Application Notes for Avaya Aura™ Session Manager and Avaya Aura™ Communication Manager, and NextGen NX-E1010 integration – Issue 1.0

Abstract

These Application Notes describe the steps used to configure the Avaya Aura™ Session Manager, Avaya Aura™ Communication Manager, and NextGen NX-E1010 integration. NextGen NX-E1010 is a SIP-to-SIP (Session Initiation Protocol) carrier adapter, which integrates signaling and media control for SIP and has the registration capability as a User Agent (UA) with a SIP carrier's registrar.

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 steps used to configure Avaya Aura™ Session Manager and Avaya Aura™ Communication Manager with NextGen NX-E1010.

The NextGen NX-E1010 is a SIP-to-SIP (Session Initiation Protocol) carrier adapter, which integrates signaling and media control for SIP and has the registration capability as a User Agent (UA) with a SIP carrier's registrar. It resides at the enterprise network border and serves as both the source and destination for all SIP signaling messages and media streams coming into or going out the enterprise network.

Session Manager functions as the SIP trunking "hub" where all inbound and outbound SIP call routing (and other call processing) decisions is made. Communication Manager SIP trunks and NextGen NX-E1010 are provisioned to terminate at Session Manager.

1.1. Interoperability Compliance Testing

The interoperability compliance test focused on verifying the SIP trunking interoperability between NextGen NX-E1010 and Avaya SIP-based solution with Session Manager. The following were tested:

- An outgoing call is routed properly, and the SIP messages are properly formatted on both sides of NextGen NX-E1010.
- An incoming call is routed to the proper extension, and the SIP messages are properly formatted on both sides of NextGen NX-E1010.
- DTMF (Dual-Tone Multi-Frequency) transmission is performed by using G.711.
- Call forwarding
  - ▷ An incoming call from the Simulated SIP Service Provider network is properly forwarded to another destination in the Simulated SIP Service Provider network.
  - ▷ An incoming call from the Simulated SIP Service Provider network is properly forwarded to the extension in the enterprise site.
  - ▷ A call originated in the enterprise site is properly forwarded to another destination in the Simulated SIP Service Provider network.
- Call Transfer
  - ▷ An incoming call from the Simulated SIP Service Provider network is properly transferred to another destination in the Simulated SIP Service Provider network.
  - ▷ An incoming call from the Simulated SIP Service Provider network is properly transferred to the extension in the enterprise site.
  - ▷ A call originated in the enterprise site is properly transferred to another destination in the Simulated SIP Service Provider network.
- Call Conference - A conference between some extensions and participants through the Simulated SIP Service Provider network is properly established.
- Calling Line Identification Presentation (CLIP) and Calling Line Identification Restriction (CLIR).

1.2. Support

Contact NextGen for technical support on NX-E1010 via email.

- **Email:** e1010_support@nextgen.co.jp

2. Reference Configuration

Figure 1 illustrates the configuration that was used to verify the interoperability between NextGen NX-E1010 with Session Manager and Communication Manager. The Avaya solution located on the customer enterprise site consists of:

- Communication Manager.
  - ▷ SIP trunks for Inbound and Outbound Voice traffic.
    - ▪ Inbound Signaling Group defined with <blank> Far-end Domain field.
    - ▪ Voice components assigned to IP-Network-Region 1.
    - ▪ IP-Network-Region 1 specifies Avaya Customer Premises Equipment (CPE) Fully Qualified Domain Name (FQDN) and IP-Codec 1.
    - ▪ IP-Codec 1 specifies G.711Mu.
  - ▷ Disable the use of Diversion Headers (default).
- Session Manager with SM-100 Security Module.
  - ▷ Route all Inbound and Outbound SIP calls based on request Uniform Resource Identifier (URI) header information.
  - ▷ For outbound calls, convert the local IP address sent by Communication Manager in the request URI to the Avaya CPE FQDN.
- Avaya Aura™ System Manager.
- Avaya S8500C Server with an Avaya G650 Media Gateway. The S8500C served as the host processor for Communication Manager.
- Avaya 9600 Series IP telephones using the H.323 software bundle.

NextGen NX-E1010 used as edge device has the following functionality:

- Private/Public Network Address translation (NAT).
- SIP header manipulation.

The simulated SIP Service Provider Network has the following functionality:

- SIP Proxy server
- SIP Registrar server
- Location Service
- End users

In this configuration, one network interface on NextGen NX-E1010 is connected to the customer enterprise site and the other network interface is connected to the simulated SIP Service Provider Network. One SIP trunk group which is administered on Communication Manager is configured between Communication Manager and Session Manager, and is used for the sessions through NextGen NX-E1010. Session Manager recognizes Communication Manager and NextGen NX-E1010 as trusted SIP Entities. NextGen NX-E1010 terminates the SIP signaling messages and media streams between the customer enterprise site and the simulated SIP Service Provider Network.

Generally, telephone numbers are assigned to subscribers by the SIP Service Provider. In these Application Notes, one pilot number "050-3387-0005" is assigned. This is registered with the SIP Registrar server in the simulated SIP Service Provider Network by using the SIP REGISTER request.

The numbering plan in these Application Notes is as follows:

- The pilot number is always sent to the simulated SIP Service Provider Network as the calling party number.
  - ▷ Within the enterprise site, the calling party number of a call originating from an extension is treated as the extension of the caller.
  - ▷ NextGen NX-E1010 converts from the extension to the pilot number.
- All called party numbers of incoming calls from the simulated SIP Service Provider Network are conveyed to Communication Manager without any conversion.
  - ▷ Communication Manager converts from the public number to the corresponding extension.

The administration of the network infrastructure shown in **Figure 1** is not the focus of these Application Notes and will not be described. For administration of the network infrastructure shown in **Figure 1**, refer to the appropriate documentation listed in **Section 10**.

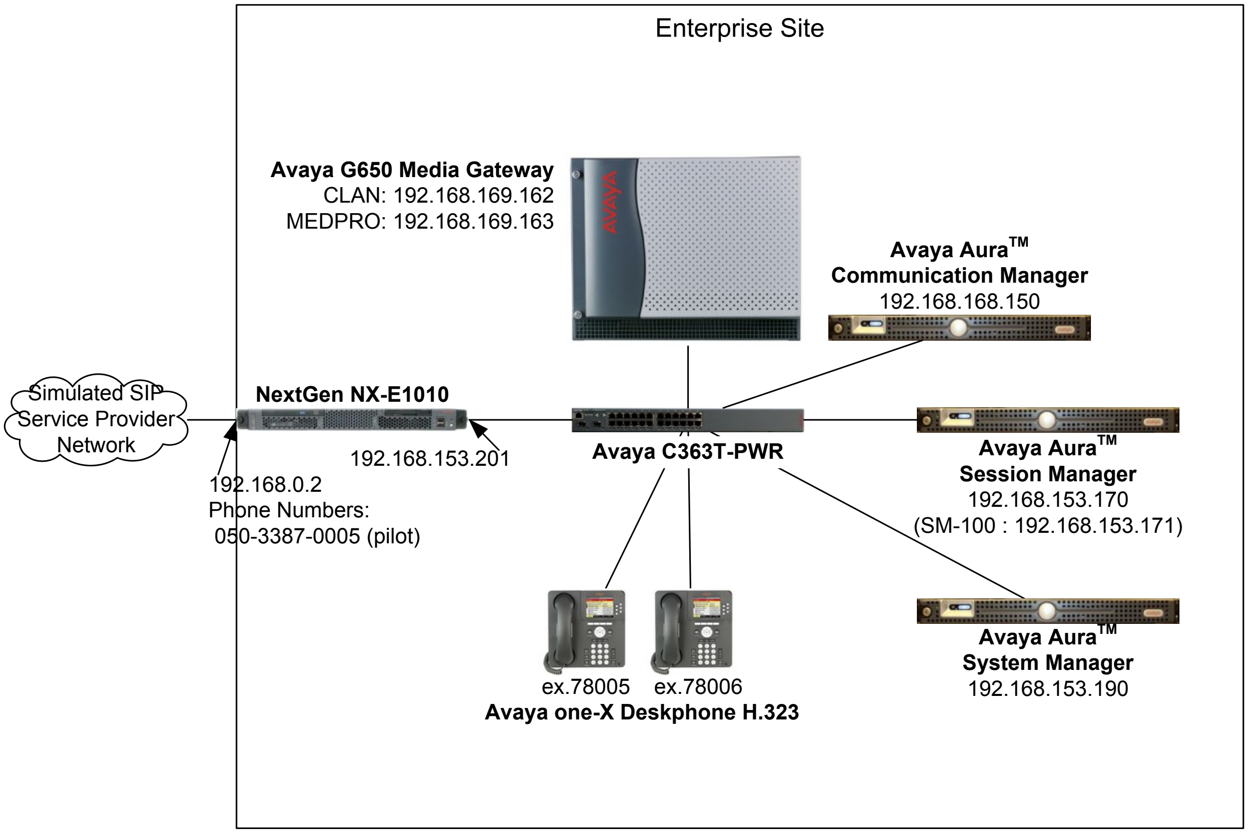


Figure 1: Test Configuration

3. Equipment and Software Validated

The following equipment and software were used for the test configuration in **Figure 1**.

Table 1: Equipment and Software

Equipment	Software
Avaya Aura™ Session Manager SM-100 (Security Module)	Release 1.1 SP1 (Build 111013) Version 1.1.0.0.111006
Avaya Aura™ System Manager	Release 1.0 SP2 （Build 112003）
Avaya S8500C Server	Avaya Aura™ Communication Manager 5.2.1 (R015x.02.1.015.0) with Patch 1004 (02.1.015.0-1004)
Avaya G650 Media Gateway • TN2312BP IP Server Interface (HW36) • TN799DP C-LAN Interface (HW01) • TN2302AP IP Media Processor (HW03)	- FW048 FW034 FW094
Avaya 9650 IP Telephones	Release 3.0.2 (H.323)
NextGen NX-E1010 (IBM x306)	Version 3.3 RedHat Enterprise Linux Server 5.3
NextGen NXS-VNS (DELL Latitude D630) that simulates SIP Service Provider Network	Version 3.0.1 (Build 2009/06/12)

4. Configure Communication Manager

This section provides the procedures for configuring Communication Manager. The procedures include the following areas:

- Verify Communication Manager Software Options
- Administer Dial Plan
- Administer IP Node Name for C-LAN
- Administer IP Interface for C-LAN
- Administer IP Network Region
- Administer IP Codecs
- Administer Signaling Group
- Administer Trunk Group
- Administer Calling Party Number Information
- Administer Call Routing
- Administer Incoming Digit Translation
- Save Communication Manager Changes

The SIP trunk is established between Communication Manager and Session Manager. This trunk will convey the SIP signaling messages and Real-time Transport Protocol (RTP) voice packets from / to NextGen NX-E1010.

SIP signaling messages for all incoming calls from the SIP Service Provider Network to the enterprise network are terminated at NextGen NX-E1010, which forwards them to Session Manager and are routed to Communication Manager via the SIP trunk. All outgoing calls to the SIP Service Provider network via NextGen NX-E1010 are routed through Communication Manager in order to use features such as automatic route selection and class of restrictions. Communication Manager creates the outbound SIP signaling messages that are routed via Session Manager to NextGen NX-E1010.

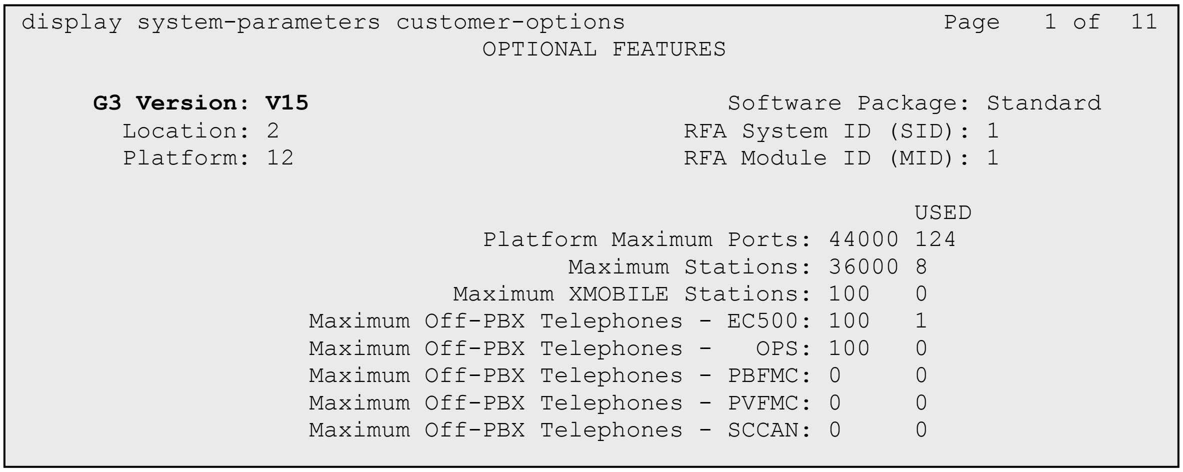
The Communication Manager commands described in these Application Notes were administered using the System Access Terminal (SAT).

The steps shown in this section were configured on Avaya S8500C Server at the enterprise site.

Note - The initial installation, configuration, and provisioning of the Avaya Server for Communication Manager, Avaya Media Gateway and their associated boards, as well as Avaya telephones, are presumed to have been previously completed and are not discussed in these Application Notes.

4.1. Verify Communication Manager Software Options

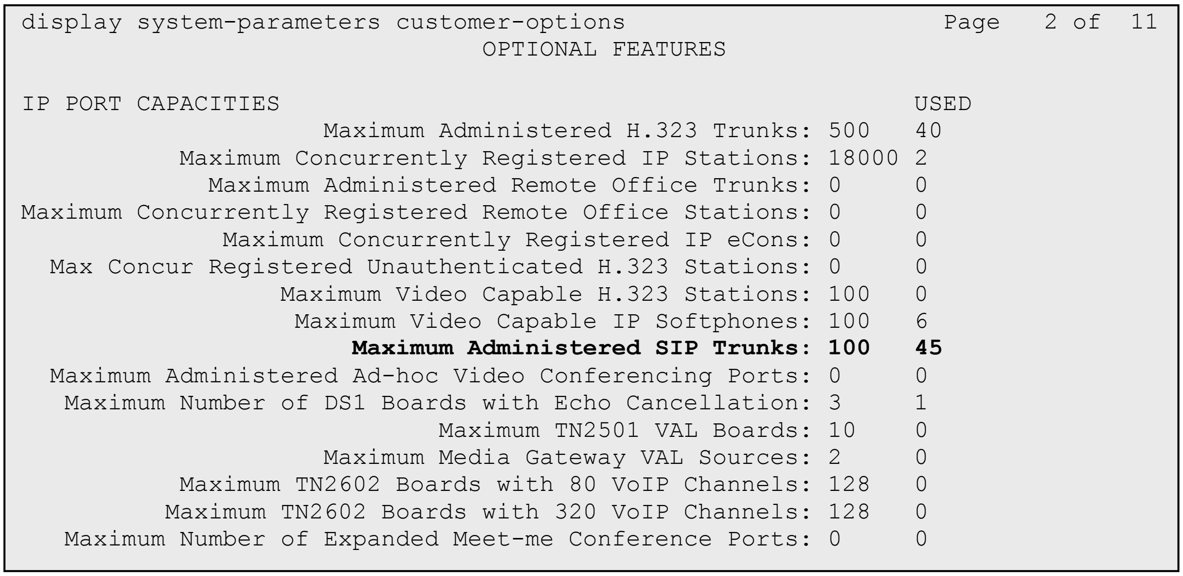
Log into the SAT to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the **display system-parameters customer-options** command to verify that the **G3 Version** field is set to ***V15*** on **Page 1**, as shown below.



```
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: 12                              RFA Module ID (MID): 1

                                                               USED
                                Platform Maximum Ports: 44000 124
                                      Maximum Stations: 36000 8
                              Maximum XMOBILE Stations: 100   0
                    Maximum Off-PBX Telephones - EC500: 100   1
                    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 2: System-Parameters Customer-Options Form – Page 1

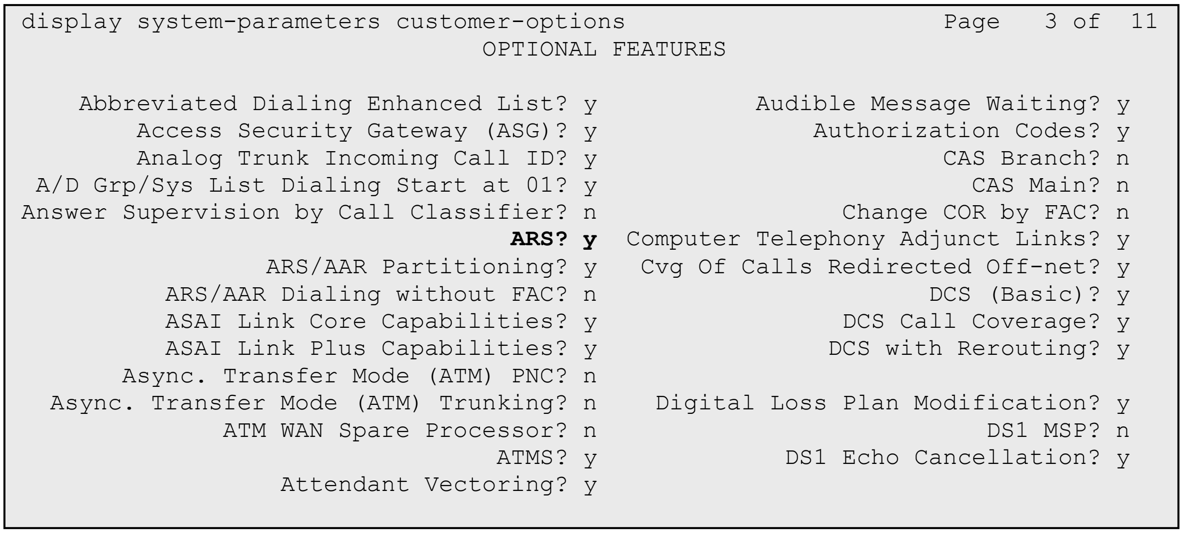
Navigate to **Page 2**, and verify that the number of the **Maximum Administered SIP Trunks** field is sufficient for the combination of trunks to Session Manager, SIP endpoints, and any other SIP trunks.



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

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 500   40
           Maximum Concurrently Registered IP Stations: 18000 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: 100   0
                   Maximum Video Capable IP Softphones: 100   6
                       Maximum Administered SIP Trunks: 100   45
  Maximum Administered Ad-hoc Video Conferencing Ports: 0     0
   Maximum Number of DS1 Boards with Echo Cancellation: 3     1
                             Maximum TN2501 VAL Boards: 10    0
                     Maximum Media Gateway VAL Sources: 2     0
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   0
   Maximum Number of Expanded Meet-me Conference Ports: 0     0
```

Figure 3: System-Parameters Customer-Options Form – Page 2

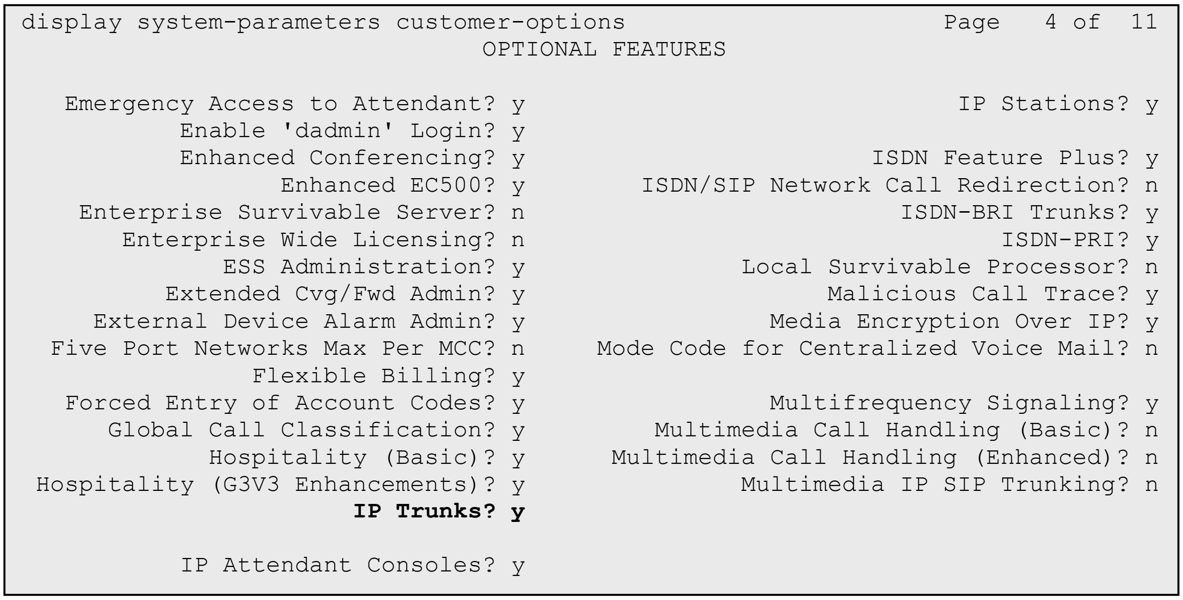
On **Page 3**, verify that the **ARS** feature is enabled.



```
display system-parameters customer-options                      Page   3 of  11
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? y           Audible Message Waiting? y
        Access Security Gateway (ASG)? y               Authorization Codes? y
        Analog Trunk Incoming Call ID? y                        CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? y                          CAS Main? n
Answer Supervision by Call Classifier? n                Change COR by FAC? n
                                  ARS? y  Computer Telephony Adjunct Links? y
                 ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? n                       DCS (Basic)? y
          ASAI Link Core Capabilities? y                 DCS Call Coverage? y
          ASAI Link Plus Capabilities? y                DCS with Rerouting? y
       Async. Transfer Mode (ATM) PNC? n
  Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? y
              ATM WAN Spare Processor? n                           DS1 MSP? n
                                 ATMS? y             DS1 Echo Cancellation? y
                  Attendant Vectoring? y
```

Figure 4: System-Parameters Customer-Options Form – Page 3

On **Page 4**, verify that the **IP Trunks** feature is enabled.



```
display 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? y
                  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? y                Local Survivable Processor? n
          Extended Cvg/Fwd Admin? y                      Malicious Call Trace? y
     External Device Alarm Admin? y                  Media Encryption Over IP? y
  Five Port Networks Max Per MCC? n     Mode Code for Centralized Voice Mail? n
                Flexible Billing? y
   Forced Entry of Account Codes? y                  Multifrequency Signaling? y
      Global Call Classification? y        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? y
```

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

4.2. Administer Dial Plan

In the reference configuration the Avaya CPE environment uses five digit local extensions, 78xxx. Trunk Access Codes (TAC) are 3 digits in length and begin with #. The Feature Access Code (FAC) to access ARS is one digit in length (digit 0).

The dial plan is modified with the **change dialplan analysis** command. On **Page 1** of the form:

- Local extensions:
  - ▹ In the **Dialed String** field enter ***78***
  - ▹ In the **Total Length** field enter ***5***
  - ▹ In the **Call Type** field enter ***ext***
- TAC codes:
  - ▹ In the **Dialed String** field enter **#**
  - ▹ In the **Total Length** field enter ***3***
  - ▹ In the **Call Type** field enter ***dac***
- FAC code – ARS access:
  - ▹ In the **Dialed String** field enter ***0***
  - ▹ In the **Total Length** field enter ***1***
  - ▹ In the **Call Type** field enter ***fac***

```
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
     78           5    ext
     #            3    dac
```

Figure 6: Dial Plan Analysis Form – Page 1

4.3. Administer IP Node Name for C-LAN

Use the **change node-names ip** command, to add entries for Session Manager and the C-LAN that will be used for connectivity.

For the SM-100 Security Module installed into Session Manager:

- In the **Name** field enter ***SM02***.
- In the **IP Address** field enter ***192.168.153.171***.

The reason IP address for SM-100 is specified instead of IP address for Session Manager is that all SIP messages to/from Session Manager must pass through SM-100.

For the C-LAN:

- In the **Name** field enter ***gumma-clan***.
- In the **IP Address** field enter ***192.168.169.162***.

The actual node names and IP addresses may vary. Submit these changes.

```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
Gateway001          192.168.168.1
Gateway002          192.168.169.1
SM02                192.168.153.171
aomori              192.168.163.140
chofu               192.168.147.203
default             0.0.0.0
gumma-ESS           192.168.169.160
gumma-clan          192.168.169.162
gumma-cmm           192.168.168.169
gumma-med2          192.168.168.163
gumma-medpro        192.168.169.163
nx-e1010            192.168.153.201
```

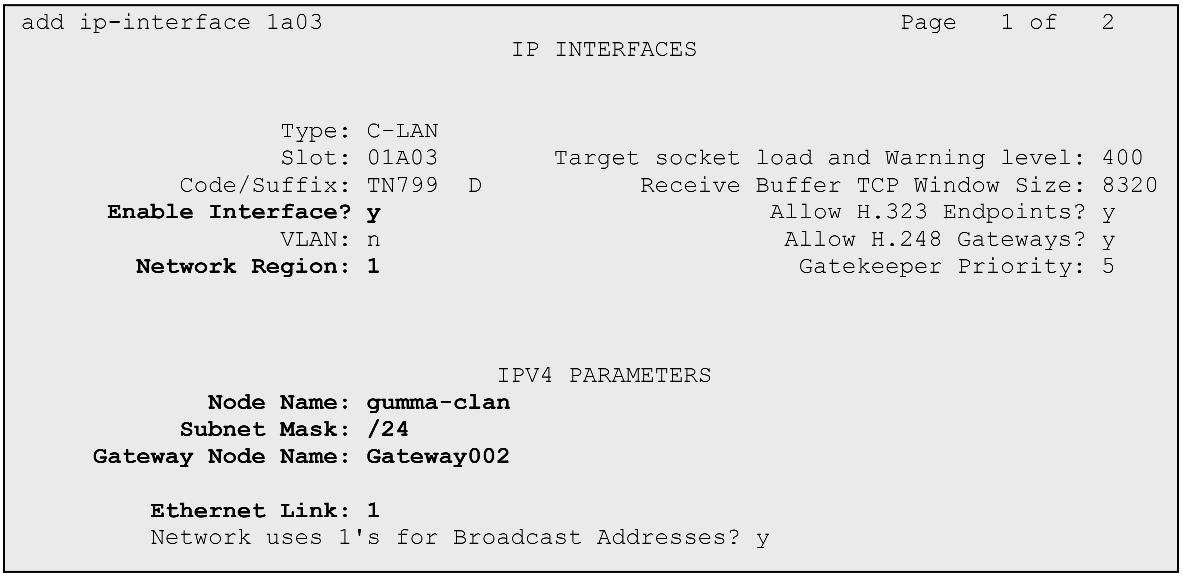
Figure 7: IP Node Names Form

4.4. Administer IP Interface for C-LAN

Add the C-LAN to the system configuration using the **add ip-interface 1a03** command. The actual slot number may vary. In this case, **1a03** is used as the slot number. Enter the C-LAN node name assigned in **Section 4.3** in the **Node Name** field. Enter proper values for the **Network Region**, **Subnet Mask**, **Gateway Node Name**, and **Ethernet Link** fields. Default values may be used in the remaining fields. In this case:

- In the **Node Name** field enter ***gumma-clan***.
- In the **Network Region** field enter ***1***.
- In the **Subnet Mask** field enter ***24***.
- In the **Gateway Node Name** field enter ***Gateway002***.
- In the **Ethernet Link** field enter ***1***.

After that, set the **Enable Interface?** field to ***y***, and submit these changes.



```
add ip-interface 1a03                                           Page   1 of   2
                                  IP INTERFACES


                  Type: C-LAN
                  Slot: 01A03        Target socket load and Warning level: 400
           Code/Suffix: TN799  D           Receive Buffer TCP Window Size: 8320
      Enable Interface? y                           Allow H.323 Endpoints? y
                  VLAN: n                            Allow H.248 Gateways? y
        Network Region: 1                              Gatekeeper Priority: 5



                                 IPV4 PARAMETERS
             Node Name: gumma-clan
           Subnet Mask: /24
     Gateway Node Name: Gateway002

         Ethernet Link: 1
         Network uses 1's for Broadcast Addresses? y
```

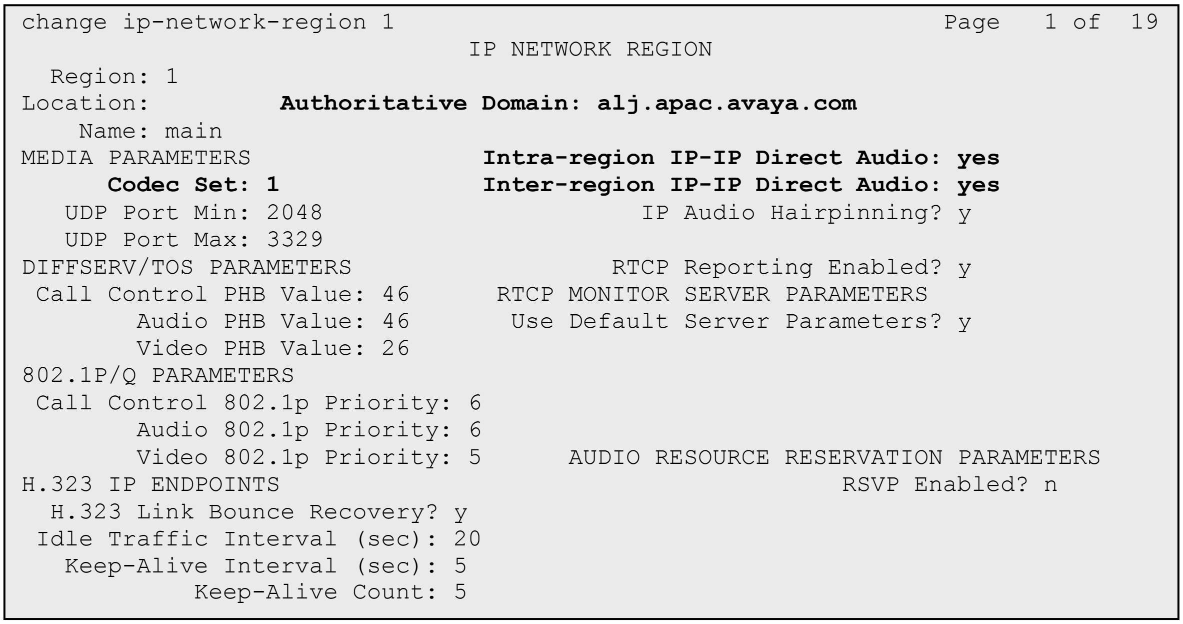
Figure 8: IP Interface Form

4.5. Administer IP Network Region

In the IP Network Region form, define the parameter associated with the SIP trunk group serving Session Manager. Use the **change ip-network-region 1** command to configure the network in the enterprise site. The actual Region number may vary. In this case, ***1*** is used as the **Region** number.

- The **Authoritative Domain** field is configured to match the domain name configured on the Session Manager. In this configuration, the domain name is ***alj.apac.avaya.com***.
- By default, **IP-IP Direct Audio** is enabled to allow audio traffic to be sent directly between endpoints without using media resources in the Avaya G650 Media Gateway.
- The **Codec Set** is set to the number of the IP codec set to be used for calls within IP network region ***1***. In this configuration, this codec set will apply to calls with NextGen NX-E1010 as well as any IP phones within the enterprise.

In this case, the SIP trunk is assigned to the same IP network region as the G650 Media Gateway.

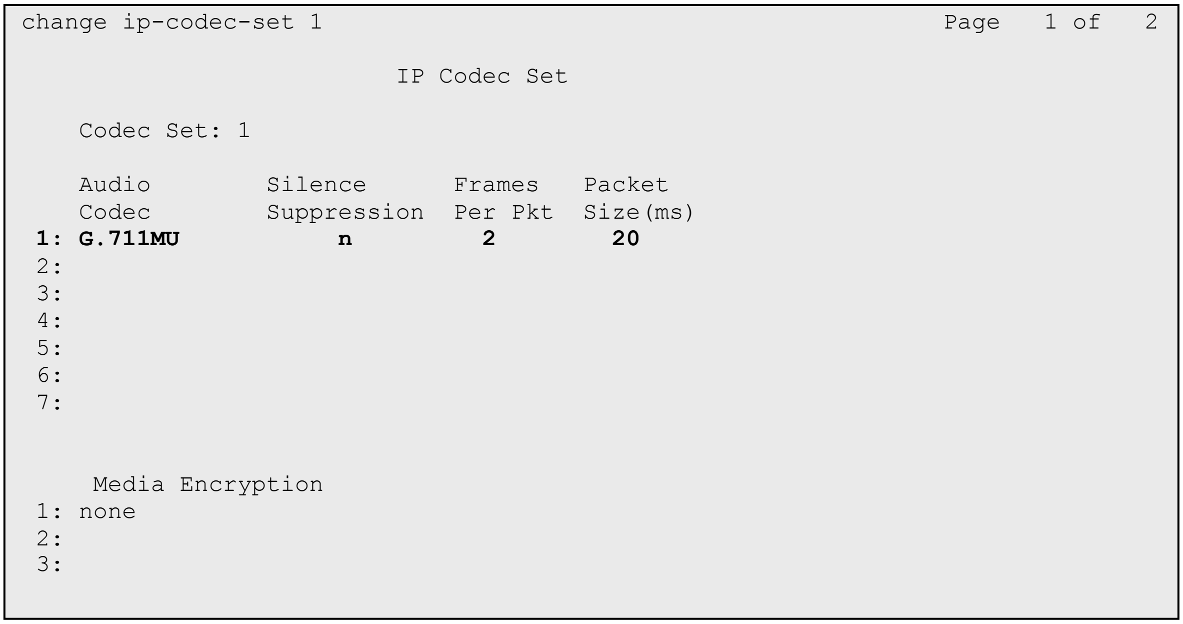


```
change ip-network-region 1                                     Page   1 of  19
                               IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain: alj.apac.avaya.com
    Name: main
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? y
   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. Administer IP Codecs

In the **IP Codec Set** form, define the **Codec Set** value specified in the IP Network Region form (**Figure 9**). Although multiple codecs can be listed in priority order in this form, only ***G.711MU*** is shown in this case because the simulated SIP Service Provider Network supports only G.711 mu-law and NextGen NX-E1010 doesn't have the capability to convert codecs.



```
change ip-codec-set 1                                         Page   1 of   2

                          IP Codec Set

    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU           n         2        20
 2:
 3:
 4:
 5:
 6:
 7:



     Media Encryption
 1: none
 2:
 3:
```

Figure 10: IP Codec Set Form

4.7. Administer Signaling Group

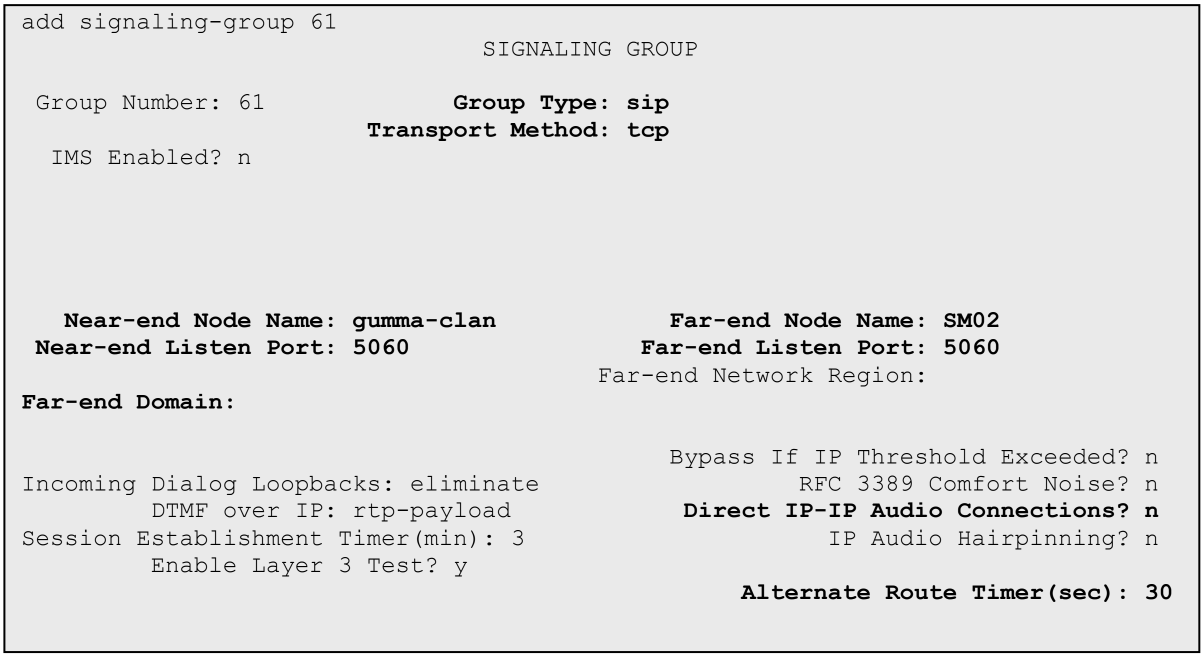
Configure the **Signaling Group** form using the "**add signaling-group**" command to add a new signaling group for SIP trunk between Communication Manager and Session Manager.

- Set the **Group Type** field to ***sip***.
- The **Transport Method** field will display ***tls*** as the default. In these Application Notes, this field was changed to ***tcp*** to allow the capture of SIP messages between Communication Manager and Session Manager.
- Specify the node names (i.e. ***gumma-clan*** and ***SM02***) assigned to the C-LAN board of the Avaya G650 Media Gateway and the SM-100 in Session Manager as shown in **Figure 7** of **4.3** in the **Near-end Node Name** field and **Far-end Node Name** field, respectively.
- Ensure that the recommended TCP port value of ***5060*** is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields. (Note: If using ***tls*** as the transport method, these values should be set to ***5061***.)
- **Direct IP-IP Audio Connections** field must be set to ***n*** because NextGen NX-E1010 cannot bridge two or more media streams. For example, assume the case that a call has been established between a user (user-A) in the enterprise site and a user (user-B) in the SIP service provider and user-A transfers the call to another user (user-C) in the SIP service provider. If the field is ***n***, two SIP trunks (trunk-a and trunk-b) assigned to the signaling group terminate the media streams between user-A and user-B (where trunk-a

terminates the media stream for user-A and trunk-b terminates the media stream for user-B). When the established call between user-A and user-B is transferred to user-C, another SIP trunk (trunk-c) assigned to the signaling group terminates the new media stream for user-C, trunk-a is released, and trunk-b and trunk-c bridge between user-B and user-C. If the field is set to ***y***, no SIP trunk bridges such call and the transferred call will be dropped.

- Extend the value for the **Alternate Route Timer (sec)** field from the default value "6" if necessary. If the period from sending INVITE request from the SIP trunk to receiving a non-100 response message exceeds this value, Communication Manager regards the request as being failed and tries to establish the call by using a different route. The actual Timer value may vary. In this case, the value is extended to ***30***.

Note that the **Far-end Domain** field must be blank. If this field is set, the value is used as the host portion in the Uniform Resource Identifier (URI) of the "SIP To Address" and the Request URI in the INVITE message, and only SIP messages which involve the value in the host portion of the SIP From Address are accepted by Communication Manager. This means an anonymous call will be rejected because the "From" address for a typical anonymous call doesn't include IP address, e.g. "anonymous@anonymous.invalid". Therefore the **Far-end Domain** field must be empty. In this case, IP address of the Near-end Node will be used for the host portion of the SIP To Address in the INVITE message.



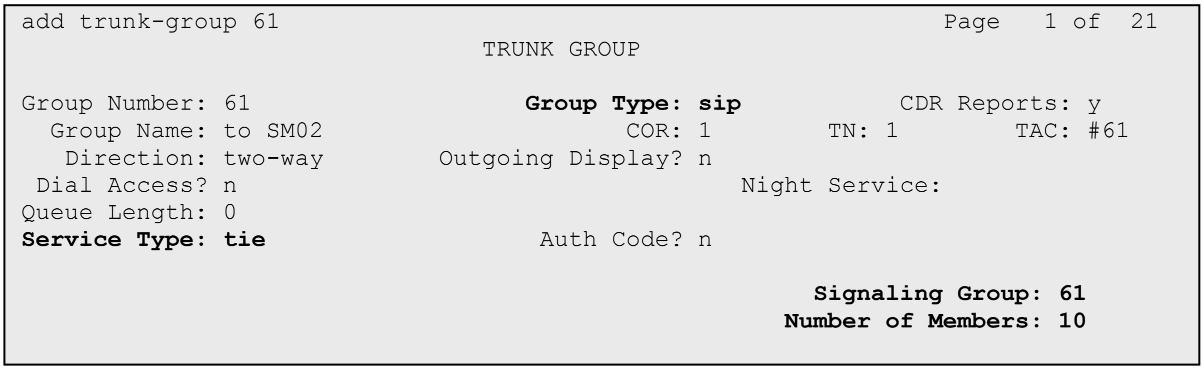
```
add signaling-group 61
                                SIGNALING GROUP

 Group Number: 61             Group Type: sip
                        Transport Method: tcp
  IMS Enabled? n





   Near-end Node Name: gumma-clan            Far-end Node Name: SM02
 Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                        Far-end Network Region:
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? y
                                                  Alternate Route Timer(sec): 30
```

Figure 11: Signaling Group Form

4.8. Administer Trunk Group

Configure the **Trunk Group** form using the “**add trunk-group**” command to add a new trunk group for SIP trunk between Communication Manager and Session Manager. On Page 1 of this form:

- Set the **Group Type** field to ***sip***.
- Set the **Service Type** field to ***tie***.
- Specify the signaling group associated with this trunk group in the **Signaling Group** field as previously specified in **Figure 11** of **4.7**. In this case, ***61*** is used.
- Specify the **Number of Members** supported by this SIP trunk group. The actual number of trunk members may vary. In this case, ***10*** is set.

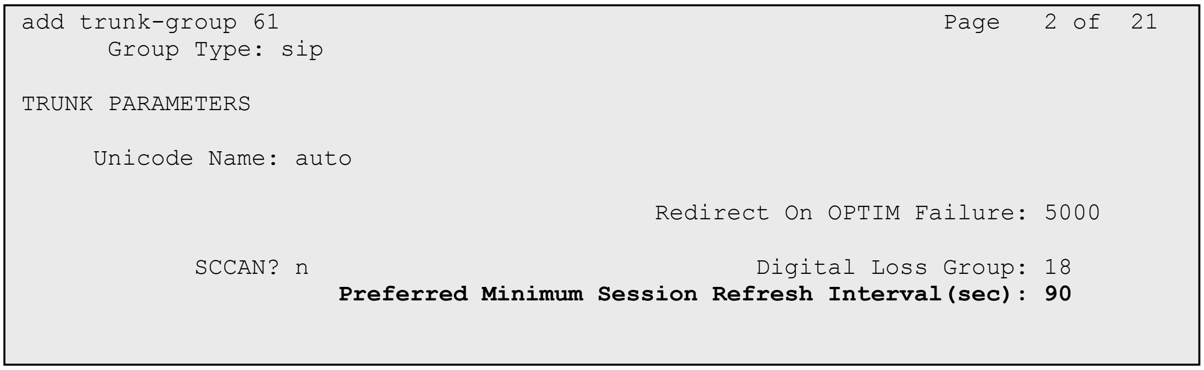


```
add trunk-group 61                                              Page   1 of  21
                                TRUNK GROUP

Group Number: 61                   Group Type: sip           CDR Reports: y
  Group Name: to SM02                     COR: 1        TN: 1        TAC: #61
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n

                                                       Signaling Group: 61
                                                     Number of Members: 10
```

Figure 12: Trunk Group Form – Page 1

On **Page 2** of this form:

- To reduce SIP messages, make the session refresh interval the same value on both sides, Communication Manager and NextGen NX-E1010. If the value on Communication Manager is larger than one on NextGen NX-E1010, Communication Manager replies “422 Session Interval Too Small” response during the session timer negotiation. Note that double the value of the **Preferred Minimum Session Refresh Interval (sec)** field is set to Min-SE and Session-Expires header fields. The actual timer value may vary. In this case, Communication Manager and NextGen NX-E1010 use ***90***.

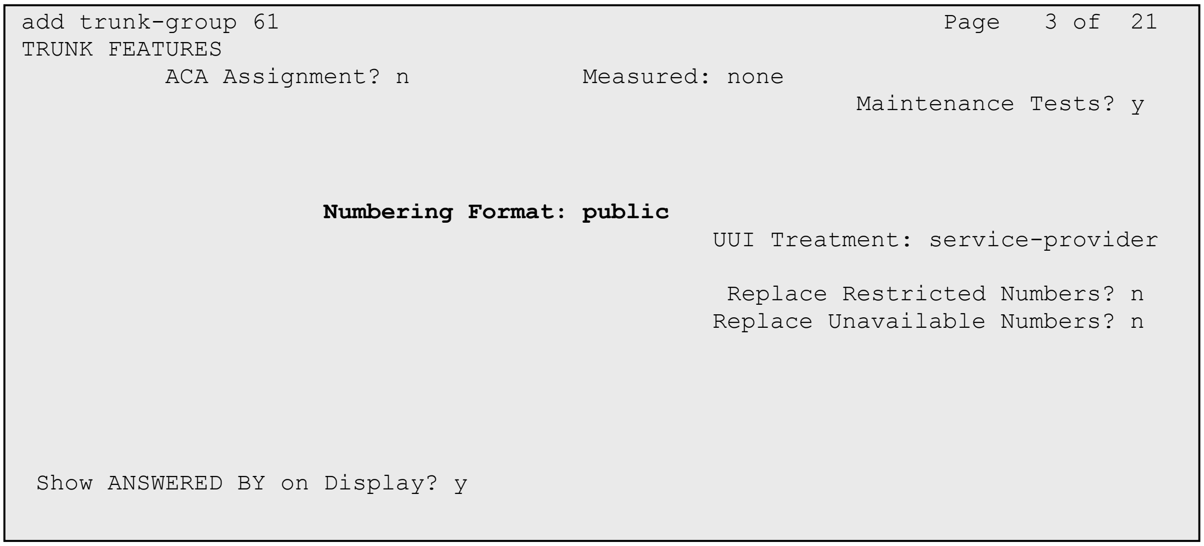


```
add trunk-group 61                                              Page   2 of  21
      Group Type: sip

TRUNK PARAMETERS

     Unicode Name: auto

                                            Redirect On OPTIM Failure: 5000

            SCCAN? n                               Digital Loss Group: 18
                      Preferred Minimum Session Refresh Interval(sec): 90
```

Figure 13: Trunk Group Form – Page 2

On **Page 3** of this form:

- Set the **Numbering Format** field to ***public***



```
add trunk-group 61                                              Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y



                     Numbering Format: public
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n





 Show ANSWERED BY on Display? y
```

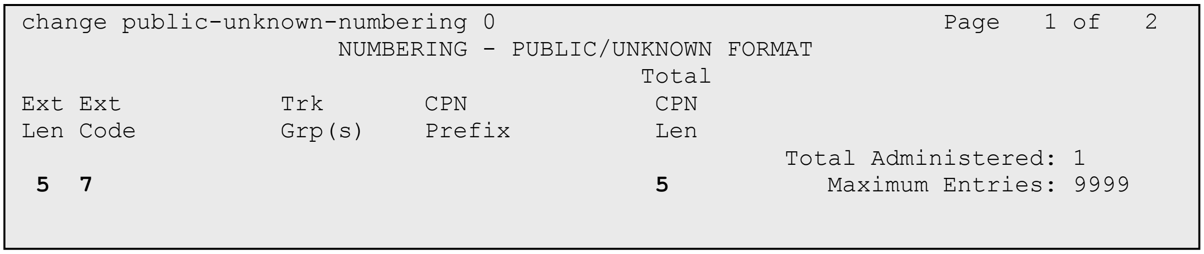
Figure 14: Trunk Group Form – Page 3

4.9. Administer Calling Party Number Information

Configure the **Numbering Public/Unknown Format** form to send the calling party extension to NextGen NX-E1010.

In these Application Notes, when a call is originated from a station in the enterprise site, the extension number assigned to the station is used as the calling party number of the call. If the call goes to the simulated SIP Service Provider via NextGen NX-E1010, NextGen NX-E1010 converts from the extension number to the pilot number.

Use the **change public-unknown-numbering 0** command and configure as shown below since all stations in the enterprise site have a 5-digit extension beginning with 7.



```
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  7                                      5            Maximum Entries: 9999
```

Figure 15: Numbering Public/Unknown Format Form

4.10. Administer Call Routing

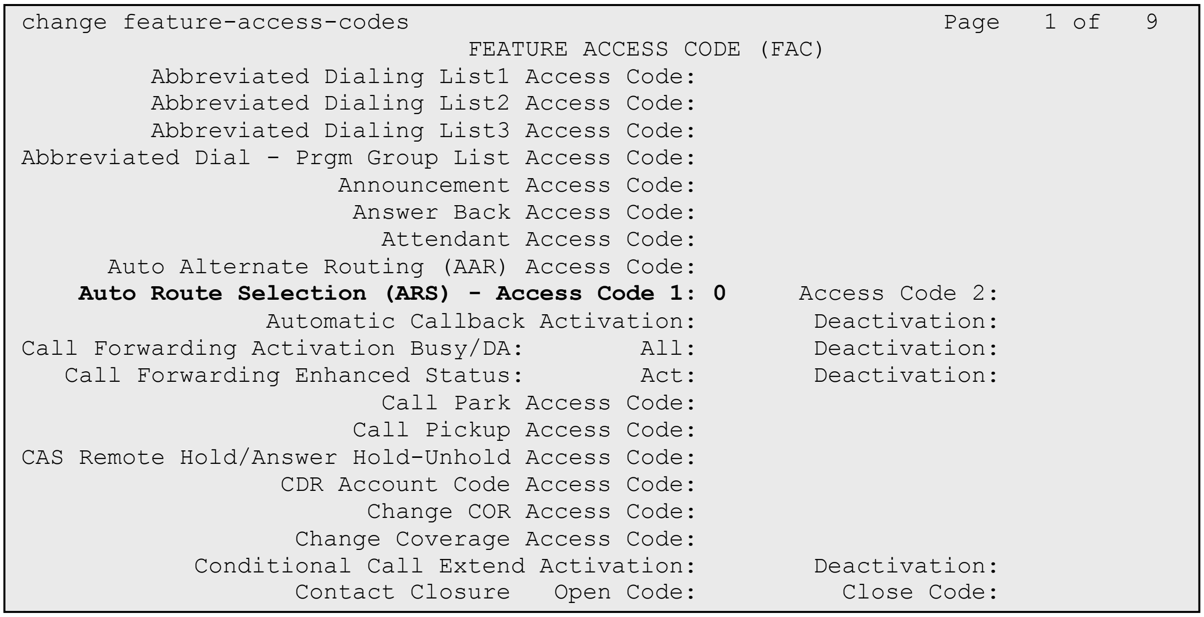
The following Sections describe Communication Manager provisioning required for outbound dialing. Communication Manager uses ARS to direct outbound calls to Session Manager.

4.10.1. Administer ARS

The Automatic Route Selection feature is used to route calls via the SIP trunks to Session Manager, which in turn completes the calls to NextGen NX-E1010. In the reference configuration ARS is triggered by dialing a 0 (feature access code or FAC) and then dialing the called number. ARS matches on the called number and sends the call to a specified route pattern.

Use the **change feature-access-codes** command to specify **0** as the access code for external dialing.

- Set **Auto Route Selection (ARS) – Access Code 1:** to ***0***.



```
change feature-access-codes                                     Page   1 of   9
                               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:
```

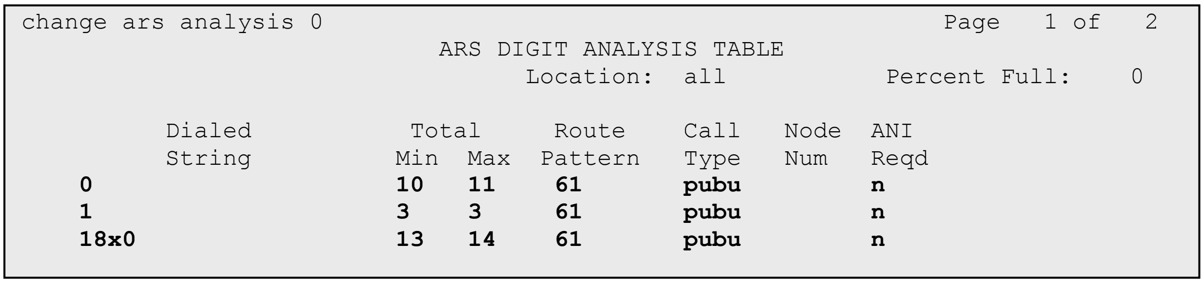
Figure 16: Feature Access Code Form

Use the **change ars analysis** command to configure the route pattern selection rule based upon the number dialed following the ARS access digit "0". In the reference configuration, outbound calls are placed to the Simulated SIP Service Provider Network:

Dialed digits			Notes
Beginning with	Min.	Max.	
0	10	11	Public telephone numbers in Japan e.g. 03-5575-8700 (PSTN), 090-2625-9509 (Cellular), 050-3381-3855 (IP telephony service)
18x0	13	14	CLIR/CLIP prefix (184/186) + Public telephone number The length of these prefixes is 3, and the length of the public telephone numbers is from 10 to 11. Thus the length of this is from 13 to 14.
1	3	3	Numbers for emergency/public related services

To specify these calls, enter the command **change ars analysis 0** and enter the following values:

- For the 0 calls:
  - ▷ Set the **Dialed String** field to ***0***
  - ▷ Set the **Total Min** field to ***10***
  - ▷ Set the **Total Max** field to ***11***
  - ▷ Set the **Route Pattern** field to ***61*** (will direct to SIP trunk)
  - ▷ Set the **Type** field to ***pubu***
- For the 1 calls:
  - ▷ Set the **Dialed String** field to
  - ▷ Set the **Total Min** field to ***3***
  - ▷ Set the **Total Max** field to ***3***
  - ▷ Set the **Route Pattern** field to ***61*** (will direct to SIP trunk)
  - ▷ Set the **Type** field to ***pubu***
- For the 18 calls:
  - ▷ Set the **Dialed String** field to ***18x0***
  - ▷ Set the **Total Min** field to ***13***
  - ▷ Set the **Total Max** field to ***14***
  - ▷ Set the **Route Pattern** field to ***61*** (will direct to SIP trunk)
  - ▷ Set the **Type** field to ***pubu***

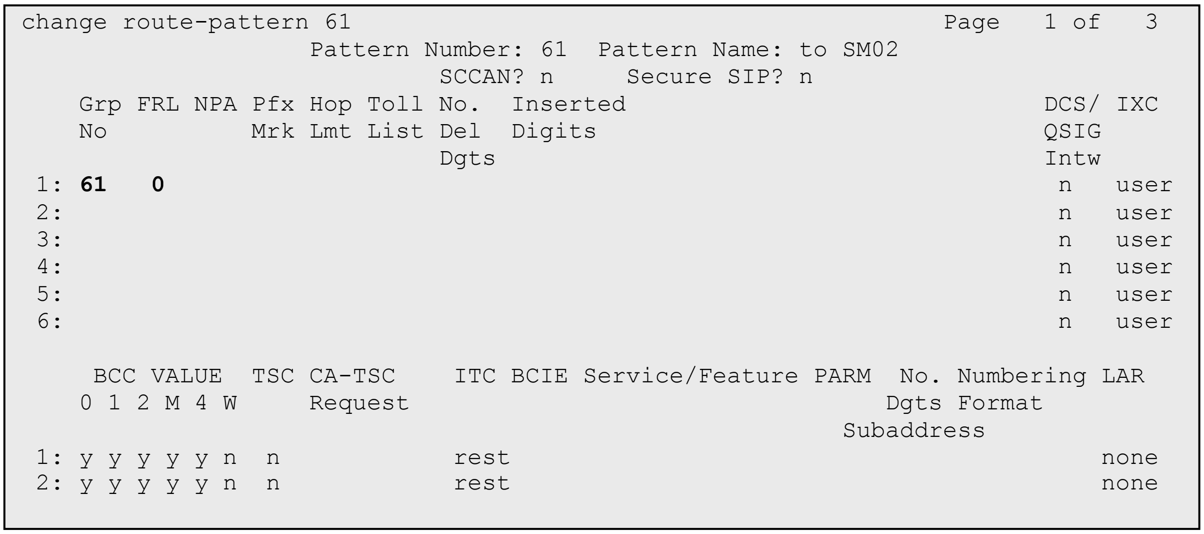


```
change ars analysis 0                                           Page   1 of   2
                             ARS DIGIT ANALYSIS TABLE
                                   Location:  all           Percent Full:    0

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    0                     10   11    61       pubu         n
    1                     3    3     61       pubu         n
    18x0                  13   14    61       pubu         n
```

Figure 17: ARS Digit Analysis Form

4.10.2. Administer Route Pattern

Configure the **Route Pattern** form to route calls to the SIP trunk. The number of the SIP trunk group for Session Manager, which is administered on **4.8**, is ***61***. Thus, set **61** for the **Grp No** field.

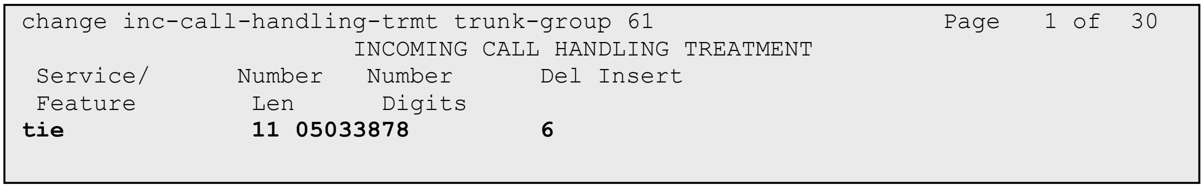


```
change route-pattern 61                                         Page   1 of   3
                    Pattern Number: 61  Pattern Name: to SM02
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                             DCS/ IXC
    No          Mrk Lmt List Del  Digits                               QSIG
                             Dgts                                      Intw
 1: 61   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
```

Figure 18: Route Pattern Form

4.11. Administer Incoming Digit Translation

Configure the **Incoming Call Handling Treatment** form to map incoming DID calls to the proper extension.
In these Application Notes, the last five-digit numbers of the public telephone numbers assigned by the Simulated SIP Service Provider are used as the extensions within the enterprise site. And each public telephone number is an eleven-digit number beginning with "05033878". Therefore the first six digits of the incoming called number are deleted to convert from a public telephone number to the corresponding extension.



```
change inc-call-handling-trmt trunk-group 61                Page   1 of  30
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
tie             11 05033878         6
```

Figure 19: Incoming Call Handling Treatment Form

4.12. Save Communication Manager Changes

Enter "**save translations**" to make the changes permanent.

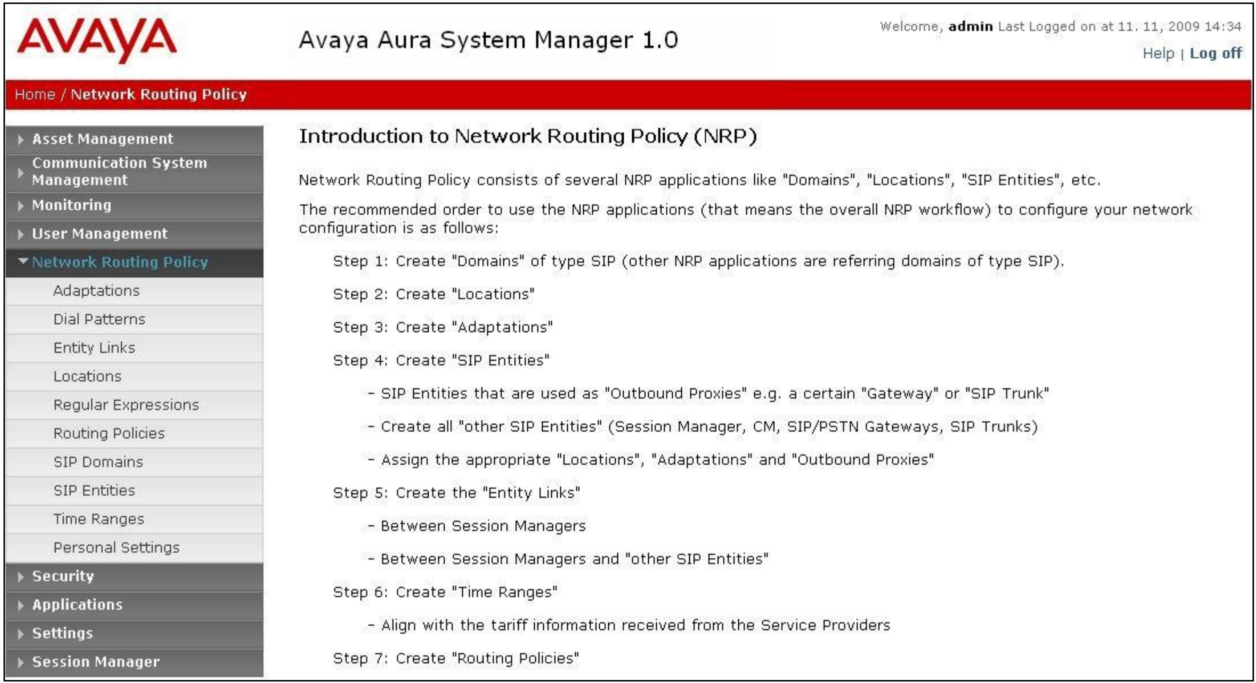
5. Configure Session Manager

This section provides the procedures for configuring Session Manager. Session Manager must be administered via System Manager. The procedures include the following steps:

- Create “Domains” of type SIP
- Create “Locations”
- Create “Adaptations”
- Create “SIP Entities” (Session Manager, SIP Trunk, and NextGen NX-E1010)
- Create “Entity Links” between Session Manager and other SIP Entities
- Create “Routing Policies”
- Create “Dial Pattern”, and assign the appropriate “Locations” and “Routing Policies” to the “Dial Pattern”

5.1. Log into System Manager

Access System Manager web interface, by entering ***http://<ip-addr>/SMGR*** as the URL in a web browser, where ***<ip-addr>*** is the IP address or FQDN of System Manager.
Select the **Network Routing Policy** link from the left pane of the home screen shown after logged in to the System Manager. The System Manager **Network Routing Policy** screen shown in **Figure 20** should be displayed.



Introduction to Network Routing Policy (NRP)

Network Routing Policy consists of several NRP applications like "Domains", "Locations", "SIP Entities", etc.

The recommended order to use the NRP applications (that means the overall NRP workflow) to configure your network configuration is as follows:

Step 1: Create "Domains" of type SIP (other NRP applications are referring domains of type SIP).

Step 2: Create "Locations"

Step 3: Create "Adaptations"

Step 4: Create "SIP Entities"

- SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
- Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)
- Assign the appropriate "Locations", "Adaptations" and "Outbound Proxies"

Step 5: Create the "Entity Links"

- Between Session Managers
- Between Session Managers and "other SIP Entities"

Step 6: Create "Time Ranges"

- Align with the tariff information received from the Service Providers

Step 7: Create "Routing Policies"

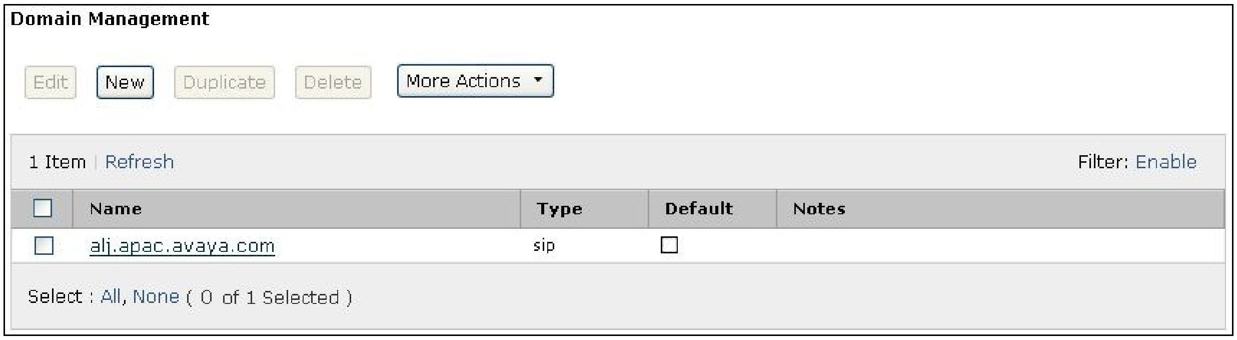
Figure 20: Network Routing Policy Screen

5.2. Create SIP Domain

To create a SIP Domain, select the "**SIP Domains**" option from the left pane menu and click the **New** button.

- Enter the domain name specified to the **Authoritative Domain** field on the **IP Network Region** form (**Figure 9)** in the **Name** field. In this case, it is ***alj.apac.avaya.com*** (not shown).
- Select ***sip*** as the **Type** (not shown).
- Click the **Commit** button to save these (not shown).

The SIP domain enables Session Manager to use domain-based routing. This information is used to determine if a SIP user is part of the SIP network. **Figure 21** shows the page after creating the SIP Domain.



□	Name	Type	Default	Notes
□	alj.apac.avaya.com	sip	□	

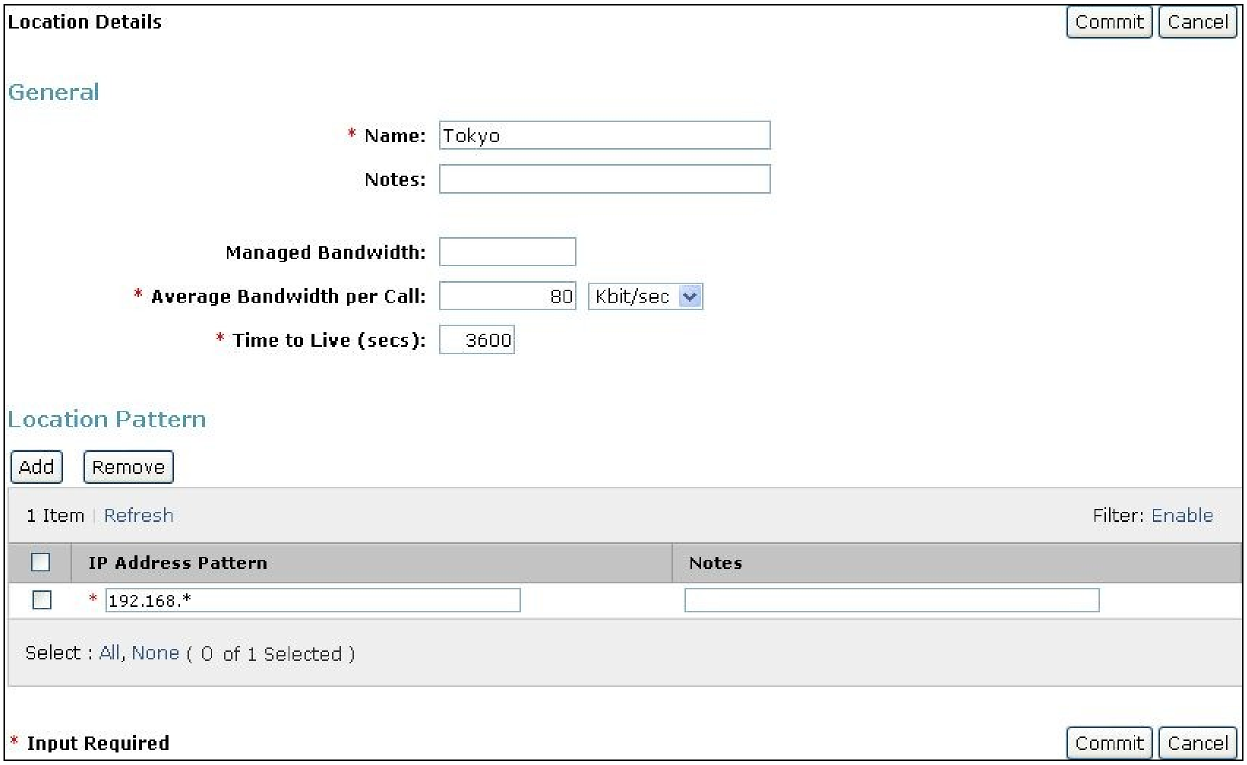
Select : All, None (0 of 1 Selected)

Figure 21: SIP Domains Screen

5.3. Create Location

To create a Location for the enterprise site, select the "**Locations**" option from the left pane menu and click the **New** button (not shown).

- Enter a descriptive name in the **Name** field. In this case, it is ***Tokyo***.
- Click the **Add** button to specify the IP address for the location.
- Enter IP address pattern assigned to the enterprise site in the **IP Address Pattern** field. In these Application Notes, the enterprise site uses some subnets, 192.168.153.0/24, 192.168.168.0/24, and so on. Therefore ***192.168.**** is set, where "*" means a wild card.
- Click the **Commit** button to save them.



Location Details

General

* Name:	Tokyo
Notes:	
Managed Bandwidth:	
* Average Bandwidth per Call:	80 Kbit/sec
* Time to Live (secs):	3600

Location Pattern

1 Item | Refresh

□	IP Address Pattern	Notes
□	* 192.168.*	

Select : All, None (0 of 1 Selected)

* Input Required

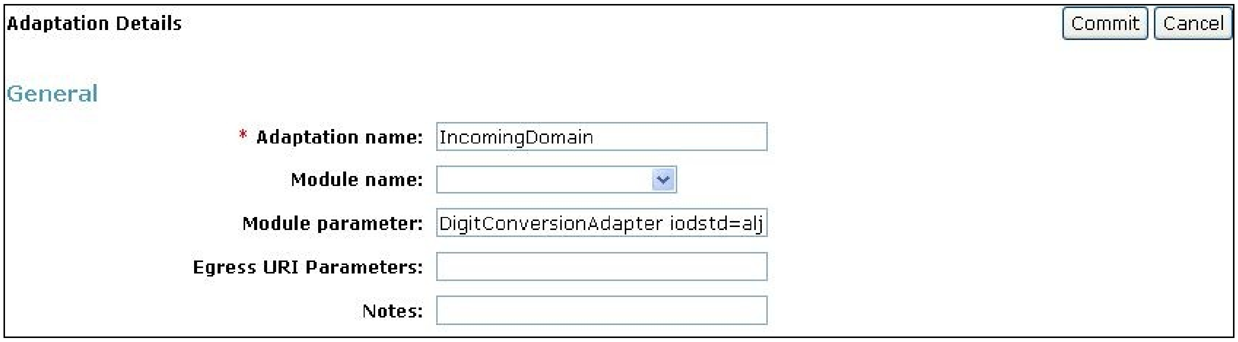
Figure 22: Locations Screen

5.4. Create Adaptation

Session Manager makes domain-based routing. However the Request URI of SIP messages from Communication Manager contain an IP address, not a DNS domain name, because the **Far-end Domain** field of the SIP signaling group form is empty as mentioned in **Section 4.7**. In these Application Notes, an Adaptation module is used to modify the IP address in the Request URI to a proper DNS domain name so that Session Manager can treat SIP messages based on domain-based routing.

To create an Adaptation module, select the "**Adaptations**" option from the left pane menu and click the **New** button (not shown).

- Enter a descriptive name in the **Adaptation name** field. In this case, it is ***IncomingDomain***.
- Enter a proper adapter module name and parameter in the **Module parameter** field. In these Application Notes, ***DigitConversionAdapter*** module is specified as the **Module name**, and ***iodstd=alj.apac.avaya.com*** is specified as the parameter. This replaces the host part of Request URI with "alj.apac.avaya.com" for all incoming SIP messages to Session Manager.
- Click the **Commit** button to save them.



* Adaptation name:	IncomingDomain
Module name:	
Module parameter:	DigitConversionAdapter iodstd=alj
Egress URI Parameters:	
Notes:	

Figure 23: Adaptations Screen

5.5. Create SIP Entities

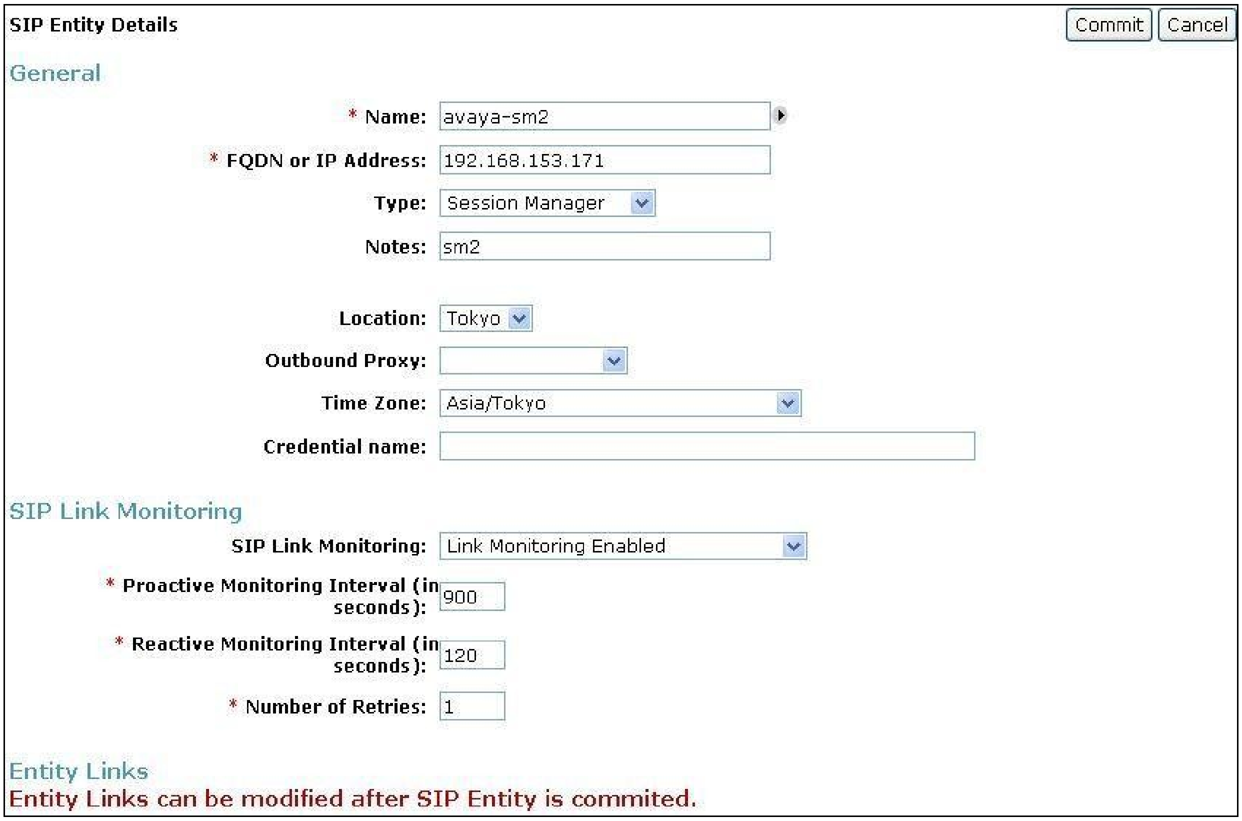
In these Application Notes, three SIP Entities, Session Manager, SIP trunk on Communication Manager, and NextGen NX-E1010 should be created. To create a SIP Entity, select the "**SIP Entities**" option from the left pane menu and click the **New** button on the **SIP Entities** screen.

Figure 24: SIP Entities Screen

5.5.1. Create SIP Entity for Session Manager

On the **SIP Entity Details** screen which is displayed by clicking the **New** button on the **SIP Entities** screen, perform the following to create SIP Entity for Session Manager:

- Enter a descriptive name in the **Name** field. In this case, it is "***avaya-sm2***".
- Enter FQDN or IP address of SM-100 Security Module in the **FQDN or IP Address** field. In this case, it is IP address of SM-100, "***192.168.153.171***" (see **Figure 1** and **Figure 8**).
- Select ***Session Manager*** from the drop-down list for the **Type** field.
- Select ***Tokyo*** from the drop-down list for the **Location** field as the location for the enterprise site.
- Select ***Asia/Tokyo*** from the drop-down list for the **Time Zone** field as the time zone of Tokyo.
- Add SIP transport protocols supported by this Session Manager on the **Port** section. The SIP trunk for Session Manager on Communication Manager is administered as using TCP (see **Figure 11**), and NextGen NX-E1010 supports only User Datagram Protocol (UDP). Therefore ***TCP*** and ***UDP*** are added and the default port, ***5060*** is specified for them. (Note that TLS is not used in these Application Notes.)
- Click the **Commit** button to save them.



General

* Name: avaya-sm2

* FQDN or IP Address: 192.168.153.171

Type: Session Manager

Notes: sm2

Location: Tokyo

Outbound Proxy:

Time Zone: Asia/Tokyo

Credential name:

SIP Link Monitoring

SIP Link Monitoring: Link Monitoring Enabled

* Proactive Monitoring Interval (in seconds): 900

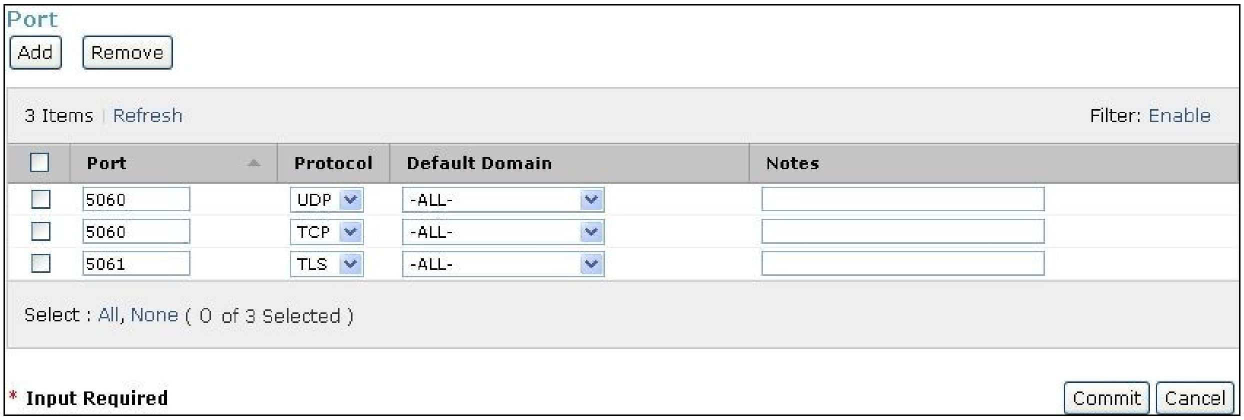
* Reactive Monitoring Interval (in seconds): 120

* Number of Retries: 1

Entity Links

Entity Links can be modified after SIP Entity is commited.

Figure 25: SIP Entity Details Screen for Session Manager



Port

Add Remove

3 Items | Refresh   Filter: Enable

□	Port	Protocol	Default Domain	Notes
□	5060	UDP	-ALL-	
□	5060	TCP	-ALL-	
□	5061	TLS	-ALL-	

Select : All, None (0 of 3 Selected)

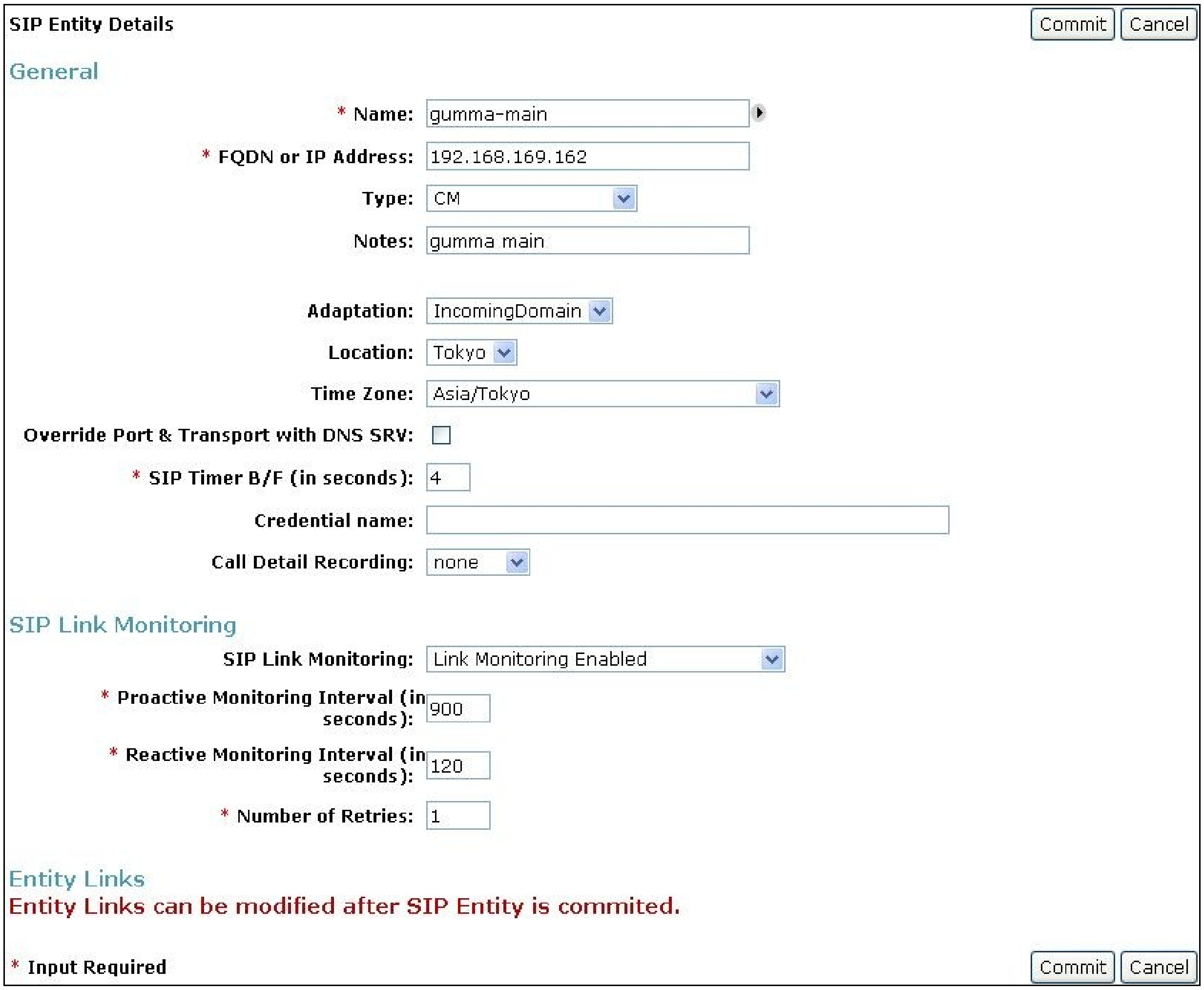
* Input Required   Commit Cancel

Figure 26: SIP Entity Details Screen – Port Section

5.5.2. Create SIP Entity for Communication Manager

On the **SIP Entity Details** screen which is displayed by clicking the **New** button on the **SIP Entities** screen, perform the following to create SIP Entity for Communication Manager:

- Enter a descriptive name in the **Name** field. In this case, it is "***gumma-main***".
- Enter FQDN or IP address of the SIP trunk on Communication Manager in the **FQDN or IP Address** field. In this case, it is IP address of CLAN, "***192.168.169.162***" (see **Figure 1** and **Figure 8**).
- Select ***CM*** from the drop-down list for the **Type** field.
- Select the ***IncomingDomain*** adaptation module from the drop-down list for the **Adaptation** field. This adaptation module will be applied all SIP messages from this SIP Entity.
- Select ***Tokyo*** from the drop-down list for the **Location** field as the location for the enterprise site.
- Select ***Asia/Tokyo*** from the drop-down list for the **Time Zone** field as the time zone of Tokyo.
- Select ***Link Monitoring Enabled*** from the drop-down list for the **SIP Link Monitoring** filed so that Session Manager can monitor the link between this SIP Entity and itself.
- Click the **Commit** button to save them.



General

* Name:	gumma-main
* FQDN or IP Address:	192.168.169.162
Type:	CM
Notes:	gumma main
Adaptation:	IncomingDomain
Location:	Tokyo
Time Zone:	Asia/Tokyo
Override Port & Transport with DNS SRV:	□
* SIP Timer B/F (in seconds):	4
Credential name:	
Call Detail Recording:	none

SIP Link Monitoring

SIP Link Monitoring:	Link Monitoring Enabled
* Proactive Monitoring Interval (in seconds):	900
* Reactive Monitoring Interval (in seconds):	120
* Number of Retries:	1

Entity Links

Entity Links can be modified after SIP Entity is commited.

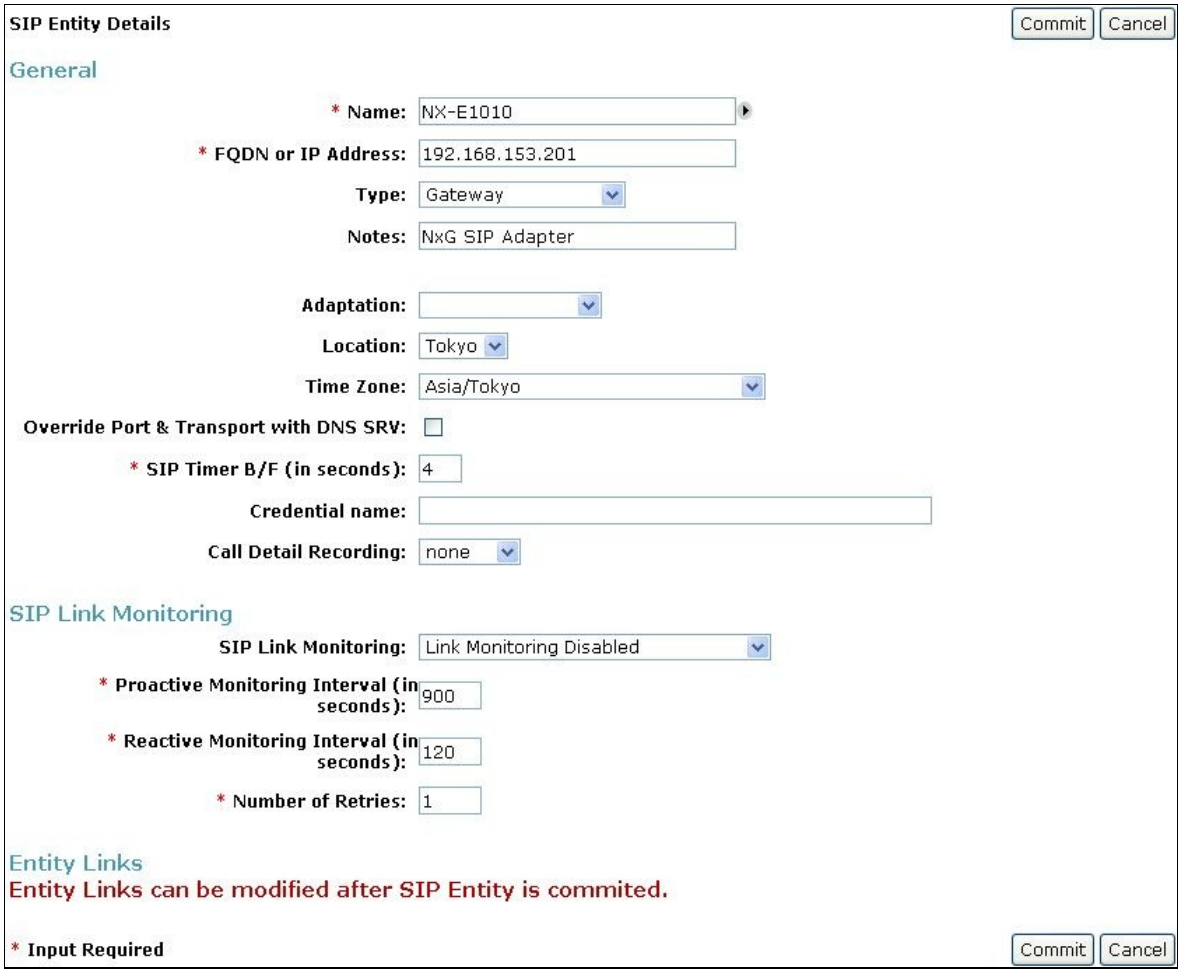
* Input Required

Figure 27: SIP Entity Details Screen for Communication Manager

5.5.3. Create SIP Entity for NextGen NX-E1010

On the **SIP Entity Details** screen which is displayed by clicking the **New** button on the **SIP Entities** screen, perform the following to create SIP Entity for NextGen NX-E1010:

- Enter a descriptive name in the **Name** field. In this case, it is "***NX-E1010***".
- Enter FQDN or IP address of the network interface on the enterprise side of the NextGen NX-E1010 in the **FQDN or IP Address** field. In this case, it is IP address of CLAN, "***192.168.153.201***" (see **Figure 1).**
- Select ***Gateway*** from the drop-down list for the **Type** field.
- Select ***Tokyo*** from the drop-down list for the **Location** field as the location for the enterprise site.
- Select ***Asia/Tokyo*** from the drop-down list for the **Time Zone** field as the time zone of Tokyo.
- Select ***Link Monitoring Disabled*** from the drop-down list for the **SIP Link Monitoring** filed. The SIP Link Monitoring is done by periodically sending an OPTIONS message from Session Manager. However NextGen NX-E1010 doesn't support the OPTIONS request.
- Click the **Commit** button to save them.



SIP Entity Details

General

* Name:	NX-E1010
* FQDN or IP Address:	192.168.153.201
Type:	Gateway
Notes:	NxG SIP Adapter
Adaptation:	
Location:	Tokyo
Time Zone:	Asia/Tokyo
Override Port & Transport with DNS SRV:	□
* SIP Timer B/F (in seconds):	4
Credential name:	
Call Detail Recording:	none

SIP Link Monitoring

SIP Link Monitoring:	Link Monitoring Disabled
* Proactive Monitoring Interval (in seconds):	900
* Reactive Monitoring Interval (in seconds):	120
* Number of Retries:	1

Entity Links

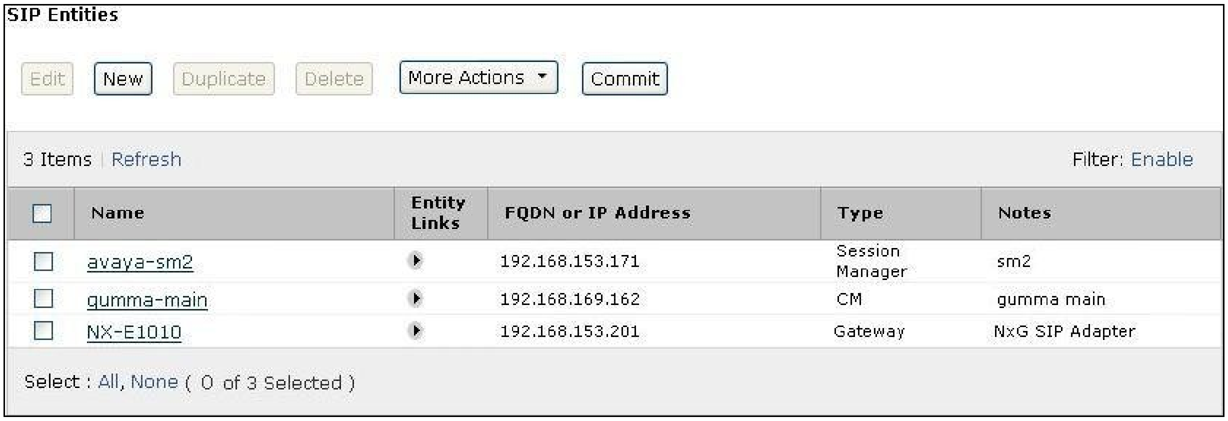
Entity Links can be modified after SIP Entity is commited.

* Input Required

Figure 28: SIP Entity Details Screen for NextGen NX-E1010

5.5.4. Confirm SIP Entities

As a result of the above administration, three SIP Entities are created.



□	Name	Entity Links	FQDN or IP Address	Type	Notes
□	avaya-sm2	▸	192.168.153.171	Session Manager	sm2
□	gumma-main	▸	192.168.169.162	CM	gumma main
□	NX-E1010	▸	192.168.153.201	Gateway	NxG SIP Adapter

Figure 29: Result of Creating SIP Entities

5.6. Create Entitiy Links

In these Application Notes, two Entity Links, between Session Manager and Communication Manager, and between Session Manager and NextGen NX-E1010, should be created. To create an Entity Link, select the "**Entity Links**" option from the left pane menu and click the **New** button on the **Entity Links** screen.

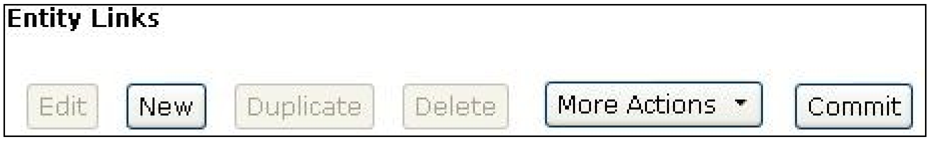
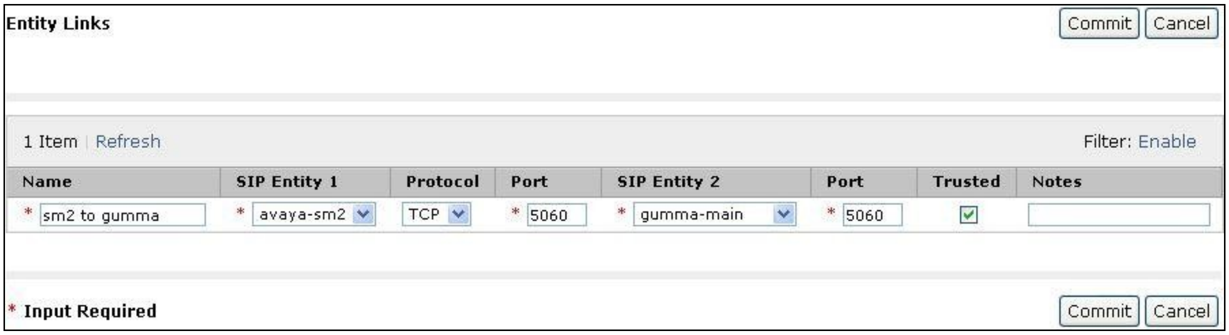


Figure 30: Entity Links Screen

5.6.1. Create Entity Link between Communication Manager and Session Manager

On the **Entity Links** screen which is displayed by clicking the **New** button on the **Entity Links** screen, perform the following to create an Entity Link between Communication Manager and Session Manager:

- Enter a descriptive name in the **Name** field. In this case, it is "***sm2 to gumma***".
- Select ***avaya-sm2*** as the SIP Entity name for Session Manager from the drop-down list for the **SIP Entity 1** field.
- Select ***gumma-main*** as the SIP Entity name for Communication Manager from the drop-down list for the **SIP Entity 2** field.
- Select ***TCP*** as the SIP transport protocol for this Entity Link from the drop-down list for the **Protocol** field.
- Make sure that both Port fields display the port number, ***5060*** which is specified on the **Port** section of the SIP Entity Details screen for Session Manager (see **Figure 26**).
- Check the **Trusted** check box so that "avaya-sm2" can accept SIP messages from "gumma-main".
- Click the **Commit** button to save them.



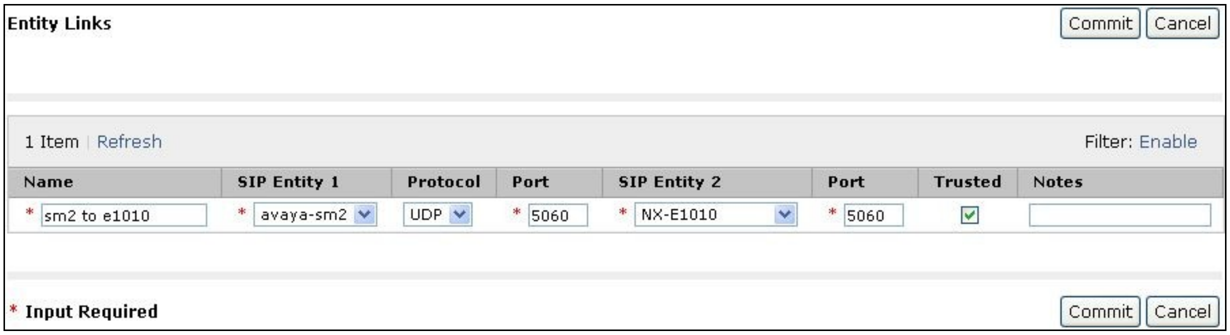
Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* sm2 to gumma	* avaya-sm2	TCP	* 5060	* gumma-main	* 5060	☑	

Figure 31: Entity Links Setting Screen (1)

5.6.2. Create Entity Link between NextGen NX-E1010 and Session Manager

On the **Entity Links** screen which is displayed by clicking the **New** button on the **Entity Links** screen, perform the following to create an Entity Link between NextGen NX-E1010 and Session Manager:

- Enter a descriptive name in the **Name** field. In this case, it is "***sm2 to e1010***".
- Select ***avaya-sm2*** as the SIP Entity name for Session Manager from the drop-down list for the **SIP Entity 1** field.
- Select ***NX-E1010*** as the SIP Entity name for NextGen NX-E1010 from the drop-down list for the **SIP Entity 2** field.
- Select ***UDP*** as the SIP transport protocol for this Entity Link from the drop-down list for the **Protocol** field.
- Make sure that both Port fields display the port number, ***5060*** which is specified on the **Port** section of the SIP Entity Details screen for Session Manager (see **Figure 26**).
- Check the **Trusted** check box so that "avaya-sm2" can accept SIP messages from "NX-E1010".
- Click the **Commit** button to save them.

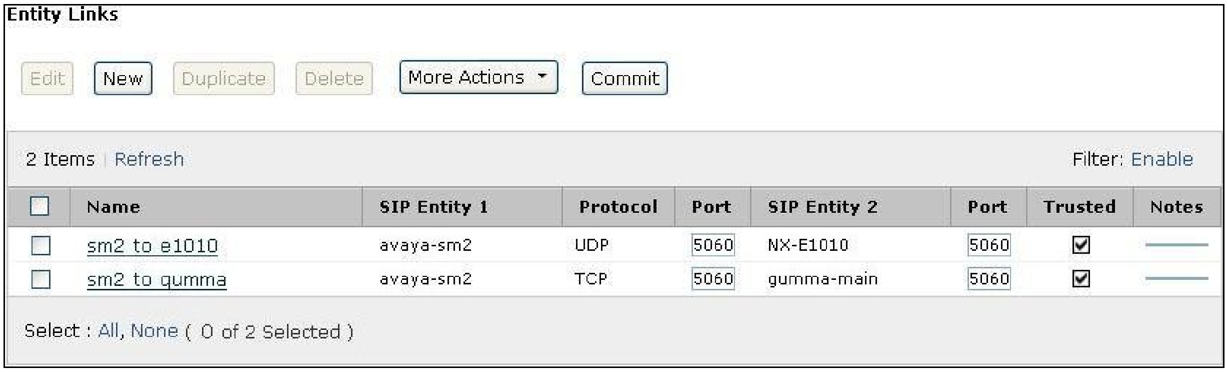


Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* sm2 to e1010	* avaya-sm2	UDP	* 5060	* NX-E1010	* 5060	☑	

Figure 32: Entity Links Setting Screen (2)

5.6.3. Confirm Entity Links

As a result of the above administration, two Entity Links are created.



□	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
□	sm2 to e1010	avaya-sm2	UDP	5060	NX-E1010	5060	☑	
□	sm2 to gumma	avaya-sm2	TCP	5060	gumma-main	5060	☑	

Figure 33: Result of Creating Entity Links

5.7. Create Routing Policies

A Routing Policy should be created for each "Routing Destination". In these Application Notes, there are two Routing Destinations, Communication Manager and NextGen NX-E1010.
To create a Routing Policy, select the "**Routing Policies**" option from the left pane menu and click the **New** button on the **Routing Policies** screen.

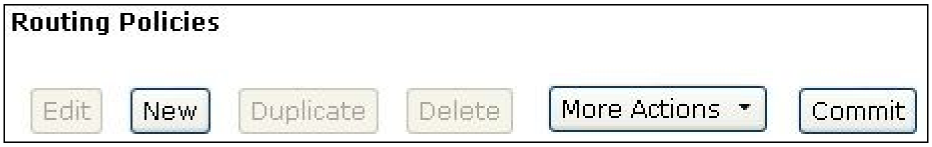
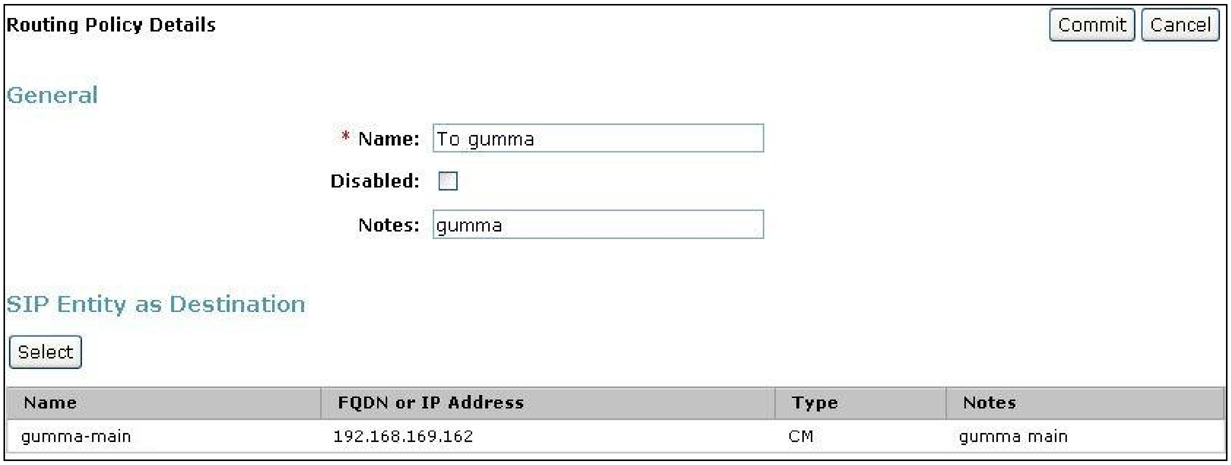


Figure 34: Routing Policies Screen

5.7.1. Create Routing Policy for Communication Manager

On the **Routing Policy Details** screen which is displayed by clicking the **New** button on the **Routing Policies** screen, perform the following to create a Routing Policy for Communication Manager:

- Enter a descriptive name in the **Name** field. In this case, it is "***To gumma***".
- Click the **Select** button on the **SIP Entity as Destination** section to define a SIP Entity as the Routing Destination for this Routing Policy. Select ***gumma-main*** as the Routing Destination from the SIP Entity List (**Figure 36**) which is displayed after clicking the **Select** button, and click the **Select** button to confirm the choice.
- Click the **Commit** button to save them.



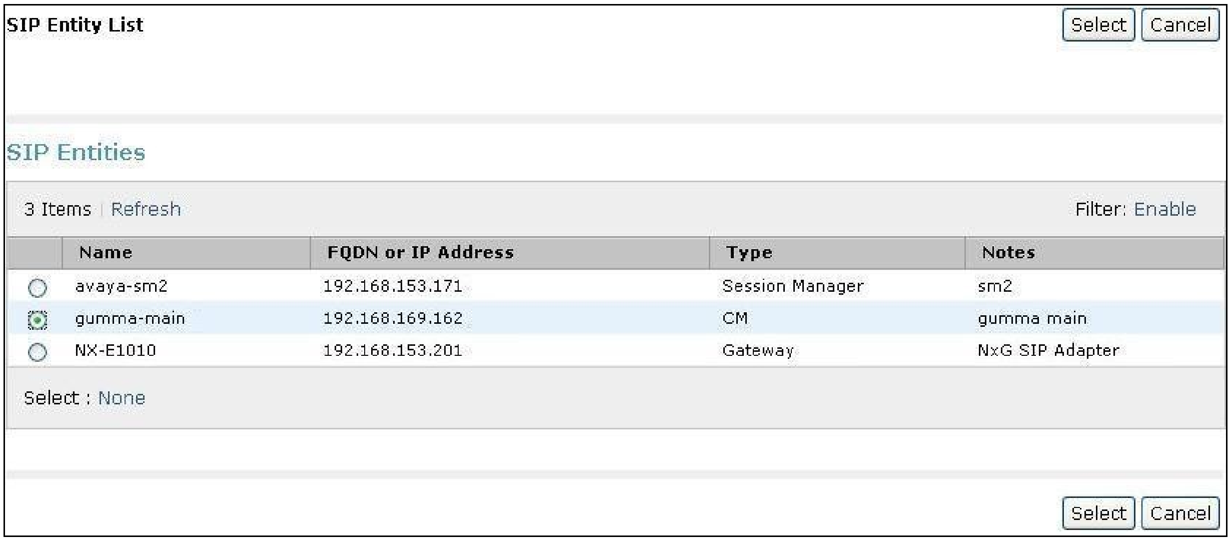
* Name: To gumma

Disabled: □

Notes: gumma

Name	FQDN or IP Address	Type	Notes
gumma-main	192.168.169.162	CM	gumma main

Figure 35: Routing Policy Details (1)



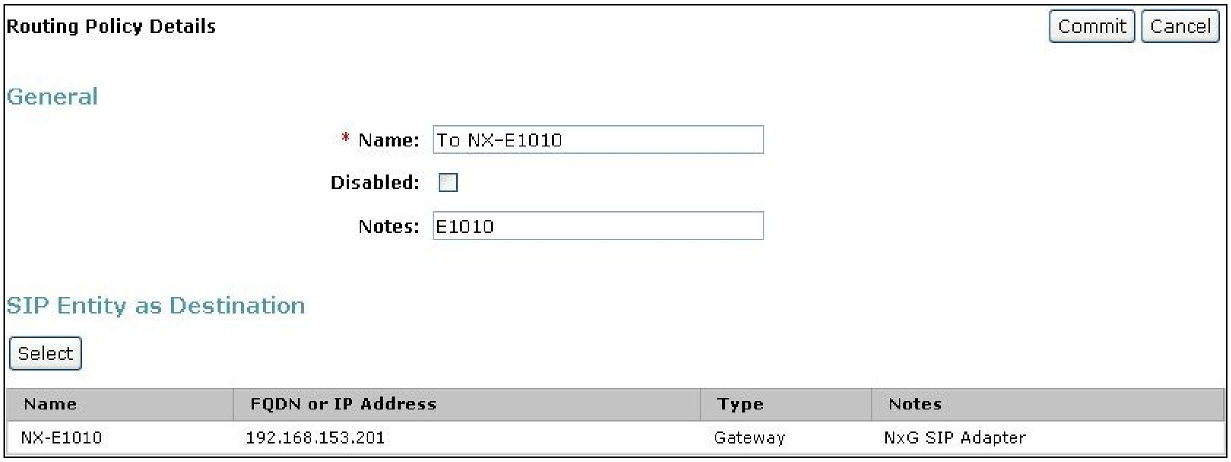
	Name	FQDN or IP Address	Type	Notes
○	avaya-sm2	192.168.153.171	Session Manager	sm2
●	gumma-main	192.168.169.162	CM	gumma main
○	NX-E1010	192.168.153.201	Gateway	NxG SIP Adapter

Figure 36: SIP Entity List for Routing Destination

5.7.2. Create Routing Policy for NextGen NX-E1010

On the **Routing Policy Details** screen which is displayed by clicking the **New** button on the **Routing Policies** screen, perform the following to create a Routing Policy for NextGen NX-E1010:

- Enter a descriptive name in the **Name** field. In this case, it is "***To NX-E1010***".
- Click the **Select** button on the **SIP Entity as Destination** section to define a SIP Entity as the Routing Destination for this Routing Policy. Select ***NX-E1010*** as the Routing Destination from the SIP Entity List (**Figure 36**) which is displayed after clicking the **Select** button, and click the **Select** button to confirm the choice.
- Click the **Commit** button to save them.



* Name: To NX-E1010

Disabled: □

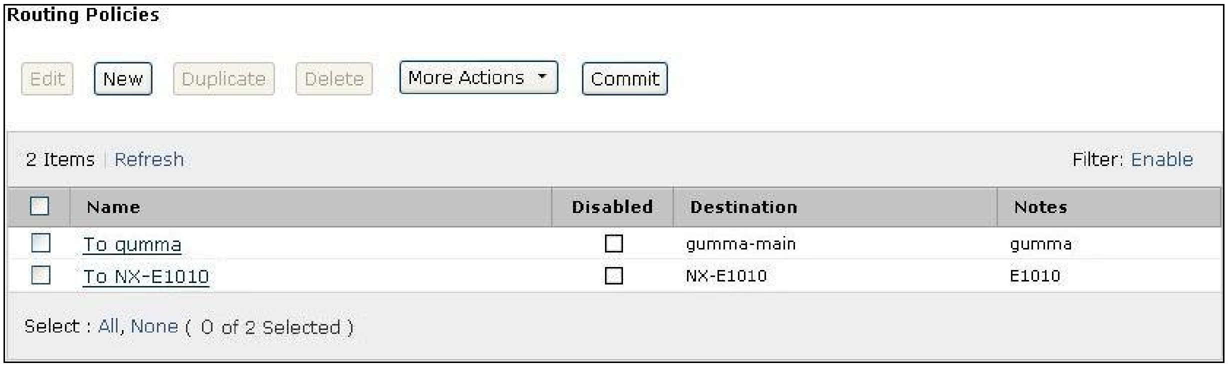
Notes: E1010

Name	FQDN or IP Address	Type	Notes
NX-E1010	192.168.153.201	Gateway	NxG SIP Adapter

Figure 37: Routing Policy Details (2)

5.7.3. Confirm Routing Policies

Two Routing Policies are created by the above.



Routing Policies

□	Name	Disabled	Destination	Notes
□	To gumma	□	gumma-main	gumma
□	To NX-E1010	□	NX-E1010	E1010

Select : All, None (0 of 2 Selected)

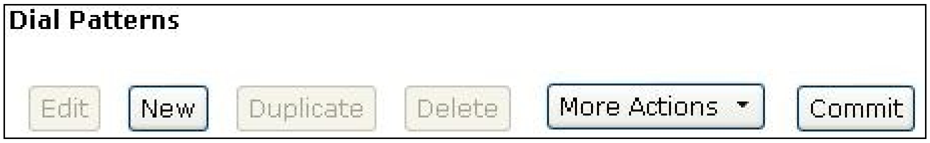
Figure 38: Result of Creating Routing Policies

5.8. Create Dial Pattern

The appropriate "Locations" and "Routing Policies" should be assigned to the "Dial Pattern". These Application Notes assume that the following dial patterns are used:

Dialed digits			Destination	Notes
Beginning with	Min.	Max.		
050338780	11	11	gumma-main	Subscription numbers for the enterprise site
0	10	11	NX-E1010	Public telephone numbers in Japan e.g. 03-5575-8700 (PSTN), 090-2625-9509 (Cellular), 050-3381-3855 (IP telephony service)
18	13	14	NX-E1010	CLIR/CLIP prefix (184/186) + Public telephone number The length of these prefixes is 3, and the length of the public telephone numbers is from 10 to 11. Thus the length of this is from 13 to 14.
1	3	3	NX-E1010	Numbers for emergency/public related services

To create a Dial Pattern, select the "**Dial Patterns**" option from the left pane menu and click the **New** button on the **Dial Patterns** screen.



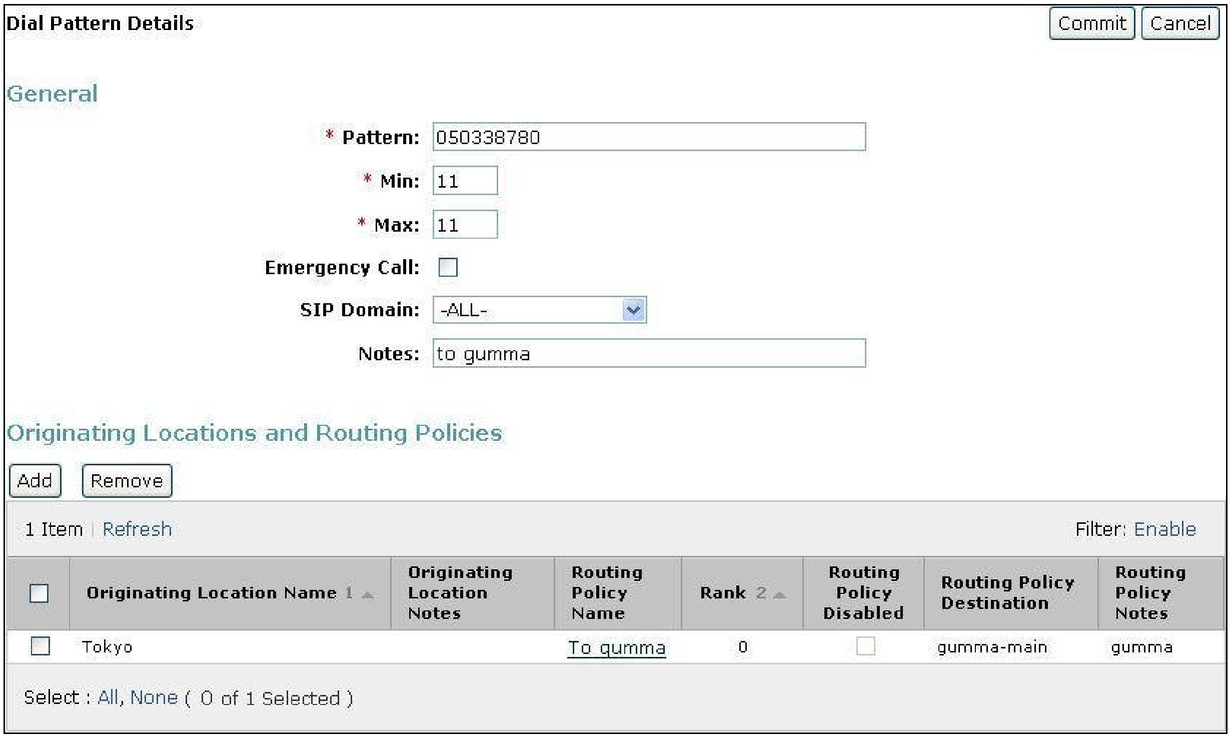
Dial Patterns

Figure 39: Dial Patterns Screen

5.8.1. Create Dial Pattern 050338780

On the **Dial Pattern Details** screen which is displayed by clicking the **New** button on the **Dial Patterns** screen, perform the following to create a Dial Pattern "050338780":

- Enter "***050338780***" as the dialed digits in the **Pattern** field.
- Enter "***11***" as the minimum length of the dial pattern in the **Min** field.
- Enter "***11***" as the maximum length of the dial pattern in the **Max** field.
- Click the **Add** button on the **Originating Locations and Routing Policies** section to define the Originating Location and the Routing Destination. Then, on the **Originating Location and Routing Policy List** (**Figure 41**) which is displayed after clicking the **Add** button, select ***Tokyo*** on the **Originating Location** section and ***To gumma*** on the **Routing Policies** section. And click the **Select** button to save them.
- Click the **Commit** button to save them.



Dial Pattern Details

General

* Pattern: 050338780

* Min: 11

* Max: 11

Emergency Call: □

SIP Domain: -ALL-

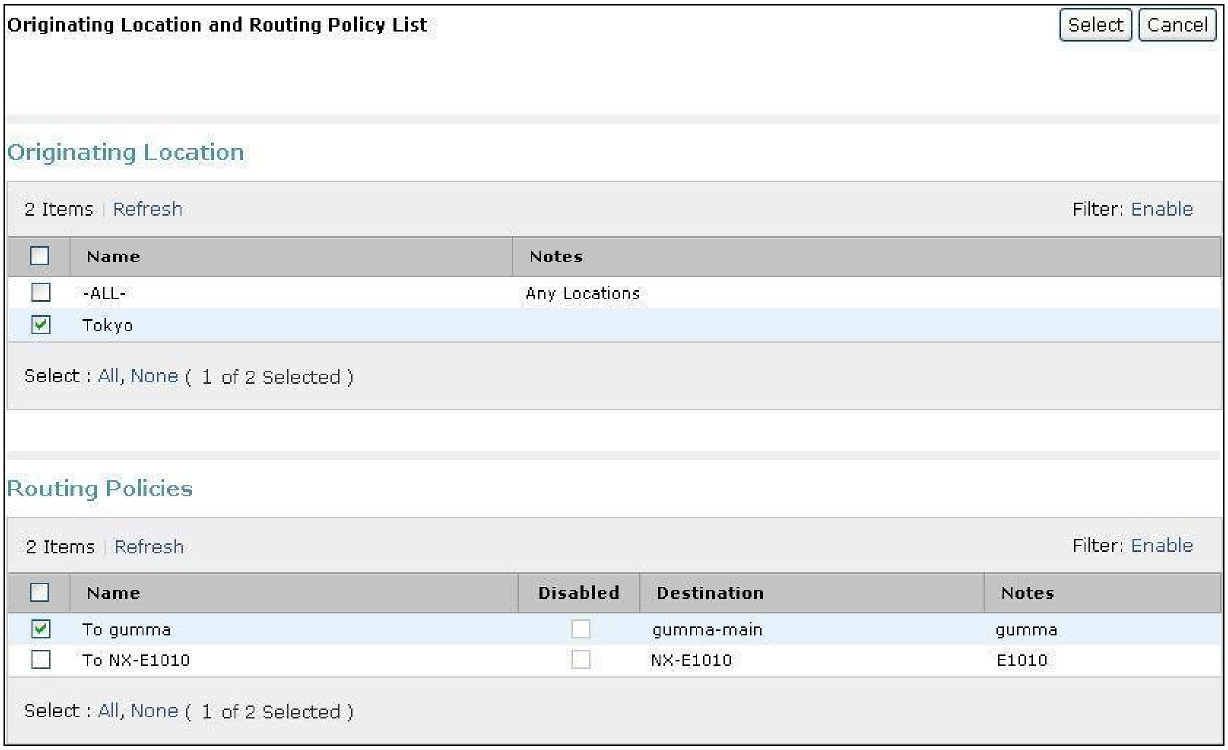
Notes: to gumma

Originating Locations and Routing Policies

□	Originating Location Name 1	Originating Location Notes	Routing Policy Name	Rank 2	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	Tokyo		To gumma	0	□	gumma-main	gumma

Select : All, None (0 of 1 Selected)

Figure 40: Dial Pattern Details Screen - 050338780



Originating Location and Routing Policy List

Originating Location

2 Items | Refresh — Filter: Enable

□	Name	Notes
□	-ALL-	Any Locations
☑	Tokyo	

Select : All, None (1 of 2 Selected)

Routing Policies

2 Items | Refresh — Filter: Enable

□	Name	Disabled	Destination	Notes
☑	To gumma	□	gumma-main	gumma
□	To NX-E1010	□	NX-E1010	E1010

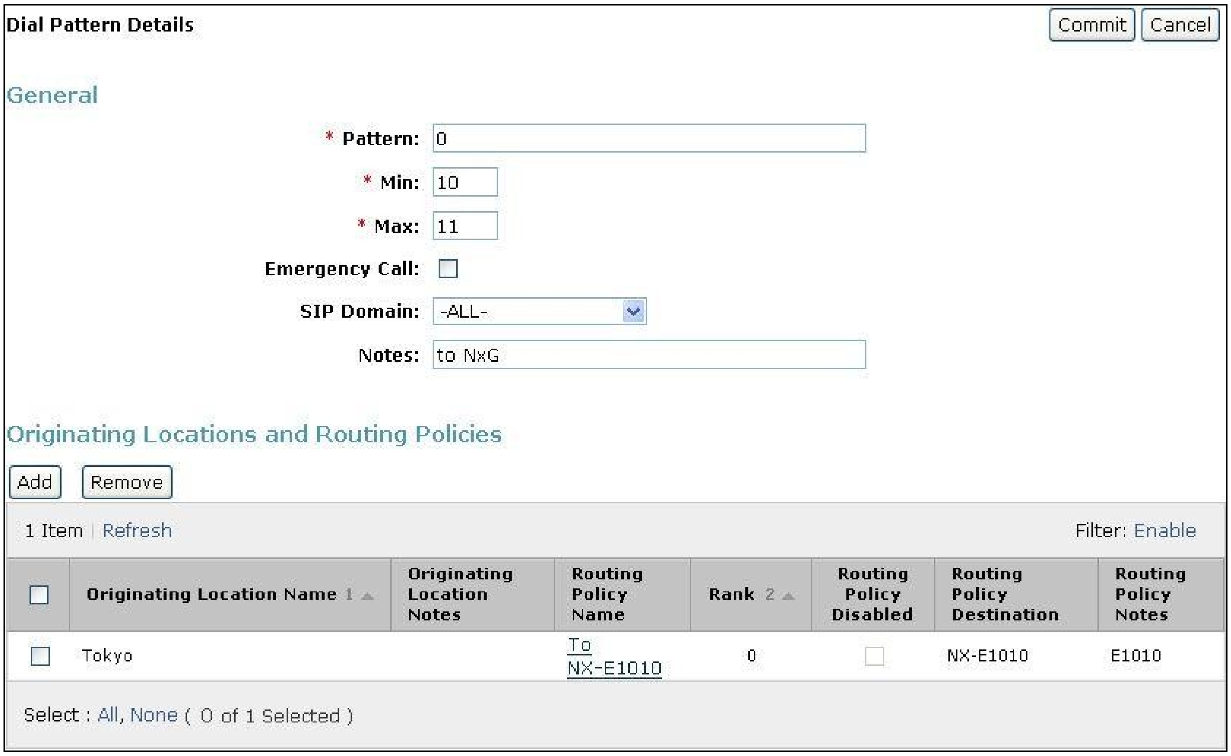
Select : All, None (1 of 2 Selected)

Figure 41: Originating Location and Routing Policy List – "To gumma"

5.8.2. Create Dial Pattern 0

On the **Dial Pattern Details** screen which is displayed by clicking the **New** button on the **Dial Patterns** screen, perform the following to create a Dial Pattern "0":

- Enter "***0***" as the dialed digits in the **Pattern** field.
- Enter "***10***" as the minimum length of the dial pattern in the **Min** field.
- Enter "***11***" as the maximum length of the dial pattern in the **Max** field.
- Click the **Add** button on the **Originating Locations and Routing Policies** section to define the Originating Location and the Routing Destination. Then, on the **Originating Location and Routing Policy List** (**Figure 43**) which is displayed after clicking the **Add** button, select ***Tokyo*** on the **Originating Location** section and ***To NX-E1010*** on the **Routing Policies** section. And click the **Select** button to save them.
- Click the **Commit** button to save them.



Dial Pattern Details

General

* Pattern: 0

* Min: 10

* Max: 11

Emergency Call: □

SIP Domain: -ALL-

Notes: to NxG

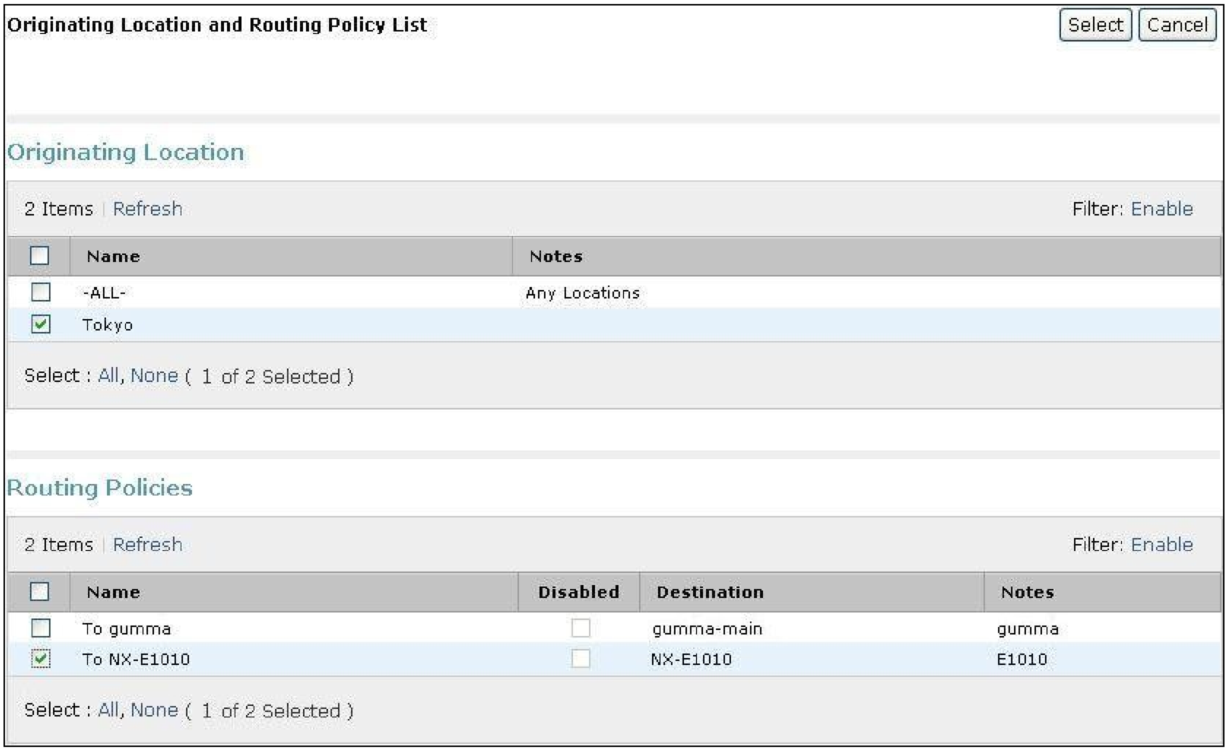
Originating Locations and Routing Policies

1 Item | Refresh   Filter: Enable

□	Originating Location Name 1	Originating Location Notes	Routing Policy Name	Rank 2	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	Tokyo		To NX-E1010	0	□	NX-E1010	E1010

Select : All, None (0 of 1 Selected)

Figure 42: Dial Pattern Details Screen - 0



Originating Location and Routing Policy List

Originating Location

2 Items | Refresh   Filter: Enable

□	Name	Notes
□	-ALL-	Any Locations
☑	Tokyo	

Select : All, None (1 of 2 Selected)

Routing Policies

2 Items | Refresh   Filter: Enable

□	Name	Disabled	Destination	Notes
□	To gumma	□	gumma-main	gumma
☑	To NX-E1010	□	NX-E1010	E1010

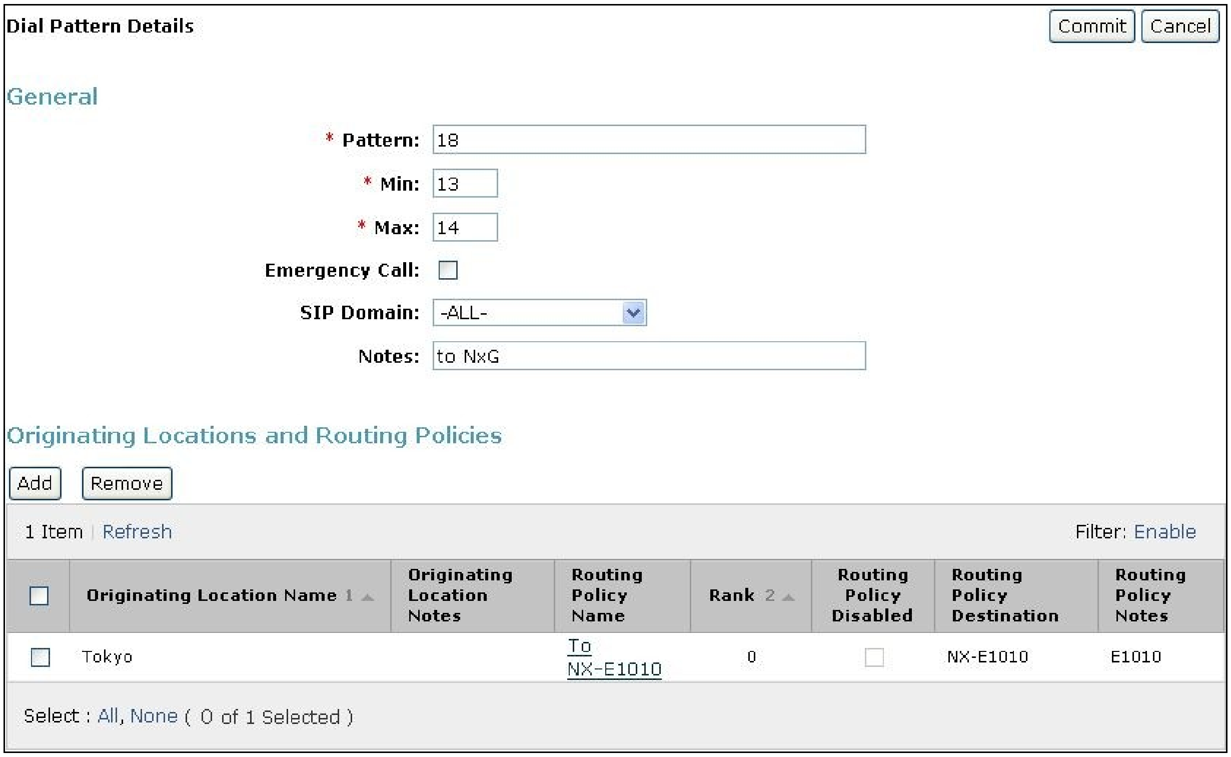
Select : All, None (1 of 2 Selected)

Figure 43: Originating Location and Routing Policy List – “To NX-E1010”

5.8.3. Create Dial Pattern 18

On the **Dial Pattern Details** screen which is displayed by clicking the **New** button on the **Dial Patterns** screen, perform the following to create a Dial Pattern "18":

- Enter "***18***" as the dialed digits in the **Pattern** field.
- Enter "***13***" as the minimum length of the dial pattern in the **Min** field.
- Enter "***14***" as the maximum length of the dial pattern in the **Max** field.
- Click the **Add** button on the **Originating Locations and Routing Policies** section to define the Originating Location and the Routing Destination. Then, on the **Originating Location and Routing Policy List** (**Figure 43**) which is displayed after clicking the **Add** button, select ***Tokyo*** on the **Originating Location** section and ***To NX-E1010*** on the **Routing Policies** section. And click the **Select** button to save them.
- Click the **Commit** button to save them.



* Pattern:	18
* Min:	13
* Max:	14
Emergency Call:	□
SIP Domain:	-ALL-
Notes:	to NxG

□	Originating Location Name 1	Originating Location Notes	Routing Policy Name	Rank 2	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	Tokyo		To NX-E1010	0	□	NX-E1010	E1010

Select : All, None (0 of 1 Selected)

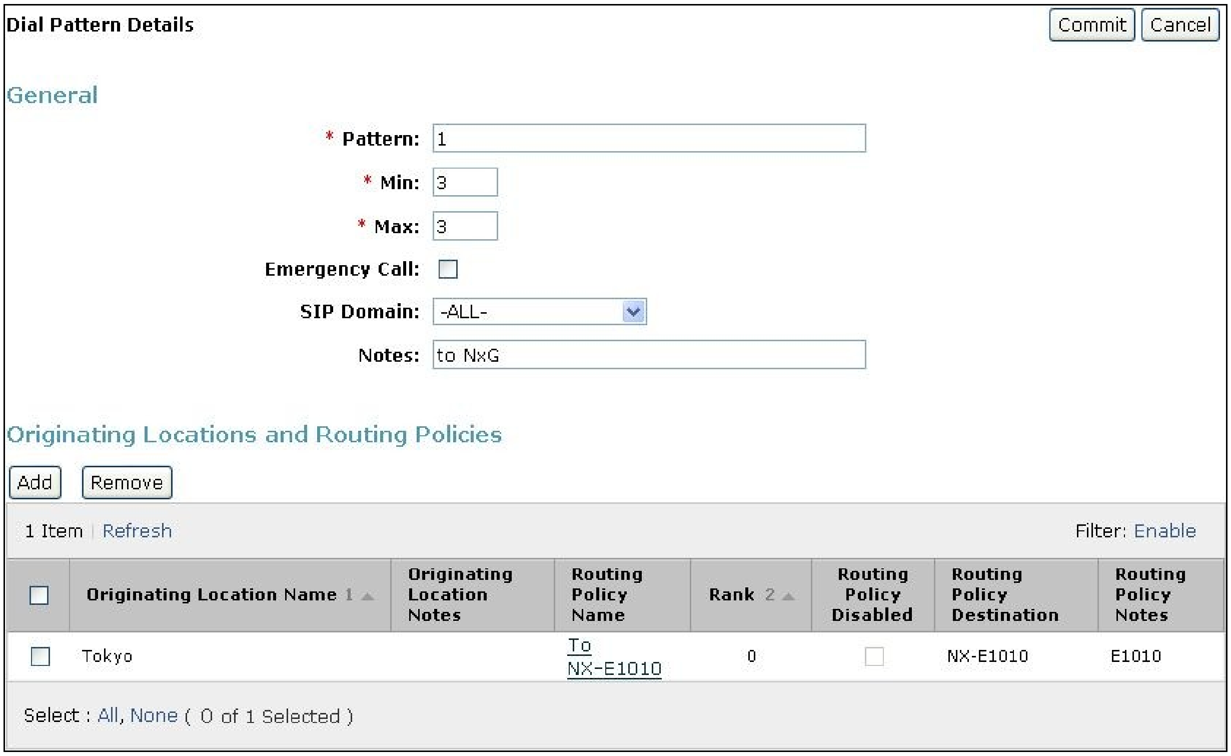
Figure 44: Dial Pattern Details Screen - 18

5.8.4. Create Dial Pattern 1

On the **Dial Pattern Details** screen which is displayed by clicking the **New** button on the **Dial Patterns** screen, perform the following to create a Dial Pattern "1":

- Enter "***1***" as the dialed digits in the **Pattern** field.
- Enter "***3***" as the minimum length of the dial pattern in the **Min** field.
- Enter "***3***" as the maximum length of the dial pattern in the **Max** field.
- Click the **Add** button on the **Originating Locations and Routing Policies** section to define the Originating Location and the Routing Destination. Then, on the **Originating Location and Routing Policy List** (**Figure 43**) which is displayed after clicking the **Add** button, select ***Tokyo*** on the **Originating Location** section and ***To NX-E1010*** on the **Routing Policies** section. And click the **Select** button to save them.

- Click the **Commit** button to save them.



Dial Pattern Details

General

* Pattern: 1

* Min: 3

* Max: 3

Emergency Call: □

SIP Domain: -ALL-

Notes: to NxG

Originating Locations and Routing Policies

1 Item | Refresh   Filter: Enable

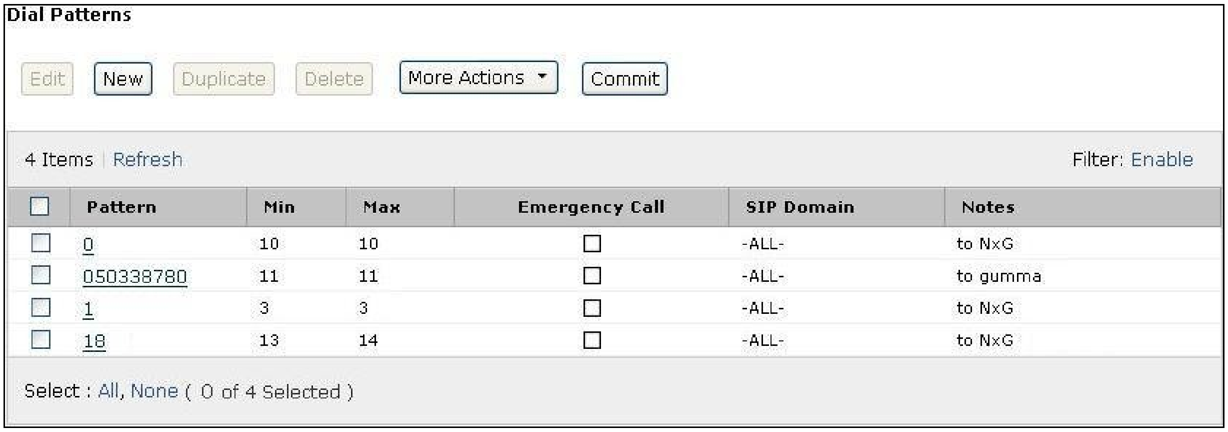
□	Originating Location Name 1	Originating Location Notes	Routing Policy Name	Rank 2	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	Tokyo		To NX-E1010	0	□	NX-E1010	E1010

Select : All, None (0 of 1 Selected)

Figure 45: Dial Pattern Details Screen - 1

5.8.5. Confirm Dial Patterns

As a result of the above administration, four Dial Patterns are created.



□	Pattern	Min	Max	Emergency Call	SIP Domain	Notes
□	0	10	10	□	-ALL-	to NxG
□	050338780	11	11	□	-ALL-	to gumma
□	1	3	3	□	-ALL-	to NxG
□	18	13	14	□	-ALL-	to NxG

Figure 46: Result of Creating Dial Patterns

6. Configure NextGen NX-E1010

This section provides the procedures for configuring NextGen NX-E1010 as a session border controller between the SIP Service Provider Network and Session Manager in the enterprise site. These Application Notes assume that NextGen NX-E1010 has been properly installed in advance and configuration files specific to Session Manager have been installed as well. NextGen NX-E1010 is installed to /home/nextgen/NXS, which is described as $NXS_HOME in these Application Notes. For additional information on these installation tasks, refer to [6].

NextGen NX-E1010 is administered with some configuration files. The configuration files which should be modified in these Application Notes are:

- $NXS_HOME/conf/mcc_router.xml
  - ▷ This xml file defines rules for converting SIP messages between UAs and routing calls in NextGen NX-E1010.
- $NXS_HOME/conf/registrant.dat
  - ▷ This describes parameters for REGISTER requests NextGen NX-E1010 sends to a SIP Service Provider. For the details of contents, refer to the section 3.3.2 of [6].

6.1. Modify mcc_router.xml

Edit the mcc_router.xml file with a text editor, for example the "vi" command. For the details, refer the section 3.3.3 of [6].

6.1.1. Modify <authinfolist> element

This element describes the information for INVITE authentication, which is provided by a SIP Service Provider. Attributes in this element that should be modified are:

- user : user name for the authentication
- pass : password for the authentication

```
<authinfolist>
  <authinfo name="auth1" user="slt2180090" pass="slt2180090" />
</authinfolist>
```

Figure 47: <authinfolist> element

6.1.2. Modify <serverlist> element

This element describes the information about servers to which NextGen NX-E1010 accesses and the **<server>** elements in this element describe attributes for each server. Information which should be modified is the **<hostport>** element in each **<server>** element.

- <hostport> : defines FQDN or IP address and port number of the server

In these Application Notes, two servers are used, one is Session Manager in the enterprise site and the other is in the Simulated SIP Service Provider network. The **<server>** element which has "***avaya***" as the **name** attribute defines the information about Session Manager. And the **<server>** elements which have "***kddi***" and "***kddi184***" as the **name** attribute define the information about the server in the Simulated SIP Service Provider network.
For the **<hostport>** element in the **<server>** element of ***name="avaya"*** attribute, the IP address "***192.168.153.171***" which is administered as the SIP Entity "***avaya-sm2***" at **5.5.1** and the port number "***5060***" for UDP are specified.
For the **<hostport>** element in the **<server>** element of ***name="kddi"*** attribute, the FQDN "***tsip3.kddi.ne.jp***" which is defined in the /etc/hosts file as the host name for the Simulated SIP Service Provider network and the port number "***5060***" for UDP are specified.
The **<hostport>** element in the **<server>** element of ***name="kddi184"*** attribute has the same settings as the **<server>** element of ***name="kddi"*** attribute has.

```
  <serverlist>
    <server name="avaya" type="2" transport="default" rtpifid="1" convertteltosip="true"
convertteltosipoption="0" serveroption="0" >
      <hostport>192.168.153.171:5060</hostport>
    </server>
    <server name="kddi" type="4" timeout="3" transport="${GLOBALIPADDRESSIFNAME}" rtpifid="2"
authinfo="auth1"
     convertteltosip="true" serveroption="0" convertteltosipoption="0" privacyoption="26" error_response="486"
select="roundrobin" >
      <hostport>tsip3.kddi.ne.jp:5060</hostport><!--see /etc/hosts-->
    </server>
    <server name="kddi184" type="4" timeout="3" transport="${GLOBALIPADDRESSIFNAME}" rtpifid="2"
authinfo="auth1"
     convertteltosip="true" serveroption="0" convertteltosipoption="45" privacyoption="26"
error_response="486" select="roundrobin" >
      <hostport>tsip3.kddi.ne.jp:5060</hostport>
    </server>
  </serverlist>
```

Figure 48: <serverlist> element

6.1.3. Modify <dmrulelist> element

This element lists the rules for converting SIP URI between the UA on the Simulated SIP Service Provider Network side and the UA on the enterprise site side, and each **<dmrule>** element in this element describes the conversion rule with the following attributes:

- **name**: a descriptive name for the conversion rule
- **type**: a type of the conversion
- **target**: a header field that this rule is applied to
- **param**: a parameter that this rule is applied to
- **replace_string**: the parameter (which is specified by "param") in the header field (which is specified by "target") is replaced with this
- The **replace_string** attribute of the following <dmrule> elements should be modified:
- name="**replace_uri_host**": This replaces the host part of the Request-URI in SIP messages from NextGen NX-E1010 to the Simulated SIP Service Provider Network. In these Application Notes, the **replace_string** attributes for this rule is "***tsip3.kddi.ne.jp***". This is the FQDN of the SIP server in the Simulated SIP Service Provider Network.
- name="**replace_from_host**": This replaces the host part of the SIP URI in the From header field in SIP messages from NextGen NX-E1010 to the Simulated SIP Service Provider Network. In these Application Notes, the **replace_string** attributes for this rule is "***tsip7.kddi.ne.jp***". This is the host part of the AoR (Address of Record) which is assigned for the pilot number of the enterprise site by the Simulated SIP Service Provider Network.
- name="**replace_from_pilotnum**": This replaces the user part of the SIP URI in the From header field in SIP messages from NextGen NX-E1010 to the Simulated SIP Service Provider Network. In these Application Notes, the **replace_string** attributes for this rule is "***nod2180090***". This is the user part of the AoR which is assigned for the pilot number of the enterprise site by the Simulated SIP Service Provider Network.
- name="**replace_from_host_avaya**": This replaces the host part of the SIP URI in the From header field in SIP messages from NextGen NX-E1010 to Session Manager. In these Application Notes, the **replace_string** attributes for this rule is "***alj.apac.avaya.com***" so that Session Manager can perform domain-base routing.
- name="**replace_to_host_avaya**": This replaces the host part of the SIP URI in the To header field in SIP messages from NextGen NX-E1010 to Session Manager. In these Application Notes, the **replace_string** attributes for this rule is "***alj.apac.avaya.com***" so that Session Manager can perform domain-base routing.
- name="**replace_requesturi_host_avaya**": This replaces the host part of the Request-URI in SIP messages from NextGen NX-E1010 to Session Manager. In these Application Notes, the **replace_string** attributes for this rule is "***alj.apac.avaya.com***" so that Session Manager can perform domain-base routing.

```
 <dmrulelist>
   <dmrule name="replace_ruri_host" type="replace" target="requesturi" param="host"
replace_string="tsip3.kddi.ne.jp" />
   <dmrule name="del_ruri_port" type="delete" target="requesturi" param="port" />
   <dmrule name="del_ruri_param" type="delete" target="requesturi" param="parameter"/>
   <dmrule name="replace_from_host" type="replace" target="from" param="host"
replace_string="tsip7.kddi.ne.jp" />
   <dmrule name="replace_from_pilotnum" type="replace" target="from" param="user"
replace_string="nod2180090" />
   <dmrule name="del_from_port" type="delete" target="from" param="port" />
   <dmrule name="del_from_param" type="delete" target="from" param="parameter" />
   <dmrule name="del_from_displayname" type="delete" target="from" param="displayname"
delete_position="0" delete_length="128"/>
   <dmrule name="copy_ruri2to" type="copy" target="to" param="all" copy_from="requesturi"
copy_from_param="all" />
   <dmrule name="del_to_displayname" type="delete" target="to" param="displayname" delete_position="0"
delete_length="128"/>
   <dmrule name="copy_to2ruri_userid" type="copy" target="requesturi" param="user" copy_from="to"
copy_from_param="user" />
   <dmrule name="replace_num2userid" type="replace" target="from" param="user" datatable="num2userid"
keyheader="from" keyparam="user" valuecolumn= "2" />

   <dmrule name="replace_from_host_avaya" type="replace" target="from" param="host"
replace_string="alj.apac.avaya.com" />
   <dmrule name="replace_to_host_avaya" type="replace" target="to" param="host"
replace_string="alj.apac.avaya.com" />
   <dmrule name="replace_requesturi_host_avaya" type="replace" target="requesturi" param="host"
replace_string="alj.apac.avaya.com" />
   <dmrule name="copy_ruri2to_userid" type="copy" target="to" param="user" copy_from="requesturi"
copy_from_param="user" />
   <dmrule name="replace_ruri_by_registrant_file" type="replace" target="requesturi" param="user"
keyheader=”requri” keyparam=”user” column=4” valuecolumn="5" responsecode="404"/>
   <dmrule name="copy_from_displayname" type="copy" target="from" param="user" copy_from="from"
copy_from_param="displayname" />
   <dmrule name="replace_from_by_registrant_file" type="replace" target="from" param="user"
datatable="data_userid" keyheader="from" keyparam="user" valuecolumn="4" responsecode="404"/>
 </dmrulelist>
```

Figure 49: <dmrulelist> element

6.2. Modify registrant.dat

Edit the registrant.dat file with a text editor, for example the “vi” command. For the details, refer the section 3.3.2 of [6].
This involves the information which is used when NextGen NX-E1010 sends REGISTER requests to a SIP Service Provider. Each line consists of the eleven items which are separated with one tab (0x09):

- 1st column: Index. In these Application Notes, “***1***” is used.
- 2nd column: SIP server address (IP address or FQDN) that NextGen NX-E1010 sends REGISTER requests to. These Application Notes assume the SIP server is “***tsip3.kddi.ne.jp***” as defined in the <serverlist> element (**6.1.2**).
- 3rd column: port number of the SIP server which is defined at the 2nd column. These Application Notes use “***5060***”.
- 4th column: user part of the SIP URI which is specified in From/To header. These Application Notes use “***nod2180090***” as defined in the <dmrule name=“replace_from_pilotnum” …/> element (**6.1.3**).
- 5th column: user part of the SIP URI which is specified in Contact header. These Application Notes use “***05033878005***” as the pilot number for the enterprise site.
- 6th column: host part of the SIP URI which is specified in Request Line, From/To header. These Application Notes use “***tsip7.kddi.ne.jp***” as defined in the <dmrule name=“replace_from_host” …/> element (**6.1.3**).
- 7th column: user name which is used for the registration authentication. These Application Notes use “***fsc2180090***”.
- 8th column: password which is used for the registration authentication. These Application Notes use “***fsc2180090***”.
- 9th column: number indicating seconds how long would like the registration to be valid. These Application Notes use “***3600***”.
- 10th column: whether or not REGISTER is sent automatically when NextGen NX-E1010 starts up. These Application Notes use “***true***”. This means REGISTER is sent automatically when NextGen NX-E1010 starts up.
- 11th column: whether or not user part in Contact header is random. These Application Notes use “***true***”. This means user part in Contact header is random.

```
1  tsip3.kddi.ne.jp  5060  nod2180090   05033878005 tsip7.kddi.ne.jp  fsc2180090  fsc2180090  3600  true  true
```

Figure 50: registrant.dat file

7. General Test Approach and Test Results

All test cases that were described in **Section 1.1** were executed and passed. The following was noted:

- NextGen NX-E1010 Version 3.3 only supports the UDP protocol as the SIP transport protocol.

8. Verification Steps

This section provides verification steps that may be performed in the field to verify and that the endpoints can place outbound and receive inbound the SIP Service Provider network through NextGen NX-E1010.

8.1. Verify Communication Manager

8.1.1. Verify Communication Manager is Up

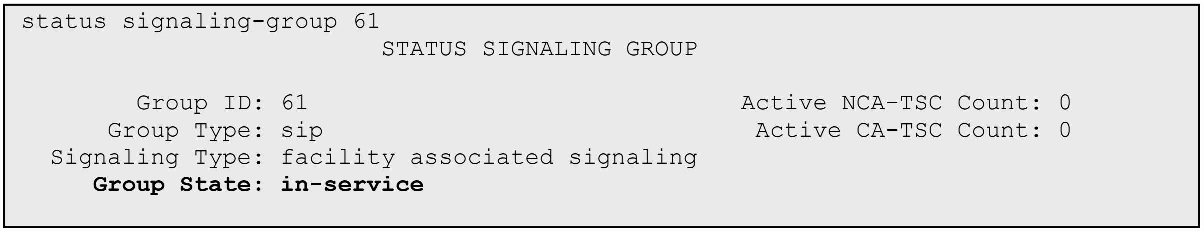
Verify with the **statapp** command from the bash command line interface of Communication Manager if all processes of Communication Manager are up. If a process shows “DOWN” or a numerator and a denominator of a process shows different numbers, restart Communication Manager by using the **stop -acf** and **start -ac** commands. **Figure 55** shows an example that all processes of Communication Manager are up.

```
dadmin@gumma> statapp
Watchdog         9/ 9 UP SIMPLEX
ModemMtty        1/ 1 UP SIMPLEX
TraceLogger      3/ 3 UP SIMPLEX
LicenseServer    3/ 3 UP SIMPLEX
SME              8/ 8 UP SIMPLEX
MasterAgent      1/ 1 UP SIMPLEX
MIB2Agent        1/ 1 UP SIMPLEX
MVSubAgent       1/ 1 UP SIMPLEX
LoadAgent        1/ 1 UP SIMPLEX
FPAgent          1/ 1 UP SIMPLEX
INADSAlarmAgent  1/ 1 UP SIMPLEX
GMM              4/ 4 UP SIMPLEX
SNMPManager      1/ 1 UP SIMPLEX
filesyncd        8/ 8 UP SIMPLEX
MCD              1/ 1 UP SIMPLEX
CommunicaMgr    87/87 UP SIMPLEX
Messaging       1/ 1 UP SIMPLEX
dadmin@gumma>
```

Figure 51: Result of statapp command

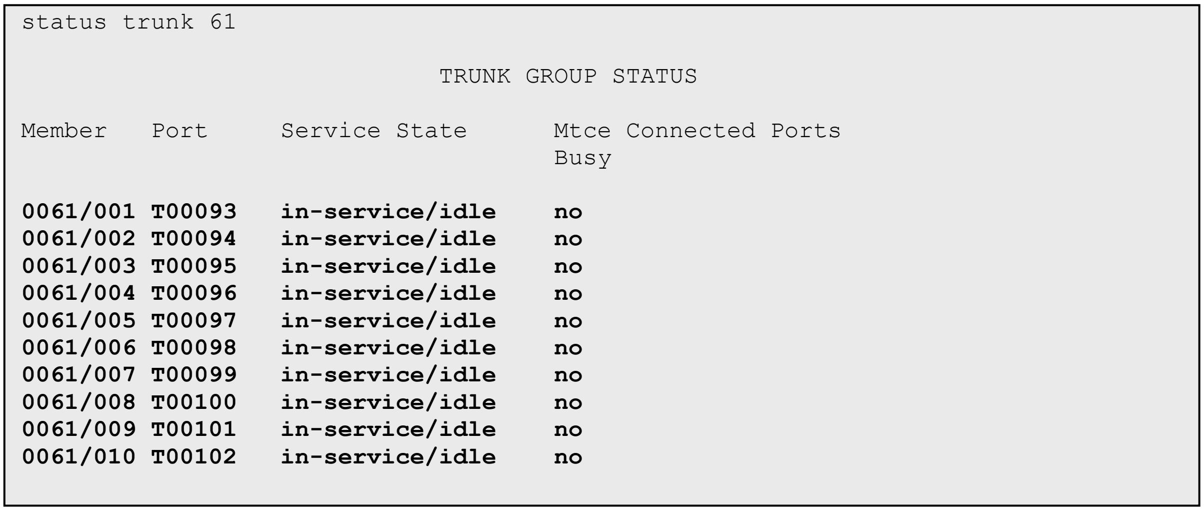
8.1.2. Verify the status of SIP Trunk to Session Manager

Verify the status of the signaling group and trunk group to Session Manager is "***in-service***". Perform the **status signaling-group** and **status trunk** commands from the SAT. If both show "***in-service***" then they are properly working. In this case, the number of signaling group and trunk group is "***61***" as administered in **Section 4.7** and **Section 4.8**.



```
status signaling-group 61
                         STATUS SIGNALING GROUP

        Group ID: 61                             Active NCA-TSC Count: 0
      Group Type: sip                             Active CA-TSC Count: 0
  Signaling Type: facility associated signaling
     Group State: in-service
```

Figure 52: Status of Signaling Group



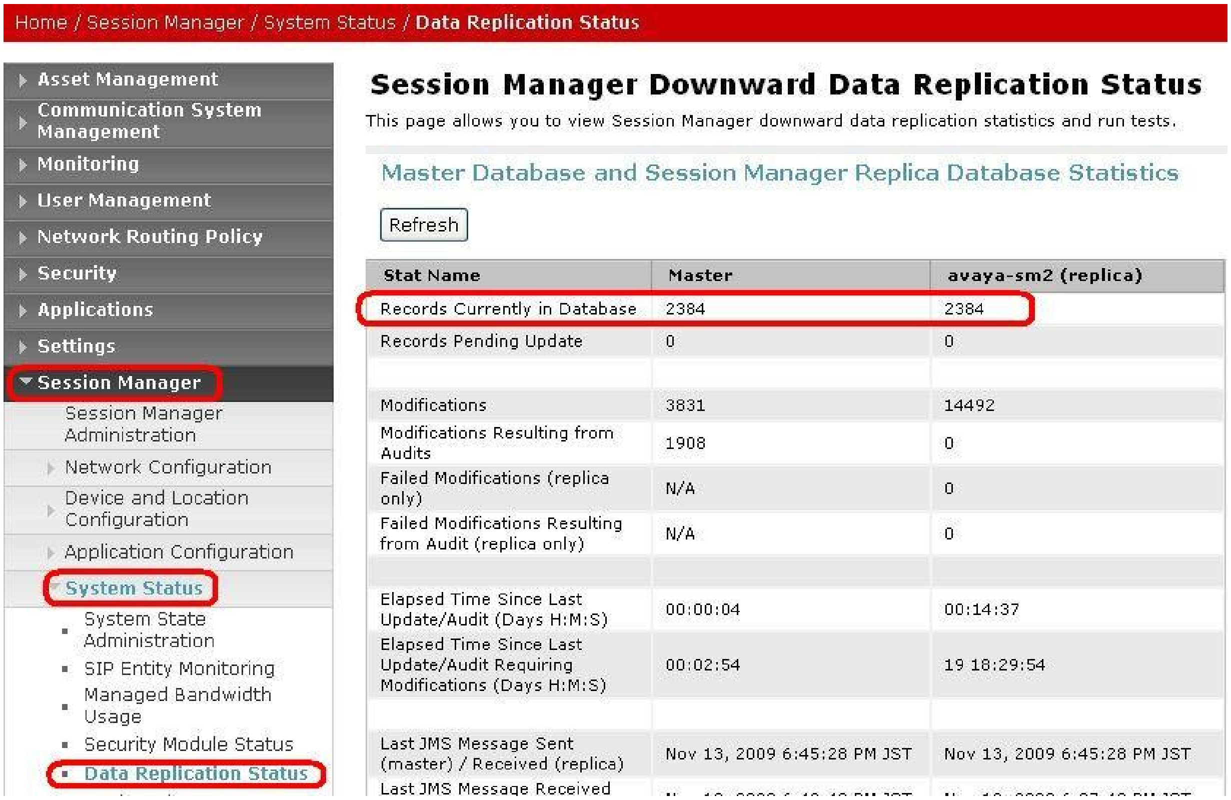
```
status trunk 61

                             TRUNK GROUP STATUS

Member   Port     Service State      Mtce Connected Ports
                                     Busy

0061/001 T00093   in-service/idle    no
0061/002 T00094   in-service/idle    no
0061/003 T00095   in-service/idle    no
0061/004 T00096   in-service/idle    no
0061/005 T00097   in-service/idle    no
0061/006 T00098   in-service/idle    no
0061/007 T00099   in-service/idle    no
0061/008 T00100   in-service/idle    no
0061/009 T00101   in-service/idle    no
0061/010 T00102   in-service/idle    no
```

Figure 53: Status of Trunk Group

8.2. Verify Session Manager

8.2.1. Verify Session Manager is Configured

To verify whether or not Session Manager has the configuration data which were administered through System Manager, visit the **Data Replication Status** screen which is displayed by selecting **Session Manager** -> **System Status** -> **Data Replication Status** from the left pane of the System Manager home screen. If the value of the **Records Currently in Database** status of the Replica (in this case "avaya-sm2") is the same as one of the Master, Session Manager has been properly configured.



Session Manager Downward Data Replication Status

This page allows you to view Session Manager downward data replication statistics and run tests.

Master Database and Session Manager Replica Database Statistics

Stat Name	Master	avaya-sm2 (replica)
Records Currently in Database	2384	2384
Records Pending Update	0	0
Modifications	3831	14492
Modifications Resulting from Audits	1908	0
Failed Modifications (replica only)	N/A	0
Failed Modifications Resulting from Audit (replica only)	N/A	0
Elapsed Time Since Last Update/Audit (Days H:M:S)	00:00:04	00:14:37
Elapsed Time Since Last Update/Audit Requiring Modifications (Days H:M:S)	00:02:54	19 18:29:54
Last JMS Message Sent (master) / Received (replica)	Nov 13, 2009 6:45:28 PM JST	Nov 13, 2009 6:45:28 PM JST
Last JMS Message Received		

Figure 54: Data Replication Status Screen

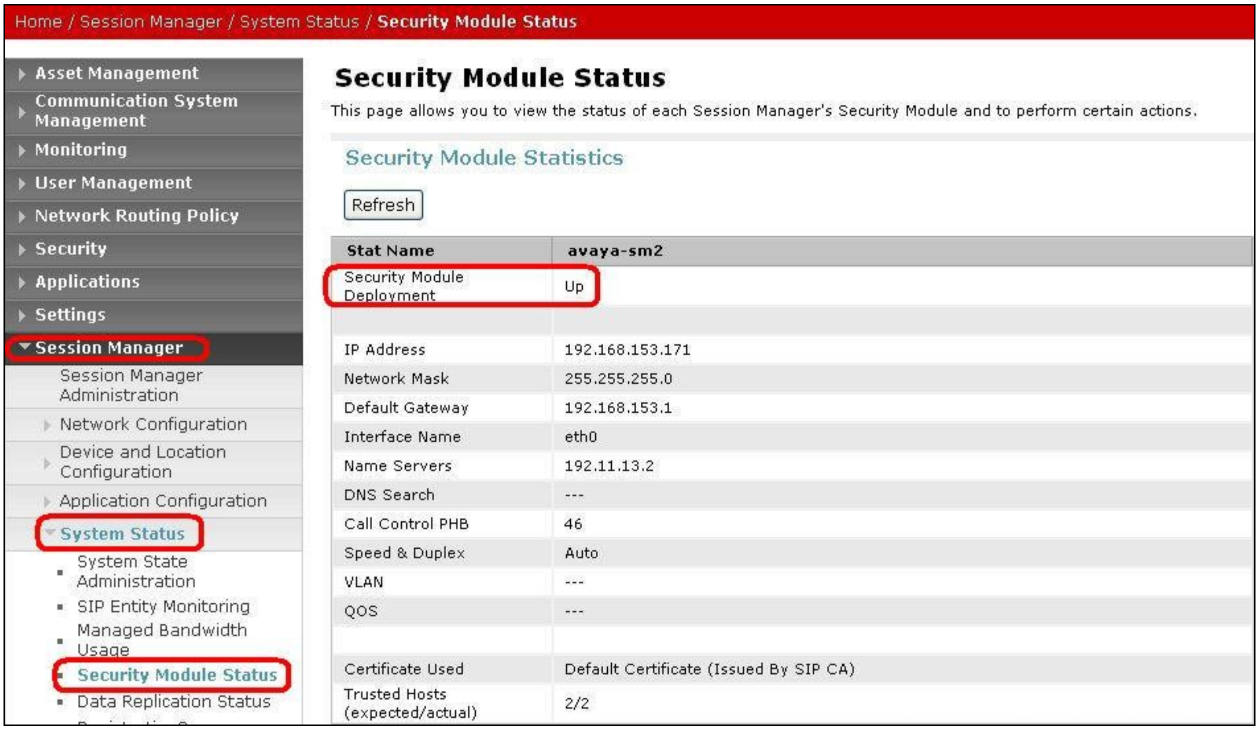
8.2.2. Verify Session Manager is Up

Verify with the **statapp** command from the bash command line interface of Session Manager if all processes of Session Manager are up. If a process shows "DOWN" or a numerator and a denominator of a process shows different numbers, restart Session Manager by using the **stop -acf** and **start -ac** commands.

```
-bash-3.2$ statapp
Watchdog           9/   9 UP
logevent          18/  18 UP
ppm-SMS            9/   9 UP
postgres-db       29/  29 UP
sm-mgmt          121/121 UP
sm-maint         179/179 UP
sipas-MS         108/108 UP
sipas-SD         164/164 UP
sipas-SH         217/217 UP
sipas-LH          23/  23 UP
sipas-CDR         23/  23 UP
sal-agent         70/  70 UP
secmod             1/   1 UP
-bash-3.2$
```

Figure 55: Result of statapp command

Verify that the **Security Module Deployment** status on the **Security Module Status** screen which is displayed by selecting **Session Manager** -> **System Status** -> **Security Module Status** from the left pane of the home screen shown after logged in to System Manager shows "***Up***". This shows whether or not Session Manager is up.



Security Module Status

This page allows you to view the status of each Session Manager's Security Module and to perform certain actions.

Security Module Statistics

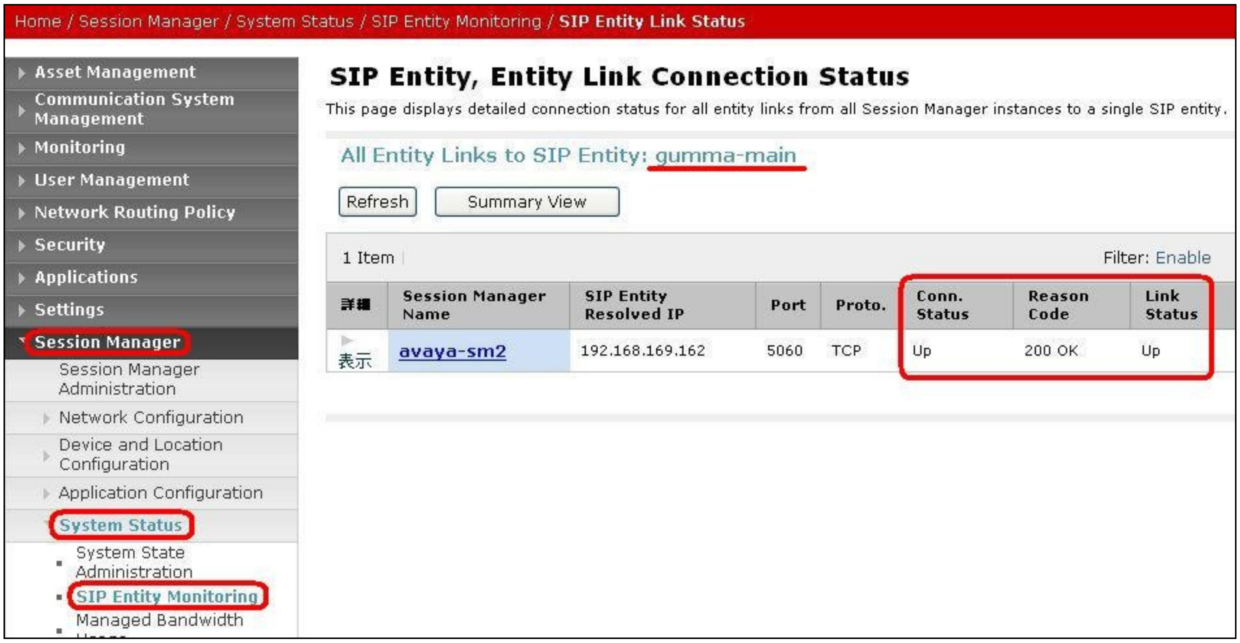
Stat Name	avaya-sm2
Security Module Deployment	Up
IP Address	192.168.153.171
Network Mask	255.255.255.0
Default Gateway	192.168.153.1
Interface Name	eth0
Name Servers	192.11.13.2
DNS Search	---
Call Control PHB	46
Speed & Duplex	Auto
VLAN	---
QOS	---
Certificate Used	Default Certificate (Issued By SIP CA)
Trusted Hosts (expected/actual)	2/2

Figure 56: Security Module Status Screen

8.2.3. Verify Link Connection Between Session Manager and Communication Manager

To verify whether or not the link connection between Session Manager and Communication Manager is up, visit the **SIP Entity Monitoring** screen which is displayed by selecting **Session Manager** -> **System Status** -> **SIP Entity Monitoring** from the left pane of the System Manager home screen and select the SIP Entity created for Communication Manager (in this case, "***gumma-main***") from the **All Monitored SIP Entities** section. The section lists the SIP entities which are administered as ***Link Monitoring Enabled*** on the SIP Entity Details screen (see **section 5.5**).

If the **Conn. Status** and **Link Status** columns show "***Up***", then the link to the Communication Manager is up.


Home / Session Manager / System Status / SIP Entity Monitoring / SIP Entity Link Status
Asset Management
Communication System Management
Monitoring
User Management
Network Routing Policy
Security
Applications
Settings
Session Manager
Session Manager Administration
Network Configuration
Device and Location Configuration
Application Configuration
System Status
System State Administration
SIP Entity Monitoring
Managed Bandwidth Usage
Refresh
Summary View
Filter: Enable

SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

All Entity Links to SIP Entity: gumma-main

1 Item

詳細	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
▶ 表示	avaya-sm2	192.168.169.162	5060	TCP	Up	200 OK	Up

Figure 57: SIP Entity Monitoring Screen

8.3. Verify NextGen NX-E1010

Verify the status of the processes with the ***$NXS_HOME/bin/nxs.sh status*** command.

If all processes are running then the command shows the result like **Figure 58**.

```
[nextgen@nxe1010 NXS]$ bin/nxs.sh status
------------+-----+-----+-----+------+------+-------------+-------------
name         pid   %cpu  %mem  vsz    rss    time          elapsed
------------+-----+-----+-----+------+------+-------------+-------------
ham          23835  0.49  0.80 271008   8372       0:00:35       3:04:40
logobserver  23853  0.00  0.67 229464   6988       0:00:05       3:04:40
datastore    23854  0.00  0.63 102904   6600       0:00:00       3:04:40
mccb2bua     23855  0.00  1.49 437972  15488       0:00:00       3:04:40
registrant   23856  0.00  0.89 263708   9280       0:00:00       3:04:40
smediaserv   23857  0.00  0.87 177612   9072       0:00:08       3:04:40
------------+-----+-----+-----+------+------+-------------+-------------
[nextgen@nxe1010 NXS]$
```

Figure 58: Result of "nxs.sh status" command – Running all processes

If it returns "***hamanager is not running!***" (**Figure 59**), then start NextGen NX-E1010 by executing the ***$NXS_HOME/bin/nxs.sh start*** command.

```
[nextgen@nxe1010 NXS]$ bin/nxs.sh status
hamanager is not running!
[nextgen@nxe1010 NXS]$
```

Figure 59: Result of "nxs.sh status" command – not Running at all

If the status of one or more processes shows "***Stopped***" (**Figure 60**), then stop and start NextGen NX-E1010 by executing ***$NXS_HOME/bin/nxs.sh stop*** and ***$NXS_HOME/bin/nxs.sh start*** commands.

```
[nextgen@nxe1010 NXS]$ bin/nxs.sh status
------------+-----+-----+-----+------+------+-------------+-------------
name         pid   %cpu  %mem  vsz    rss    time          elapsed
------------+-----+-----+-----+------+------+-------------+-------------
ham          28514  0.52  0.80 250520   8280       0:00:00       0:00:15
logobserver  28529  0.00  0.66 229464   6888       0:00:00       0:00:14
datastore    28532  0.00  0.63 113148   6544       0:00:00       0:00:14
mccb2bua     Stopped
registrant   28534  0.00  0.86 260636   8992       0:00:00       0:00:14
smediaserv   28535  0.00  0.66 165280   6860       0:00:00       0:00:14
------------+-----+-----+-----+------+------+-------------+-------------
[nextgen@nxe1010 NXS]$
```

Figure 60: Result of "nxs.sh status" command – one process stopped

9. Conclusion

These Application Notes describe the configuration steps required to connect an enterprise site consists of Avaya Aura™ Session Manager and Avaya Aura™ Communication Manager to a SIP Service Provider network via NextGen NX-E1010. The Avaya SIP-based telephony solution with NX-E1010 provides enterprise customers with the cost effective converged network by integrating their telecommunication network with their broadband Internet access network. All feature test cases were completed successfully.

10. Additional References

10.1. Documentation

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

10.1.1. Avaya

The following Avaya product documentation is available at: http://support.avaya.com/

[1] *Administrator Avaya Aura™ Communication Manager*, Document 03-300509, Issue 5.0, Release 5.2, May 2009.

[2] *Feature Description and Implementation for Avaya Communication Manager*, Document 555-245-205, Issue 6, January 2008.

[3] *SIP Support in Avaya Aura™ Communication Manager Running on Avaya S8xxx Servers*, Document 555-245-206, Issue 9, May 2009.

[4] *Installing and Administering Avaya Aura™ Session Manager*, Document 03-603324, Issue 1.1, Release 1.1, June 2009.

[5] *Maintaining and Troubleshooting Avaya Aura™ Session Manager*, Document 03-603325, Issue 1.1, Release 1.1, June 2009.

10.1.2. NextGen

The following documentation was included with NextGen NX-E1010.

[6] *NextGen SIP Server Family NX-E1010 Version 3.3 Users Manual*, NXG-1182, Issue 1, Standard, February 2008 (In Japanese).

The following documentation was included with NextGen NX-VNS Trial Edition.

[7] *NX-VNS Version 3.0 Trial Edition Users Manual*, NXG-1634, Issue 2, September 2009 (In Japanese).

Additional information about NextGen NX-E1010 is available at http://www.nextgen.co.jp/english/index.html.

10.2. Glossary

AOR: An AOR (address-of-record) is a SIP or SIPS (Secure SIP) URI that points to a domain with a location service that can map the URI to another URI where the user might be available. Typically, the location service is populated through registrations. An AOR is frequently thought of as the "public address" of the user.

CLIP: Calling Line Identification Presentation. The feature allows the phone set to display the caller’s phone number before you answer it.

CLIR: Calling Line Identification Restriction. The feature allows you to conceal your identity / phone number when you are making a call to other phone.

Header: A header is a component of a SIP message that conveys information about the message. It is structured as a sequence of header fields.

Header Field: A header field is a component of the SIP message header. A header field can appear as one or more header field rows. Header field rows consist of a header field name and zero or more header field values. Multiple header field values on a given header field row are separated by commas. Some header fields can only have a single header field value, and as a result, always appear as a single header field row.

Location Service: A location service is used by a SIP redirect or proxy server to obtain information about a callee's possible location(s). It contains a list of bindings of address-of-record keys to zero or more contact addresses. The bindings can be created and removed in many ways; this specification defines a REGISTER method that updates the bindings.

Proxy Server: An intermediary entity that acts as both a server and a client for the purpose of making requests on behalf of other clients. A proxy server primarily plays the role of routing, which means its job is to ensure that a request is sent to another entity "closer" to the targeted user. Proxies are also useful for enforcing policy (for example, making sure a user is allowed to make a call). A proxy interprets, and, if necessary, rewrites specific parts of a request message before forwarding it.

Registrar: A registrar is a server that accepts REGISTER requests and places the information it receives in those requests into the location service for the domain it handles.

TLS: Transport Layer Security. TLS is a cryptographic protocol which provides secure communication on the Internet, and is the successor to SSL (Secure Socket Layer).

User Agent Client (UAC): A user agent client is a logical entity that creates a new request, and then uses the client transaction state machinery to send it. The role of UAC lasts only for the duration of that transaction. In other words, if a piece of software initiates a request, it acts as a UAC for the duration of that transaction. If it receives a request later, it assumes the role of a user agent server for the processing of that transaction.

User Agent Server (UAS): A user agent server is a logical entity that generates a response to a SIP request. The response accepts, rejects, or redirects the request. This role lasts only for the duration of that transaction. In other words, if a piece of software responds to a request, it acts as a UAS for the duration of that transaction. If it generates a request later, it assumes the role of a user agent client for the processing of that transaction.

User Agent (UA): A logical entity that can act as both a user agent client and user agent server.

Appendix A: Sample SIP INVITE Messages

This section displays the format of the SIP INVITE messages sent by NextGen NX-E1010 and Session Manager at the enterprise site. Customers may use these INVITE message for comparison and troubleshooting purposes. Differences in these messages may indicate different configuration options selected.

Sample SIP INVITE Message from NextGen NX-E1010 to Session Manager:

```
INVITE sip:05033878005@alj.apac.avaya.com SIP/2.0
Via: SIP/2.0/UDP 192.168.153.201:5060;branch=z9hG4bK0f9147ec
From: <sip:0330000000@alj.apac.avaya.com:5060>;tag=1ba83974
To: <sip:05033878005@alj.apac.avaya.com>
Call-ID: 72307560-69747e27-21b02751@alj-dell630-2--_6b8b4574
CSeq: 1 INVITE
Max-Forwards: 70
Contact: <sip:192.168.153.201:5060>
Supported: 100rel,timer
Allow: INVITE,ACK,BYE,CANCEL,PRACK
Session-Expires: 180
Min-SE: 180
Content-Type: application/sdp
Content-Length: 134

v=0
o=- 0 0 IN IP4 192.168.153.201
s=-
c=IN IP4 192.168.153.201
t=0 0
m=audio 10000 RTP/AVP 0
a=rtpmap:0 PCMU/8000
a=sendrecv
```

Sample SIP INVITE Message from Session Manager to NextGen NX-E1010:

```
INVITE sip:0330000000@alj.apac.avaya.com;user=phone SIP/2.0
From: "gumma"
<sip:78005@alj.apac.avaya.com;user=phone>;tag=016a6feac3de195534ac71e9c00
To: "0330000000" <sip:0330000000@192.168.153.171;user=phone>
Call-ID: 016a6feac3de196534ac71e9c00
CSeq: 1 INVITE
Max-Forwards: 67
Record-Route: <sip:67b41d50@192.168.153.171;transport=udp;lr>
Record-Route: <sip:192.168.153.170:15060;lr;sap=318581196*1*016asm-
callprocessing.sar-1449613376~1254732492093~1697966663~1>,
<sip:67b41d50@192.168.153.171;transport=tcp;lr>
Record-Route: <sip:192.168.169.162;lr;transport=tcp>
Via: SIP/2.0/UDP
192.168.153.171;rport;branch=z9hG4bKC0A899AABADF00D00000124051DC889121243-
AP;ft=192.168.153.171~13c4
Via: SIP/2.0/UDP
192.168.153.170:5070;branch=z9hG4bKC0A899AABADF00D00000124051DC889121243;rece
ived=192.11.13.2
Via: SIP/2.0/UDP
192.168.153.170:5070;branch=z9hG4bKC0A899AABADF00D00000124051DC889121241;sap=
318581196*1*016asm-callprocessing.sar-1449613376~1254732492093~1697966663~1
Via: SIP/2.0/TCP 192.168.153.171;branch=z9hG4bK016a6feac3de197534ac71e9c00-
AP;ft=8855
Via: SIP/2.0/TCP
192.168.169.162;branch=z9hG4bK016a6feac3de197534ac71e9c00;received=192.168.16
9.162
User-Agent: Avaya CM/R015x.02.1.015.0
Supported: timer, replaces, join, histinfo, 100rel
Allow: INVITE, CANCEL, BYE, ACK, PRACK, SUBSCRIBE, NOTIFY, REFER, OPTIONS,
INFO, PUBLISH
Contact: "gumma" <sip:78005@192.168.169.162;transport=tcp;user=phone>
Session-Expires: 180;refresher=uac
Min-SE: 180
Accept-Language: ja-JP
Content-Type: application/sdp
History-Info: <sip:0330000000@192.168.153.171;user=phone>;index=1
History-Info: "0330000000"
<sip:0330000000@192.168.153.171;user=phone>;index=1.1
Alert-Info: <cid:internal@invalid.unknown.domain>;avaya-cm-alert-
type=internal
Content-Length: 216
P-Asserted-Identity: "gumma" <sip:78005@alj.apac.avaya.com;user=phone>
Route: <sip:192.168.153.201;lr;phase=terminating>
P-Site: SM;origloc=1;termloc=1

v=0
o=- 1 1 IN IP4 192.168.169.162
s=-
c=IN IP4 192.168.169.163
b=AS:64
t=0 0
```

```
m=audio 2188 RTP/AVP 18 0 127
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:0 PCMU/8000
a=rtpmap:127 telephone-event/8000
```

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.