC500 (Page 1)	This parameter must be large enough to support the number of stations which are paired with EC500 endpoints.
Maximum Concurrently Registered IP Stations (Page 2)	The value must be sufficient to allow the number of IP stations shown in **Table 1**
Maximum Administered SIP Trunks (Page 2)	The value must be sufficient to allow the number of IP stations, including the AMX, shown in **Table 1**
Enhanced EC500 (Page 4)	This parameter must be set to “y”.
IP Trunks (Page 4)	This parameter must be set to “y”.
ISDN-PRI (Page 4)	This parameter must be set to “y”.

Table 4: Configuration Values for System-Parameters Customer-Options



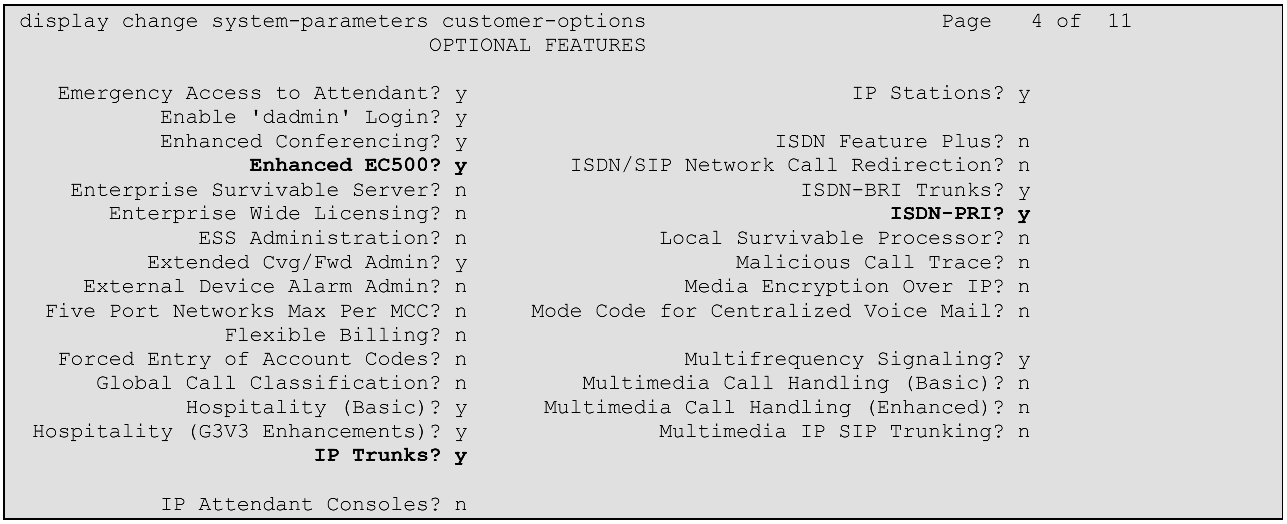
```
display system-parameters customer-options                       Page   1 of  11
                                OPTIONAL FEATURES

     G3 Version: V15                             Software Package: Standard
       Location: 2                            RFA System ID (SID): 1
       Platform: 13                           RFA Module ID (MID): 1

                                                              USED
                                Platform Maximum Ports: 900   60
                                      Maximum Stations: 450   8
                              Maximum XMOBILE Stations: 100   0
                    Maximum Off-PBX Telephones - EC500: 100   0
                    Maximum Off-PBX Telephones -   OPS: 100   0
                    Maximum Off-PBX Telephones - PBFMC: 0     0
                    Maximum Off-PBX Telephones - PVFMC: 0     0
                    Maximum Off-PBX Telephones - SCCAN: 0     0
```

Figure 3: System-Parameters Customer-Options Form, Page 1



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

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 100   10
           Maximum Concurrently Registered IP Stations: 450   2
             Maximum Administered Remote Office Trunks: 0     0
Maximum Concurrently Registered Remote Office Stations: 0     0
              Maximum Concurrently Registered IP eCons: 0     0
  Max Concur Registered Unauthenticated H.323 Stations: 0     0
                  Maximum Video Capable H.323 Stations: 0     0
                   Maximum Video Capable IP Softphones: 0     0
                       Maximum Administered SIP Trunks: 100   19
   Maximum Administered Ad-hoc Video Conferencing Ports: 0     0
    Maximum Number of DS1 Boards with Echo Cancellation: 0     0
                             Maximum TN2501 VAL Boards: 0     0
                     Maximum Media Gateway VAL Sources: 10    1
           Maximum TN2602 Boards with 80 VoIP Channels: 0     0
          Maximum TN2602 Boards with 320 VoIP Channels: 0     0
   Maximum Number of Expanded Meet-me Conference Ports: 0     0
```

Figure 4: System-Parameters Customer-Options Form, Page 2



```
display change system-parameters customer-options                       Page   4 of  11
                                OPTIONAL FEATURES

   Emergency Access to Attendant? y                              IP Stations? y
           Enable 'dadmin' Login? y
           Enhanced Conferencing? y                        ISDN Feature Plus? n
                  Enhanced EC500? y        ISDN/SIP Network Call Redirection? n
    Enterprise Survivable Server? n                          ISDN-BRI Trunks? y
       Enterprise Wide Licensing? n                                 ISDN-PRI? y
              ESS Administration? n               Local Survivable Processor? n
          Extended Cvg/Fwd Admin? y                     Malicious Call Trace? n
     External Device Alarm Admin? n                 Media Encryption Over IP? n
  Five Port Networks Max Per MCC? n     Mode Code for Centralized Voice Mail? n
                Flexible Billing? n
   Forced Entry of Account Codes? n                 Multifrequency Signaling? y
      Global Call Classification? n         Multimedia Call Handling (Basic)? n
            Hospitality (Basic)? y      Multimedia Call Handling (Enhanced)? n
 Hospitality (G3V3 Enhancements)? y               Multimedia IP SIP Trunking? n
                       IP Trunks? y

           IP Attendant Consoles? n
```

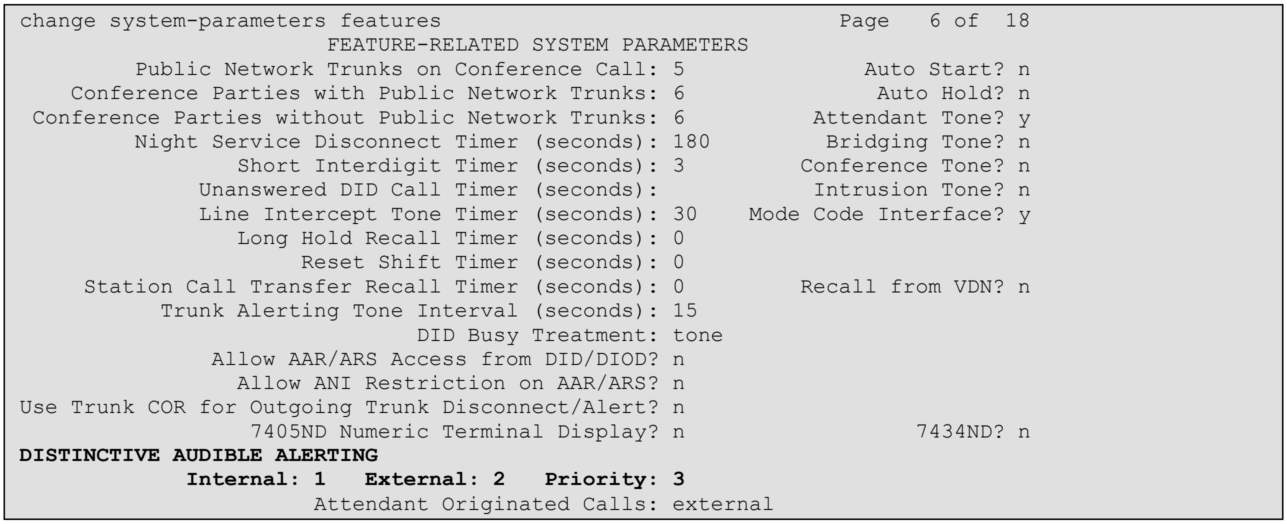
Figure 5: System-Parameters Customer-Options Form, Page 4

4.3. Verify System-Parameters Features

Use the **change system-parameters features** command to set required features as shown in the following table.

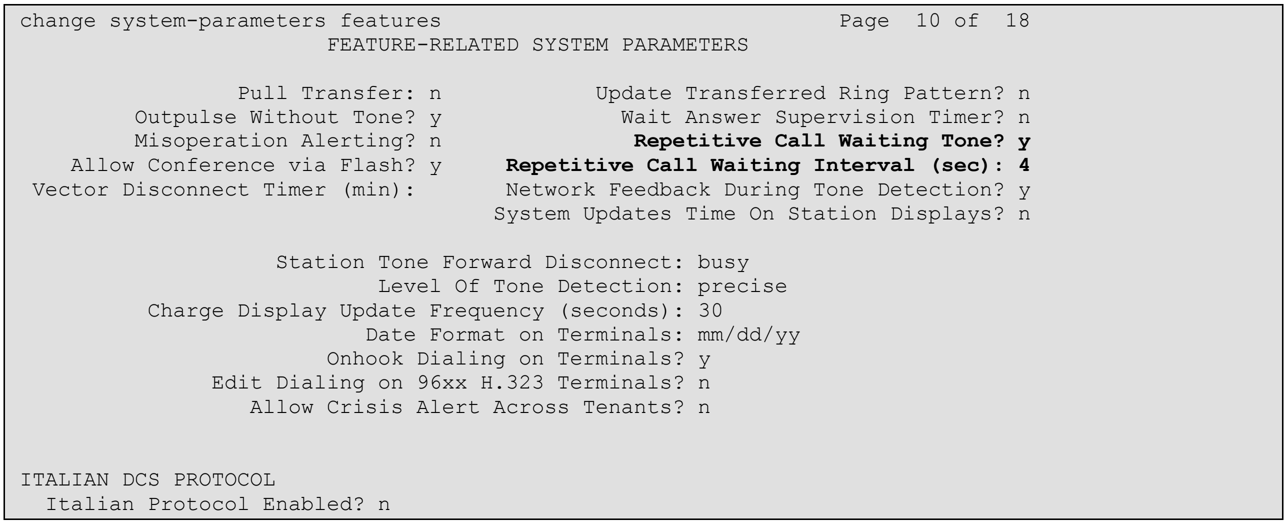
Parameter	Usage
Distinctive Audible Alerting (Page 6)	Set the ring count parameters as follows. “Internal”: 1, “External”: 2, “Priority”: 3.
Repetitive Call Waiting Tone (Page 10)	Set this to “y”.
Repetitive Call Waiting Interval (Page 10)	Set this to the interval that busy handsets should repeat the call waiting tone. Set this to 4 seconds.

Table 5: Configuration Values for System-Parameters Features



```
change system-parameters features                               Page   6 of  18
                        FEATURE-RELATED SYSTEM PARAMETERS
         Public Network Trunks on Conference Call: 5              Auto Start? n
    Conference Parties with Public Network Trunks: 6               Auto Hold? n
 Conference Parties without Public Network Trunks: 6          Attendant Tone? y
         Night Service Disconnect Timer (seconds): 180         Bridging Tone? n
                 Short Interdigit Timer (seconds): 3         Conference Tone? n
              Unanswered DID Call Timer (seconds):            Intrusion Tone? n
              Line Intercept Tone Timer (seconds): 30    Mode Code Interface? y
                 Long Hold Recall Timer (seconds): 0
                      Reset Shift Timer (seconds): 0
     Station Call Transfer Recall Timer (seconds): 0         Recall from VDN? n
           Trunk Alerting Tone Interval (seconds): 15
                               DID Busy Treatment: tone
               Allow AAR/ARS Access from DID/DIOD? n
                 Allow ANI Restriction on AAR/ARS? n
Use Trunk COR for Outgoing Trunk Disconnect/Alert? n
                  7405ND Numeric Terminal Display? n                  7434ND? n
DISTINCTIVE AUDIBLE ALERTING
             Internal: 1   External: 2   Priority: 3
                       Attendant Originated Calls: external
```

Figure 6: System-Parameters Features Form, Page 6

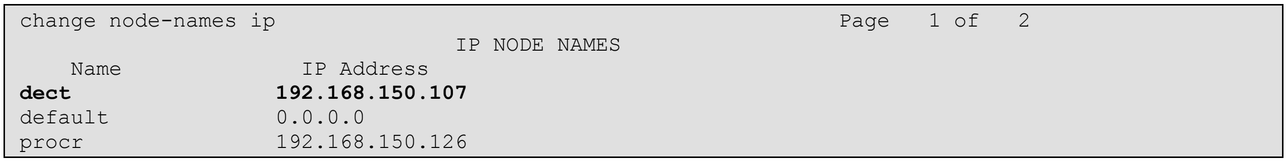


```
change system-parameters features                               Page  10 of  18
                        FEATURE-RELATED SYSTEM PARAMETERS

                Pull Transfer: n            Update Transferred Ring Pattern? n
        Outpulse Without Tone? y              Wait Answer Supervision Timer? n
        Misoperation Alerting? n               Repetitive Call Waiting Tone? y
     Allow Conference via Flash? y     Repetitive Call Waiting Interval (sec): 4
 Vector Disconnect Timer (min):        Network Feedback During Tone Detection? y
                                      System Updates Time On Station Displays? n

                   Station Tone Forward Disconnect: busy
                           Level Of Tone Detection: precise
          Charge Display Update Frequency (seconds): 30
                          Date Format on Terminals: mm/dd/yy
                       Onhook Dialing on Terminals? y
              Edit Dialing on 96xx H.323 Terminals? n
                 Allow Crisis Alert Across Tenants? n


ITALIAN DCS PROTOCOL
  Italian Protocol Enabled? n
```

Figure 7: System-Parameters Features Form, Page 10

4.4. Configure IP Node Names

Use the **change node-names ip** command to configure the address to be used for IP trunks.



```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
dect                  192.168.150.107
default               0.0.0.0
procr                 192.168.150.126
```

Figure 8: Node-Names IP Form

4.5. Configure Network Region

Use the **change ip-network-region** command to designate a network region to be used for voice calls over the SIP trunk using the parameters shown in the following table.

Parameter	Usage
Authoritative Domain	Enter the domain name to be used for SIP communication. This must match the values used in **Figure 36**.

Table 6: IP-Network-Region Parameters

```
change ip-network-region 1                                      Page   1 of  19
                               IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain: ffm.com
    Name:
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS                  RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

Figure 9: IP-Network-Region Form

4.6. Dial Plan

Use the **change dialplan analysis** command to configure the dial plan as shown in the following table.

Parameter	Usage
Dialed string: “0”	Use a “0” as Feature Access Code (FAC) to access external telephone numbers.
Dialed string: “1”	Five digit numbers starting with “1” are for local extensions.
Dialed string: “2”	Five digit numbers starting with “2” are AMX extensions.
Dialed string: “*0”	Strings beginning with “*0” is used for Trunk Access Codes (TAC).
Dialed string: “*8”	The dialed strings beginning with “*8” are used for Feature Access Codes.

Table 7: Dial Plan Analysis Parameters

```
change dialplan analysis                                        Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location:  all           Percent Full:    0

       Dialed   Total  Call    Dialed   Total  Call     Dialed   Total  Call
       String   Length Type    String   Length Type     String   Length Type
     0            1    fac
     1            5    ext
     2            5    ext
     *0           4    dac
     *8           3    fac
```

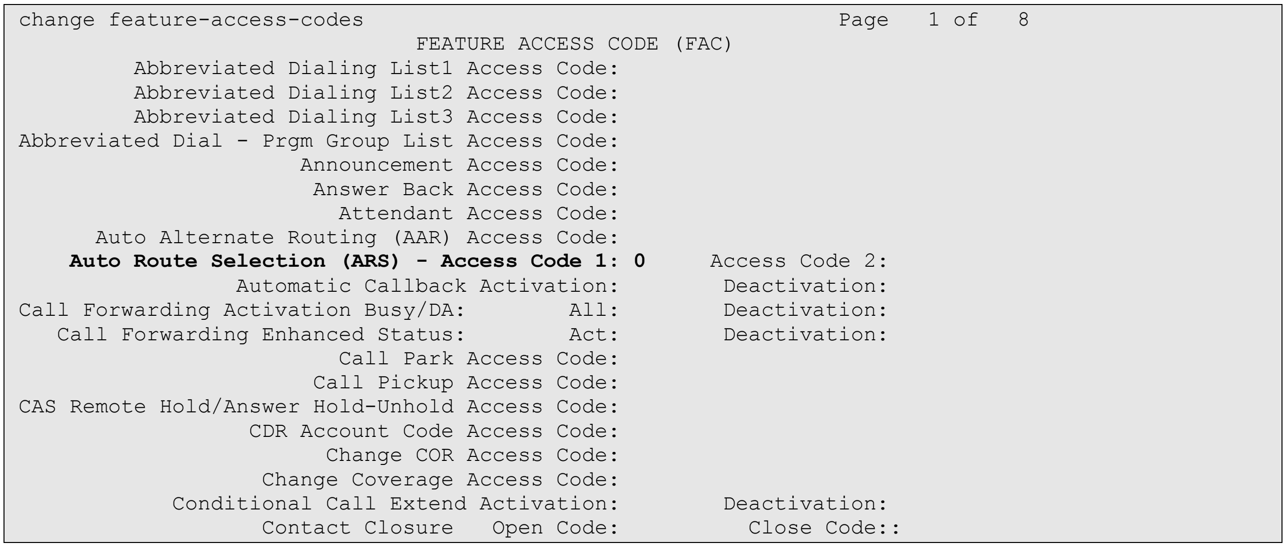
Figure 10: Dialplan Analysis Table Form

4.7. Add Feature Access Codes

Use the **change feature-access-codes** command to allocate feature access codes, as shown in the following table.

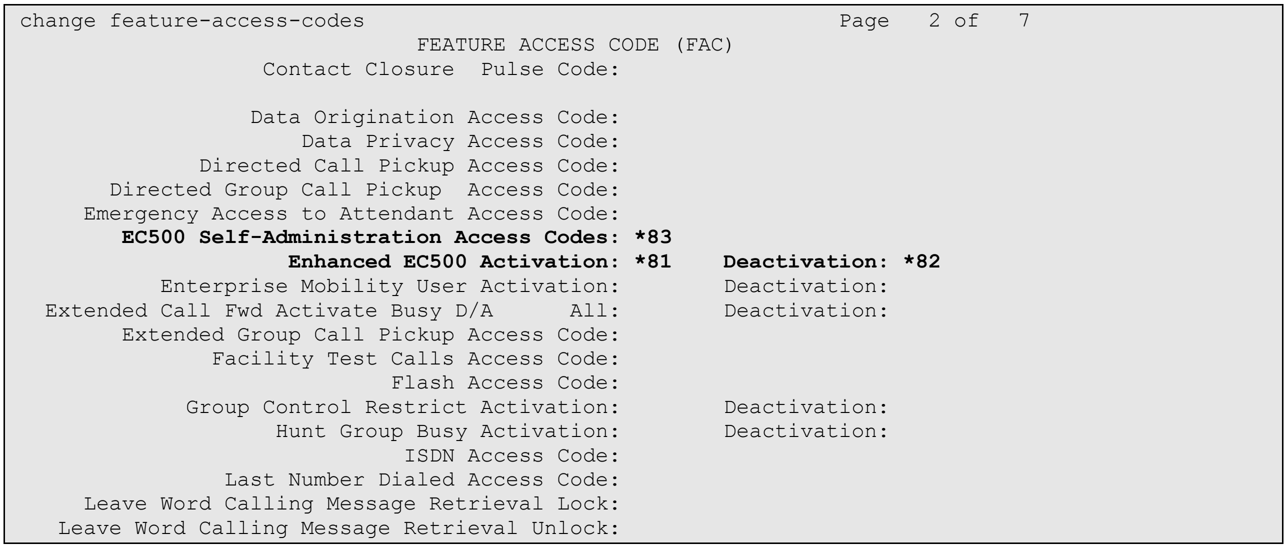
Parameter	Usage
Auto Route Selection Access Code (Page 1)	Use a “0” to use Automatic Route Selection (ARS) to route PSTN calls over a SIP trunk.
EC500 Self-Administration Access Codes (Page 2)	Enter an unused access code.
Enhanced EC500 Activation (Page 2)	Enter the code which is to be used to activate EC500.
Deactivation (Page 2)	Enter the code which is to be used to deactivate EC500.
Priority Calling Access Code	Enter an available feature code. This code is assigned to all incoming calls from the AMX trunk in **Figure 34**.

Table 8: Feature Access Code Parameters



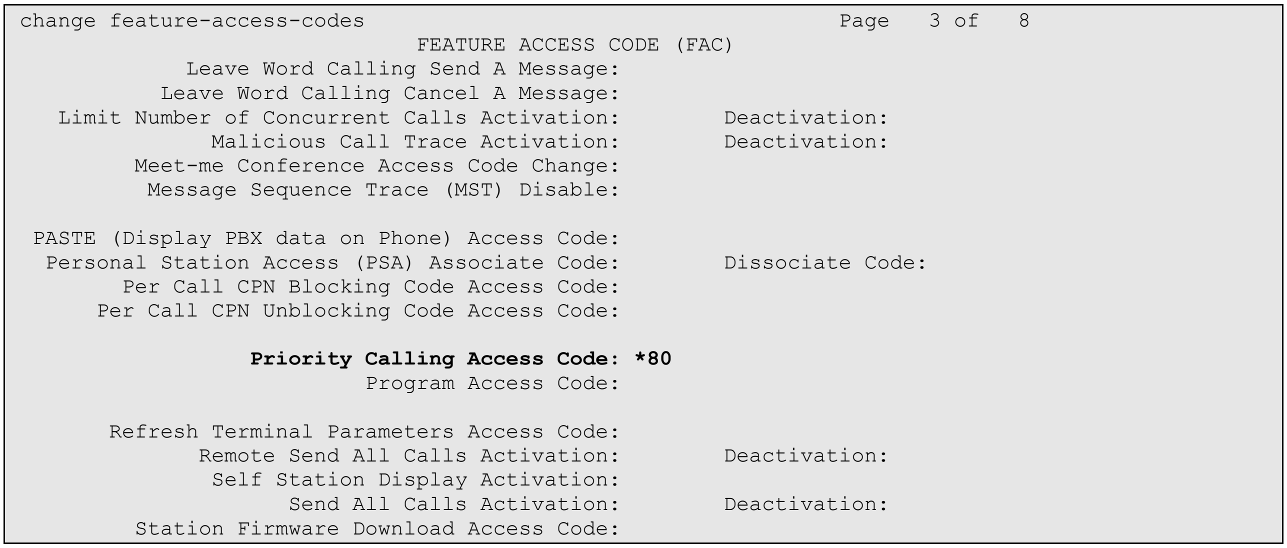
```
change feature-access-codes                                     Page   1 of   8
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code:
                       Answer Back Access Code:
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code:
    Auto Route Selection (ARS) - Access Code 1: 0     Access Code 2:
                 Automatic Callback Activation:        Deactivation:
Call Forwarding Activation Busy/DA:        All:        Deactivation:
   Call Forwarding Enhanced Status:        Act:        Deactivation:
                         Call Park Access Code:
                       Call Pickup Access Code:
CAS Remote Hold/Answer Hold-Unhold Access Code:
                  CDR Account Code Access Code:
                        Change COR Access Code:
                   Change Coverage Access Code:
            Conditional Call Extend Activation:        Deactivation:
                   Contact Closure   Open Code:          Close Code::
```

Figure 11: Feature-Access-Codes Form, Page 1



```
change feature-access-codes                                     Page   2 of   7
                               FEATURE ACCESS CODE (FAC)
                   Contact Closure  Pulse Code:

                  Data Origination Access Code:
                      Data Privacy Access Code:
              Directed Call Pickup Access Code:
       Directed Group Call Pickup  Access Code:
     Emergency Access to Attendant Access Code:
        EC500 Self-Administration Access Codes: *83
                     Enhanced EC500 Activation: *81    Deactivation: *82
           Enterprise Mobility User Activation:        Deactivation:
  Extended Call Fwd Activate Busy D/A      All:        Deactivation:
        Extended Group Call Pickup Access Code:
               Facility Test Calls Access Code:
                             Flash Access Code:
             Group Control Restrict Activation:        Deactivation:
                    Hunt Group Busy Activation:        Deactivation:
                              ISDN Access Code:
                Last Number Dialed Access Code:
     Leave Word Calling Message Retrieval Lock:
   Leave Word Calling Message Retrieval Unlock:
```

Figure 12: Feature Access Code Form, Page 2



```
change feature-access-codes                                     Page   3 of   8
                               FEATURE ACCESS CODE (FAC)
             Leave Word Calling Send A Message:
           Leave Word Calling Cancel A Message:
   Limit Number of Concurrent Calls Activation:        Deactivation:
               Malicious Call Trace Activation:        Deactivation:
         Meet-me Conference Access Code Change:
          Message Sequence Trace (MST) Disable:

 PASTE (Display PBX data on Phone) Access Code:
  Personal Station Access (PSA) Associate Code:        Dissociate Code:
         Per Call CPN Blocking Code Access Code:
       Per Call CPN Unblocking Code Access Code:

                  Priority Calling Access Code: *80
                           Program Access Code:

       Refresh Terminal Parameters Access Code:
              Remote Send All Calls Activation:        Deactivation:
               Self Station Display Activation:
                     Send All Calls Activation:        Deactivation:
         Station Firmware Download Access Code:
```

Figure 13: Feature Access Code Form, Page 3

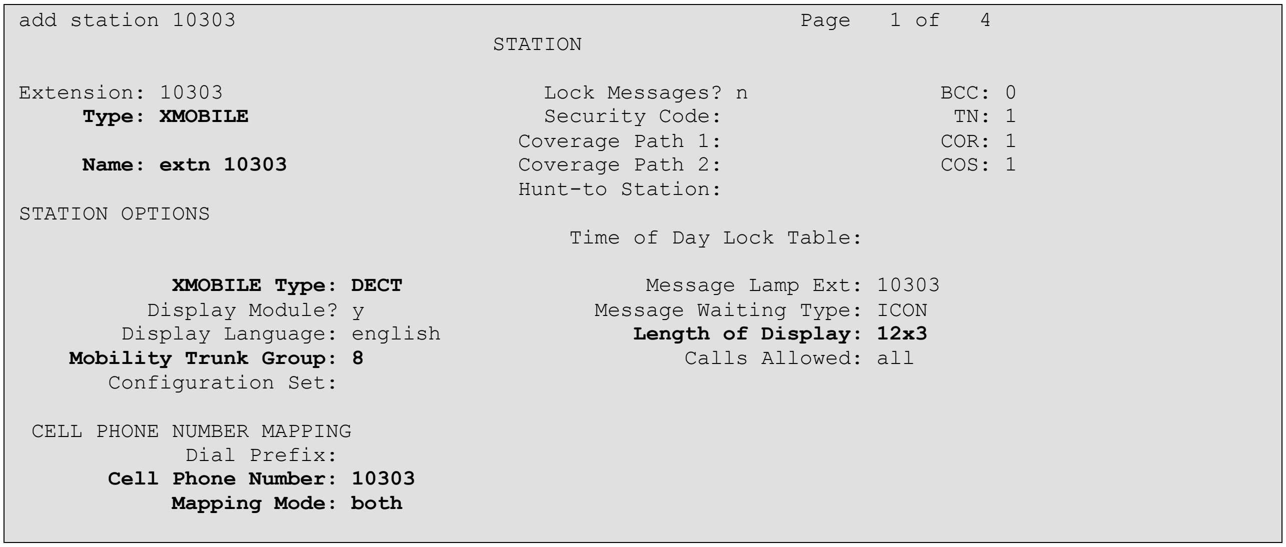
4.8. Add Stations

4.8.1. Add Mobile Stations

Use the **add station** command to add an extension for each of the mobile extensions listed in **Table 1** using the parameters shown in the following table.

Parameter	Usage
Type	Enter “XMOBILE” for an analog telephone.
Name	Enter an appropriate name to identify the station.
XMOBILE Type	Enter “DECT”.
Mobility Trunk Group	Enter the number of the trunk group which allocated in **Figure 8** for connection to the Avaya R4 base station.
Cell Phone Number	Enter the number allocated to this station.
Mapping Mode	Enter “both”.
Length of Display	Enter “12x3”.

Table 9: Mobile Station Parameters



```
add station 10303                                            Page   1 of   4
                                     STATION

Extension: 10303                         Lock Messages? n               BCC: 0
     Type: XMOBILE                       Security Code:                  TN: 1
                                       Coverage Path 1:                 COR: 1
     Name: extn 10303                  Coverage Path 2:                 COS: 1
                                       Hunt-to Station:
STATION OPTIONS
                                           Time of Day Lock Table:

            XMOBILE Type: DECT                   Message Lamp Ext: 10303
          Display Module? y                  Message Waiting Type: ICON
        Display Language: english               Length of Display: 12x3
    Mobility Trunk Group: 8                         Calls Allowed: all
       Configuration Set:

 CELL PHONE NUMBER MAPPING
             Dial Prefix:
       Cell Phone Number: 10303
            Mapping Mode: both
```

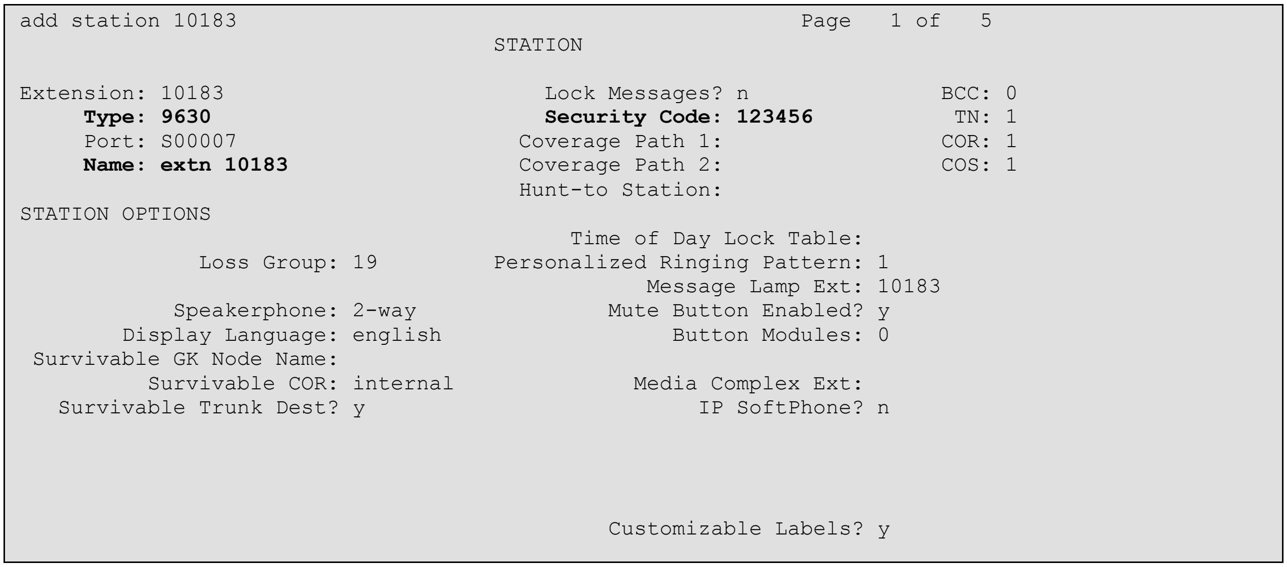
Figure 14: Mobile Station Form

4.8.2. Add IP Stations

Use the **add station** command to add an extension for each of the IP extensions listed in **Table 1** using the parameters shown in the following table.

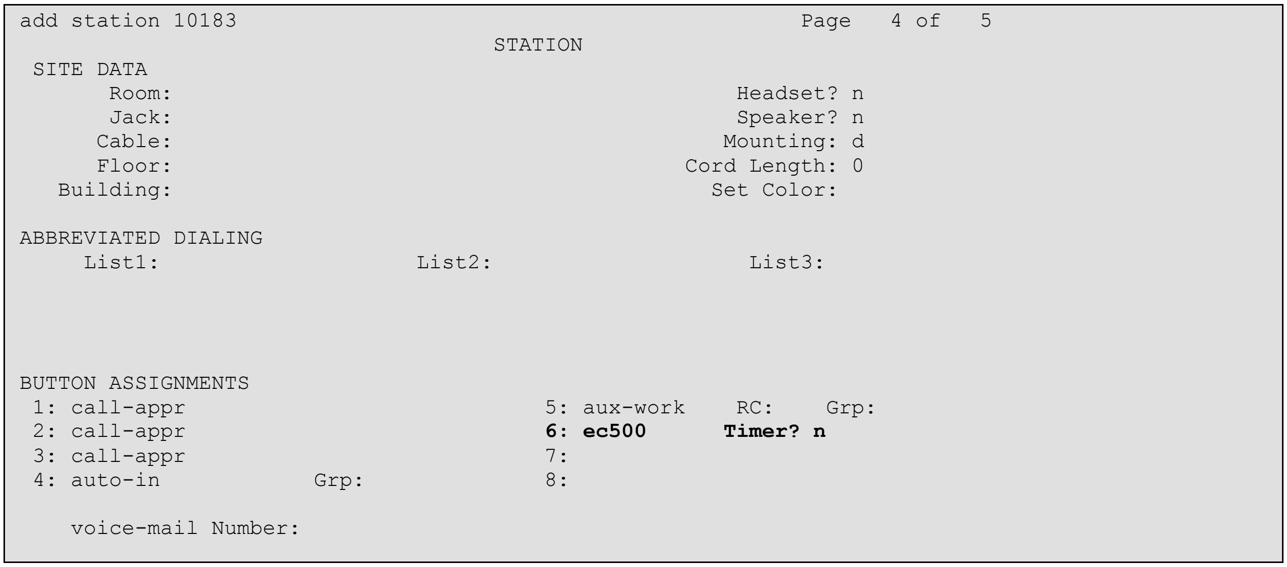
Parameter	Usage
Type (Page 1)	Enter endpoint type as shown in **Table 1**.
Name (Page 1)	Enter an appropriate name to identify the station.
Security Code (Page 1)	Enter an appropriate security code for the station.
EC500 (Page 4)	Add an EC500 button to activate/deactivate EC500.

Table 10: IP Station Parameters



```
add station 10183                                            Page   1 of   5
                                     STATION

Extension: 10183                         Lock Messages? n               BCC: 0
     Type: 9630                          Security Code: 123456           TN: 1
     Port: S00007                      Coverage Path 1:                 COR: 1
     Name: extn 10183                  Coverage Path 2:                 COS: 1
                                       Hunt-to Station:
STATION OPTIONS
                                           Time of Day Lock Table:
              Loss Group: 19         Personalized Ringing Pattern: 1
                                                 Message Lamp Ext: 10183
            Speakerphone: 2-way               Mute Button Enabled? y
        Display Language: english                  Button Modules: 0
 Survivable GK Node Name:
          Survivable COR: internal                Media Complex Ext:
   Survivable Trunk Dest? y                                IP SoftPhone? n




                                              Customizable Labels? y
```

Figure 15: IP Station Form

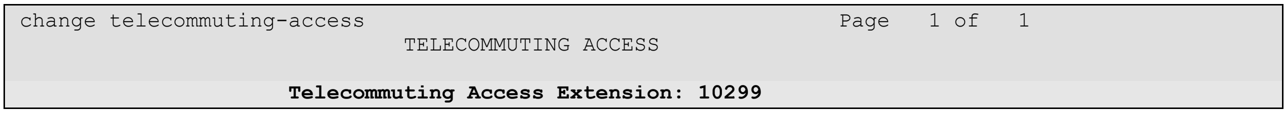


```
add station 10183                                            Page   4 of   5
                                     STATION
 SITE DATA
       Room:                                            Headset? n
       Jack:                                            Speaker? n
      Cable:                                           Mounting: d
      Floor:                                        Cord Length: 0
   Building:                                          Set Color:

ABBREVIATED DIALING
     List1:                   List2:                   List3:




BUTTON ASSIGNMENTS
 1: call-appr                           5: aux-work     RC:    Grp:
 2: call-appr                           6: ec500       Timer? n
 3: call-appr                           7:
 4: auto-in            Grp:             8:

    voice-mail Number:
```

Figure 16: IP Station Form

4.9. Configure EC500

Enter the **change telecommuting-access** command to specify an available extension that is to be dialed from mobile phones to perform EC500 commands.



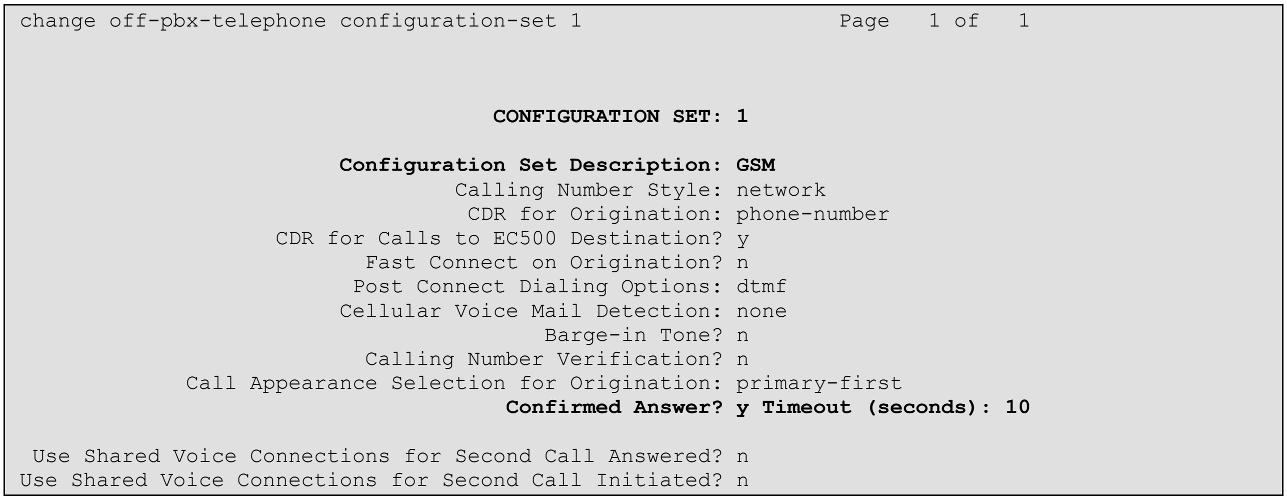
```
change telecommuting-access                                     Page   1 of   1
                              TELECOMMUTING ACCESS

                     Telecommuting Access Extension: 10299
```

Figure 17: Telecommuting-Access Form

Enter the **change off-pbx-telephone configuration-set** command to define a configuration set to be used by GSM endpoints, using the parameters shown in the following table.

Parameter	Usage
Configuration Set	Select an available configuration set number.
Configuration Set Description	Enter a descriptive name to identify the configuration set.
Confirmed Answer	Set this value to “y”, so that EC500 alarm calls to GSM endpoints must be acknowledged via keypad input.
Timeout	Select an appropriate time to accommodate human response time.

Table 11: EC500 Feature Access Code Parameters



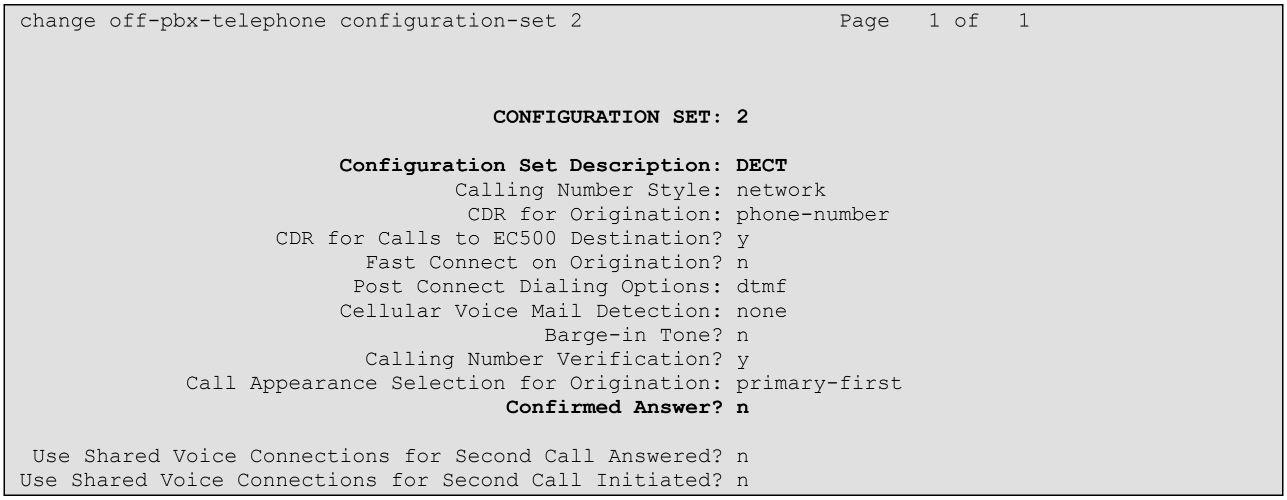
```
change off-pbx-telephone configuration-set 1                    Page   1 of   1



                                     CONFIGURATION SET: 1

                         Configuration Set Description: GSM
                                  Calling Number Style: network
                                   CDR for Origination: phone-number
                    CDR for Calls to EC500 Destination? y
                           Fast Connect on Origination? n
                          Post Connect Dialing Options: dtmf
                         Cellular Voice Mail Detection: none
                                        Barge-in Tone? n
                           Calling Number Verification? n
             Call Appearance Selection for Origination: primary-first
                                     Confirmed Answer? y Timeout (seconds): 10

 Use Shared Voice Connections for Second Call Answered? n
Use Shared Voice Connections for Second Call Initiated? n
```

Figure 18: GSM Off-Pbx-Telephone Configuration-Set Form

Enter the **change off-pbx-telephone configuration-set** command to define a configuration set to be used by DECT endpoints, using the parameters shown in the following table.

Parameter	Usage
Configuration Set	Select an available configuration set number.
Configuration Set Description	Enter a descriptive name to identify the configuration set.
Confirmed Answer	Set this value to “n”, so that EC500 alarm calls to DECT endpoints need not be acknowledged via keypad input.

Table 12: EC500 Feature Access Code Parameters



```
change off-pbx-telephone configuration-set 2                    Page   1 of   1



                                    CONFIGURATION SET: 2

                        Configuration Set Description: DECT
                                 Calling Number Style: network
                                  CDR for Origination: phone-number
                    CDR for Calls to EC500 Destination? y
                           Fast Connect on Origination? n
                          Post Connect Dialing Options: dtmf
                         Cellular Voice Mail Detection: none
                                        Barge-in Tone? n
                           Calling Number Verification? y
              Call Appearance Selection for Origination: primary-first
                                     Confirmed Answer? n

 Use Shared Voice Connections for Second Call Answered? n
Use Shared Voice Connections for Second Call Initiated? n
```

Figure 19: DECT Off-Pbx-Telephone Configuration-Set Form

Enter the **change off-pbx-telephone station-mapping** command for the extension to be paired to GSM endpoints, and enter the parameters shown in the table below.

Parameter	Usage
Application	Enter “EC500”.
Phone Number	Enter the number of the GSM phone which is to be coupled with this extension. Do not include an additional leading “0” to select ARS.
Trunk Selection	Enter “ARS”.
Config Set	Enter the number of the “GSM” configuration set which was configured in **Figure 18**.

Table 13: EC500 Feature Access Code Parameters

```
change off-pbx-telephone station-mapping 10183                  Page   1 of   3
                  STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station       Application Dial   CC  Phone Number    Trunk       Config  Dual
 Extension                 Prefix                     Selection   Set     Mode
 10183            EC500        -      02222222222      ARS        1
```

Figure 20: GSM Off-Pbx-Telephone Station-Mapping Form (Page 1)

Enter the **change off-pbx-telephone station-mapping** command for the extension to be paired to DECT endpoints, and enter the parameters shown in the table below.

Parameter	Usage
Application	Enter “EC500”.
Phone Number	Enter the number of the DECT phone which is to be coupled with this extension.
Trunk Selection	Enter the number of the DECT base station trunk.
Config Set	Enter the number of the configuration “DECT” set which was configured in **Figure 19**.

Table 14: EC500 Feature Access Code Parameters

```
change change off-pbx-telephone station-mapping 10094                  Page   1 of   3
                  STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station       Application Dial   CC  Phone Number    Trunk       Config  Dual
 Extension                 Prefix                     Selection   Set     Mode
 10094            EC500        -      10304            8          2
```

Figure 21: DECT Off-Pbx-Telephone Station-Mapping Form (Page 1)

4.10. Configure Trunk Interfaces

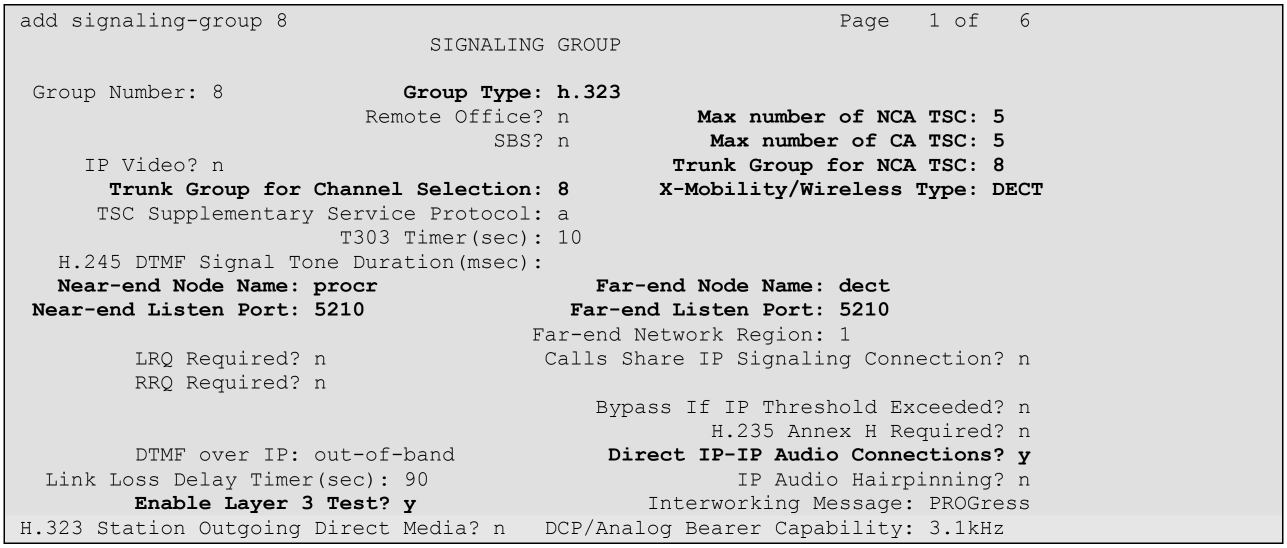
4.10.1. Interface to Avaya R4

The signaling group and trunk group described in this section are closely interrelated. If the signaling group is allocated first, all trunk group parameters must initially be set to blank and entered in a subsequent step, after the trunk group has been added.

Use the **add signaling-group** command to allocate a signaling group for interface to the Avaya R4 using the following parameters:

Parameter	Usage
Group Type	Enter "h.323".
Max number of NCA TSC	Enter a value of 1 or greater.
Max number of CA TSC	Enter a value of 1 or greater.
Trunk Group for NCA TSC	Enter the number of the DECT trunk group allocated in **Figure 23**.
X-Mobility/Wireless Type	Enter "DECT".
Trunk Group for Channel Selection	Enter the number of the DECT trunk group allocated in **Figure 23**.
Near-end Node Name	Enter "procr" to designate the S8300 processor as the near end node name.
Far-end Node Name	Enter "dect" to assign the Avaya R4 base station as the far end node name.
Near-end Listen Port	Specify an otherwise unused port to be used to listen for incoming voice traffic.
Far-end Listen Port	Specify the port assigned to the Avaya R4 as "Local Port" in **Figure 59**.
Direct IP-IP Audio Connections	Enter "y" to allow direct IP-IP endpoint connections (shuffling).

Table 15: Avaya R4 Signaling-Group Parameters



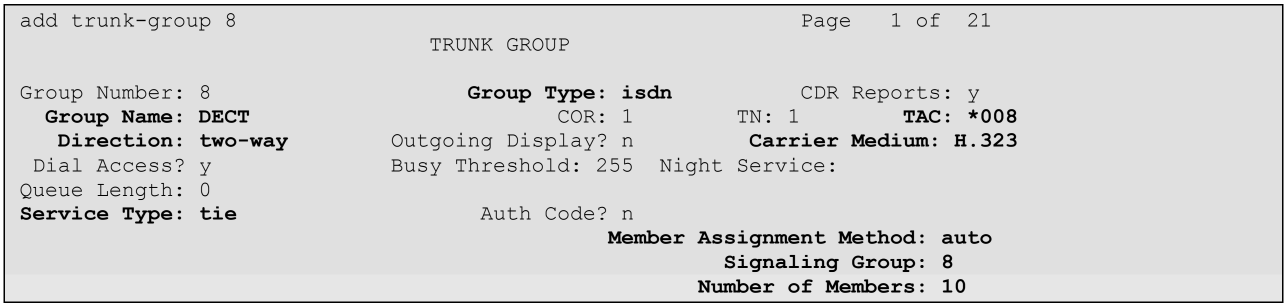
```
add signaling-group 8                                           Page   1 of   6
                                SIGNALING GROUP

 Group Number: 8             Group Type: h.323
                          Remote Office? n         Max number of NCA TSC: 5
                                    SBS? n          Max number of CA TSC: 5
     IP Video? n                                 Trunk Group for NCA TSC: 8
       Trunk Group for Channel Selection: 8       X-Mobility/Wireless Type: DECT
      TSC Supplementary Service Protocol: a
                        T303 Timer(sec): 10
   H.245 DTMF Signal Tone Duration(msec):
   Near-end Node Name: procr                 Far-end Node Name: dect
 Near-end Listen Port: 5210                Far-end Listen Port: 5210
                                        Far-end Network Region: 1
        LRQ Required? n                  Calls Share IP Signaling Connection? n
        RRQ Required? n
                                             Bypass If IP Threshold Exceeded? n
                                                      H.235 Annex H Required? n
        DTMF over IP: out-of-band             Direct IP-IP Audio Connections? y
  Link Loss Delay Timer(sec): 90                        IP Audio Hairpinning? n
        Enable Layer 3 Test? y                    Interworking Message: PROGress
H.323 Station Outgoing Direct Media? n   DCP/Analog Bearer Capability: 3.1kHz
```

Figure 22: Avaya R4 Signaling-Group Form

Use the **add trunk-group <n>** command, where <n> is an unused trunk number, to allocate a trunk group to be used as an interface to the Belgacom VoIP Access SIP Service. Use the parameters show in the following table.

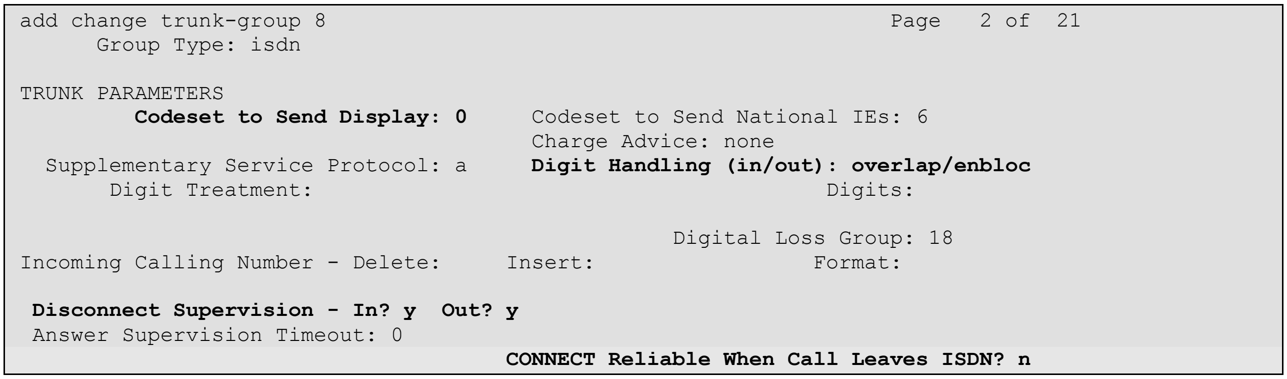
Parameter	Usage
Group Type (Page 1)	Enter “isdn”.
Group Name (Page 1)	Assign a name for identification purposes.
TAC (Page 1)	Enter the Trunk Access Code to be used to identify this trunk.
Direction (Page 1)	Enter “two-way”.
Carrier Medium (Page 1)	Enter “H.323”.
Service Type (Page 1)	Enter “tie”.
Member Assignment Method (Page 1)	Enter “auto”.
Signaling Group (Page 1)	Enter number of the signaling group allocated in Figure 22.
Number of Members (Page 1)	Enter a number large enough to support the maximum number of anticipated simultaneous calls to be made via the DECT trunk.
Codeset to Send Display (Page 2)	Enter “0”.
Digit Handling (in/out) (Page 2)	Enter “overlap/enbloc”
Disconnect Supervision In / Out (Page 2)	Enter “y” / “y”.
CONNECT Reliable When Call Leaves ISDN (Page 2)	Enter “n”.
NCA-TSC Trunk Member (Page 3)	Enter “1”.
Send Calling Number (Page 3)	Enter “y”.
Format (Page 3)	Enter “unk-pvt”
Send Connected Number (Page 3)	Enter “y”.

Table 16: Avaya R4 Trunk-Group Parameters



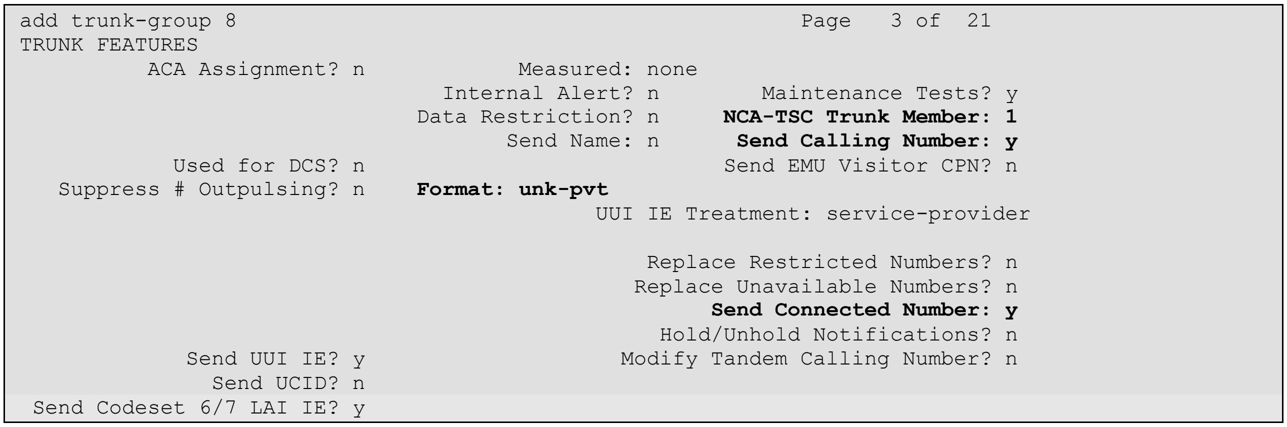
```
add trunk-group 8                                              Page   1 of  21
                                TRUNK GROUP

Group Number: 8                  Group Type: isdn          CDR Reports: y
  Group Name: DECT                      COR: 1        TN: 1        TAC: *008
   Direction: two-way        Outgoing Display? n        Carrier Medium: H.323
 Dial Access? y              Busy Threshold: 255  Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n
                                            Member Assignment Method: auto
                                                     Signaling Group: 8
                                                   Number of Members: 10
```

Figure 23: Avaya R4 Trunk-Group Form, Page 1



```
add change trunk-group 8                                            Page   2 of  21
      Group Type: isdn

TRUNK PARAMETERS
         Codeset to Send Display: 0     Codeset to Send National IEs: 6
                                        Charge Advice: none
  Supplementary Service Protocol: a     Digit Handling (in/out): overlap/enbloc
       Digit Treatment:                                        Digits:

                                                   Digital Loss Group: 18
Incoming Calling Number - Delete:     Insert:                 Format:

 Disconnect Supervision - In? y  Out? y
 Answer Supervision Timeout: 0
                                      CONNECT Reliable When Call Leaves ISDN? n
```

Figure 24: Avaya R4 Trunk-Group Form, Page 2



```
add trunk-group 8                                            Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                 Internal Alert? n       Maintenance Tests? y
                               Data Restriction? n     NCA-TSC Trunk Member: 1
                                      Send Name: n      Send Calling Number: y
            Used for DCS? n                            Send EMU Visitor CPN? n
   Suppress # Outpulsing? n    Format: unk-pvt
                                             UUI IE Treatment: service-provider

                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n
                                                      Send Connected Number: y
                                                  Hold/Unhold Notifications? n
             Send UUI IE? y                    Modify Tandem Calling Number? n
               Send UCID? n
 Send Codeset 6/7 LAI IE? y
```

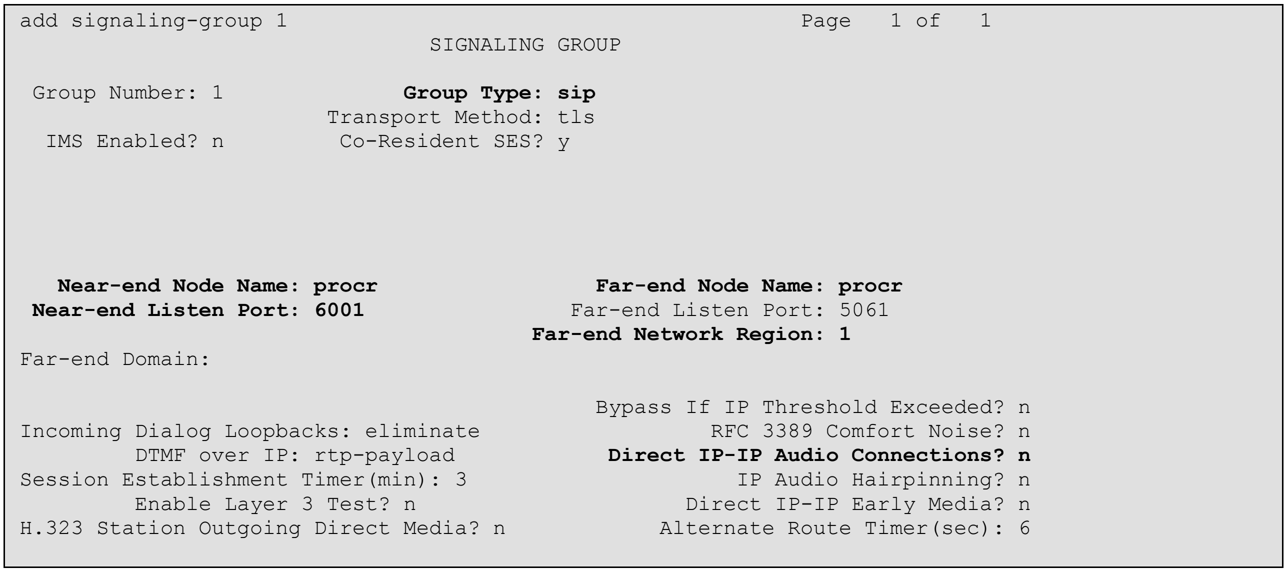
Figure 25: Avaya R4 Trunk-Group Form, Page 3

4.10.2. Configure SIP Interface to Avaya SES

Use the **add signaling-group** command to configure the Signaling Group parameters for the SIP trunk group. Assign values for this command as shown in the following table.

Parameter	Usage
Group Type	Enter the Group Type as “sip”.
Near-end Node Name	Enter “procr”.
Near-end Listen Port	Enter “6001”. This must be the same value which is assigned to the SES contact shown in **Figure 44**.
Far-end Node Name	Enter “procr”.
Far-end Network Region	Enter “1”.
Far-end Domain	Enter a blank value.
Direct IP-IP Audio Connections	Enter “n”, as the AMX does not support SIP re-invites used by Communication Manager for Direct IP-IP Audio Connections.

Table 17: Signaling-Group Parameters for SIP Interface



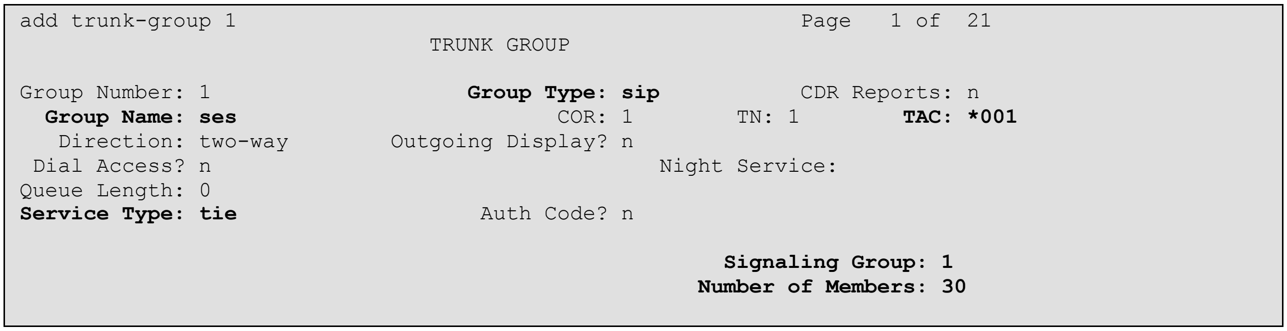
```
add signaling-group 1                                          Page   1 of   1
                                SIGNALING GROUP

 Group Number: 1              Group Type: sip
                        Transport Method: tls
  IMS Enabled? n         Co-Resident SES? y





   Near-end Node Name: procr                Far-end Node Name: procr
 Near-end Listen Port: 6001               Far-end Listen Port: 5061
                                       Far-end Network Region: 1
Far-end Domain:

                                            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? n                      Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n             Alternate Route Timer(sec): 6
```

Figure 26: Avaya SES Signaling-Group Form

Use the **add trunk-group** command to configure the SIP interface to Avaya SES. Assign values for this command as shown in the following table.

Parameter	Usage
Group Type	Specify the Group Type as "sip".
Group Name	Select an appropriate name to identify the device.
TAC	Specify a trunk access code that can be used to provide dial access to the trunk group. This code must be defined in **Figure 10.**
Service Type	Designate the trunk as a "tie" line to a peer system.
Signaling Group	Enter the number assigned to the SIP signaling group shown in **Figure 26**.
Number of Members	Specify sufficient number of members to support the maximum simultaneous connections required.

Table 18: Trunk-Group Parameters for the SIP Interface



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

Group Number: 1                    Group Type: sip           CDR Reports: n
  Group Name: ses                         COR: 1        TN: 1        TAC: *001
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n

                                                       Signaling Group: 1
                                                     Number of Members: 30
```

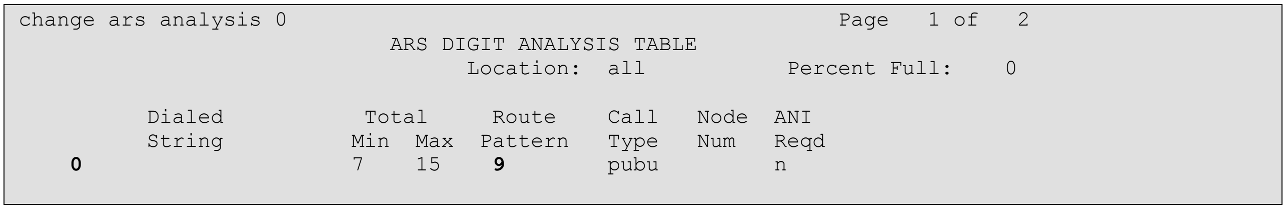
Figure 27: Trunk-Group Screen Form

4.11. Configure Call Routing

Routing for calls to DECT stations was done when the DECT station was configured, by inserting the DECT trunk number into the station form in **Figure 14**.

4.11.1. Outgoing Calls to PSTN

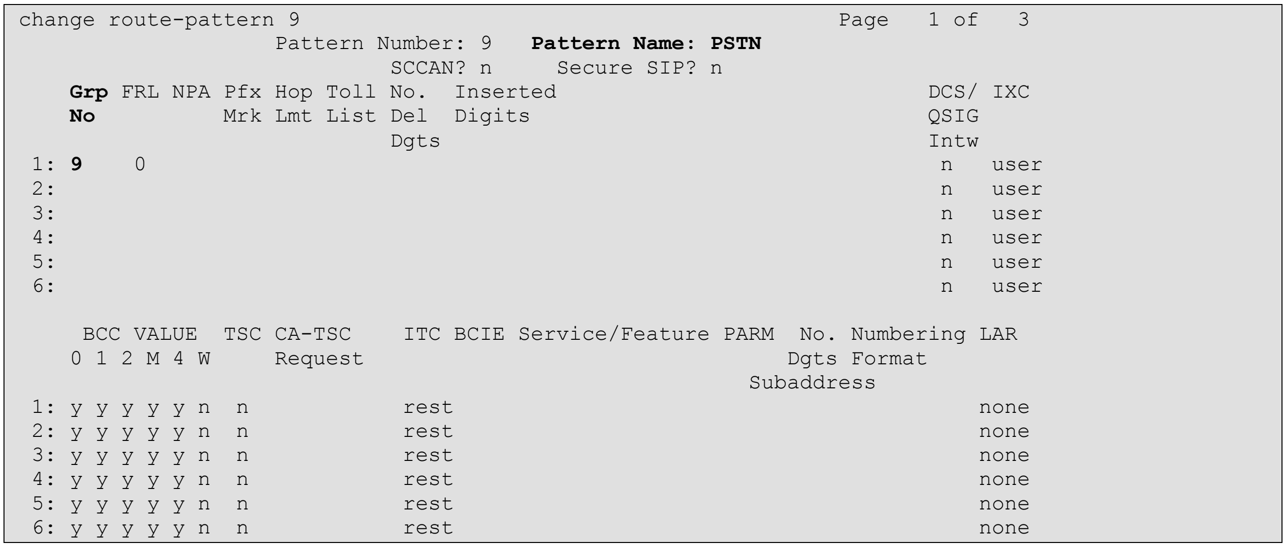
Use the **change ars analysis** command to designate that all numbers beginning with "0", be routed to the PSTN via route pattern "9".



```
change ars analysis 0                                           Page   1 of   2
                             ARS DIGIT ANALYSIS TABLE
                                   Location:  all           Percent Full:    0

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    0                     7    15    9        pubu         n
```

Figure 28: Ars Analysis Form

Use the **change route-pattern** command to designate that calls routing pattern 9 should routed to trunk 9, the PSTN trunk.

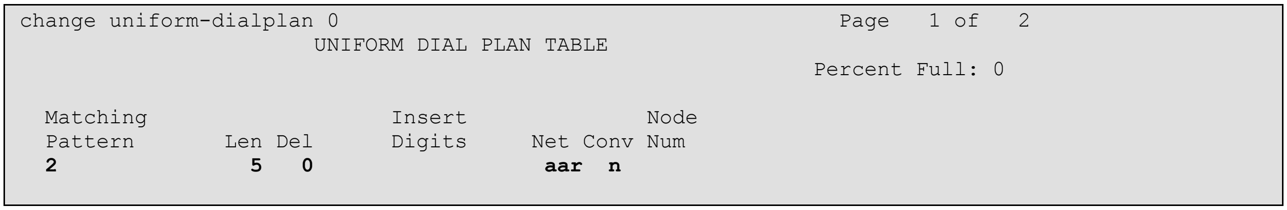


```
change route-pattern 9                                          Page   1 of   3
                    Pattern Number: 9   Pattern Name: PSTN
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                             DCS/ IXC
    No          Mrk Lmt List Del  Digits                               QSIG
                             Dgts                                      Intw
 1: 9    0                                                              n   user
 2:                                                                     n   user
 3:                                                                     n   user
 4:                                                                     n   user
 5:                                                                     n   user
 6:                                                                     n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                Dgts Format
                                                        Subaddress
 1: y y y y y n  n            rest                                        none
 2: y y y y y n  n            rest                                        none
 3: y y y y y n  n            rest                                        none
 4: y y y y y n  n            rest                                        none
 5: y y y y y n  n            rest                                        none
 6: y y y y y n  n            rest                                        none
```

Figure 29: PSTN Route Pattern Form

4.11.2. Outgoing Calls to ATT AMX Alarm Management Server

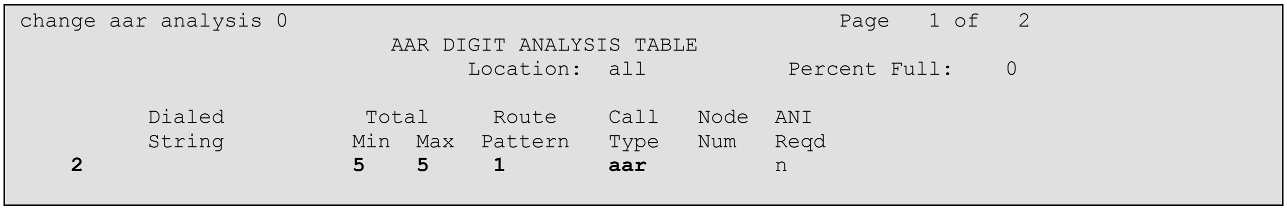
Use the **change uniform-dialplan** command to specify that calls to extensions allocated to AMX, are to be processed by Automatic Alternate Routing (aar).



```
change uniform-dialplan 0                                       Page   1 of   2
                       UNIFORM DIAL PLAN TABLE
                                                              Percent Full: 0

  Matching                   Insert             Node
  Pattern       Len Del      Digits     Net Conv Num
  2               5   0                  aar  n
```

Figure 30: AMX Uniform Dialplan Configuration

Use the **change aar analysis** command to select a route pattern for calls to AMX extensions.



```
change aar analysis 0                                           Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location:  all          Percent Full:    0

          Dialed           Total     Route     Call   Node  ANI
          String          Min  Max  Pattern    Type   Num   Reqd
    2                     5    5     1         aar          n
```

Figure 31: AMX Aar Analysis Configuration

Use the **change route-pattern** command to designate that calls to the AMX should be routed to the SES trunk, configured in **Section 4.10.2.**

```
change route-pattern 1                                          Page   1 of   3
                    Pattern Number: 1   Pattern Name: SES
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                             DCS/ IXC
    No          Mrk Lmt List Del  Digits                               QSIG
                             Dgts                                      Intw
 1: 1    0                                                              n   user
 2:                                                                     n   user
 3:                                                                     n   user
 4:                                                                     n   user
 5:                                                                     n   user
 6:                                                                     n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                Dgts Format
                                                        Subaddress
 1: y y y y y n  n            rest                                         none
 2: y y y y y n  n            rest                                         none
 3: y y y y y n  n            rest                                         none
 4: y y y y y n  n            rest                                         none
 5: y y y y y n  n            rest                                         none
 6: y y y y y n  n            rest                                         none
```

Figure 32: PSTN Route Pattern Form

4.12. Configure Number Treatment

Use the **change public-unknown-numbering** command to specify that the extension is to be used as the Calling Party Number for the AMX trunk, and to be preceded by the PSTN prefix for the PSTN trunk.

```
change public-unknown-numbering 0                               Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext           Trk       CPN             CPN
Len Code          Grp(s)    Prefix          Len
                                                     Total Administered: 1
 5  1             9         6990739887      15          Maximum Entries: 240
 5  1             1                         5
```

Figure 33: Public-Unknown-Numbering Configuration

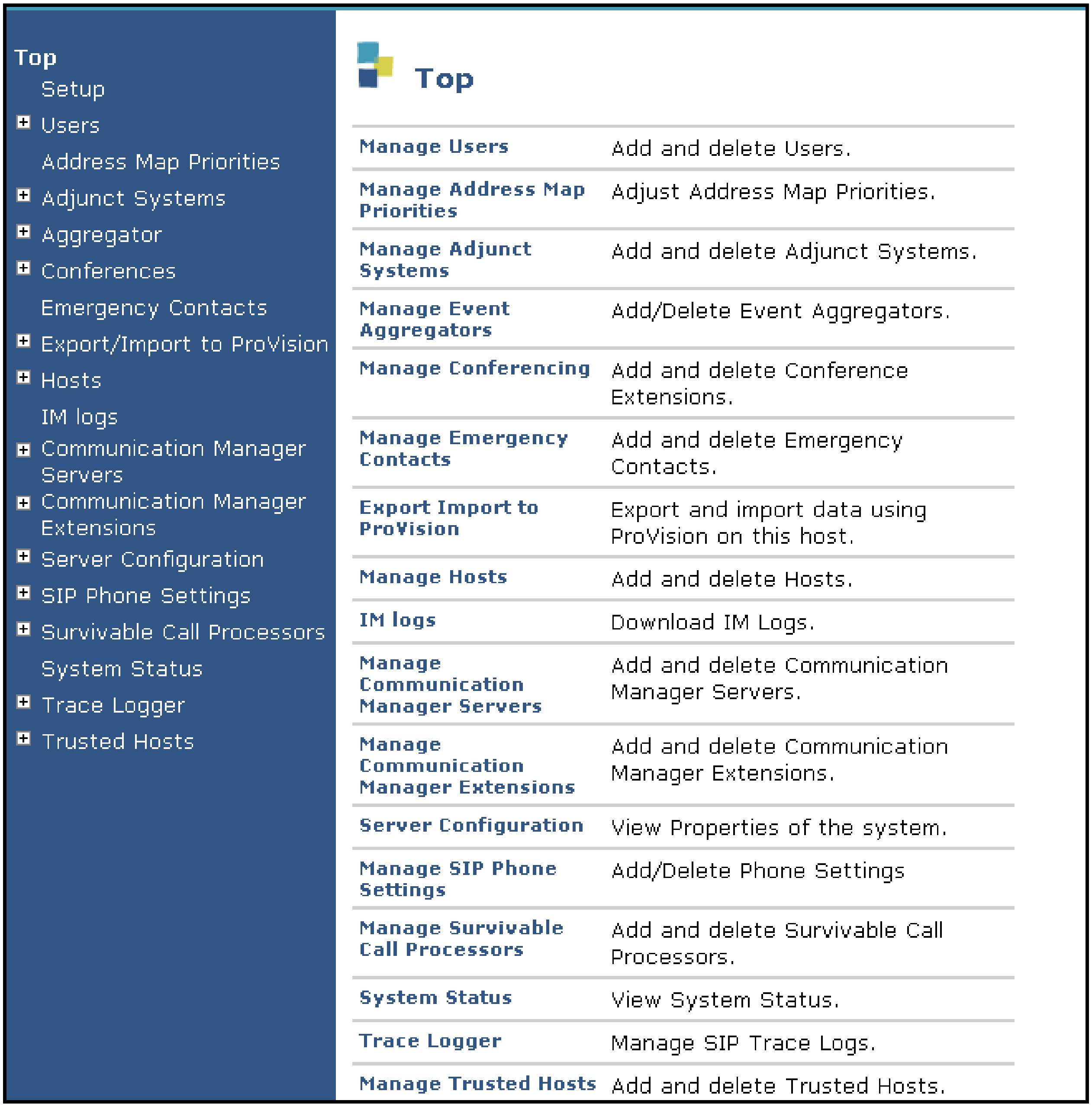
Use the **inc-call-handling-trmt trunk-group** command to insert the Priority Call feature code (defined in **Figure 11**) so that all calls arriving from the AMX trunk will be treated as Priority Calls.

```
change inc-call-handling-trmt trunk-group 1                     Page   1 of   3
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 tie             5  1                    *80
```

Figure 34: Public-Unknown-Numbering Configuration

5. Configure Avaya Aura® SIP Enablement Services

Configure SIP Enablement Service by navigating to the Communication Manager home page and logging in with the appropriate credentials (not shown). Select "SIP Enablement Services" from the "Administration" menu (not shown), to display the following screen content:



Top

Manage Users	Add and delete Users.
Manage Address Map Priorities	Adjust Address Map Priorities.
Manage Adjunct Systems	Add and delete Adjunct Systems.
Manage Event Aggregators	Add/Delete Event Aggregators.
Manage Conferencing	Add and delete Conference Extensions.
Manage Emergency Contacts	Add and delete Emergency Contacts.
Export Import to ProVision	Export and import data using ProVision on this host.
Manage Hosts	Add and delete Hosts.
IM logs	Download IM Logs.
Manage Communication Manager Servers	Add and delete Communication Manager Servers.
Manage Communication Manager Extensions	Add and delete Communication Manager Extensions.
Server Configuration	View Properties of the system.
Manage SIP Phone Settings	Add/Delete Phone Settings
Manage Survivable Call Processors	Add and delete Survivable Call Processors.
System Status	View System Status.
Trace Logger	Manage SIP Trace Logs.
Manage Trusted Hosts	Add and delete Trusted Hosts.

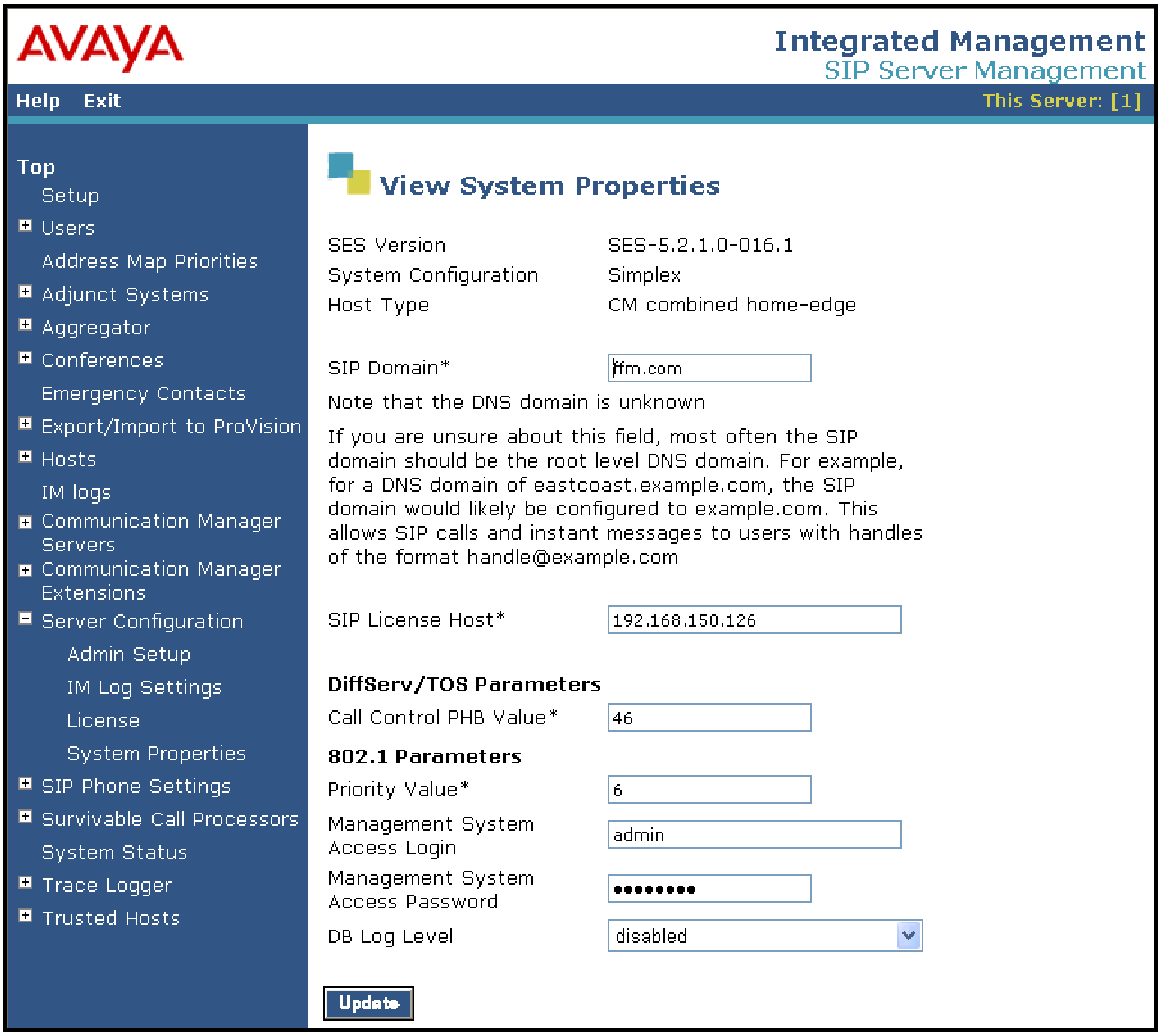
Figure 35: SIP Enablement Service "Top" Configuration Screen

5.1. Server Configuration

Select “System Properties” from the “Server Configuration” menu from the left pane of the screen. Enter values in this screen as shown in the following table:

Parameter	Usage
SIP Domain	Enter SIP domain name. This should be the same name as is configured for the “Authoritative Domain” parameter for the IP Network Region shown in **Figure 9**.
License Host	Enter the IP address of the license host, in this case the IP address of the SES server.

Table 19: Parameters for System Properties



View System Properties

SES Version SES-5.2.1.0-016.1
System Configuration Simplex
Host Type CM combined home-edge

SIP Domain* ffm.com
Note that the DNS domain is unknown

If you are unsure about this field, most often the SIP domain should be the root level DNS domain. For example, for a DNS domain of eastcoast.example.com, the SIP domain would likely be configured to example.com. This allows SIP calls and instant messages to users with handles of the format handle@example.com

SIP License Host* 192.168.150.126

DiffServ/TOS Parameters
Call Control PHB Value* 46

802.1 Parameters
Priority Value* 6
Management System Access Login admin
Management System Access Password ●●●●●●●●
DB Log Level disabled

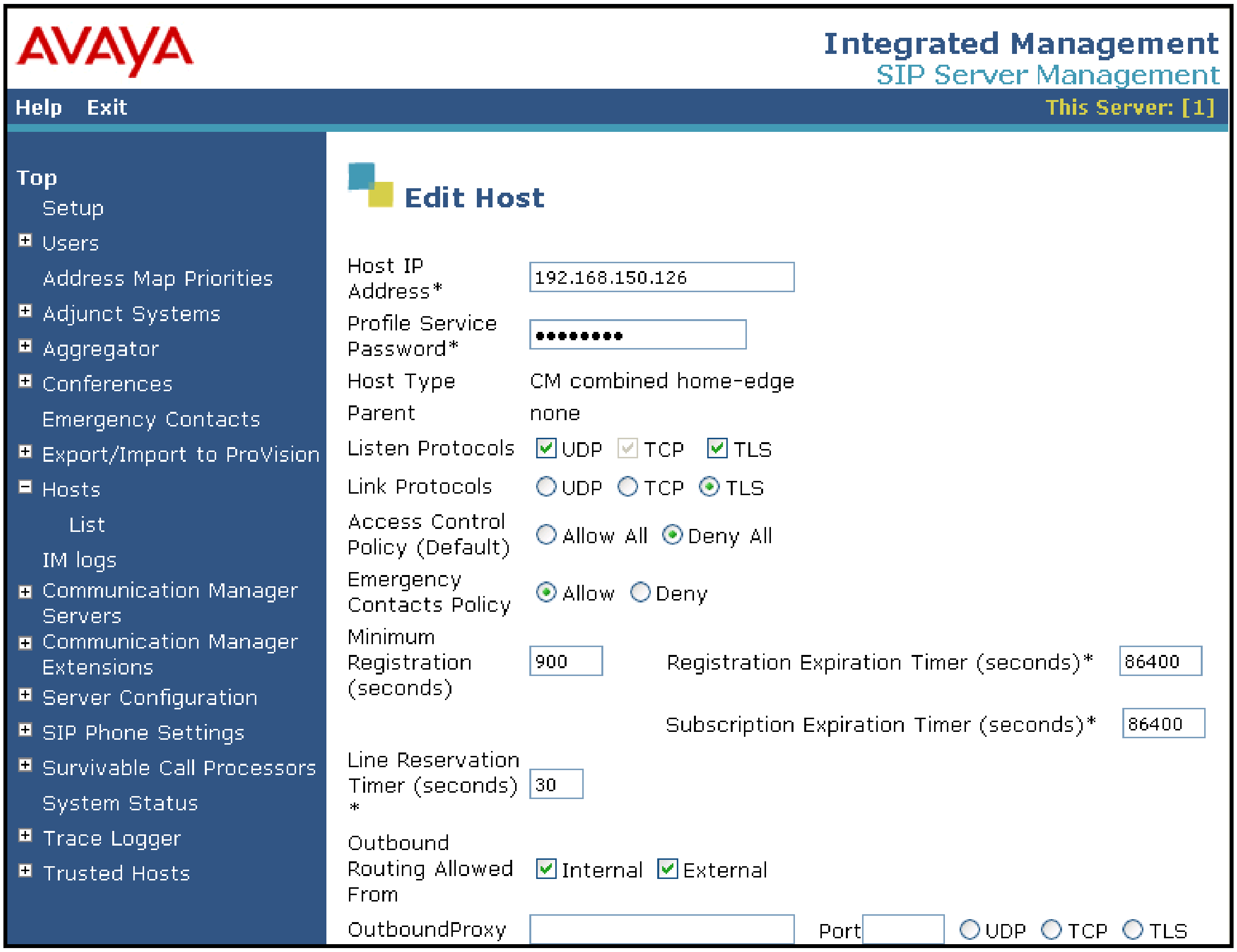
Figure 36: System Properties Screen

5.2. Add Hosts

Select "Hosts" → "Add Host" from the left pane of the top level screen shown in **Figure 35**. Enter values in this screen as shown in the following table, accepting the default values for those parameters which are not listed.

Parameter	Usage
Host IP Address	Enter the IP address of the SES server.
Profile Service Password	Enter the password which was entered from the initial setup script when SES was installed.

Table 20: "Add Host" Parameters

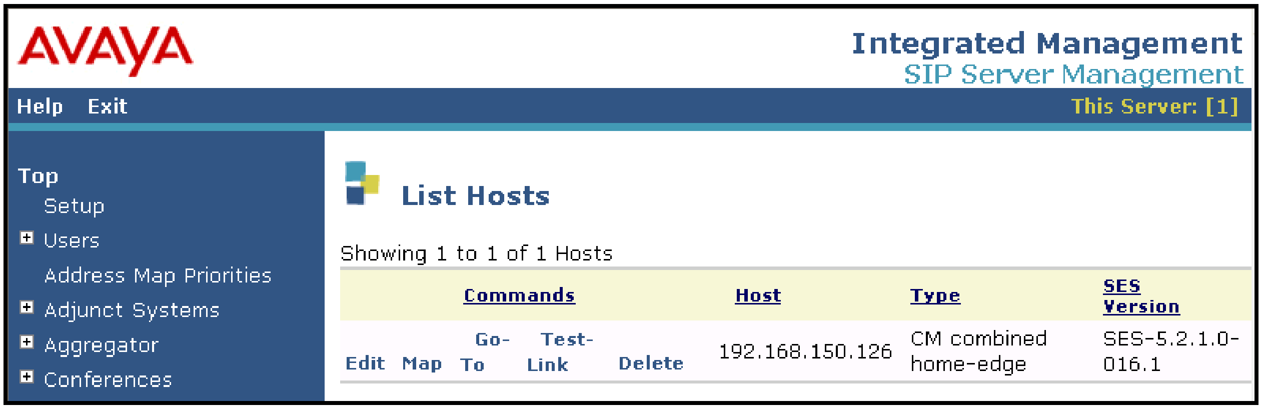


Edit Host

Host IP Address*	192.168.150.126
Profile Service Password*	••••••••
Host Type	CM combined home-edge
Parent	none
Listen Protocols	☑ UDP ☑ TCP ☑ TLS
Link Protocols	○ UDP ○ TCP ● TLS
Access Control Policy (Default)	○ Allow All ● Deny All
Emergency Contacts Policy	● Allow ○ Deny
Minimum Registration (seconds)	900
Registration Expiration Timer (seconds)*	86400
Subscription Expiration Timer (seconds)*	86400
Line Reservation Timer (seconds) *	30
Outbound Routing Allowed From	☑ Internal ☑ External
OutboundProxy	Port ○ UDP ○ TCP ○ TLS

Figure 37: Add Host Screen

Navigate to “Hosts” -> “List Hosts”. Click “Map”.



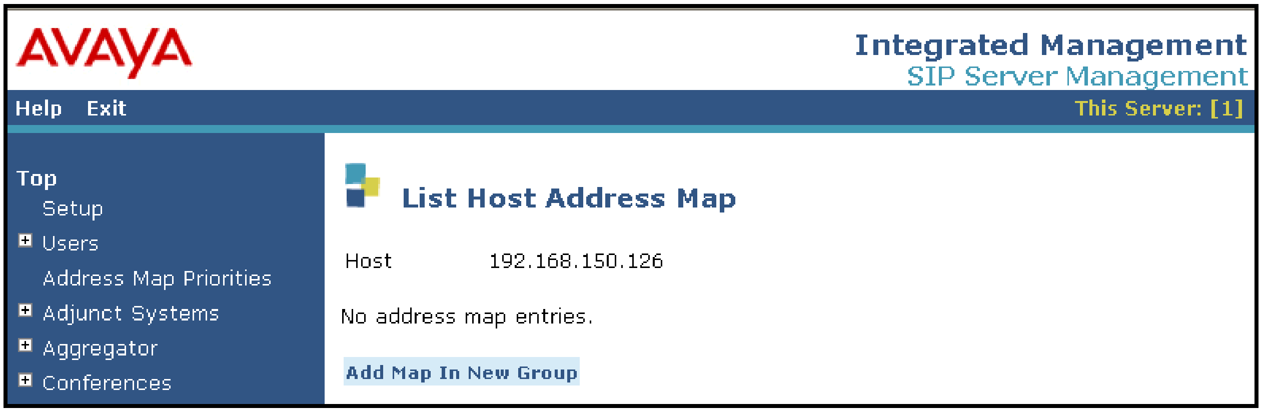
List Hosts

Showing 1 to 1 of 1 Hosts

Commands	Host	Type	SES Version
Edit Map Go-To Test-Link Delete	192.168.150.126	CM combined home-edge	SES-5.2.1.0-016.1

Figure 38: List Hosts Screen

Click “Add Map In New Group”.



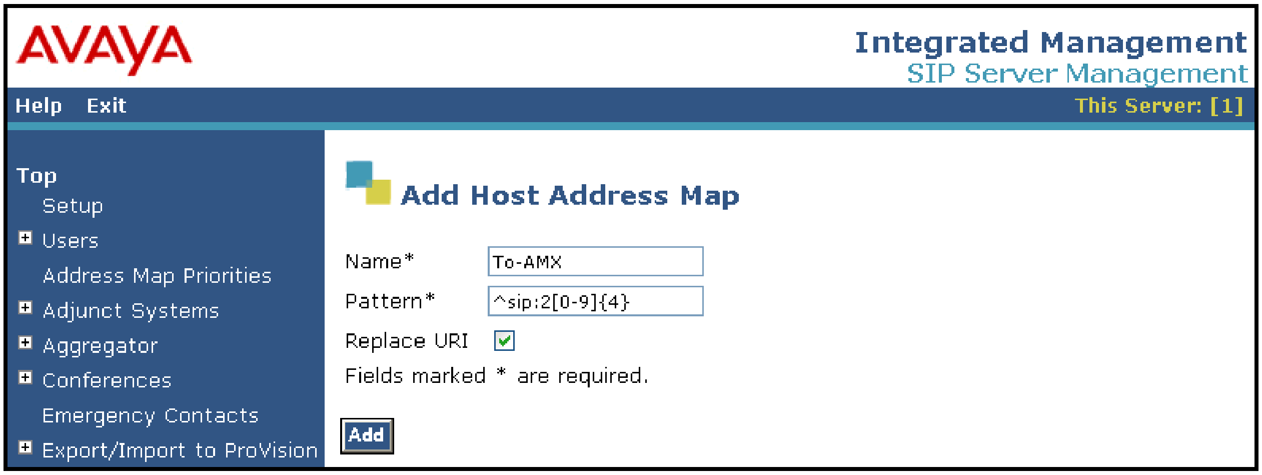
List Host Address Map

Host 192.168.150.126

No address map entries.

Figure 39: List Hosts Screen

Enter a map pattern of “^sip:2[0-9]{3} to route calls to 5-digit numbers beginning with “2” to AMX, and click “Add” followed by “Continue” (not shown).



Add Host Address Map

Name* To-AMX

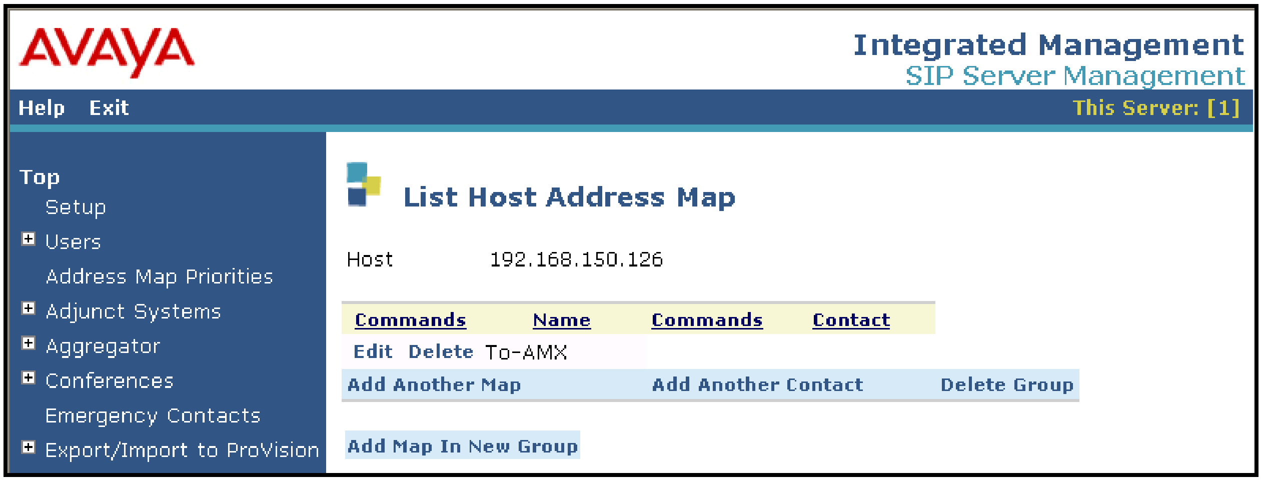
Pattern* ^sip:2[0-9]{4}

Replace URI ☑

Fields marked * are required.

Figure 40: Add Host Map Screen

Click “Add Another Contact”.



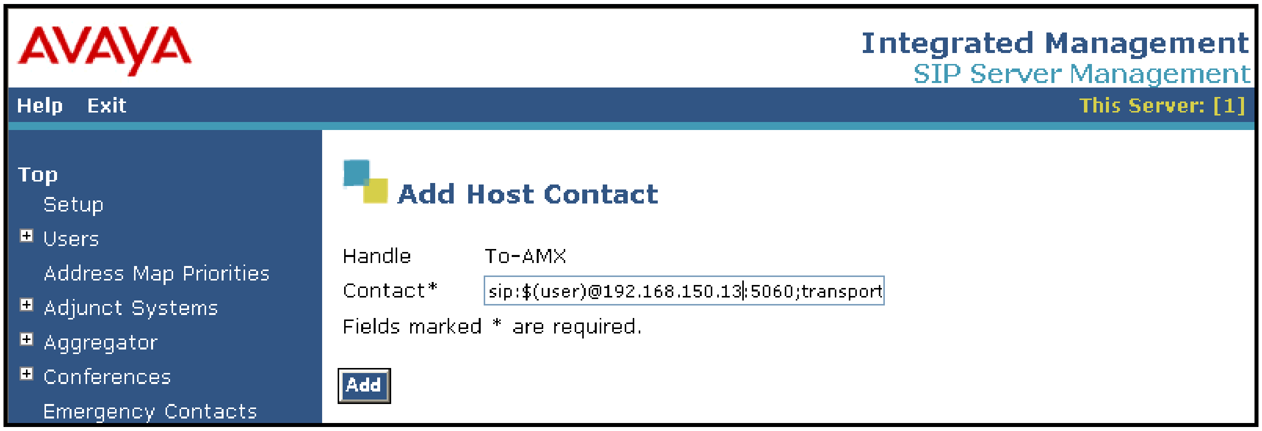
List Host Address Map

Host 192.168.150.126

Commands	Name	Commands	Contact
Edit Delete	To-AMX		

Figure 41: List Host Map Screen

Enter a contact of “sip:$(user)@<AMX-IP-address>:5060;transport=udp” and click “Add” followed by “Continue” (not shown).



Add Host Contact

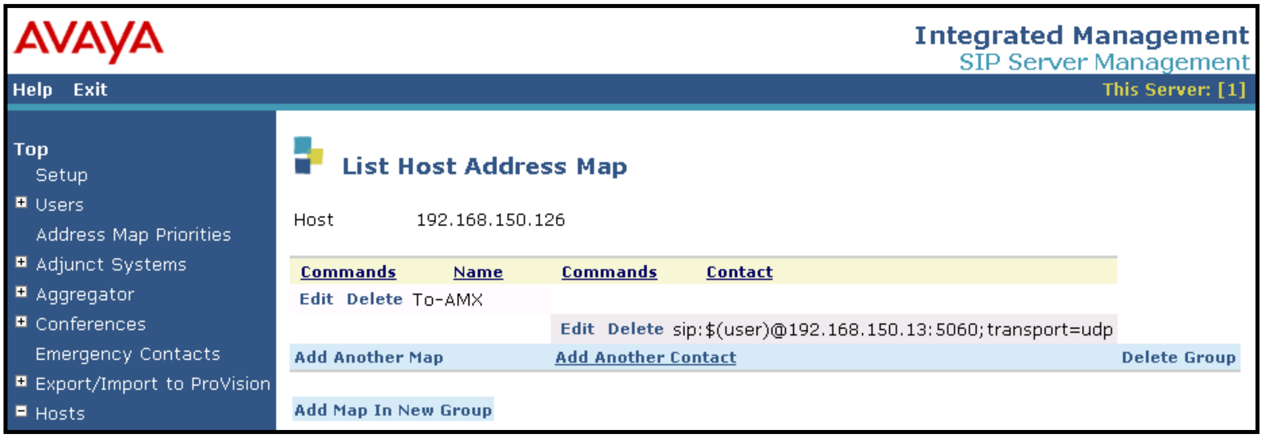
Handle To-AMX

Contact* sip:$(user)@192.168.150.13:5060;transport

Fields marked * are required.

Figure 42: AMX Contact Address Screen

The completed Host Address Map is shown below.



List Host Address Map

Host 192.168.150.126

Commands	Name	Commands	Contact
Edit Delete	To-AMX		
		Edit Delete	sip:$(user)@192.168.150.13:5060;transport=udp

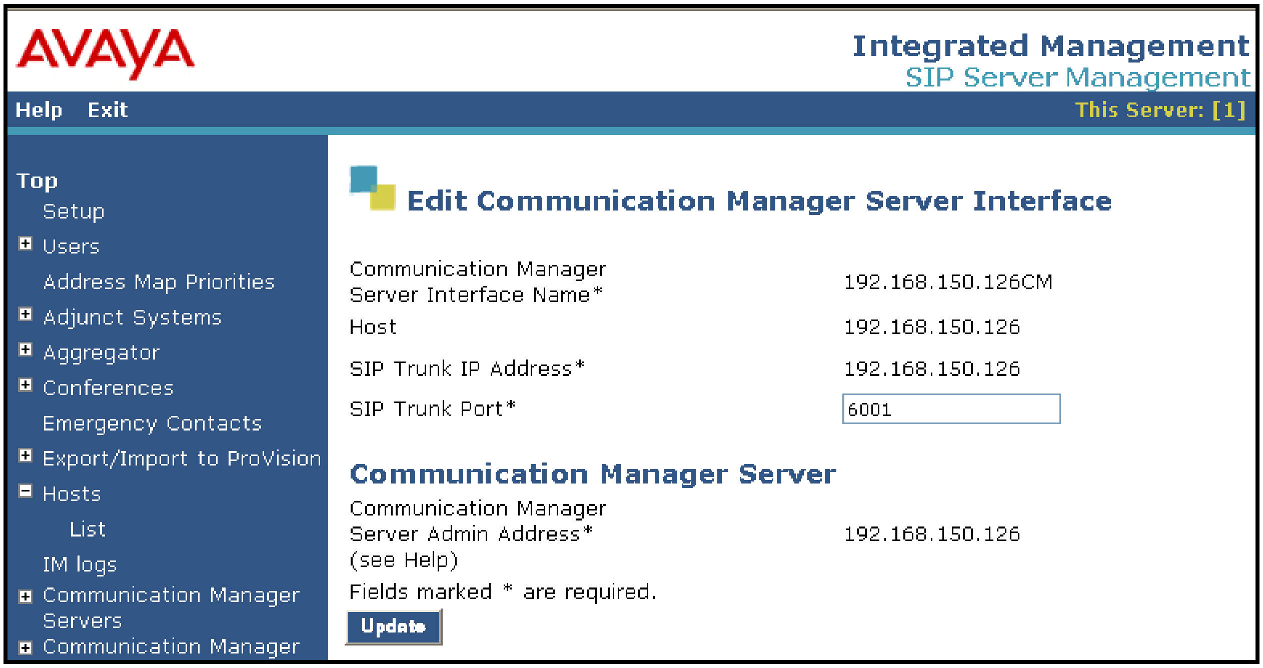
Figure 43: List Host Address Map

5.3. Add Communication Manager Server Interfaces

Select “Communication Manager Servers” → “Add” from the “Top” level menu shown in **Figure 35**, and specify the interface parameters as shown in the following table, click “Update”, followed by “Continue” (not shown).

Parameter	Usage
SIP Trunk Port	Enter the Communication Manager port to which SIP messages are to be sent. The must be the same value entered as configured for “Near-end Listen Port” in **Figure 26**.

Table 21: Add Communication Manager Server Interface Parameters



Edit Communication Manager Server Interface

Communication Manager Server Interface Name*	192.168.150.126CM
Host	192.168.150.126
SIP Trunk IP Address*	192.168.150.126
SIP Trunk Port*	6001

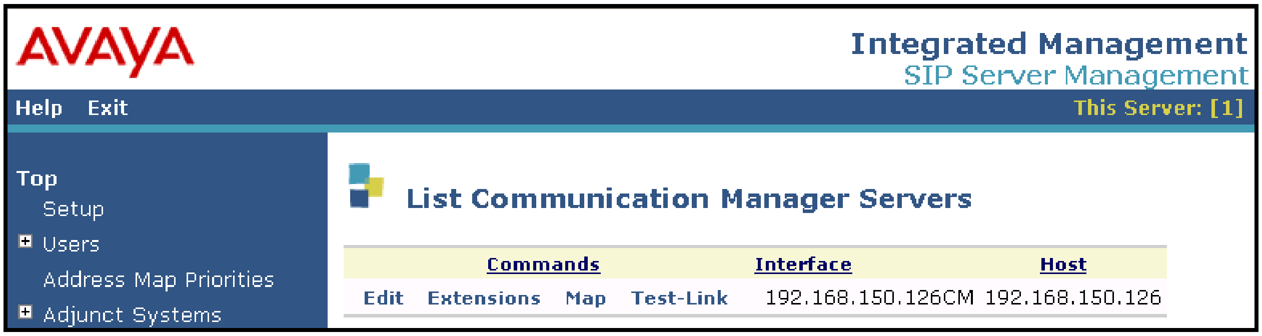
Communication Manager Server

Communication Manager Server Admin Address* (see Help)	192.168.150.126

Fields marked * are required.

Figure 44: Add Communication Manager Server Interface Screen

Select the “Map” menu point from the “List Communication Manager Servers” screen.

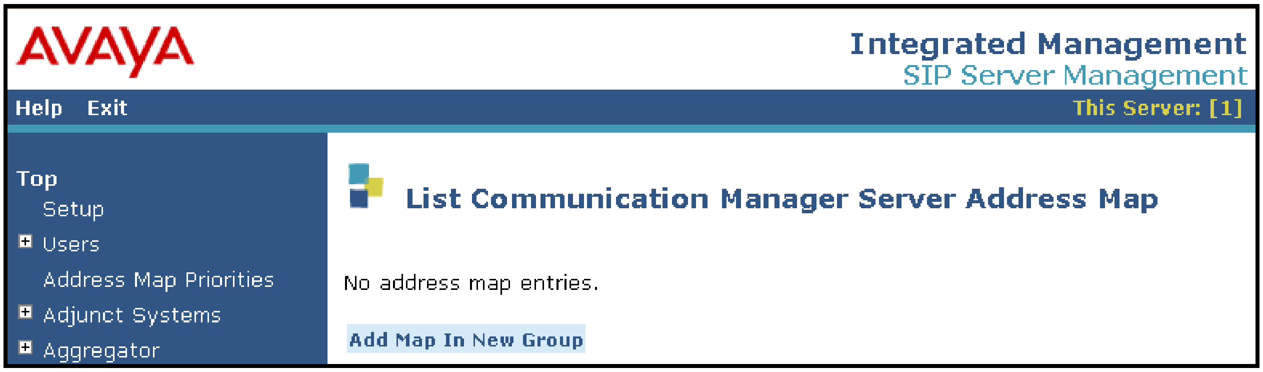


List Communication Manager Servers

Commands				Interface	Host
Edit	Extensions	Map	Test-Link	192.168.150.126CM	192.168.150.126

Figure 45: List Communication Manager Servers Screen

Click the “Add Map In New Group” control from the following screen.



List Communication Manager Server Address Map

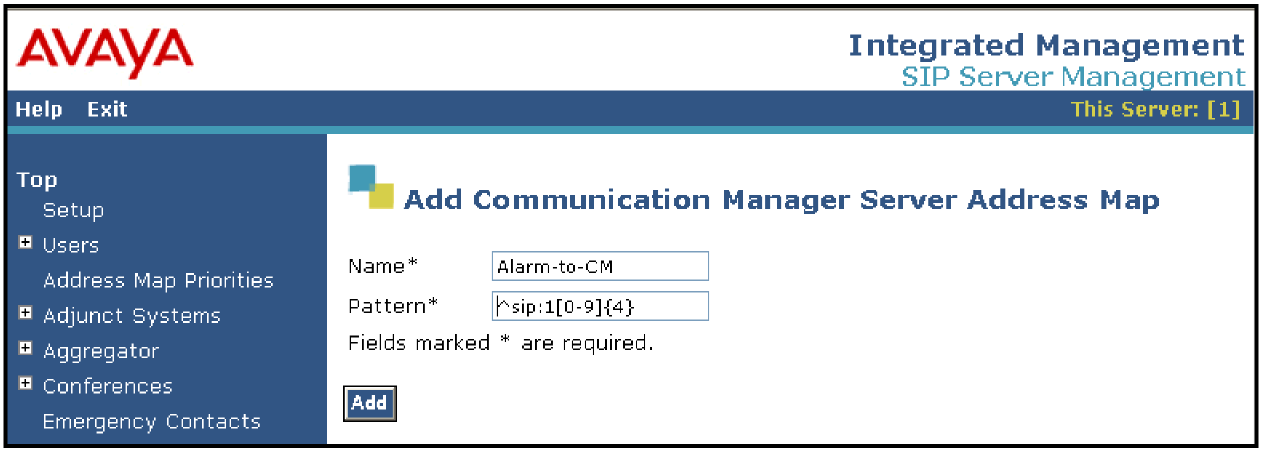
No address map entries.

Figure 46: List Communication Manager Server Address Map Screen

Enter the values shown in the following table in the “Add Communication Manager Server Address Map” screen, and click “Add” followed by “Continue” (not shown).

Parameter	Usage
Name	Enter an appropriate name to identify the map.
Pattern	Enter “^sip:1[0-9]{4} to match that called numbers for alarms from AMX.

Table 22: Add Communication Manager Server Address Map Parameters



Add Communication Manager Server Address Map

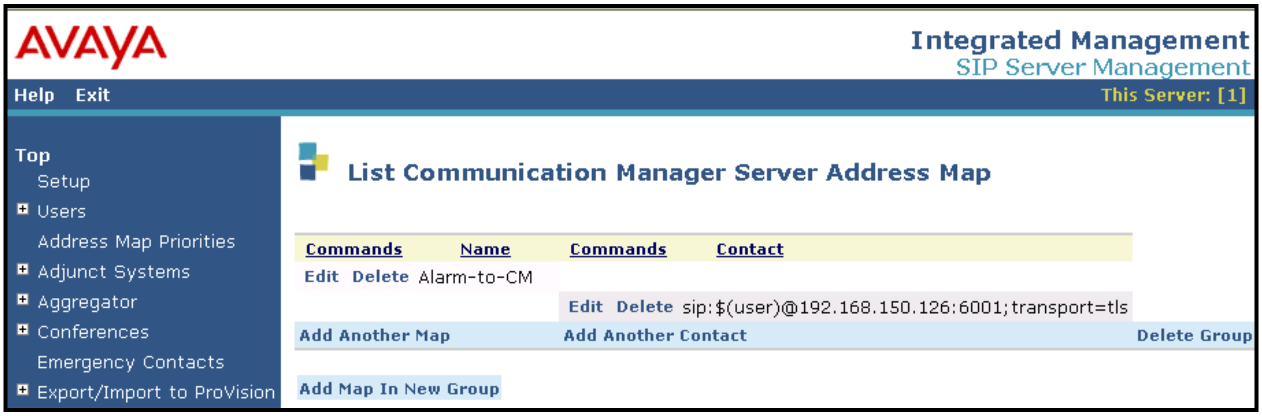
Name* Alarm-to-CM

Pattern* ^sip:1[0-9]{4}

Fields marked * are required.

Figure 47: Add Communication Manager Server Address Map

The complete Address Map is shown below.



List Communication Manager Server Address Map

Commands	Name	Commands	Contact
Edit Delete	Alarm-to-CM		
		Edit Delete	sip:$(user)@192.168.150.126:6001;transport=tls

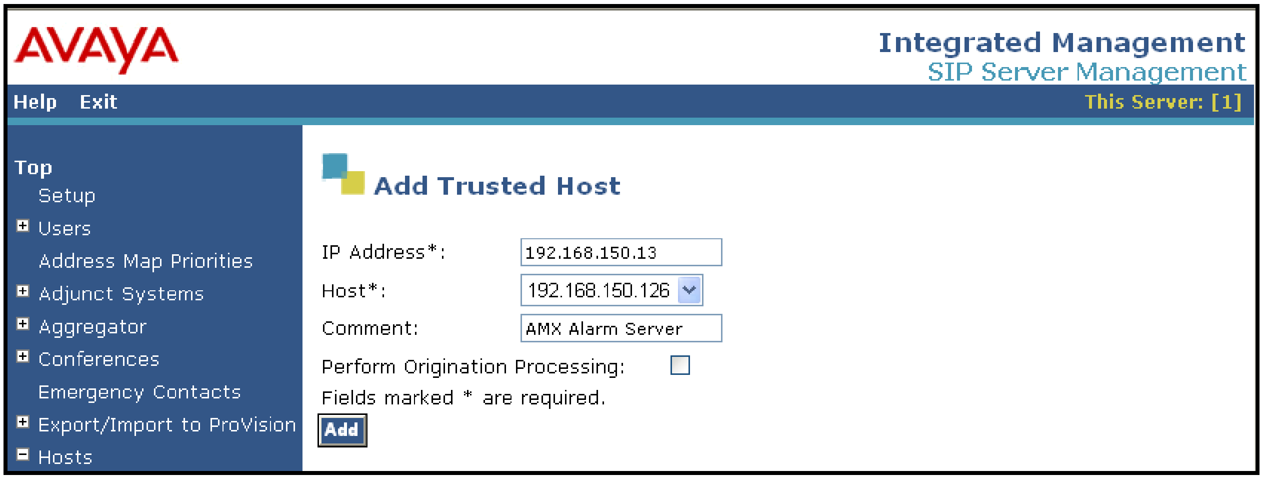
Figure 48: Add Communication Manager Server Address Map

5.4. Configure Trusted Host

Select "Trusted Hosts" → "Add" from the "Top" level menu shown in **Figure 35**, specify the parameters as shown in the following table, and click "Add" followed by "Continue" (not shown).

Parameter	Usage
IP Address	Enter the IP address on the AMX server.
Host	Select the IP address of the SES server from the drop-down box.
Comment	Enter an appropriate name to identify the Alarm Server.

Table 23: Add Trusted Host Parameters



Add Trusted Host

IP Address*: 192.168.150.13

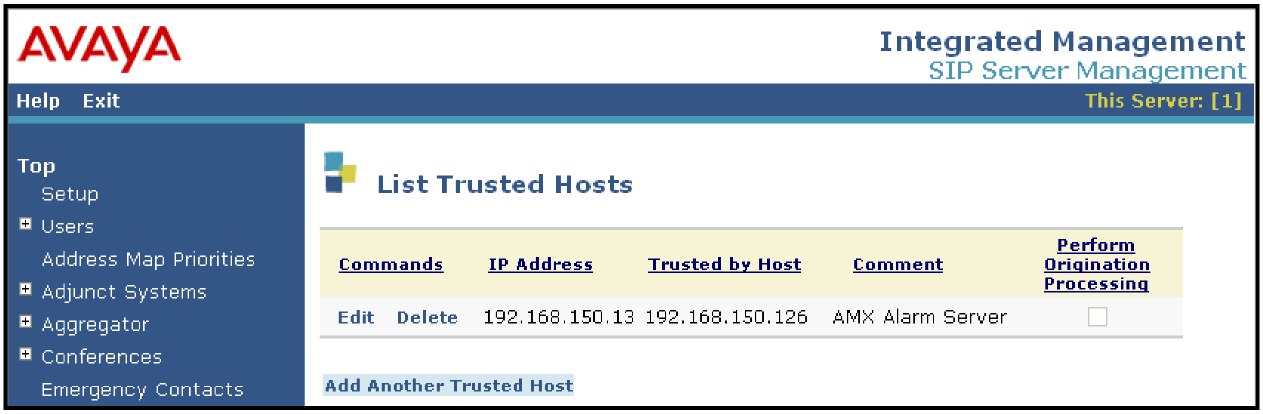
Host*: 192.168.150.126

Comment: AMX Alarm Server

Perform Origination Processing: □

Fields marked * are required.

Figure 49: Add Trusted Host Screen



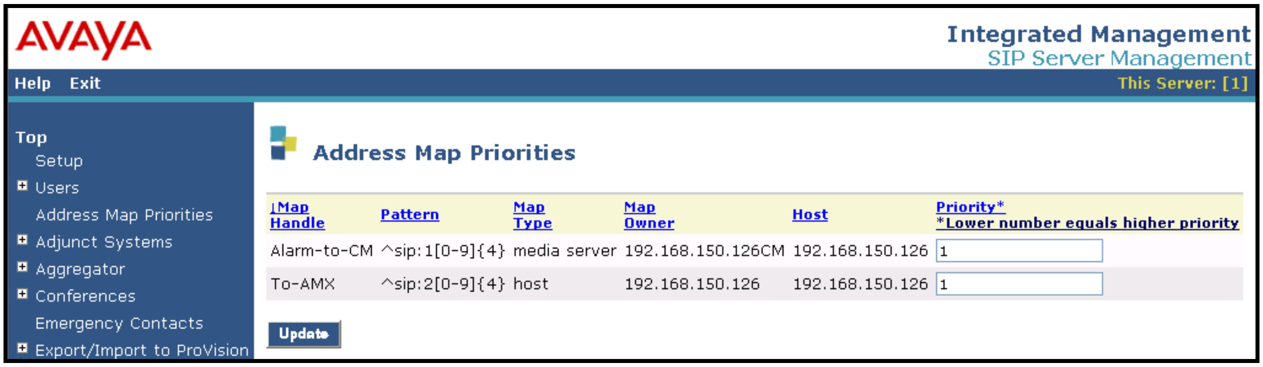
List Trusted Hosts

Commands	IP Address	Trusted by Host	Comment	Perform Origination Processing
Edit Delete	192.168.150.13	192.168.150.126	AMX Alarm Server	□

Figure 50: Add Trusted Host Screen

5.5. Show Address Map Priorities

Navigate "Address Map Priorities" to see the configured address maps.



Address Map Priorities

↓Map Handle	Pattern	Map Type	Map Owner	Host	Priority* *Lower number equals higher priority
Alarm-to-CM	^sip:1[0-9]{4}	media server	192.168.150.126CM	192.168.150.126	1
To-AMX	^sip:2[0-9]{4}	host	192.168.150.126	192.168.150.126	1

Figure 51: Address Map Priorities Screen

6. Configure Avaya R4 Base Station

In its un-configured state, the Avaya R4 base station is set to be a DHCP client. Thus, the MAC address of each base station to be included in the configuration should be entered into the DHCP server together with the IP address, network mask, and default gateway address which are to be assigned to that base station. The Avaya R4 base stations have an integrated HTTP server which allows the input of configuration parameters via a web browser.

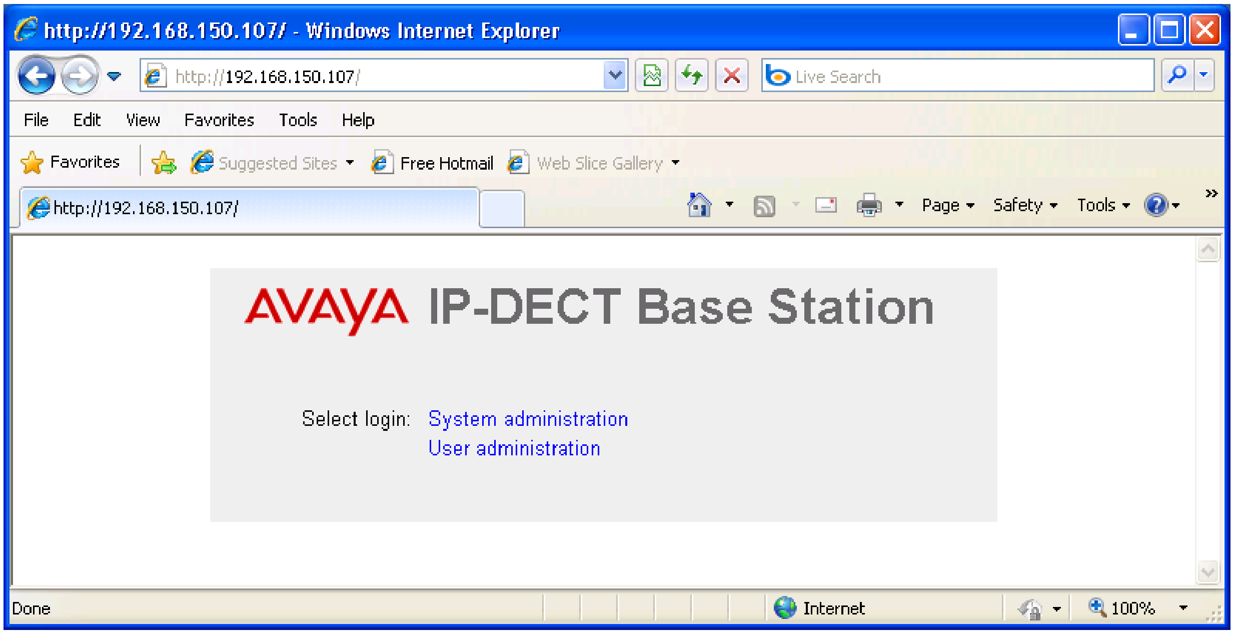
Each Avaya R4 base station consists of two independent components:

- A PBX interface component which has a trunk interface to the PBX and an IP interface to one or more radio components.
- A radio component which interfaces to wireless endpoints via DECT and via IP interface to a Master base station containing an active PBX interface component.

The unit which serves as Master has an active PBX interface component and can also have an active radio component. Any additional base stations required to extend radio coverage each have an active radio component which communicates with the Master via IP, with an inactive PBX interface component, hereafter referred to as Slave base stations.

The tested configuration included only one Master base station in the configuration, and had no Slave base stations.

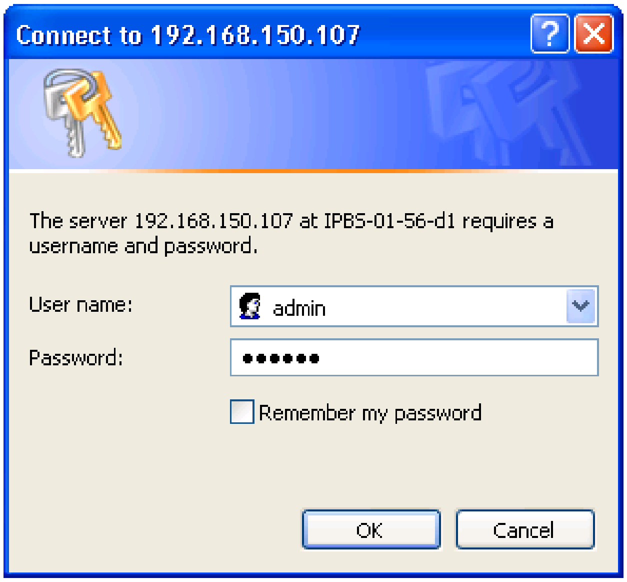
Enter the URL of the DECT base station into a web browser and select the "System administration" control.



Select login: System administration
User administration

Figure 52: DECT Base Selection

Enter the appropriate credentials and click “OK”. For the first-time login, the default password is “changeme”. After initial login, this should be changed to an appropriate value, for security reasons.



Connect to 192.168.150.107

The server 192.168.150.107 at IPBS-01-56-d1 requires a username and password.

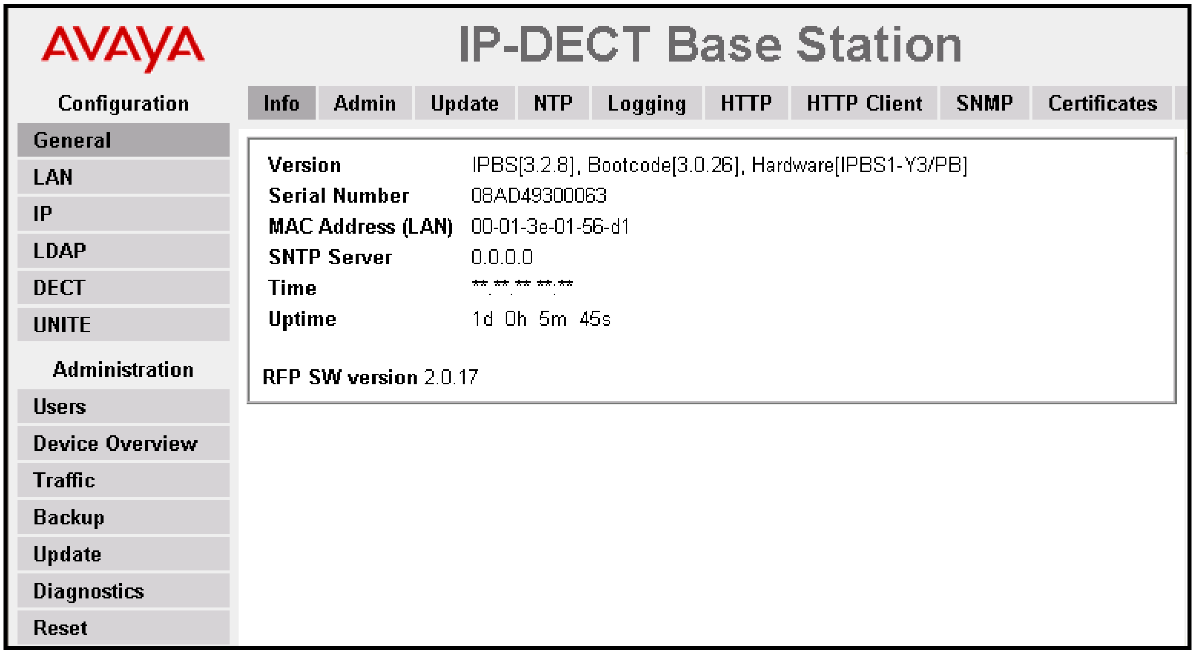
User name: admin

Password: ●●●●●●

□ Remember my password

Figure 53: DECT Base Station Login

The initial display shows the **General->Info** tab, which contains version/hardware identification information.

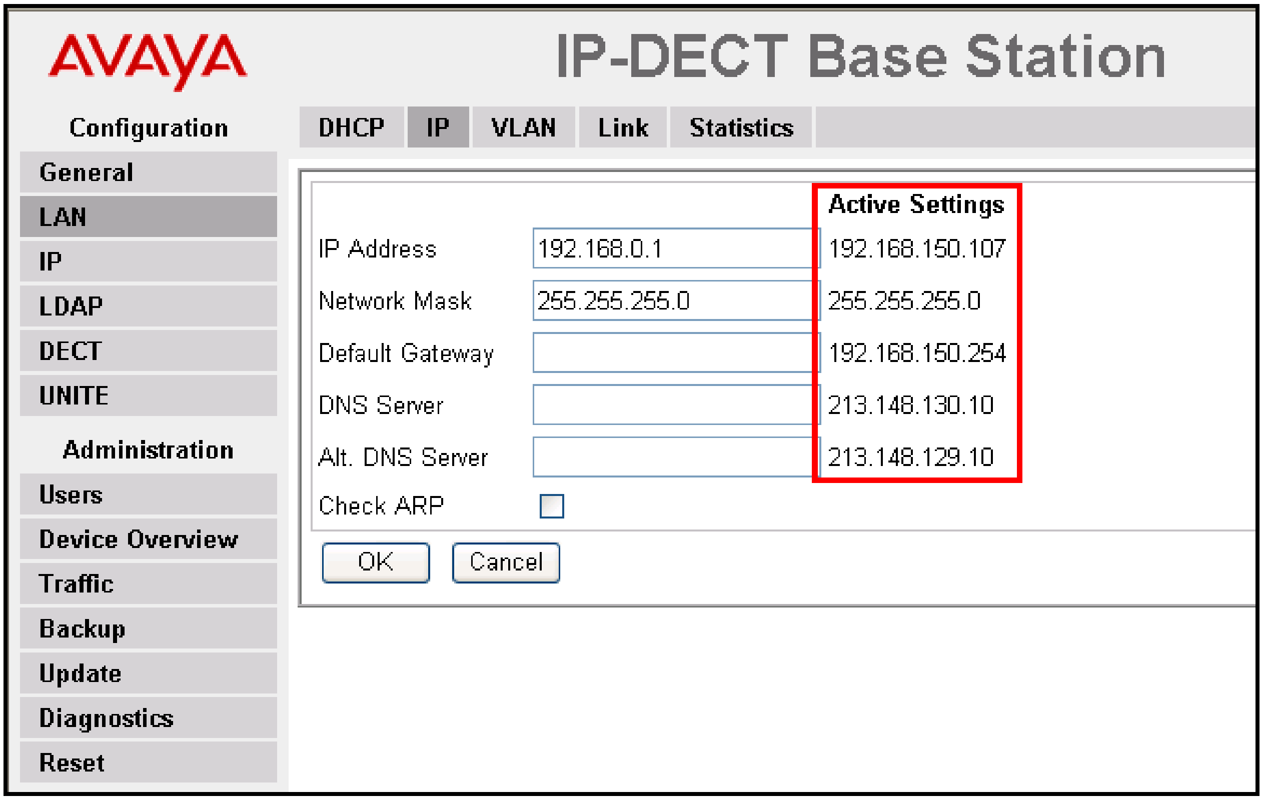


Version	IPBS[3.2.8], Bootcode[3.0.26], Hardware[IPBS1-Y3/PB]
Serial Number	08AD49300063
MAC Address (LAN)	00-01-3e-01-56-d1
SNTP Server	0.0.0.0
Time	**.**.** **:**
Uptime	1d 0h 5m 45s

RFP SW version 2.0.17

Figure 54: DECT Base Station General -> Info Tab

Select the **LAN->IP** tab. Verify that the IP parameters assigned to the base station correspond to those which are configured in the DHCP reservation.



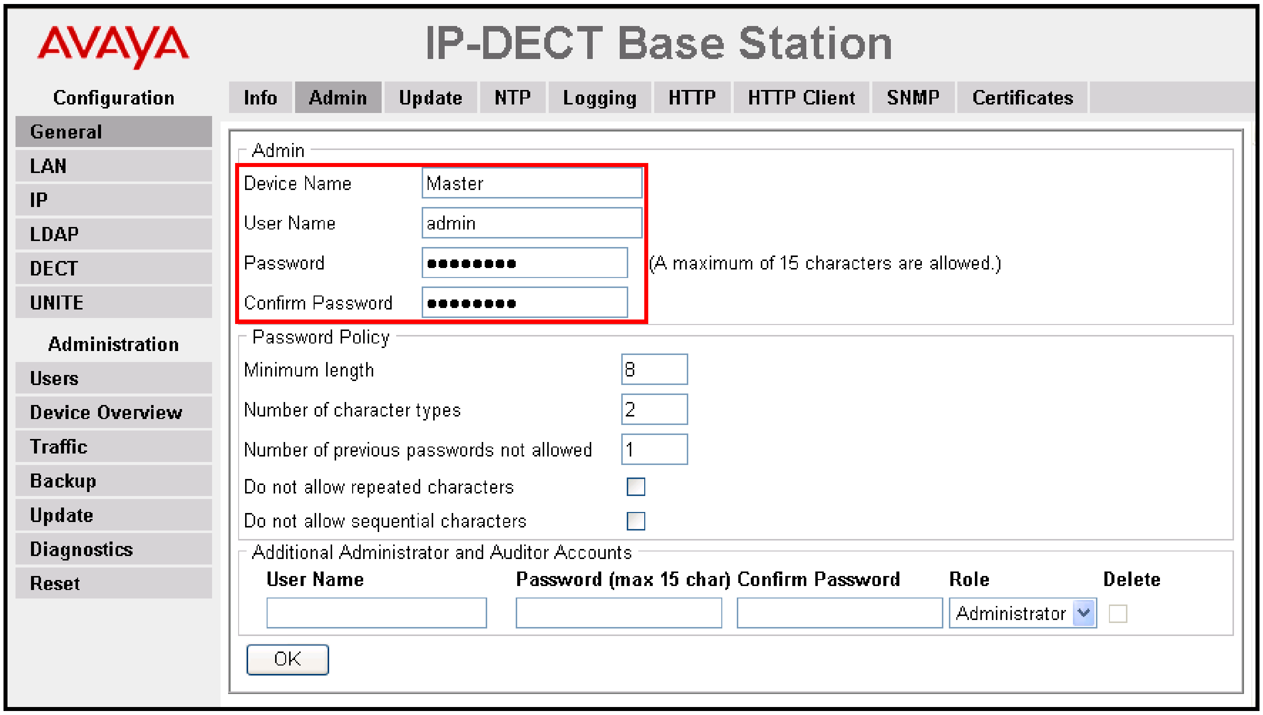
		Active Settings
IP Address	192.168.0.1	192.168.150.107
Network Mask	255.255.255.0	255.255.255.0
Default Gateway		192.168.150.254
DNS Server		213.148.130.10
Alt. DNS Server		213.148.129.10
Check ARP	□	

Figure 55: DECT Base Station LAN -> IP Tab

Select the **General->Admin** tab. Enter the parameters shown in the following table and click "OK".

Parameter	Usage
Device Name	Enter an appropriate name to identify the master base station.
User Name	Enter "admin", the default administrator user name.
Password	Enter an appropriate password.

Table 24: DECT Base Station General -> Admin Tab Parameters



Admin

Device Name: Master

User Name: admin

Password: ●●●●●●●● (A maximum of 15 characters are allowed.)

Confirm Password: ●●●●●●●●

Password Policy

Minimum length: 8

Number of character types: 2

Number of previous passwords not allowed: 1

Do not allow repeated characters □

Do not allow sequential characters □

Additional Administrator and Auditor Accounts

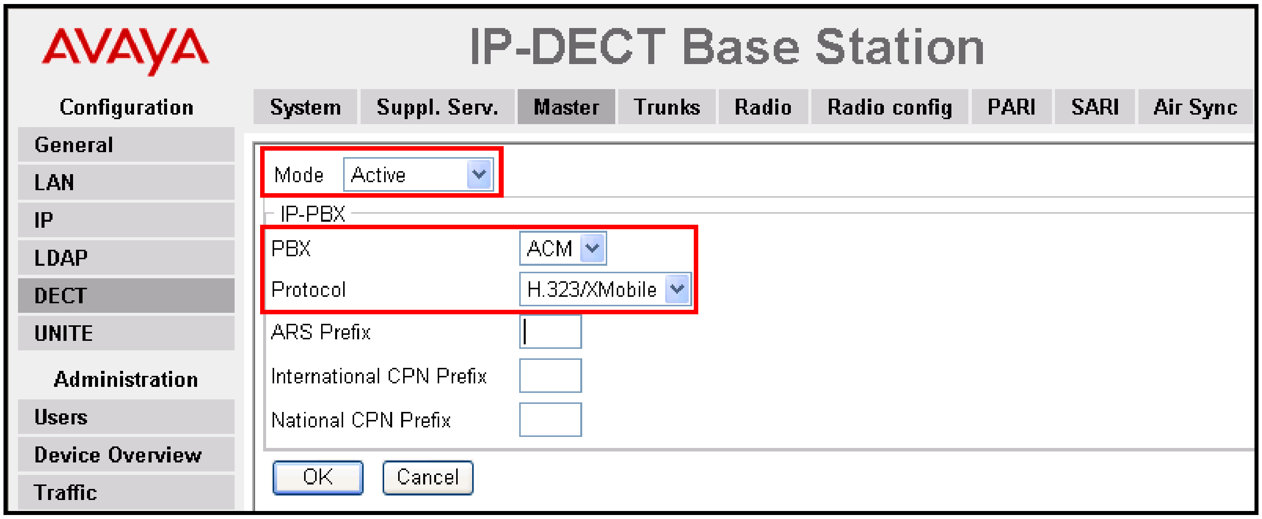
User Name	Password (max 15 char)	Confirm Password	Role	Delete
			Administrator	□

Figure 56: Master Base Station General -> Admin Tab

Select the **DECT->Master** tab Enter the parameters shown in the following table and click "OK".

Parameter	Usage
Mode	Select "Active" from the drop-down menu.
PBX	Select "ACM" from the drop-down menu.
Protocol	Select "H.323/XMobile" from the drop-down menu.

Table 25: DECT Base Station DECT -> Master Tab Parameters



Mode: Active

PBX: ACM

Protocol: H.323/XMobile

ARS Prefix:

International CPN Prefix:

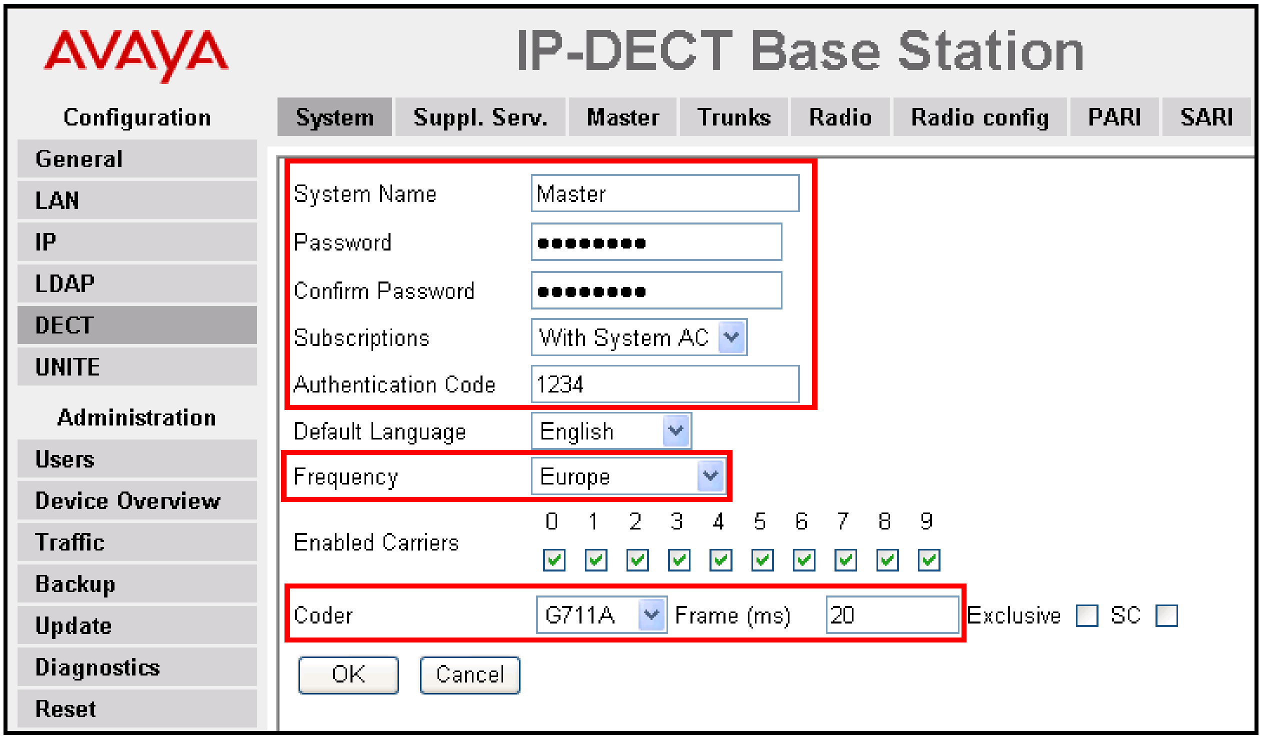
National CPN Prefix:

Figure 57: DECT Base Station DECT -> Master Tab

Select the **DECT -> System** tab. Enter the parameters shown in the following table and click "OK".

Parameter	Usage
System Name	Enter an appropriate name to identify this base station.
Password / Confirm	Enter an appropriate password for this base station.
Subscriptions	Select "With System AC" from the drop-down menu.
Authentication Code	Enter an appropriate code to be used by endpoints for registration authentication.
Frequency	Select "Europe" from the drop-down menu.
Coder	Select "G711A" from the drop-down menu.
Frame (ms)	Select "20" from the drop-down menu.

Table 26: DECT Base Station DECT -> System Tab Parameters



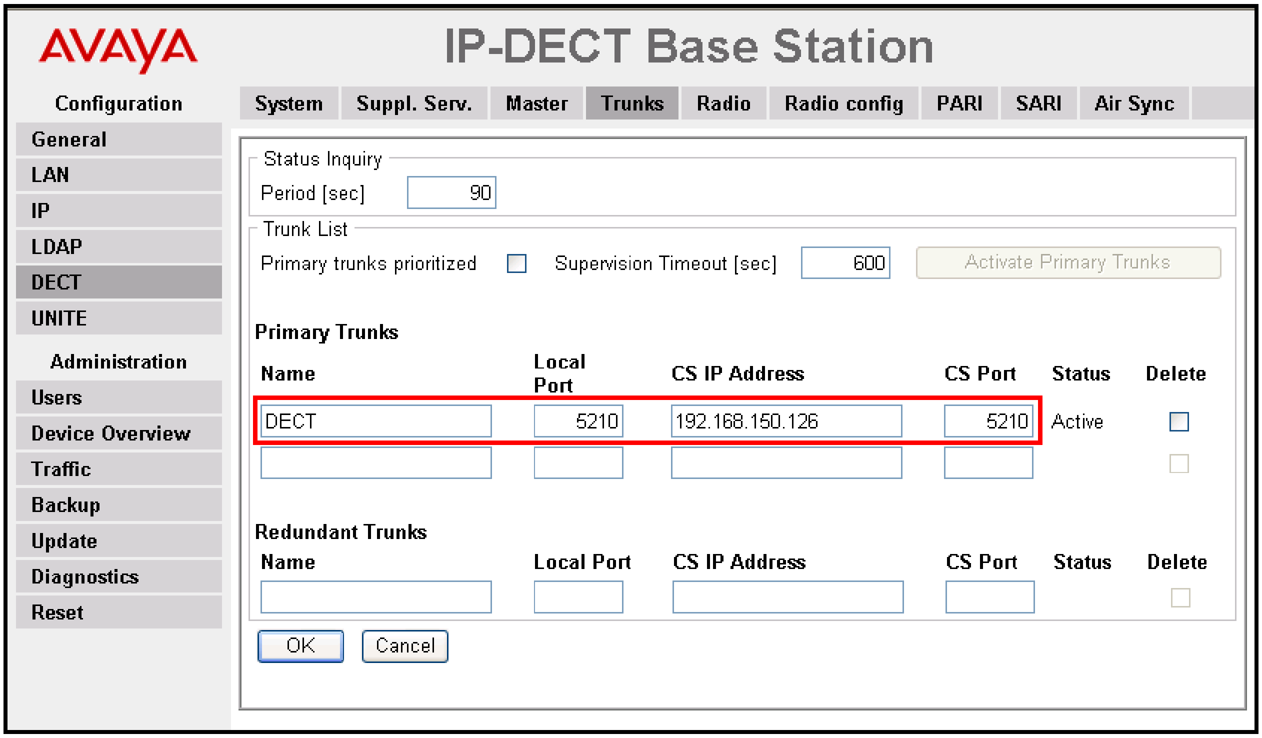
System Name	Master
Password	●●●●●●●●●
Confirm Password	●●●●●●●●●
Subscriptions	With System AC
Authentication Code	1234
Default Language	English
Frequency	Europe
Enabled Carriers	0 ☑ 1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑ 6 ☑ 7 ☑ 8 ☑ 9 ☑
Coder	G711A
Frame (ms)	20
Exclusive	□
SC	□

Figure 58: DECT Base Station DECT -> System Tab

Select the **DECT->Trunks** tab. Enter the parameters shown in the following table and click "OK".

Parameter	Usage
Name	Enter an appropriate name to identify this trunk.
Local Port	Enter the number of the local port which is read by this base station. This must be the same values assigned to "Far-end Listen Port" in **Figure 22**
CS IP Address	Enter the IP assigned to the proc interface in **Figure 8**.
CS Port	Enter the number of the local port which is read by this base station. This must be the same values assigned to "Near-end Listen Port" in **Figure 22.**

Table 27: DECT Base Station DECT -> Trunks Tab Parameters



Status Inquiry

Period [sec] 90

Trunk List

Primary trunks prioritized □ Supervision Timeout [sec] 600

Primary Trunks

Name	Local Port	CS IP Address	CS Port	Status	Delete
DECT	5210	192.168.150.126	5210	Active	□
					□

Redundant Trunks

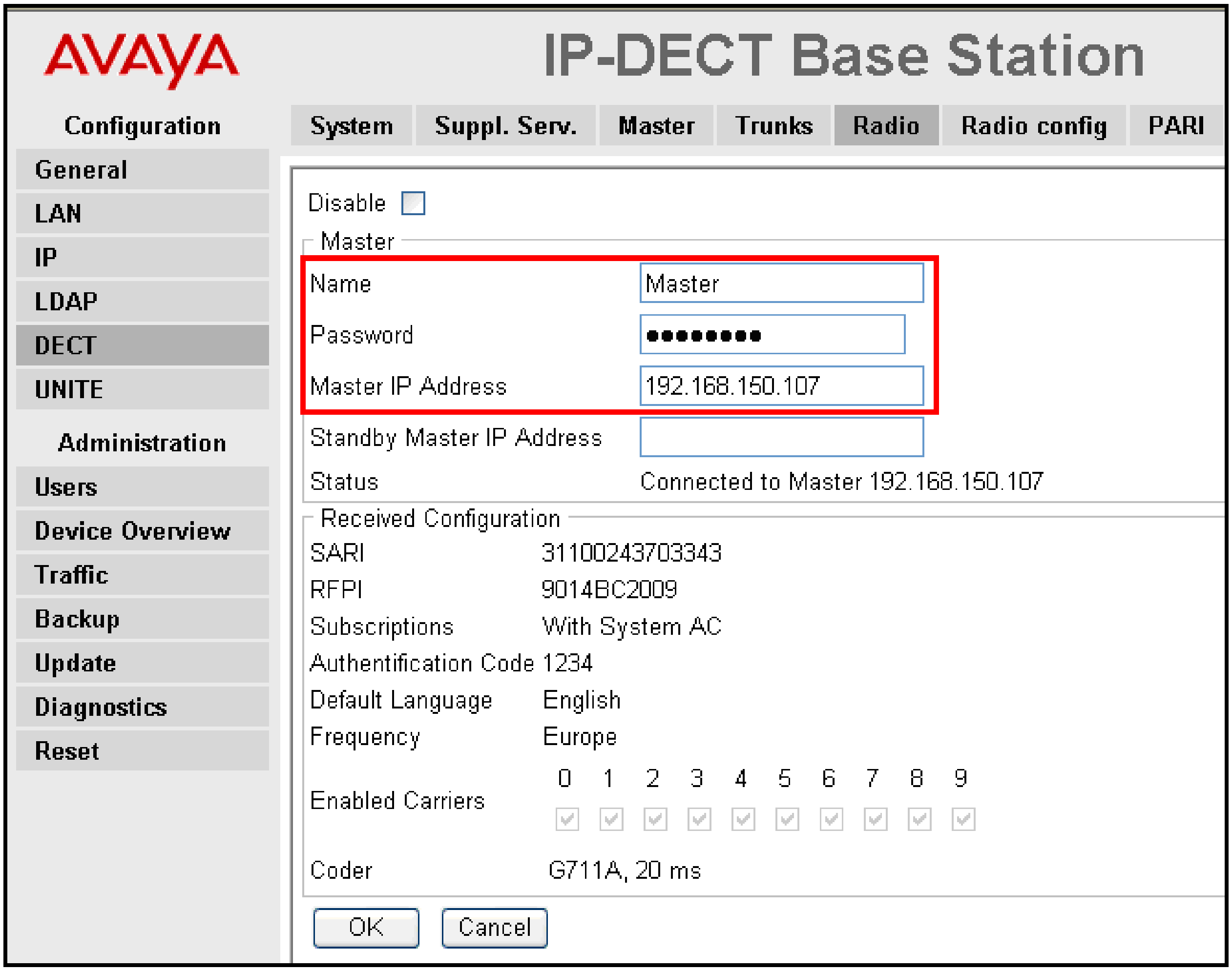
Name	Local Port	CS IP Address	CS Port	Status	Delete
					□

Figure 59: DECT Base Station DECT -> Trunks Tab

Select the **DECT->Radio** tab. Enter the parameters shown in the following table and click "OK".

Parameter	Usage
Name	Enter the System Name assigned to this base station in **Figure 58**.
Password	Enter the password assigned to this base station in **Figure 58**.
Master IP Address	Enter the IP address assigned to this base station, as displayed by the first item in the "Active Settings" list in **Figure 55**.

Table 28: DECT Base Station DECT -> Radio Tab Parameters



Disable □

Master

Name	Master
Password	●●●●●●●●●
Master IP Address	192.168.150.107
Standby Master IP Address	
Status	Connected to Master 192.168.150.107

Received Configuration

SARI	31100243703343
RFPI	9014BC2009
Subscriptions	With System AC
Authentification Code	1234
Default Language	English
Frequency	Europe

Enabled Carriers

0	1	2	3	4	5	6	7	8	9
☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

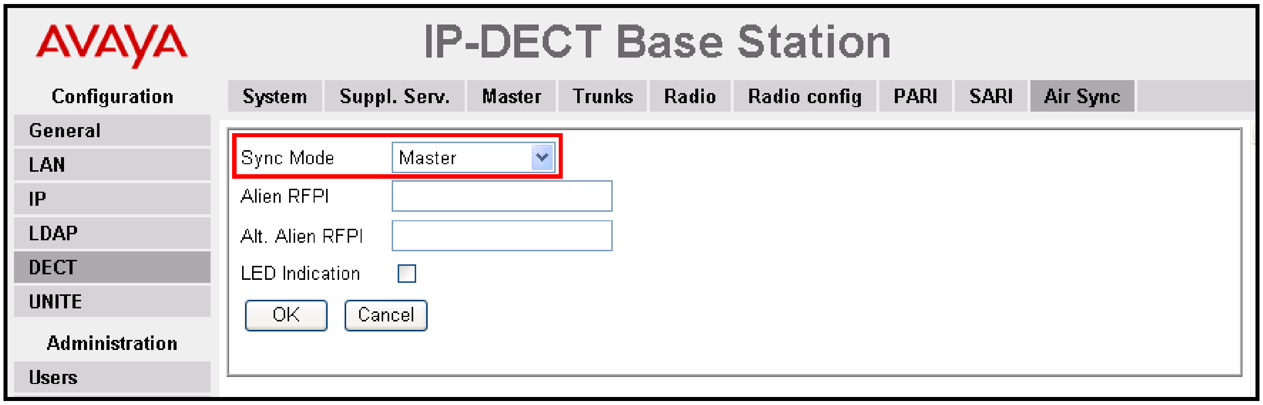
Coder G711A, 20 ms

Figure 60: DECT Base Station DECT -> Radio Tab

Select the **DECT->Air Sync** tab. Enter the parameters shown in the following table, click "OK".

Parameter	Usage
Sync Mode	Select "Master" from the drop-down menu.

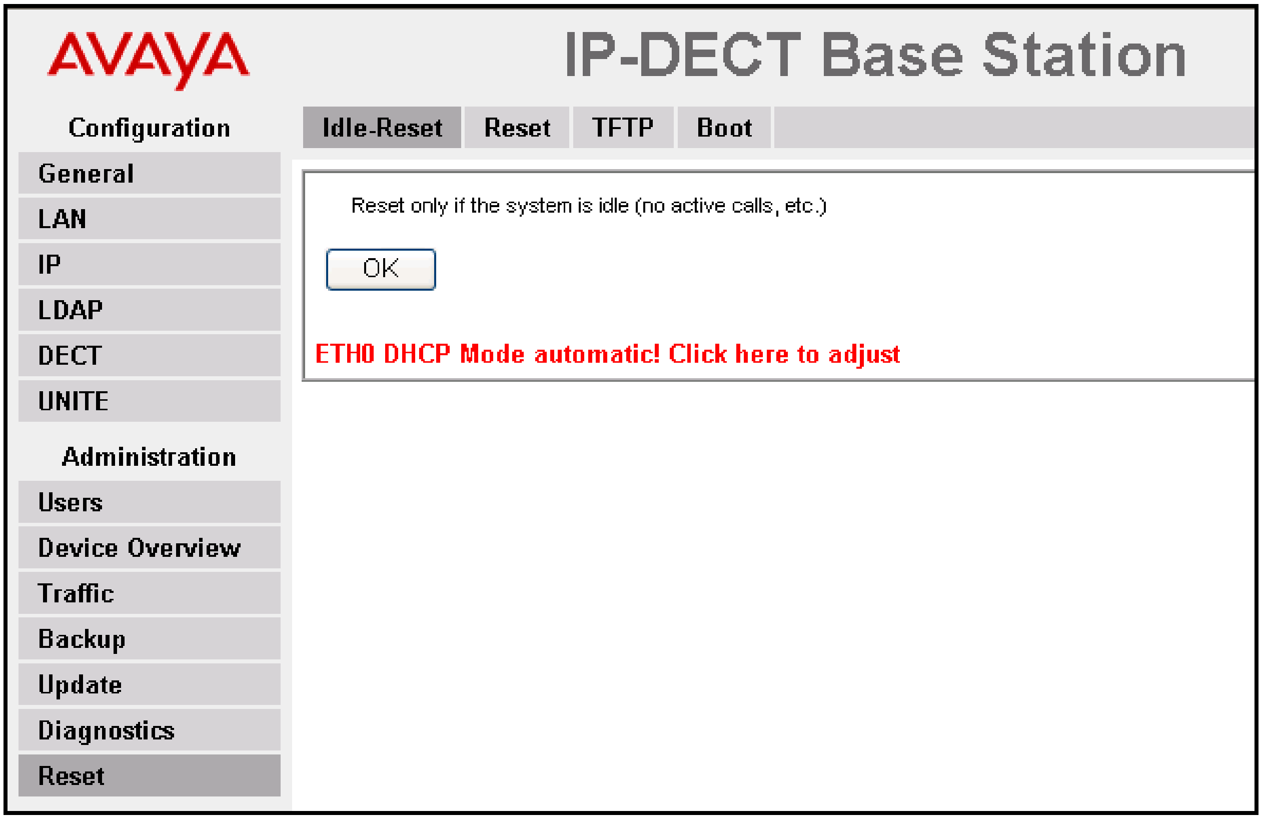
Table 29: DECT Base Station DECT -> Air Sync Tab Parameters



Sync Mode: Master
Alien RFPI:
Alt. Alien RFPI:
LED Indication: □

Figure 61: DECT Base Station DECT -> Air Sync Tab

Select the **Reset->Idle-Reset** tab. Click “OK”.



Reset only if the system is idle (no active calls, etc.)

ETH0 DHCP Mode automatic! Click here to adjust

Figure 62: DECT Base Station Reset -> Idle-Reset Tab

7. Configure ATT AMX

To set the IP address of Communication Manager, activate ScenarioBuilder on the Desktop of AMX and open Scenario under "Drivename:\Alarm\Scenario" "cc.outgoingcall_AVAYA_Voip.txt" (not shown). Double click the icon associated with "_AvayaMasterIP".

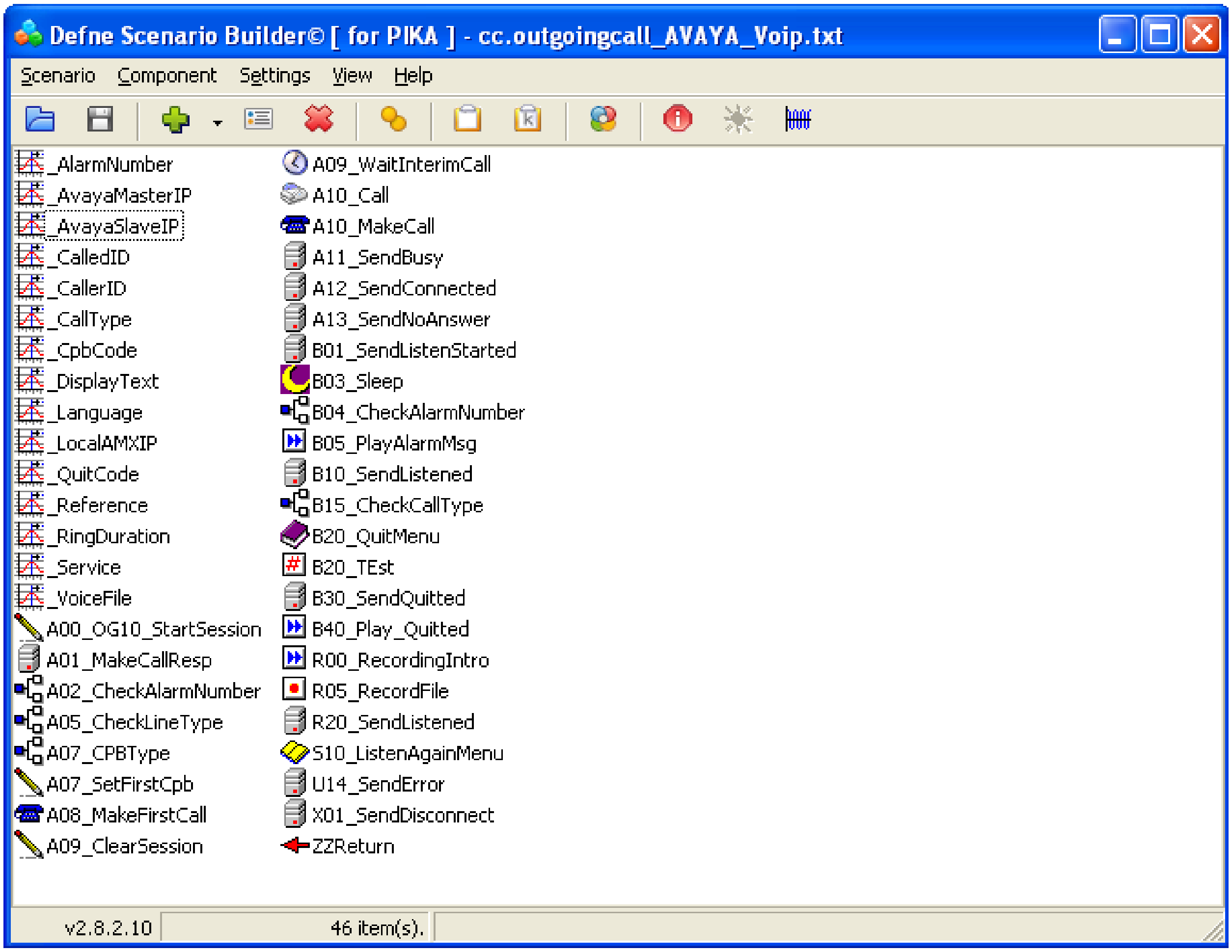
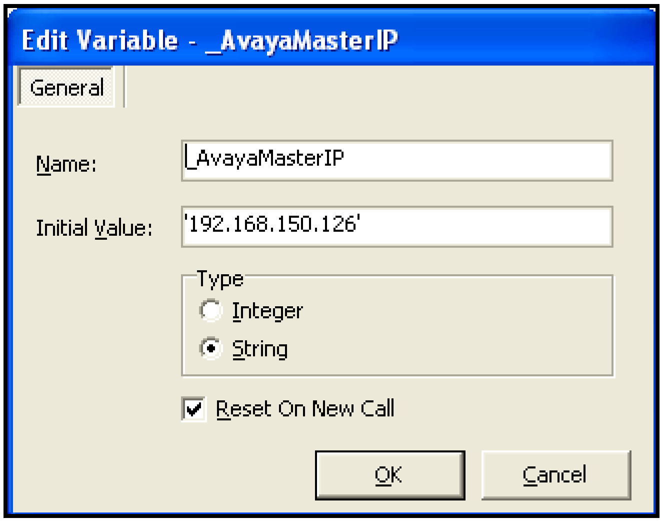


Figure 63: AMX ScenarioBuilder Screen

Enter the IP address for Communication Manager and click “OK”.


Edit Variable - _AvayaMasterIP

Name: _AvayaMasterIP

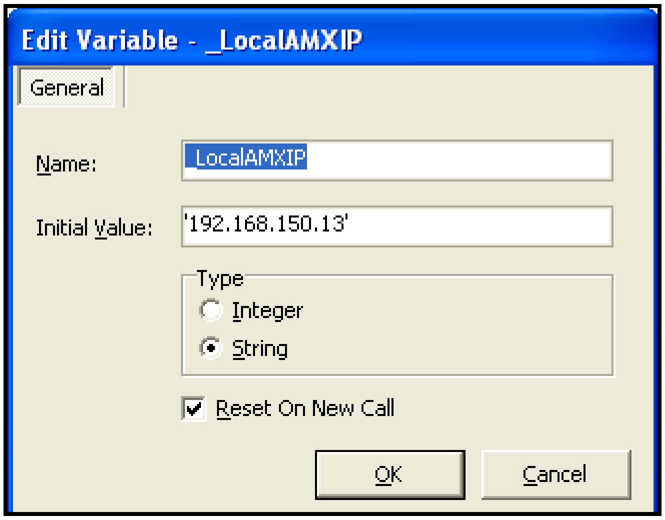
Initial Value: '192.168.150.126'

Type
○ Integer
● String

☑ Reset On New Call

Figure 64: AMX Address PBX Address Setting

Double click the icon associated with “_LocalAMXIP” shown in **Figure 63**, enter the IP address of the AMX server, and click “OK”.


Edit Variable - _LocalAMXIP

Name: _LocalAMXIP

Initial Value: '192.168.150.13'

Type
○ Integer
● String

☑ Reset On New Call

Figure 65: AMX Address PBX Address Setting

8. General Test Approach and Test Results

The compliance testing of ATT AMX Alarm Management Server interoperating with Communication Manager was performed manually. The tests were functional in nature, and no performance testing was done. The following items were encountered during testing:

- If a local fixed extension which has no available call appearance receives an incoming alarm call, the caller receives a "busy" indication: it makes no difference if it is a "priority" call.
- If an alarm call is made to a diverted (call forwarding) station, the call is diverted: it makes no difference if it is a "priority" call.
- Alarm calls to fixed stations which are paired with DECT stations via EC500, result in calls to DECT stations which do not include alarm text messages.
- If the ATT AMX Alarm Management Server is disconnected from its LAN interface, no alarms will be generated. The unit continues normal operation when the LAN interface is reconnected.

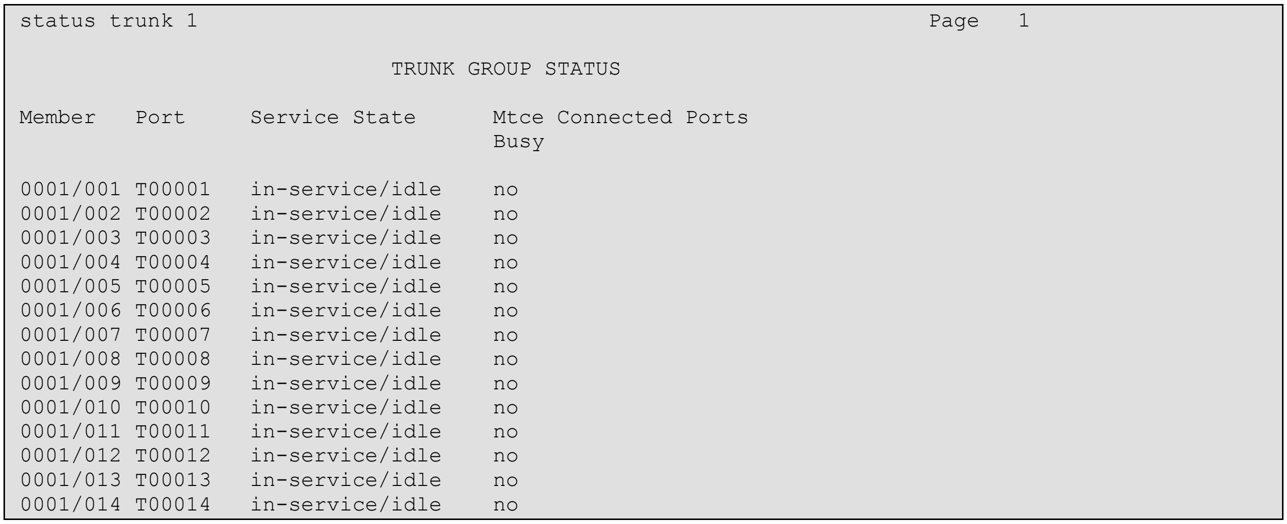
None of the above issues was considered to be a product failure. With the exception of the above-described items, all tests which were performed produced the expected result. **Section 1.1** contains a list of tests which were performed.

9. Verification Steps

The correct installation and configuration of AMX can be verified by performing the steps shown below.

9.1. Verify Avaya Aura® Configuration

Enter the "status trunk" command from the Communication Manager SAT terminal and verify that the all of the SIP trunk members are in the "in-service/idle" state.

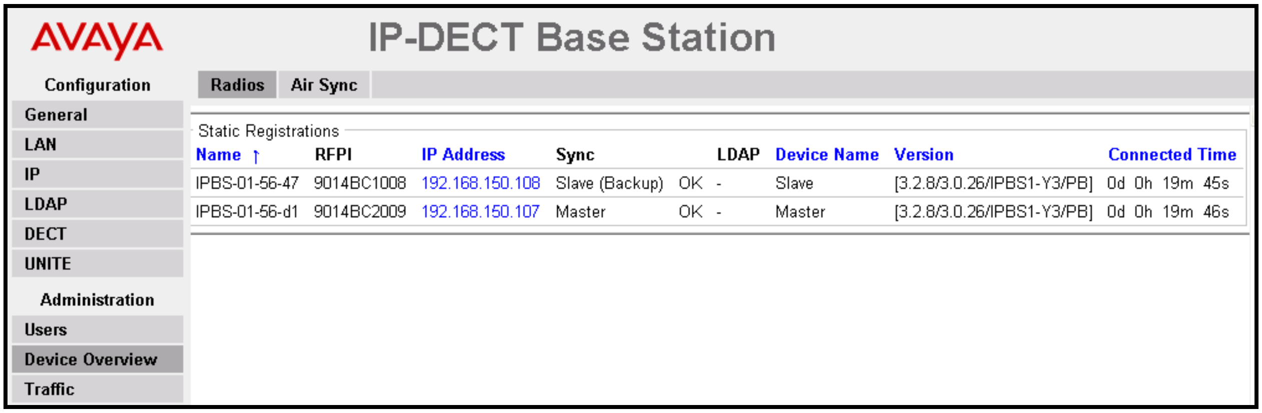


```
status trunk 1                                                     Page   1

                             TRUNK GROUP STATUS

Member   Port     Service State      Mtce Connected Ports
                                     Busy

0001/001 T00001   in-service/idle    no
0001/002 T00002   in-service/idle    no
0001/003 T00003   in-service/idle    no
0001/004 T00004   in-service/idle    no
0001/005 T00005   in-service/idle    no
0001/006 T00006   in-service/idle    no
0001/007 T00007   in-service/idle    no
0001/008 T00008   in-service/idle    no
0001/009 T00009   in-service/idle    no
0001/010 T00010   in-service/idle    no
0001/011 T00011   in-service/idle    no
0001/012 T00012   in-service/idle    no
0001/013 T00013   in-service/idle    no
0001/014 T00014   in-service/idle    no
```

Figure 66: Trunk Status

9.2. Verify Avaya R4 Master Base Station Configuration

From the Avaya R4 DECT base station, the **Device Overview** -> **Radios** tab should show registrations for the Master base station.



Static Registrations

Name ↑	RFPI	IP Address	Sync		LDAP	Device Name	Version	Connected Time
IPBS-01-56-47	9014BC1008	192.168.150.108	Slave (Backup)	OK	-	Slave	[3.2.8/3.0.26/IPBS1-Y3/PB]	0d 0h 19m 45s
IPBS-01-56-d1	9014BC2009	192.168.150.107	Master	OK	-	Master	[3.2.8/3.0.26/IPBS1-Y3/PB]	0d 0h 19m 46s

Figure 67: Master Base Station Radio Status

10. Conclusion

These Application Notes contain instructions for configuring Avaya Aura® Communication Manager to connect to the ATT AMX Alarm Management Server via SIP trunk. A list of instructions is provided to enable the user to verify that the various components have been correctly configured.

11. Additional References

This section references documentation relevant to these Application Notes. The Avaya product documentation is available at http://support.avaya.com.

[1] *Administering Avaya Aura™ Communication Manager*, May 2009, Document Number 03-300509.

[2] *Avaya Aura™ Communication Manager Feature Description and Implementation,* May 2009, Document Number 555-245-205.

[3] *Avaya DECT R4 Installation and Administration Manual,* August 2009, Document Number 21-603363.

[4] *AMX Alarm Management Server,* AMX Flyer

[5] *Personal & Alarm Management,* Version 1.2.1-EN, October 2009

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.