Avaya Solution & Interoperability Test Lab

Application Notes for Dialogic 2000 Media Gateway with Avaya Communication Manager and Avaya SIP Enablement Services – Issue 1.0

Abstract

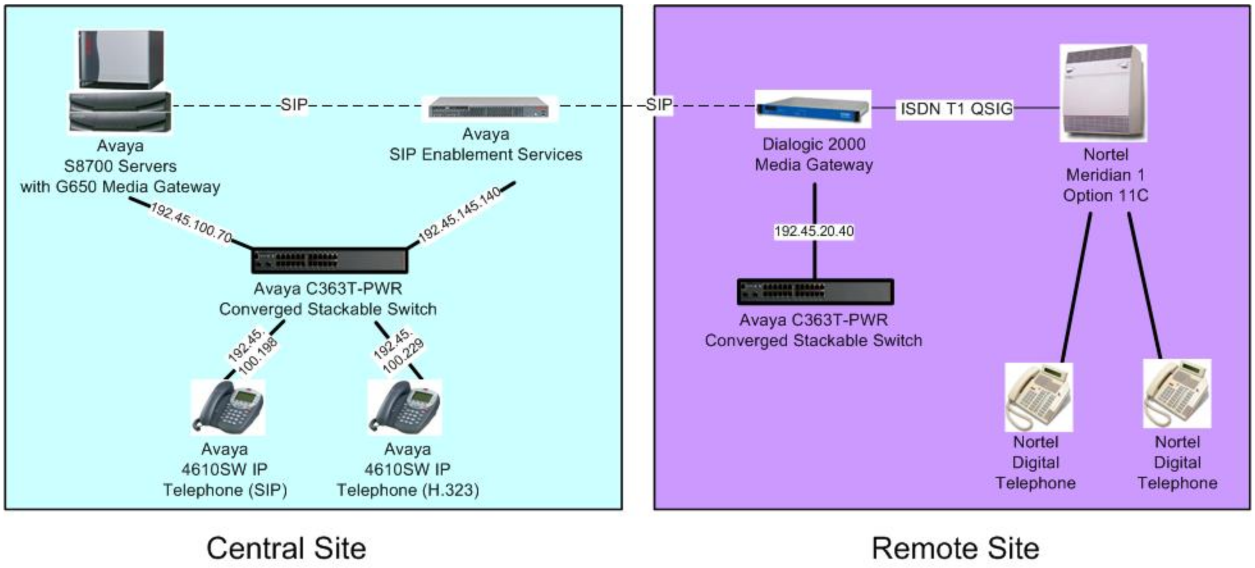
These Application Notes describe the configuration steps required for the Dialogic 2000 Media Gateway telephony gateway appliance to successfully interoperate with Avaya Communication Manager and Avaya SIP Enablement Services in an Avaya SIP Telephony environment. The Dialogic 2000 Media Gateway converts signals between circuit switched and SIP enabled equipment. The compliance testing used a Nortel Meridian 1 Option 11C as the circuit switched equipment.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

The Dialogic 2000 Media Gateway is a telephony gateway appliance that converts signals between circuit switched and SIP enabled equipments. The compliance testing used a Nortel Meridian 1 Option 11C as the circuit switched equipment.

The test configuration consists of Avaya Communication Manager and Avaya SIP Enablement Services (SES) at the Central site, and Dialogic 2000 Media Gateway and Nortel Meridian 1 Option 11C (Meridian 1) at the Remote site. The Dialogic 2000 Media Gateway has ISDN T1 QSIG connectivity to the Nortel Meridian 1 on the one side, and SIP connectivity to Avaya SES on the other. All calls between the Central and Remote sites pass through the Dialogic 2000 Media Gateway.


SIP
SIP
Avaya S8700 Servers with G650 Media Gateway
Avaya SIP Enablement Services
192.45.100.70
192.45.145.140
Avaya C363T-PWR Converged Stackable Switch
192.45.100.198
192.45.100.229
Avaya 4610SW IP Telephone (SIP)
Avaya 4610SW IP Telephone (H.323)
Dialogic 2000 Media Gateway
ISDN T1 QSIG
Nortel Meridian 1 Option 11C
192.45.20.40
Avaya C363T-PWR Converged Stackable Switch
Nortel Digital Telephone
Nortel Digital Telephone
Central Site
Remote Site

A four and five digit Uniform Dial Plan (UDP) was used to facilitate dialing between the Central and Remote sites. Unique extension ranges are associated with Avaya Communication Manager at the Central site (33xxx), and Nortel Meridian 1 at the Remote site (74xx).

These Application Notes assume the SIP connectivity between Avaya Communication Manager and Avaya SES, and the ISDN T1 QSIG connectivity between Dialogic 2000 Media Gateway and Nortel Meridian 1 are already in place and will not be described. These Application Notes will focus on the configuration of the SIP connectivity between Avaya Communication Manager and Dialogic 2000 Media Gateway via Avaya SES.

2. Equipment and Software Validated

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

Equipment	Software
Avaya S8700 Servers	Avaya Communication Manager 4.0, R014x.00.0.730.5
Avaya G650 Media Gateway • TN799DP C-LAN Circuit Pack • TN2302AP IP Media Processor	 HW01 FW024 HW11 FW116
Avaya SIP Enablement Services	3.1, SES03.1-03.1.018.0
Avaya 4610SW IP Telephone	2.2.2 (SIP)
Avaya 4610SW IP Telephone	2.7 (H.323)
Dialogic 2000 Media Gateway DMG2030DTIQ	5.1.147
Nortel Meridian 1 Option 11C • NTAK09BA DTI/PRI Card	Release 25, Version 2111, Issue 15 Release 02
Nortel 2616 Digital Telephones	NA

3. Configure Avaya Communication Manager

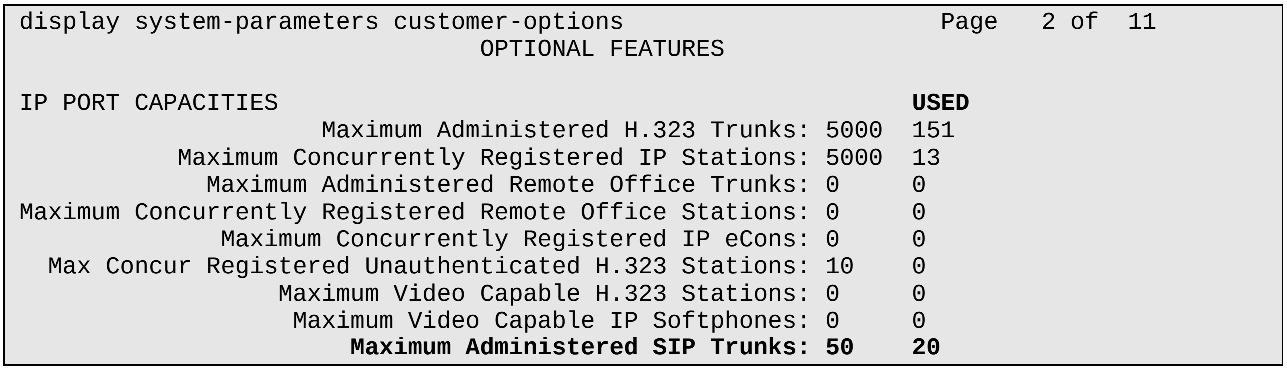
This section focuses on configuring the SIP trunks on Avaya Communication Manager to reach Dialogic 2000 Media Gateway for endpoints on Nortel Meridian 1. In addition, this section highlights selected features that are required for the interoperability, and provides a sample routing using Automatic Alternate Routing (AAR). The configuration procedures include the following areas:

- Verify Avaya Communication Manager license
- Administer system parameters features
- Administer IP codec set
- Administer IP network region
- Administer SIP trunk group
- Administer SIP signaling group
- Administer SIP trunk group members
- Administer route pattern
- Administer public unknown numbering
- Administer uniform dial plan
- Administer AAR analysis

3.1. Verify Avaya Communication Manager License

Log into the System Access Terminal (SAT) to verify that the Avaya Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the "display system-parameters customer-options" command. Navigate to **Page 2**, and verify that there is sufficient remaining capacity for SIP trunks by comparing the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column.

The license file installed on the system controls the maximum permitted. If there is insufficient capacity, contact an authorized Avaya sales representative to make the appropriate changes.

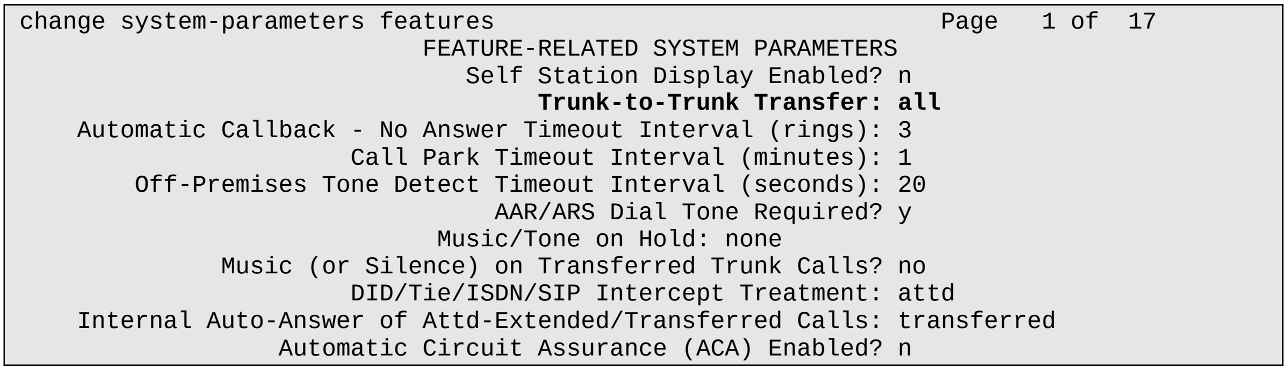


```
display system-parameters customer-options                      Page   2 of  11
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 5000  151
           Maximum Concurrently Registered IP Stations: 5000  13
             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: 10    0
                  Maximum Video Capable H.323 Stations: 0     0
                   Maximum Video Capable IP Softphones: 0     0
                       Maximum Administered SIP Trunks: 50    20
```

3.2. Administer System Parameters Features

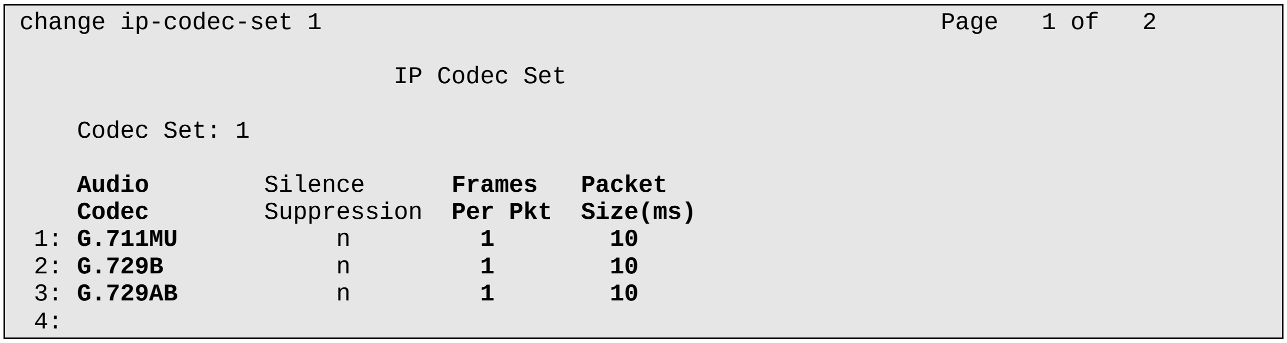
Use the "change system-parameters features" command to allow for trunk-to-trunk transfers. This feature is needed to be able to transfer an incoming call from the Remote site back out to the Remote site (incoming trunk to outgoing trunk), and to transfer an outgoing call to the Remote site to another outgoing call to the Remote site (outgoing trunk to outgoing trunk). For ease of interoperability testing, the **Trunk-to-Trunk Transfer** field was set to "all" to enable all trunk-to-trunk transfers on a system wide basis. Note that this feature poses significant security risk, and must be used with caution. For alternatives, the trunk-to-trunk feature can be implemented on the class of restriction or class of service levels. Refer to the appropriate documentation in **Section 10** for more details.



```
change system-parameters features                               Page   1 of  17
                            FEATURE-RELATED SYSTEM PARAMETERS
                               Self Station Display Enabled? n
                                    Trunk-to-Trunk Transfer: all
    Automatic Callback - No Answer Timeout Interval (rings): 3
                        Call Park Timeout Interval (minutes): 1
        Off-Premises Tone Detect Timeout Interval (seconds): 20
                                 AAR/ARS Dial Tone Required? y
                             Music/Tone on Hold: none
              Music (or Silence) on Transferred Trunk Calls? no
                        DID/Tie/ISDN/SIP Intercept Treatment: attd
    Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
                  Automatic Circuit Assurance (ACA) Enabled? n
```

3.3. Administer IP Codec Set

Use the "change ip-codec-set n" command, where "n" is an existing codec set number that will be used for integration with Dialogic 2000 Media Gateway. Enter the desired audio codec types in the **Audio Codec** fields. Codec types of "G.711MU", "G.729B", and "G.729AB" are interoperable with the Dialogic 2000 Media Gateway. Set the **Frames Per Pkt** field to "1" for each codec type, and the value for the **Packet Size (ms)** field will automatically be updated to "10".



```
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         1        10
 2: G.729B            n         1        10
 3: G.729AB           n         1        10
 4:
```

3.4. Administer IP Network Region

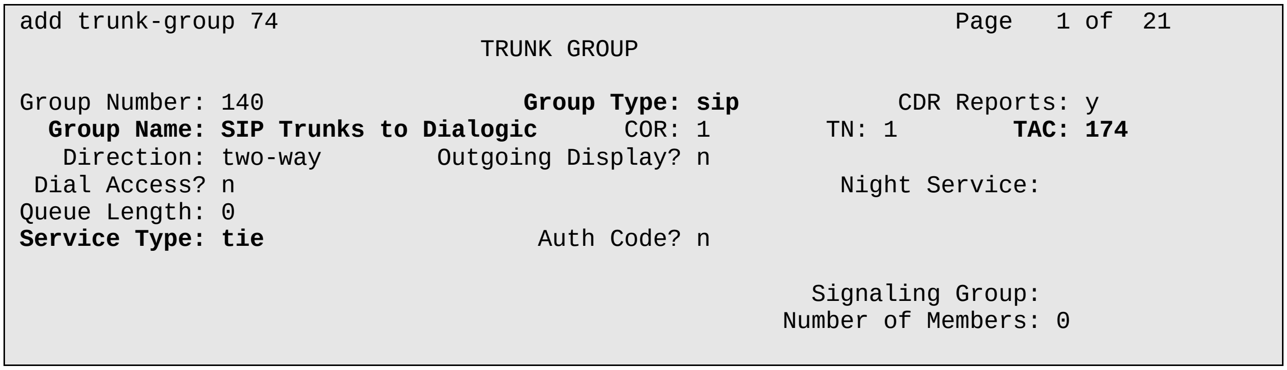
Use the “change ip-network-region n” command, where “n” is an existing network region that will be used for integration with Dialogic. For the **Authoritative Domain** field, enter the SIP domain name of the Avaya SES server, in this case “mm.com”. For the **Codec Set** field, enter the codec set number from **Section 3.3**. Disable the **Intra-region IP-IP Direct Audio**, **Inter-region IP-IP Direct Audio**, and **IP Audio Hairpinning** fields, as media shuffling cannot be used with the Nortel Meridian 1 digital endpoints. Retain the default values in the remaining fields.

In the compliance testing, the same network region is used for the Avaya endpoints. If the network configuration uses a different network region for the Avaya endpoints, then **Page 3** can be used to specify which codec set to use for calls between regions.

```
change ip-network-region 1                                      Page   1 of  19
                               IP NETWORK REGION
  Region: 1
Location:          Authoritative Domain: mm.com
    Name:
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: no
      Codec Set: 1              Inter-region IP-IP Direct Audio: no
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 65531
DIFFSERV/TOS PARAMETERS                  RTCP Reporting Enabled? y
 Call Control PHB Value: 34      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        Video PHB Value: 26
```

3.5. Administer SIP Trunk Group

Administer a SIP trunk group to interface with Dialogic. Use the “add trunk-group n” command, where “n” is an available trunk group number. Set the **Group Type** to “sip”, and **Service Type** to “tie”. Enter a descriptive **Group Name**, and an available trunk access code for the **TAC** field.

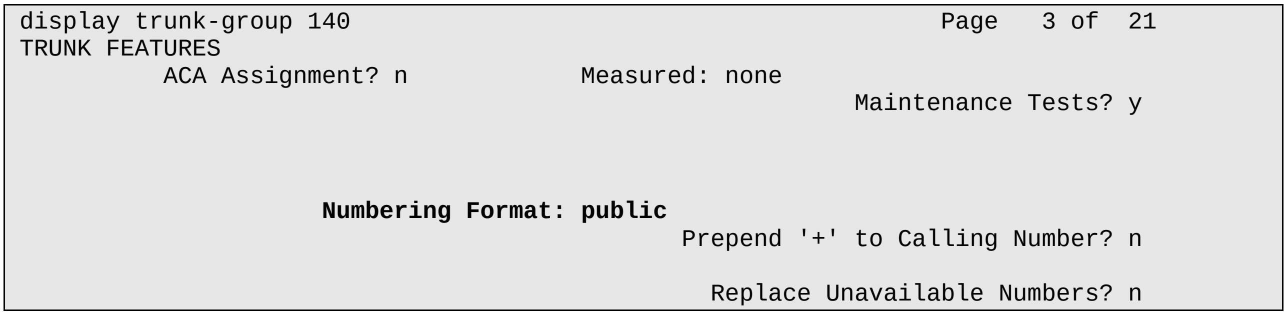


```
add trunk-group 74                                               Page   1 of  21
                                TRUNK GROUP

Group Number: 140                  Group Type: sip           CDR Reports: y
  Group Name: SIP Trunks to Dialogic      COR: 1        TN: 1        TAC: 174
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                          Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n

                                                       Signaling Group:
                                                     Number of Members: 0
```

Navigate to **Page 3**, and enter “public” for the **Numbering Format** field as shown below.



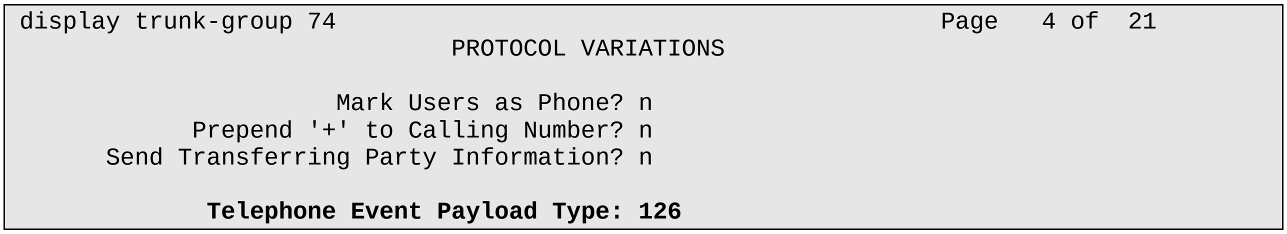
```
display trunk-group 140                                         Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y



                     Numbering Format: public
                                              Prepend '+' to Calling Number? n

                                                Replace Unavailable Numbers? n
```

Navigate to **Page 4**, and change the **Telephone Event Payload Type** field value as shown below. Note that the default value of “127” is used internally by the Dialogic 2000 Media Gateway, and calls originated from Avaya with payload type of “127” would result in immediate drops after connect acknowledgements. Therefore the default payload type must be changed, and the compliance testing was successful with payload type of “126”.



```
display trunk-group 74                                          Page   4 of  21
                              PROTOCOL VARIATIONS

                      Mark Users as Phone? n
            Prepend '+' to Calling Number? n
      Send Transferring Party Information? n

             Telephone Event Payload Type: 126
```

3.6. Administer SIP Signaling Group

Administer a SIP signaling group for the new trunk group to use for signaling. Use the “add signaling-group n” command, where “n” is an available signaling group number. Set the **Group Type** to “sip”. For the **Near-end Node Name** field, enter an existing C-LAN node name, in this case “clan2”. For the **Far-end Node Name** field, enter the Avaya SES node name, in this case “MM-SES-server”. For the **Far-end Network Region** field, enter the IP network region number from **Section 3.4**. For the **Far-end Domain** field, enter the domain name for the Dialogic 2000 Media Gateway in the network configuration. Retain the default values in the remaining fields.

```
add signaling-group 74                                            Page   1 of   1
                                SIGNALING GROUP

 Group Number: 74             Group Type: sip
                        Transport Method: tls

   Near-end Node Name: clan2                 Far-end Node Name: MM-SES-server
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                        Far-end Network Region: 1
       Far-end Domain: mm.com
                                             Bypass If IP Threshold Exceeded? n

         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? y
                                                        IP Audio Hairpinning? Y
Session Establishment Timer(min): 120
```

3.7. Administer SIP Trunk Group Members

Administer SIP trunk group members for the newly added SIP trunk group. Use the “change trunk-group n” command, where “n” is the trunk group number added in **Section 3.5**. Enter the corresponding signaling group number from **Section 3.6** into the **Signaling Group** field. Enter the desired number of trunk group members into the **Number of Members** field.

```
change trunk-group 74                                            Page   1 of  21
                                TRUNK GROUP

Group Number: 74                   Group Type: sip           CDR Reports: y
  Group Name: SIP Trunk to Nortel         COR: 1        TN: 1        TAC: 144
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                          Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n

                                                       Signaling Group: 74
                                                     Number of Members: 10
```

3.8. Administer Route Pattern

Create a route pattern to use for the newly created SIP trunk group. Use the "change route-pattern n" command, where "n" is an available route pattern. Enter a descriptive **Pattern Name**. In the **Grp No** field, enter the trunk group number from **Section 3.5**. In the **FRL** field, enter a level that allows access to this trunk with "0" being least restrictive.

```
change route-pattern 74                                         Page   1 of   3
                    Pattern Number: 74  Pattern Name: Dialogic Pattern
                             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: 74   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 3 4 W     Request                                 Dgts Format
                                                         Subaddress
 1: y y y y y n  n            rest                                         none
```

3.9. Administer Public Unknown Numbering

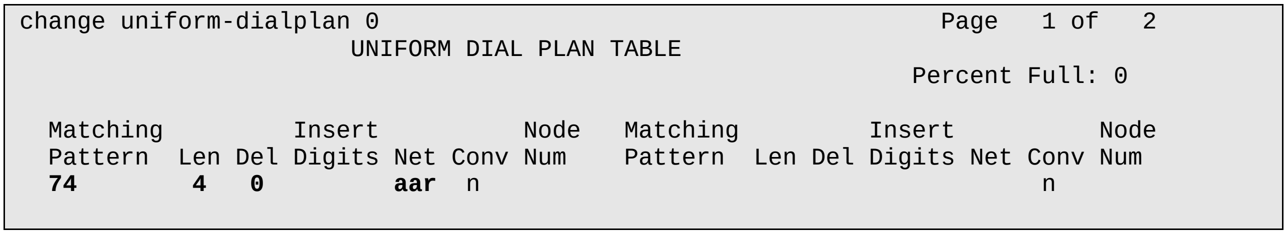
Use the "change public-unknown-numbering 0" command, to define the calling party number to send to Dialogic. Add an entry for the trunk group defined in **Section 3.5**. In the example shown below, all calls originating from a 5-digit extension beginning with 3 and routed to trunk group 74 will result in a 5-digit calling number. The calling party number will be in the SIP "From" header.

```
change public-unknown-numbering 0                               Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                   Total                                   Total
Ext Ext    Trk       CPN            CPN Ext Ext    Trk       CPN            CPN
Len Code   Grp(s)    Prefix         Len Len Code   Grp(s)    Prefix         Len

 5 3       74                        5
```

3.10. Administer Uniform Dial Plan

This section provides a sample AAR routing used for routing calls with dialed digits 74xx to Dialogic. Note that other methods of routing may be used. Use the “change uniform-dialplan 0” command, and add an entry to specify the use of AAR for routing digits 74xx, as shown below.

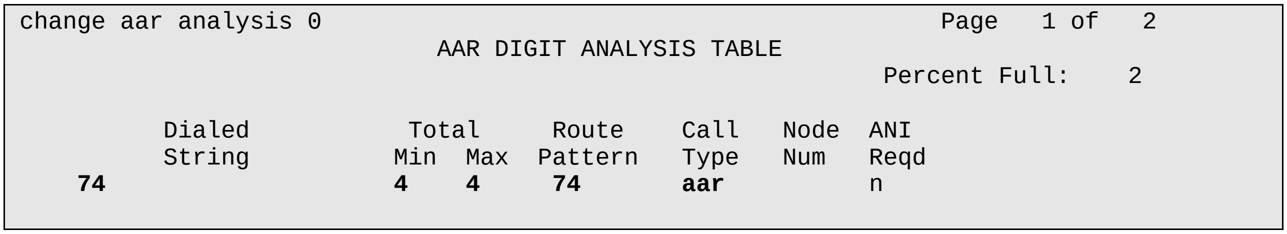


```
change uniform-dialplan 0                                       Page   1 of   2
                       UNIFORM DIAL PLAN TABLE
                                                              Percent Full: 0

  Matching         Insert          Node   Matching         Insert          Node
  Pattern  Len Del Digits Net Conv Num    Pattern  Len Del Digits Net Conv Num
  74        4   0         aar  n                                      n
```

3.11. Administer AAR Analysis

Use the “change aar analysis 0” command, and add an entry to specify how to route calls to 74xx. In the example shown below, calls with digits 74xx will be routed as an AAR call using route pattern “74” from **Section 3.8**.



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

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    74                    4    4     74       aar          n
```

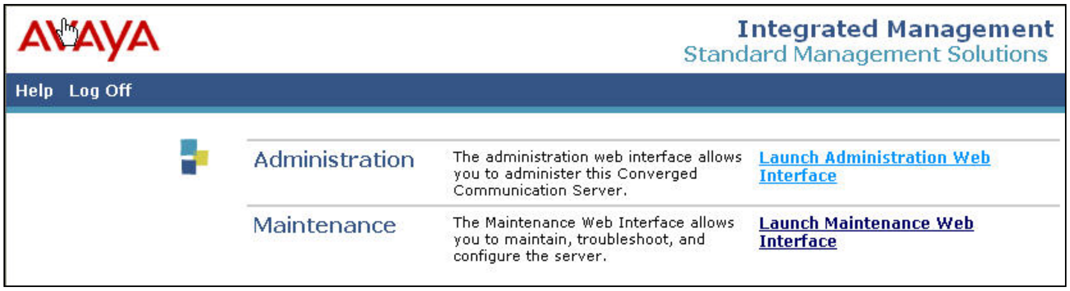
4. Configure Avaya SIP Enablement Services

This section provides the procedures for configuring Avaya SIP Enablement Services. The procedures include the following areas:

- Launch web interface
- Administer host address map
- Administer host contact
- Administer trusted host

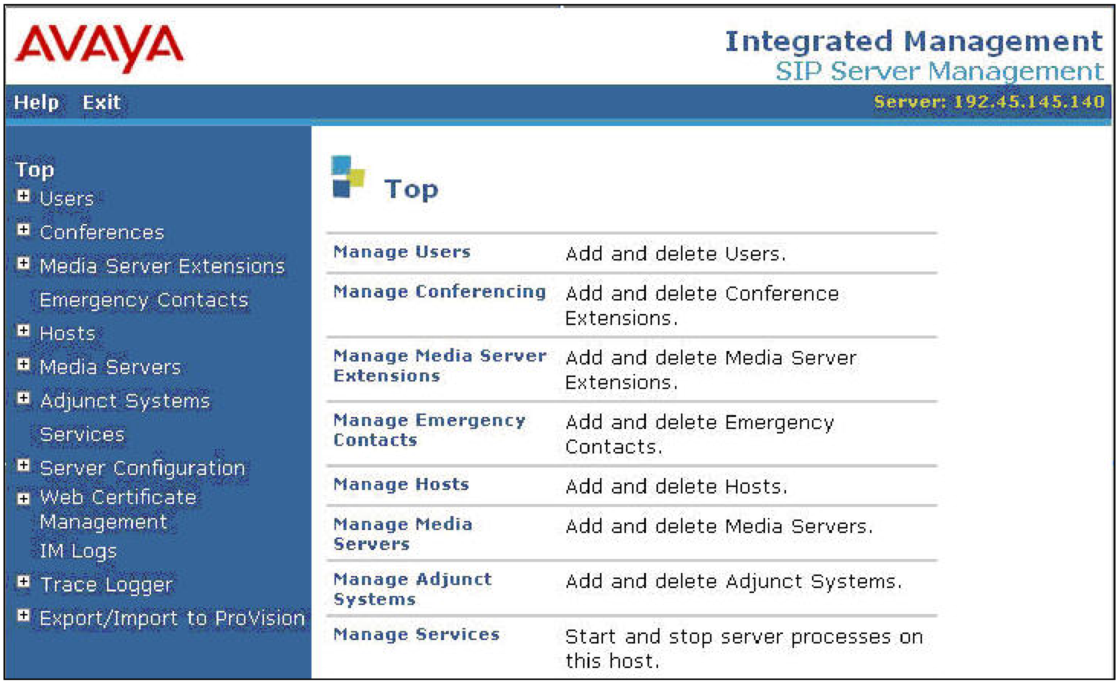
4.1. Launch Web Interface

Access the Avaya SES administration web interface by using the URL "http://<ip-address>/admin" in an Internet browser window, where "<ip-address>" is the IP address of the Avaya SES server. Note that the IP address for the Avaya SES server may vary, and in this case "192.45.145.140" is used. Log in with appropriate credentials and select the **Launch Administration Web Interface** option.



Administration	The administration web interface allows you to administer this Converged Communication Server.	Launch Administration Web Interface
Maintenance	The Maintenance Web Interface allows you to maintain, troubleshoot, and configure the server.	Launch Maintenance Web Interface

The **Top** screen is displayed, as shown below.

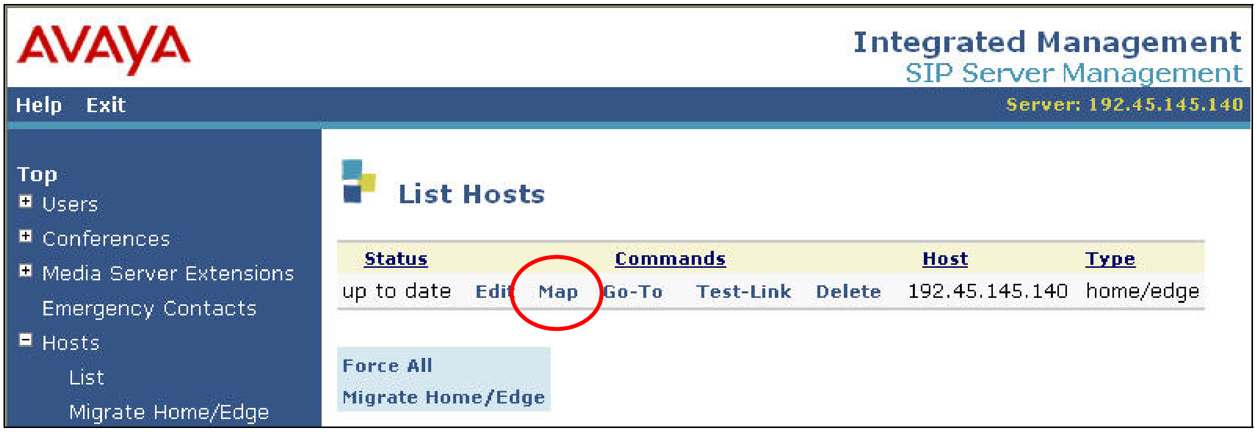


Top

Manage Users	Add and delete Users.
Manage Conferencing	Add and delete Conference Extensions.
Manage Media Server Extensions	Add and delete Media Server Extensions.
Manage Emergency Contacts	Add and delete Emergency Contacts.
Manage Hosts	Add and delete Hosts.
Manage Media Servers	Add and delete Media Servers.
Manage Adjunct Systems	Add and delete Adjunct Systems.
Manage Services	Start and stop server processes on this host.

4.2. Administer Host Address Map

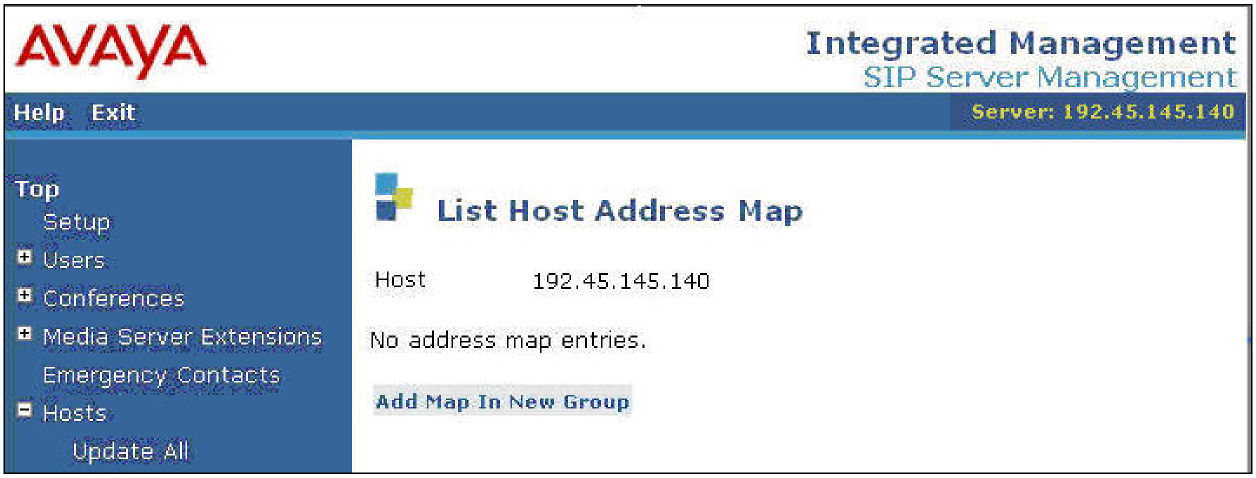
Select **Hosts** > **List** from the left pane to display the **List Hosts** screen. Click the **Map** link.



List Hosts

Status	Commands					Host	Type
up to date	Edit	Map	Go-To	Test-Link	Delete	192.45.145.140	home/edge

In the **List Host Address Map** screen below, click the **Add Map In New Group** link in the right pane.

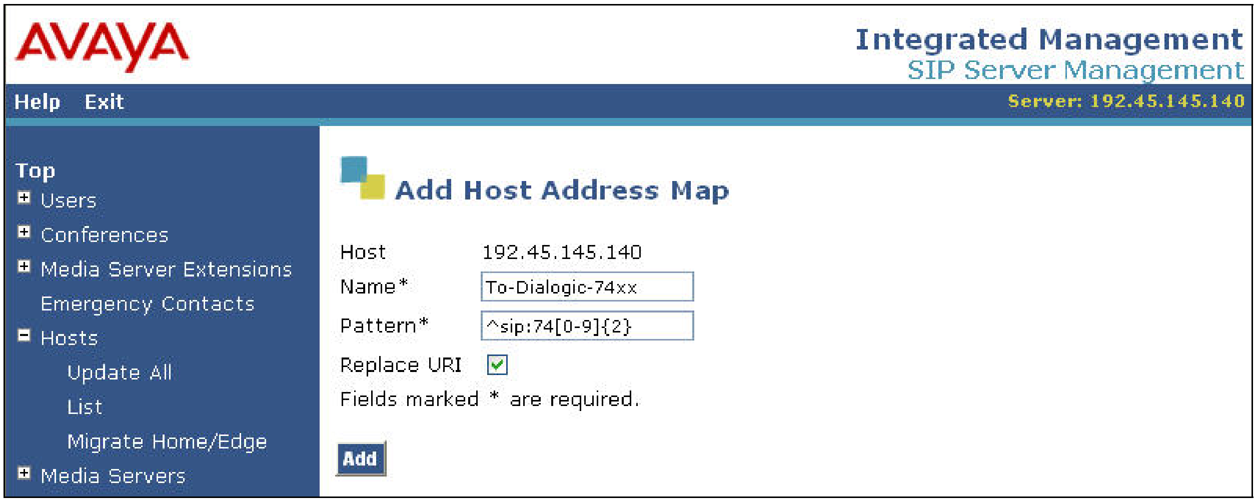


List Host Address Map

Host 192.45.145.140

No address map entries.

The **Add Host Address Map** screen is displayed next. This screen is used to specify which calls are to be routed to the Dialogic 2000 Media Gateway. For the **Name** field, enter a descriptive name to denote the routing. For the **Pattern** field, enter an appropriate syntax for address mapping. For the compliance testing, a pattern of "^sip:74[0-9]{2}" is used to match to any extensions in the range of 7400-7499 at the Remote site. Retain the check in **Replace URI**, and click **Add**.



Add Host Address Map

Host 192.45.145.140

Name* To-Dialogic-74xx

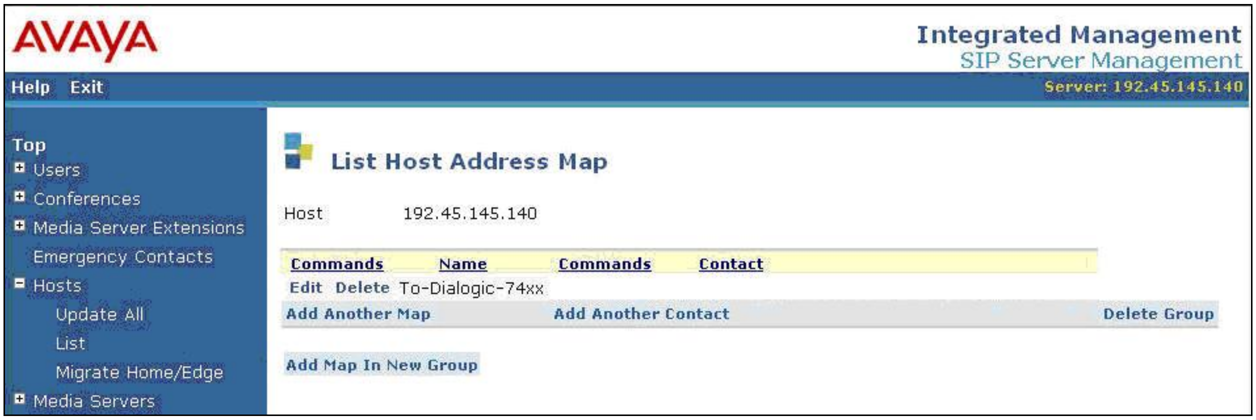
Pattern* ^sip:74[0-9]{2}

Replace URI ☑

Fields marked * are required.

4.3. Administer Host Contact

The **List Host Address Map** screen is displayed again, and updated with the newly created address map. Click **Add Another Contact** in the right pane.

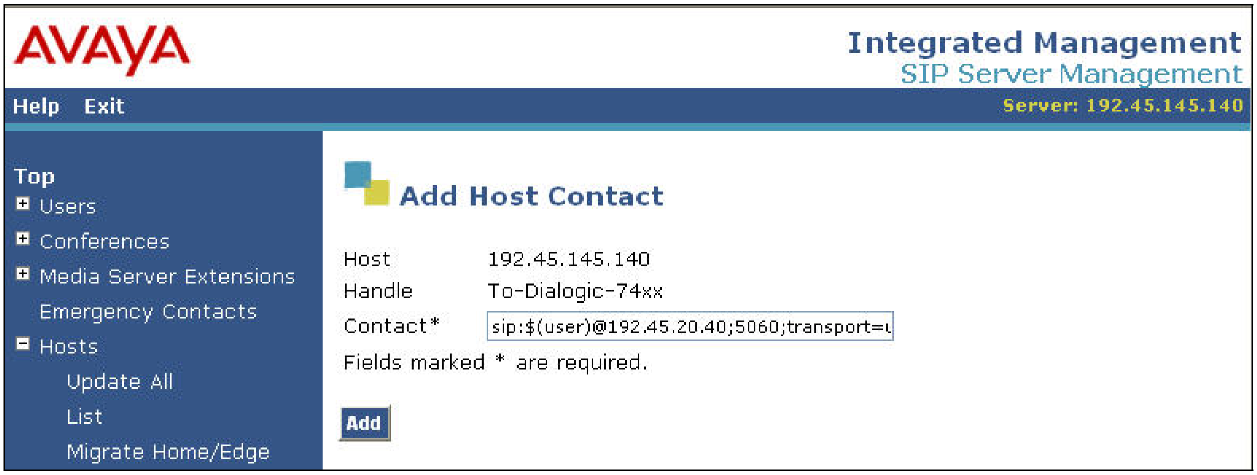


List Host Address Map

Host 192.45.145.140

Commands	Name	Commands	Contact
Edit Delete	To-Dialogic-74xx		

In the **Add Host Contact** screen, enter the contact “sip:$(user)@<destination-IP-address> :5060;transport=udp”, where the <destination-IP-address> is the IP address of the Dialogic 2000 Media Gateway. Avaya SES will substitute “$(user)” with the user portion of the request URI before sending the message. Click the **Add** button.



Add Host Contact

Host 192.45.145.140
Handle To-Dialogic-74xx
Contact* sip:$(user)@192.45.20.40;5060;transport=u
Fields marked * are required.

4.4. Administer Trusted Host

Administer the Dialogic 2000 Media Gateway as a trusted host, so that the SIP messages from Dialogic will not be challenged by Avaya SES. To configure a trusted host, use the “trustedhost –a x –n y –c z” command in the Linux shell of Avaya SES, where “x” is the IP address of the Dialogic 2000 Media Gateway, “y” is the host name or IP address of the Avaya SES server, and “z” is any desired comment.

```
craft@SES-DevCon1> trustedhost -a 192.45.20.40 -n 192.45.145.140 –c Dialogic
192.45.20.40 is added to trusted host list.
```

After configuring the trusted host, the user must go back to the Avaya SES administration web interface, and click the **Update** link in the bottom left pane (not shown) for all changes in **Section 4** to take effect.

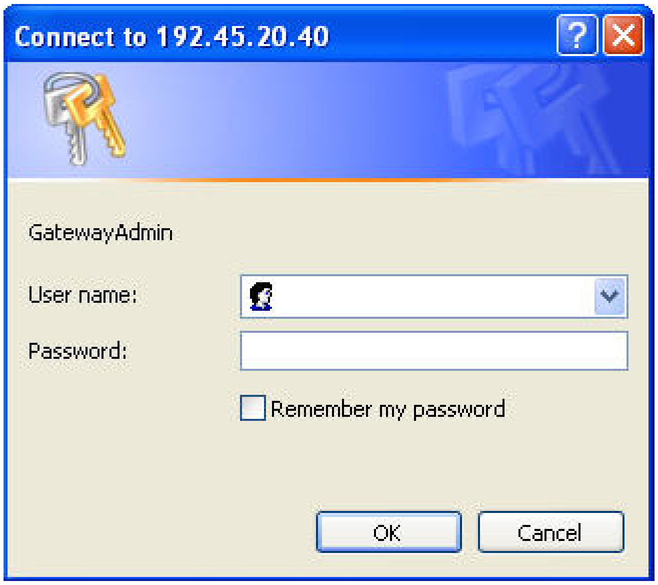
5. Configure Dialogic 2000 Media Gateway

This section provides the procedures for configuring Dialogic 2000 Media Gateway. The procedures include the following areas:

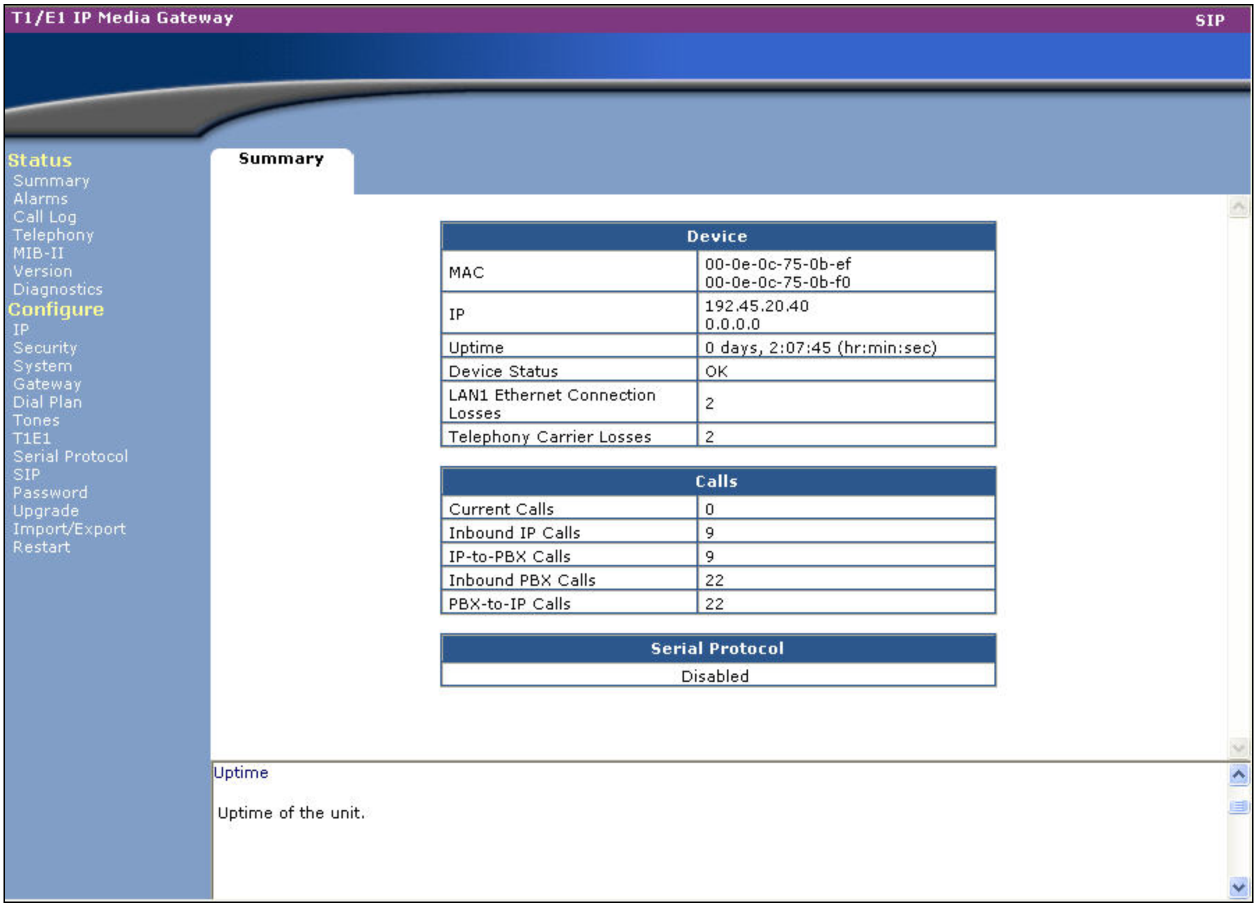
- Launch web interface
- Administer IP
- Administer system
- Administer gateway
- Administer T1E1
- Administer SIP
- Restart gateway

5.1. Launch Web Interface

Access the Dialogic web interface by using the URL "http://<ip-address>" in an Internet browser window, where "<ip-address>" is the IP address of the Dialogic 2000 Media Gateway. Note that the IP address for the gateway may vary, and in this case "192.45.20.40" is used. Log in with the appropriate credentials.



The **T1/E1 IP Media Gateway** screen is displayed, with the **Summary** tab open in the upper right pane, as shown below.



Device	
MAC	00-0e-0c-75-0b-ef 00-0e-0c-75-0b-f0
IP	192.45.20.40 0.0.0.0
Uptime	0 days, 2:07:45 (hr:min:sec)
Device Status	OK
LAN1 Ethernet Connection Losses	2
Telephony Carrier Losses	2

Calls	
Current Calls	0
Inbound IP Calls	9
IP-to-PBX Calls	9
Inbound PBX Calls	22
PBX-to-IP Calls	22

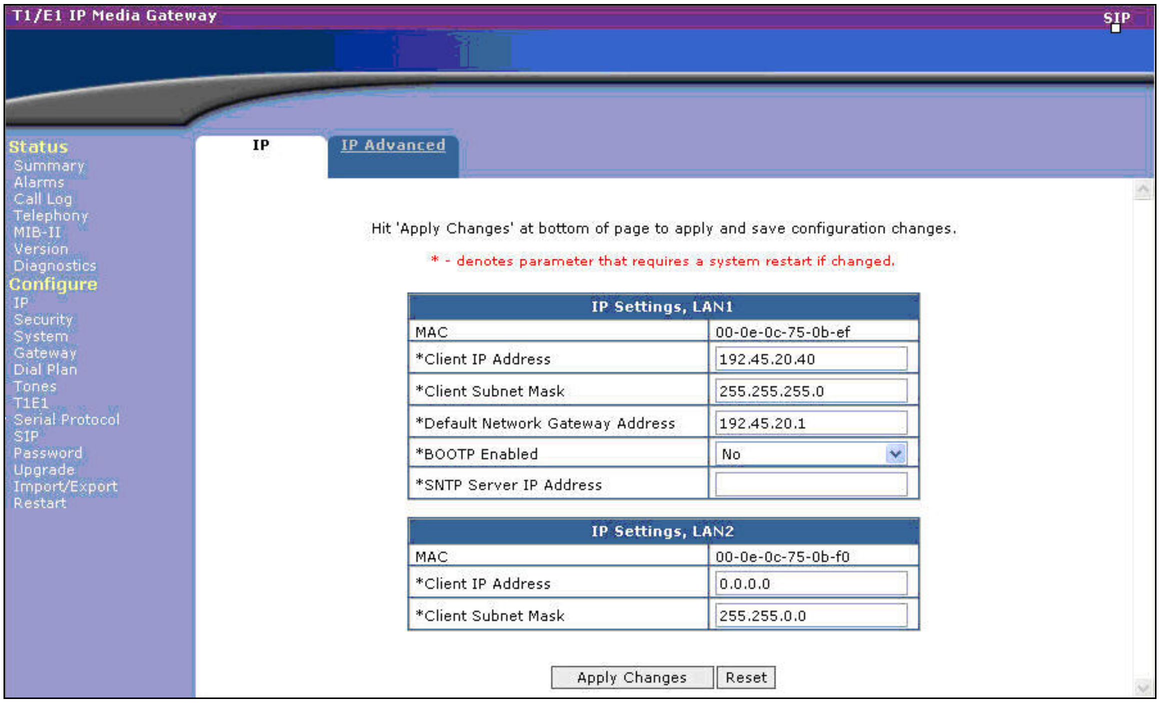
Serial Protocol
Disabled

Uptime

Uptime of the unit.

5.2. Administer IP

Select **Configure** > **IP** in the left pane. The **IP** tab is opened and displayed in the right pane. Enter the proper values for the **Client IP Address**, **Client Subnet Mask**, and **Default Network Gateway Address** fields for the network configuration. Retain the default values in the remaining fields, and click **Apply Changes**.



Hit 'Apply Changes' at bottom of page to apply and save configuration changes.

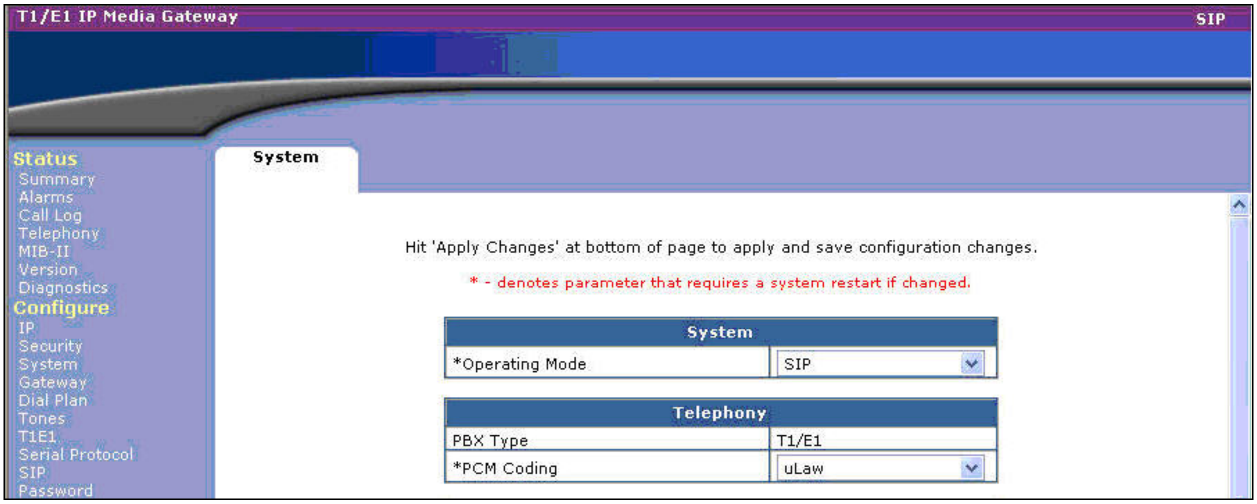
* - denotes parameter that requires a system restart if changed.

IP Settings, LAN1	
MAC	00-0e-0c-75-0b-ef
*Client IP Address	192.45.20.40
*Client Subnet Mask	255.255.255.0
*Default Network Gateway Address	192.45.20.1
*BOOTP Enabled	No
*SNTP Server IP Address	

IP Settings, LAN2	
MAC	00-0e-0c-75-0b-f0
*Client IP Address	0.0.0.0
*Client Subnet Mask	255.255.0.0

5.3. Administer System

Select **Configure** > **System** in the left pane. The **System** tab is opened and displayed in the right pane. Verify that the **Operating Mode** is defaulted to "SIP", as shown below.



Hit 'Apply Changes' at bottom of page to apply and save configuration changes.

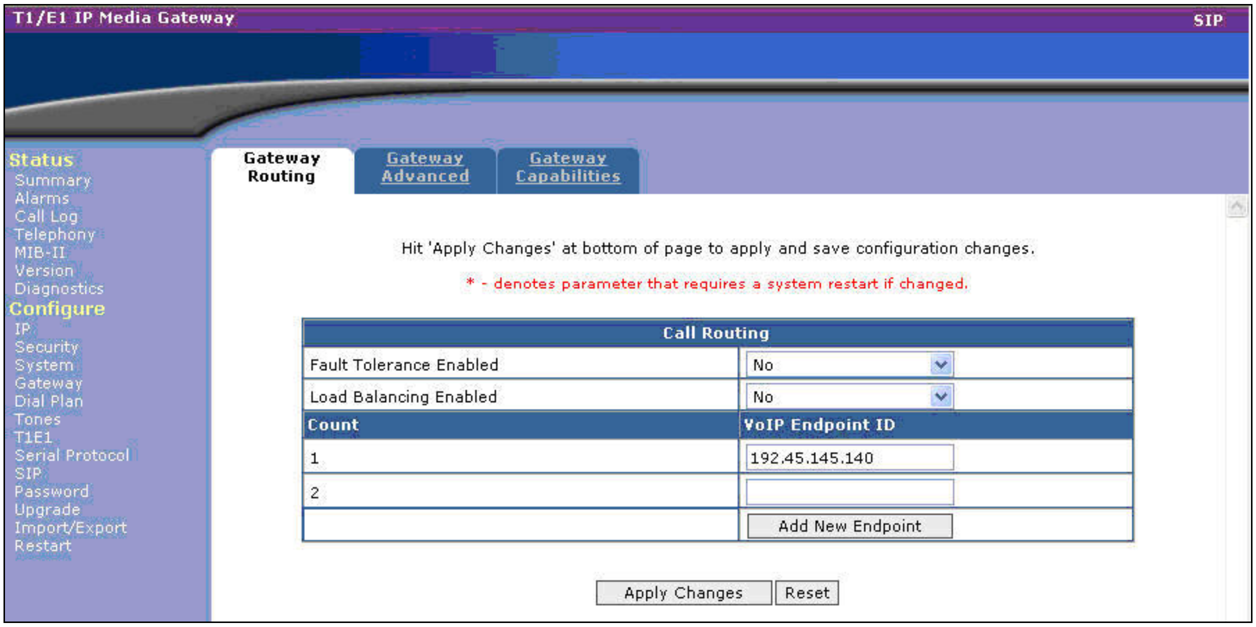
* - denotes parameter that requires a system restart if changed.

System	
*Operating Mode	SIP

Telephony	
PBX Type	T1/E1
*PCM Coding	uLaw

5.4. Administer Gateway

Select **Configure** > **Gateway** in the left pane. The **Gateway Routing** tab is opened and displayed in the right pane. Enter the IP address of Avaya SES into the first **VoIP Endpoint ID** field, as shown below. Click **Apply Changes**.

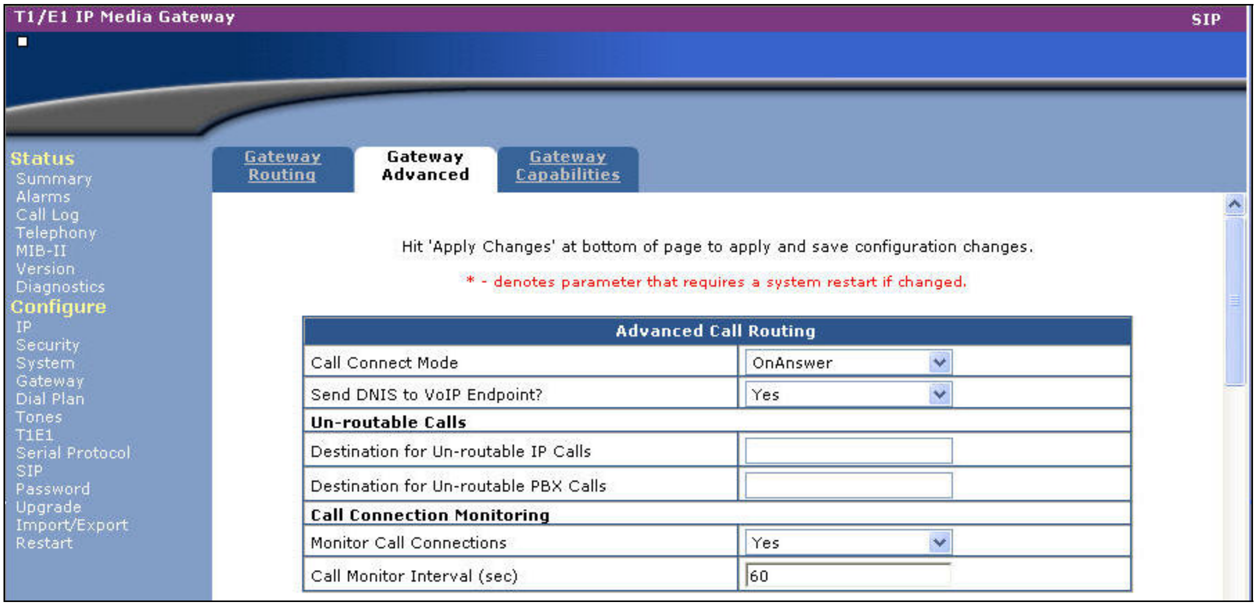


Hit 'Apply Changes' at bottom of page to apply and save configuration changes.

* - denotes parameter that requires a system restart if changed.

Call Routing	
Fault Tolerance Enabled	No
Load Balancing Enabled	No
Count	**VoIP Endpoint ID**
1	192.45.145.140
2	

Select the **Gateway Advanced** tab. In the **Send DNIS to VoIP Endpoint** field, select “Yes” from the drop-down list.

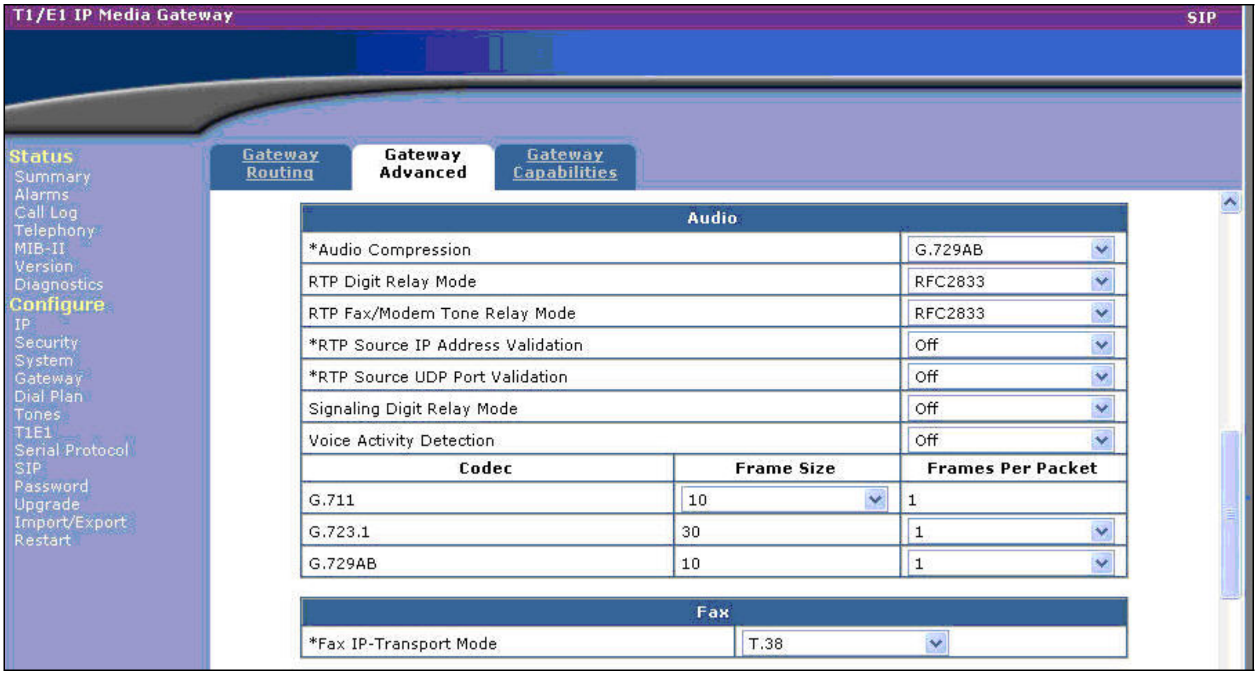


Hit 'Apply Changes' at bottom of page to apply and save configuration changes.

* - denotes parameter that requires a system restart if changed.

Advanced Call Routing	
Call Connect Mode	OnAnswer
Send DNIS to VoIP Endpoint?	Yes
Un-routable Calls	
Destination for Un-routable IP Calls	
Destination for Un-routable PBX Calls	
Call Connection Monitoring	
Monitor Call Connections	Yes
Call Monitor Interval (sec)	60

Scroll down to the **Audio** section. In the **Audio Compression** field, select the desired audio codec. If the desired audio codec is G.711, then set the corresponding **Frame Size** field to "10", and the **Frames Per Packet** field value will be updated automatically to "1". If the desired audio codec is G.729AB, then set the corresponding **Frame Per Packet** field to "1", and the **Frame Size** field value will be updated automatically to "10". Retain the default values in the remaining fields. Scroll down to the bottom of the screen, and click **Apply Changes** (not shown below).



Audio	
*Audio Compression	G.729AB
RTP Digit Relay Mode	RFC2833
RTP Fax/Modem Tone Relay Mode	RFC2833
*RTP Source IP Address Validation	Off
*RTP Source UDP Port Validation	Off
Signaling Digit Relay Mode	Off
Voice Activity Detection	Off

Codec	Frame Size	Frames Per Packet
G.711	10	1
G.723.1	30	1
G.729AB	10	1

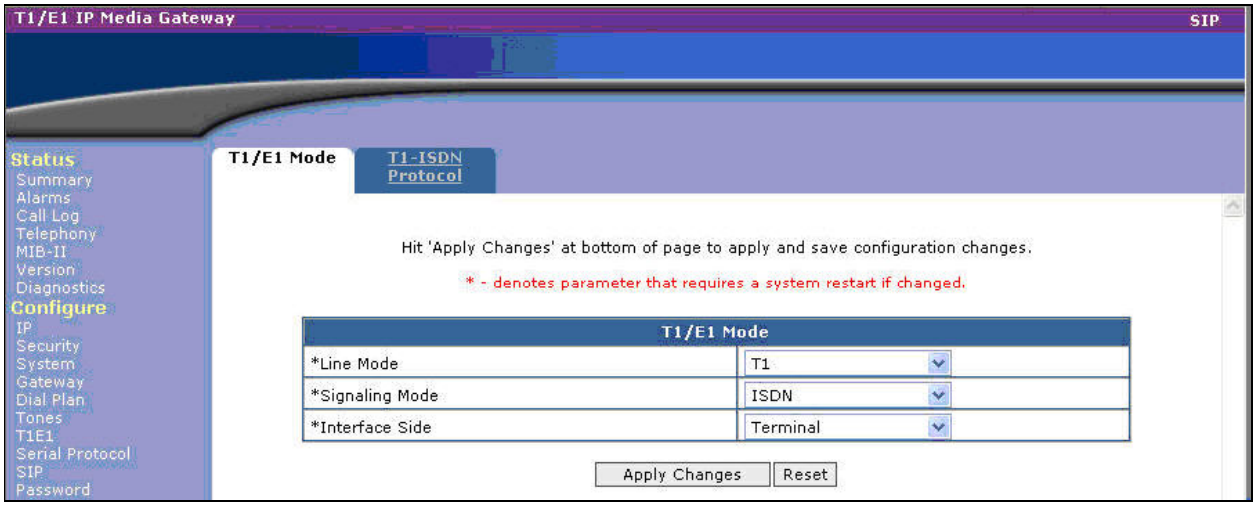
Fax	
*Fax IP-Transport Mode	T.38

The following are the audio codec types that successfully interoperated between Dialogic 2000 Media Gateway and Avaya Communication Manager during the compliance testing.

Dialogic 2000 Media Gateway	Avaya Communication Manager
G.711	G.711MU
G.729AB	G.729AB, G.729B

5.5. Administer T1E1

Select **Configure > T1E1** in the left pane. The **T1/E1 Mode** tab is opened and displayed in the right pane. Verify that the **Signaling Mode** field is set to "ISDN", as shown below. Click **Apply Changes**.

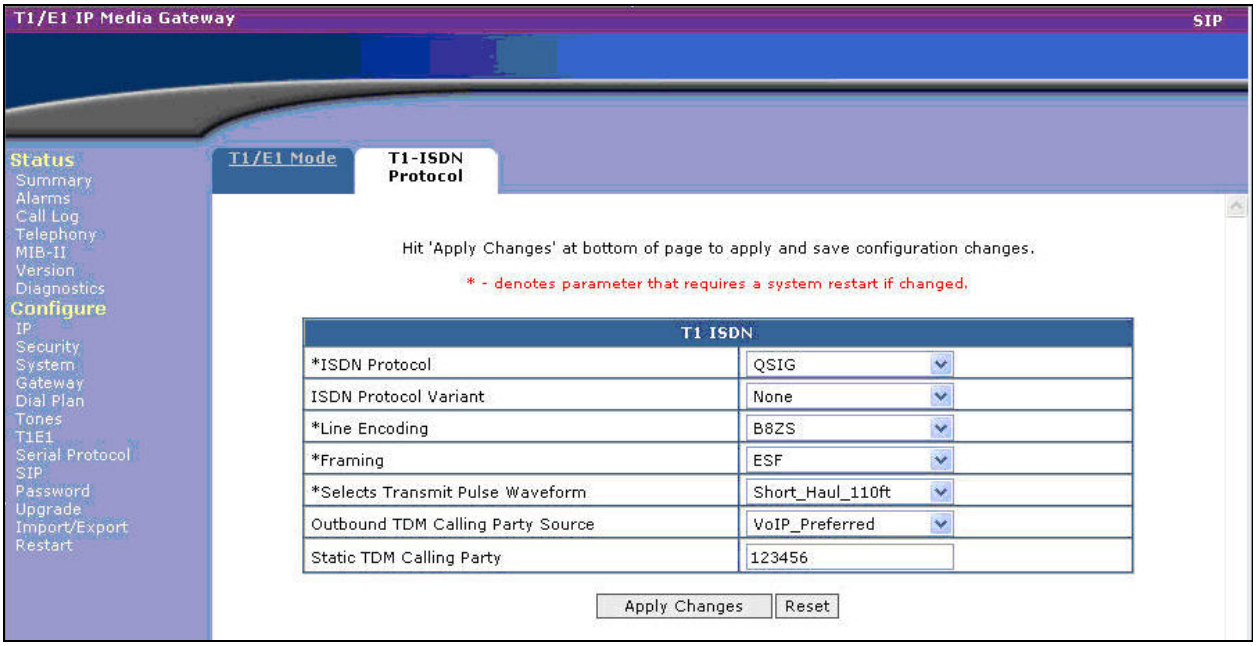


Hit 'Apply Changes' at bottom of page to apply and save configuration changes.

* - denotes parameter that requires a system restart if changed.

T1/E1 Mode	
*Line Mode	T1
*Signaling Mode	ISDN
*Interface Side	Terminal

Select the **T1-ISDN Protocol** tab. In the **Outbound TDM Calling Party Source** field, select "VoIP_Preferred" from the drop-down list to use the SIP call as the source of calling party information to provide to the TDM interface to Nortel Meridian 1. Click **Apply Changes**.



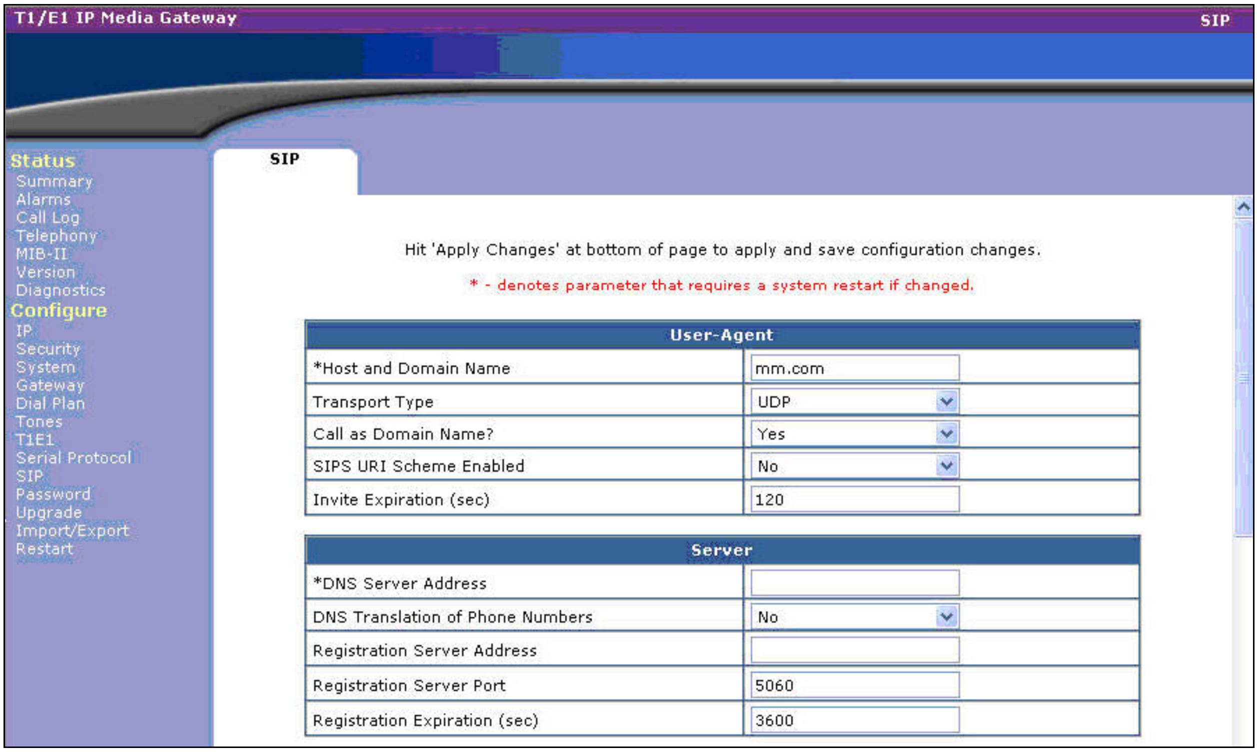
Hit 'Apply Changes' at bottom of page to apply and save configuration changes.

* - denotes parameter that requires a system restart if changed.

T1 ISDN	
*ISDN Protocol	QSIG
ISDN Protocol Variant	None
*Line Encoding	B8ZS
*Framing	ESF
*Selects Transmit Pulse Waveform	Short_Haul_110ft
Outbound TDM Calling Party Source	VoIP_Preferred
Static TDM Calling Party	123456

5.6. Administer SIP

Select **Configure > SIP** in the left pane. The **SIP** tab is opened and displayed in the right pane. For the **Host and Domain Name** field, enter the domain name for the network configuration. For the **Call as Domain Name** field, select “Yes” from the drop-down list.



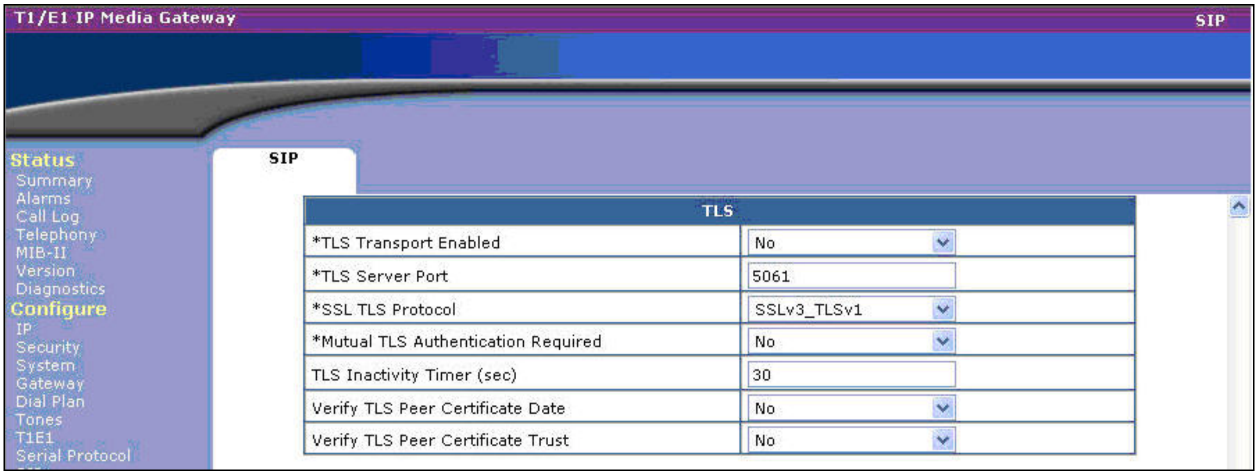
Hit 'Apply Changes' at bottom of page to apply and save configuration changes.

* - denotes parameter that requires a system restart if changed.

User-Agent	
*Host and Domain Name	mm.com
Transport Type	UDP
Call as Domain Name?	Yes
SIPS URI Scheme Enabled	No
Invite Expiration (sec)	120

Server	
*DNS Server Address	
DNS Translation of Phone Numbers	No
Registration Server Address	
Registration Server Port	5060
Registration Expiration (sec)	3600

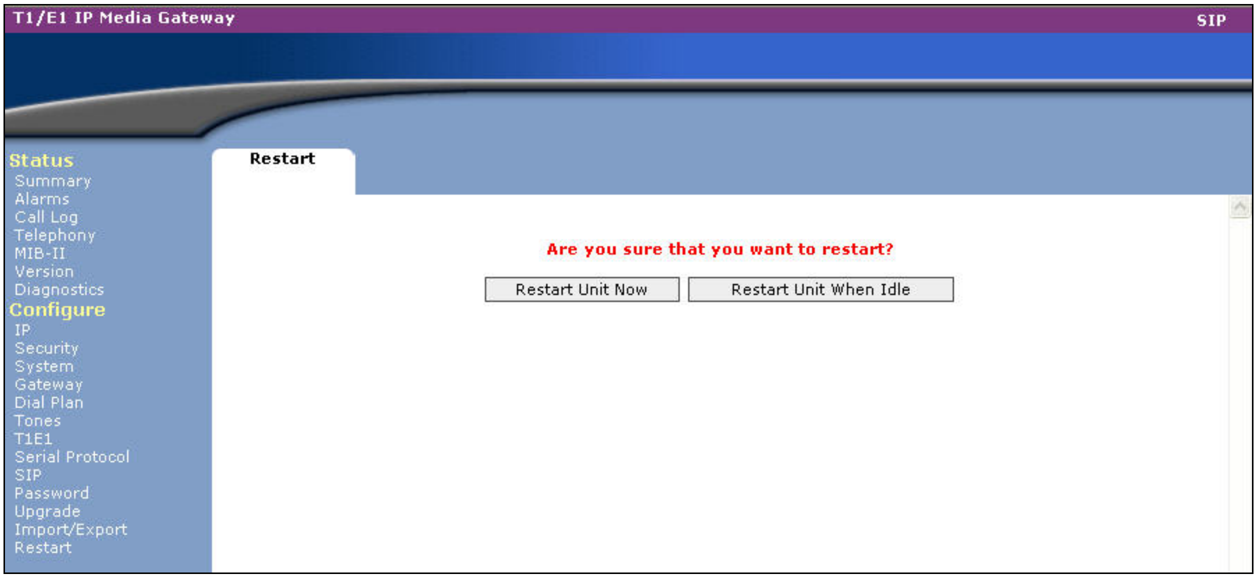
Scroll down the screen to the TLS section. For the **Mutual TLS Authentication Required**, **Verify TLS Peer Certificate Date**, and **Verify TLS Peer Certificate Trust** fields, select “No” from the drop-down lists. Retain the default values in the remaining fields, and click **Apply Changes** in the bottom of the screen (not shown below).



TLS	
*TLS Transport Enabled	No
*TLS Server Port	5061
*SSL TLS Protocol	SSLv3_TLSv1
*Mutual TLS Authentication Required	No
TLS Inactivity Timer (sec)	30
Verify TLS Peer Certificate Date	No
Verify TLS Peer Certificate Trust	No

5.7. Restart Gateway

Select **Configure > Restart** in the left pane. The **Restart** tab is opened and displayed in the right pane. Click **Restart Unit Now** to proceed with the restart, for all changes in **Section 5** to take effect.



Are you sure that you want to restart?

6. Interoperability Compliance Testing

The interoperability compliance testing included SIP feature and serviceability tests.

The feature testing included basic call, hold, transfer, conference, call forwarding, caller ID display, calling number block, and DTMF. The basic call scenarios utilized G.711 and G.729AB audio codecs without IP media shuffling. Due to feature limitations on the Nortel Meridian 1, the calling number block feature was only verified from Avaya to Dialogic and the DTMF feature was only verified from Dialogic to Avaya.

The serviceability testing included disconnecting the Ethernet cables to Avaya SES and to Dialogic 2000 Media Gateway.

6.1. General Test Approach

All tests were performed manually. The focus is on verifying that basic SIP features can work across sites via the Dialogic 2000 Media Gateway.

The serviceability testing focused on verifying the ability of Dialogic 2000 Media Gateway to recover from loss of network connectivity.

6.2. Test Results

All test cases were executed and passed.

7. Verification Steps

This section provides the tests that can be performed on Avaya Communication Manager, Avaya SES, and Dialogic 2000 Media Gateway to verify proper configuration.

7.1. Verify Avaya Communication Manager

Verify the status of the SIP trunk group by using the “status trunk n” command, where “n” is the trunk group number administered in **Section 3.5**. Verify that all trunks are in the “in-service/idle” state as shown below.

```
status trunk 74

                             TRUNK GROUP STATUS

Member   Port     Service State      Mtce Connected Ports
                                     Busy

0074/001 T00184   in-service/idle    no
0074/002 T00185   in-service/idle    no
0074/003 T00186   in-service/idle    no
0074/004 T00187   in-service/idle    no
0074/005 T00188   in-service/idle    no
0074/006 T00189   in-service/idle    no
0074/007 T00190   in-service/idle    no
0074/008 T00191   in-service/idle    no
0074/009 T00192   in-service/idle    no
0074/010 T00193   in-service/idle    no
```

Verify the status of the SIP signaling group by using the “status signaling-group n” command, where “n” is the signaling group number administered in **Section 3.6**. Verify the signaling group is “in-service” as indicated in the **Group State** field shown below.

```
status signaling-group 74
                         STATUS SIGNALING GROUP

        Group ID: 74                             Active NCA-TSC Count: 0
      Group Type: sip                             Active CA-TSC Count: 0
  Signaling Type: facility associated signaling
     Group State: in-service
```

Make a call between the two sites. Verify the status of the connected SIP trunk by using the "status trunk x/y" command, where "x" is the number of the SIP trunk group from **Section 3.5**, and "y" is the member number of the connected trunk. Verify that the **Service State** is "in-service/active", and that the IP addresses of the C-LAN and Avaya SES server are shown in the **Signaling** section. In addition, the **Audio** section shows the proper codec and the IP addresses of the Avaya IP Media Processor card and the Dialogic 2000 Media Gateway. The **Audio Connection Type** displays "ip-tdm", indicating no direct media between the endpoints.

```
status trunk 74/5                                              Page   1 of   3
                              TRUNK STATUS

 Trunk Group/Member: 0074/005              Service State: in-service/active
              Port: T00188              Maintenance Busy? no
 Signaling Group ID:

   IGAR Connection? no

    Connected Ports: S00305




                   Port     Near-end IP Addr : Port    Far-end IP Addr : Port
        Signaling: 02A0217  192. 45.100. 70  : 5061    192. 45.145.140 : 5061

G.729B      Audio: 02A0307  192. 45.100. 71  : 29020   192. 45. 20. 40 : 49060
            Video:
      Video Codec:
                                            Authentication Type: None
    Audio Connection Type: ip-tdm
```

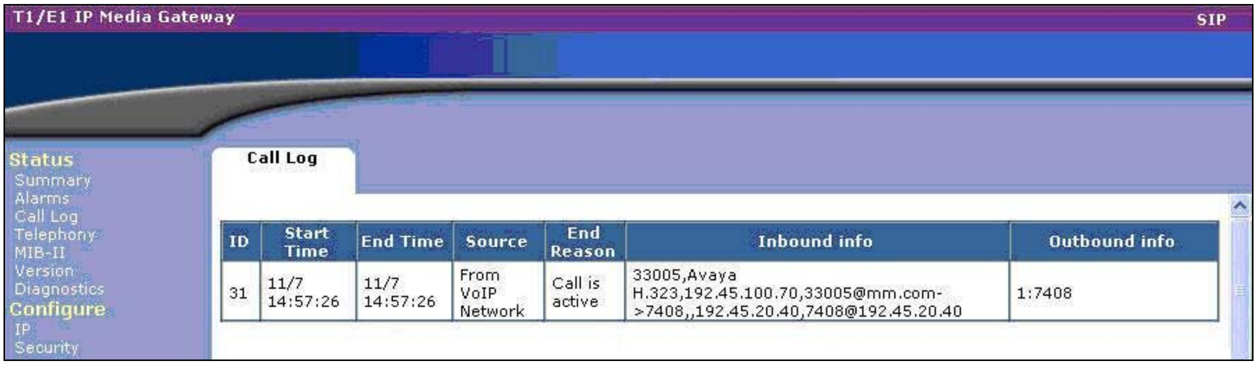
7.2. Verify Avaya SIP Enablement Services

From the Linux shell of Avaya SES, use the "trustedhost –L" command to verify the IP address of the Dialogic 2000 Media Gateway is listed as a trusted host.

```
craft@MM-SIP> trustedhost –L
Third party trusted hosts.
       Trusted Host       |       CCS Host Name       |         Comment
--------------------------+---------------------------+------------------------
192.45.20.40              | 192.45.145.140            | Dialogic
```

7.3. Verify Dialogic 2000 Media Gateway

Make a call between the two sites. From the Dialogic web interface, select **Status > Call Log** from the left pane. Verify that an entry is created for the active call, and that the **Inbound info** column displays the calling and called party information, as shown below.



ID	Start Time	End Time	Source	End Reason	Inbound info	Outbound info
31	11/7 14:57:26	11/7 14:57:26	From VoIP Network	Call is active	33005,Avaya H.323,192.45.100.70,33005@mm.com->7408,,192.45.20.40,7408@192.45.20.40	1:7408

8. Support

Technical support on Dialogic 2000 Media Gateway can be obtained through www.dialogic.com/support/default.asp.

9. Conclusion

These Application Notes describe the configuration steps required for the Dialogic 2000 Media Gateway to successfully interoperate with an Avaya SIP Telephony environment consisting of Avaya Communication Manager, Avaya SIP Enablement Services, and Avaya 4600 Series IP Telephones (SIP and H.323).

10. Additional References

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

- *Administrator Guide for Avaya Communication Manager*, Document 03-300509, Issue 3.1, February 2007, available at http://support.avaya.com.

- *Installing and Administering SIP Enablement Services R3.1*, Document ID 03-600768, Issue 2.1, March 2007, available at http://support.avaya.com.

- *SIP Support in Release 3.1 of Avaya Communication Manager Running on the S8300, S8400, S8500 series, and S8700 series Media Server*, Document 555-245-206, Issue 6.1, March 2007, available at http://support.avaya.com.

- *Dialogic 1000 and 2000 Media Gateway Series User's Guide*, Document 64-0260-02, available at http://www.dialogic.com.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.