



Front-Ending Avaya Communication Server 1000 R4.5 with an Avaya G450 Media Gateway Controlled by Avaya Aura™ Communication Manager 5.2.1 using a PRI NI-1 trunk to Support SIP Trunks to Avaya Aura™ Session Manager 5.2 – Issue 1.0

Abstract

These Application Notes present a sample configuration that uses an Avaya G450 Media Gateway as a PRI NI-1/SIP gateway to connect Avaya Communication Server 1000 R4.5 (formerly known as Nortel Communication Server 1000) with Avaya Aura™ Session Manager 5.2, which in turn can provide call routing support to other Avaya SIP products.

For the sample configuration, Session Manager runs on an Avaya S8510 Server, Communication Manager runs on Avaya S8720 servers, and Communication Server 1000 runs on Avaya Communication Server 1000S. The results in these Application Notes should be applicable to other Avaya servers and media gateways that support Communication Manager.

1 Introduction

Previous Avaya Application Notes [8] describe how Release 4.5 Avaya Communication Server 1000 (formerly known as Nortel Communication Server 1000 and hereafter referred to as the CS1000) can be directly integrated with Avaya Aura™ Session Manager using SIP trunks. Since there are installations of the CS1000 which are not SIP or IP capable, an effective solution is to front-end the CS1000 with a PRI-QSIG gateway, which then signals on SIP trunks to Session Manager. Application notes are also available documenting the configuration steps for this arrangement [9, 10]. However, there are also many installations of the CS1000 which are not PRI-QSIG capable. In these cases, front-ending using PRI-NI-1 instead of QSIG can be employed. This configuration supports basic and supplementary call features. These Application Notes document the configuration steps and parameter settings required to support front-ending the CS1000 with an Avaya G450 Media Gateway controlled by Avaya Aura™ Communication Manager using PRI NI-1, such that the CS1000 can be integrated with Avaya Aura™ Session Manager via SIP trunks.

The sample configuration is shown in **Figure 1**. The G450 Media Gateway is controlled by Communication Manager, which supports SIP trunks to the SM-100 (Security Module) network interface of Session Manager. Session Manager can support flexible inter-system call routing based on dialed number, calling number, and system location, and can also provide protocol adaptation to allow multi-vendor systems to interoperate. It is managed by a separate Avaya Aura™ System Manager, which can manage multiple Session Managers by communicating with their management network interfaces.

For the sample configuration, Session Manager and System Manager run on Avaya S8510 Servers, Communication Manager runs on Avaya S8720 servers, and the CS1000 runs on Avaya Communication Server 1000S. These Application Notes should apply to other Avaya servers and Media Gateways running Communication Manager.

As shown in **Figure 1**, Communication Manager controls the G450 Media Gateway, Avaya 9630 IP Telephone (H.323), and 6408D+ Digital Telephone. The CS1000 controls the Avaya i2004 IP Telephone and 3904 Digital Telephone (formerly sold under the Nortel label). A five digit Uniform Dial Plan (UDP) is used for dialing between systems. Unique extension ranges are associated with Communication Manager (3xxxx) and Avaya Communication Server 1000 (53xxx). Session Manager routes calls based on this five digit plan.

These Application Notes will focus on configuration of the PRI NI-1 trunk, SIP trunk, dial plan support, and call routing. Detailed administration of the endpoint telephones will not be described.

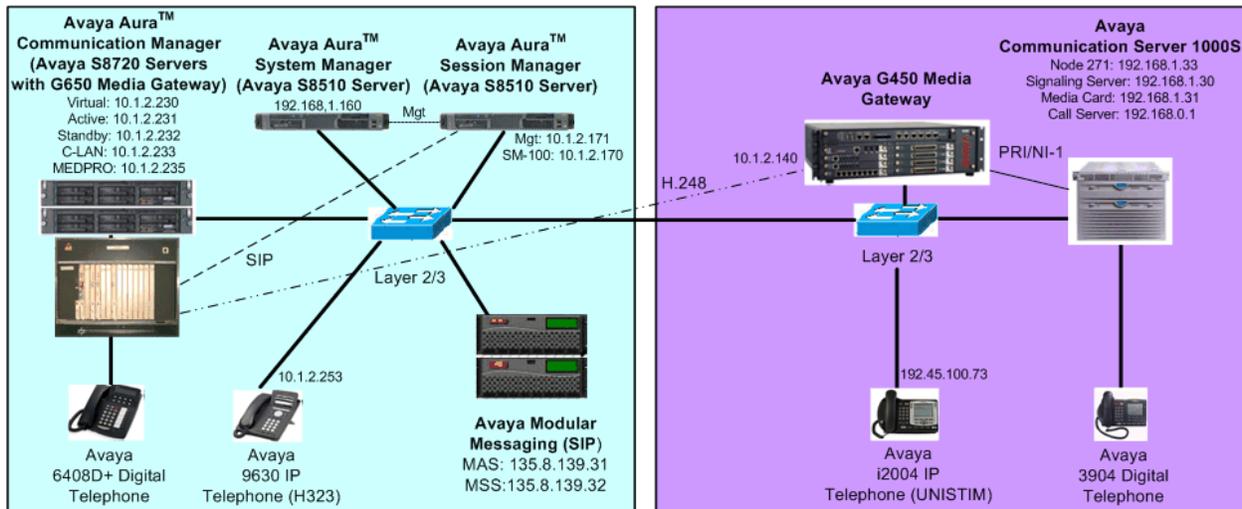


Figure 1 – Sample Configuration

2 Equipment and Software Validated

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

Hardware Component	Software Version
Avaya S8720 Servers with G450 and G650 Media Gateways	Avaya Aura™ Communication Manager 5.2.1, Load 16.4, Service Pack 2 (18111)
Avaya S8510 Server	Avaya Aura™ Session Manager 5.2 SP 2 (522007)
	Avaya Aura™ System Manager 5.2 SP 2 (522007)
Avaya 9630 IP Telephone (H.323)	3.1
Avaya 6408D+ Digital Telephone	-
Avaya Communication Server 1000S <ul style="list-style-type: none"> Call Server Signaling Server NTRB21 DTI/PRI TMDI Card 	Avaya Communication Server 1000 Release 450w, Version 2121 sse-4.50.88 NA
Avaya (formerly Nortel) 3904 Digital Telephone	NA
Avaya (formerly Nortel) I2004 IP Telephone (UNISTIM)	C502B41

3 Configure Avaya Aura™ Communication Manager

This section describes configuring Communication Manager in the following areas. Some administration screens have been abbreviated for clarity.

- Avaya Communication Manager license
- System parameters features
- IP node names
- IP interface
- IP codec set and network region
- G450 Media Gateway
- DS1 Interface
- PRI QSIG signaling group and trunk group
- SIP signaling group and trunk group
- Route pattern
- Location and public/private numbering
- Uniform dial plan and AAR analysis

3.1 Verify Avaya Aura™ Communication Manager License

Log into the System Access Terminal (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. 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 difference between the two values should be greater than or equal to the desired number of simultaneous SIP trunk connections.

The license file installed on the system controls the maximum permitted. If there is insufficient capacity or a required feature is not enabled, contact an authorized Avaya sales representative to make the appropriate changes.

display system-parameters customer-options		Page	2 of	10
OPTIONAL FEATURES				
IP PORT CAPACITIES				USED
	Maximum Administered H.323 Trunks:	800		200
	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:	0		0
	Maximum Video Capable IP Softphones:	0		0
	Maximum Administered SIP Trunks:	800		47

3.2 Configure System Parameters

Use the “change system-parameters features” command to allow for trunk-to-trunk transfers and submit the change. This feature is needed to be able to transfer an incoming/outgoing call from/to the remote switch back out to the same or another switch. For simplicity, 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 using Class Of Restriction or Class Of Service levels. Refer to the appropriate documentation in **Section 8** for more details.

```
change system-parameters features                               Page 1 of 18
      FEATURE-RELATED SYSTEM PARAMETERS
      Self Station Display Enabled? y
      Trunk-to-Trunk Transfer: all
      Automatic Callback with Called Party Queuing? n
      Automatic Callback - No Answer Timeout Interval (rings): 3
      Call Park Timeout Interval (minutes): 10
      Off-Premises Tone Detect Timeout Interval (seconds): 20
```

Use the “change system-parameters special-applications” command to enable Special Application **SA7161**, which enables compatible signaling on the PRI NI-1 interface to the CS1000.

```
change system-parameters special-applications                 Page 1 of 9
      SPECIAL APPLICATIONS

WARNING: Special App features are intended to serve specific needs and are not
recommended for general use. Activating one or more of these features
may result in unpredictable system behavior. Please review information
at http://support.avaya.com before feature activation.

Number of Features Activated: 3      Number of Restricted Features Activated: 0

      (SA7161) - NORTEL SL1 PRI and DMS Names Display? y
      (SA7291) - TAAS Pickup During Day? n
```

3.3 Configure IP Node Names

Use the “change node-names ip” command to add entries for the C-LAN that will be used for signaling, its default gateway, and Session Manager. In this case, “clan1” and “10.1.2.233” are entered as **Name** and **IP Address** for the C-LAN, “sm1” and “10.1.2.170” are entered for the Session Manager Security Module (SM-100) interface, and “Gateway001” and “10.1.2.1” are entered for the default gateway. Note that “Gateway001” will be used to configure the IP interface for the C-LAN (see **Section 3.4**). 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
      clan1         10.1.2.233
      Gateway001   10.1.2.1
      sm1          10.1.2.170
```

3.4 Configure IP Interface for C-LAN

Add the C-LAN to the system configuration using the “add ip-interface 1a02” command. The actual slot number may vary. In this case, “1a02” is used as the slot number. Enter the C-LAN node name assigned from **Section 3.3** into the **Node Name** field.

Enter proper values for the **Subnet Mask** and **Gateway Node Name** fields. In this case, “24” and “Gateway001” are used to correspond to the network configuration in these Application Notes. Set the **Enable Interface** and **Allow H.323 Endpoints** fields to “y”. Default values may be used in the remaining fields. Submit these changes.

```
add ip-interface 1a02                                     Page 1 of 3
                                                         IP INTERFACES
Type: C-LAN
Slot: 01A02      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: clan1
Subnet Mask: /24
Gateway Node Name: Gateway001

Ethernet Link: 2
Network uses 1's for Broadcast Addresses? y
```

3.5 Configure IP Codec Set and Network Region

Configure the IP codec set to use for calls to other SIP products via Session Manager. Use the “change ip-codec-set n” command, where “n” is an existing codec set number to be used for interoperability. Enter the desired audio codec type in the **Audio Codec** field. Retain the default values for the remaining fields and submit these changes. In the sample configuration, the basic G.711 mu-law codec is used for the Avaya 9600 series IP Telephones.

```
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:
```

In the test configuration, network region “1” was used for calls to Session Manager. Use the “change ip-network-region 1” command to configure this network region. For the **Authoritative Domain** field, enter the SIP domain name configured for this enterprise network (See **Section 4.1**). This value is used to populate the SIP domain in the From header of SIP INVITE messages for outbound calls. It also must match the SIP domain in the request URI of incoming INVITEs from other systems. Enter a descriptive **Name**. For the **Codec Set** field, enter the corresponding audio codec set configured above in this section. Enable the **Intra-region IP-IP Direct Audio**, and **Inter-region IP-IP Direct Audio**. These settings will enable direct media between Avaya IP telephones. Retain the default values for the remaining fields, and submit these changes.

```
change ip-network-region 1                                     Page 1 of 19
                                                           IP NETWORK REGION
Region: 1
Location:      Authoritative Domain: avaya.com
Name: ASM
MEDIA PARAMETERS      Intra-region IP-IP Direct Audio: yes
Codec Set: 1          Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048    IP Audio Hairpinning? n
UDP Port Max: 10001
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
```

3.6 Add G450 Media Gateway

The Avaya G450 Media Gateway is used to support the PRI NI-1 trunk connection to the CS1000. Install and configure the G450 Media Gateway as described in [6], noting its serial number, and specifying the IP address of the C-LAN configured in **Section 3.3** in its controller list. The following screen shows the G450 Media Gateway Command Line Interface commands to obtain the serial number (**show system**), and to set and verify the controller list (**set mgc list**, **show mgc list**):

```
G450-FE-???(super)# show system
System Name      :
System Location  :
System Contact   :
Uptime (d,h:m:s) : 46,21:32:25
MV Time         : 09:51:53 11 MAR 2010
Serial No       : 08IS38199678
Model           : G450
.
.
.
G450-FE-???(super)# set mgc list 10.1.2.233
Done!
G450-FE-???(super)# show mgc list

CONFIGURED MGC HOST
-----
10.1.2.233
-- Not Available --
-- Not Available --
-- Not Available --
```

On Communication Manager, use the “add media-gateway n” command, where “n” is an unused media gateway number. Enter the following values for the specified fields, and retain the default values for all remaining fields. Submit these changes.

- **Type:** “g450”
- **Name:** A descriptive name.
- **Serial No:** Serial number obtained from the G450 media gateway above

```

add media-gateway 1                                     Page 1 of 1
                MEDIA GATEWAY
    Number: 1                                           Registered? n
      Type: g450                                         FW Version/HW Vintage:
      Name: Avaya CS1000                                 MGP IP Address:
      Serial No: 08IS38199678                           Controller IP Address:
    Encrypt Link? y                                     MAC Address:
    Network Region: 1   Location: 1
                Site Data:
    Recovery Rule: none

Slot  Module Type      Name                DSP Type  FW/HW version
V1:
V2:
V3:
  
```

Make sure that the DS1 interface card (MM710) is installed in the desired slot in the gateway. When the media gateway is registered with Communication Manager, the DS1 interface should be displayed in that slot, as shown below for the sample configuration.

```

display media-gateway 1
                MEDIA GATEWAY
    Number: 1                                           Registered? y
      Type: g450                                         FW Version/HW Vintage: 30 .10 .4 /1
      Name: Avaya CS1000                                 MGP IP Address: 10 .1 .2 .140
      Serial No: 08IS38199678                           Controller IP Address: 10 .1 .2 .233
    Encrypt Link? y                                     MAC Address: 00:1b:4f:03:52:18
    Network Region: 1   Location: 1
                Site Data:
    Recovery Rule: none

Slot  Module Type      Name                DSP Type  FW/HW version
V1:   MM710           DS1 MM             MP80      29 3
V2:
V3:
  
```

3.7 Add DS1 Interface

The DS1 circuit pack is used for connectivity to the CS1000. Use the “add ds1 1v1” command. Note that the actual slot number may vary. In this case “1v1” is used as the slot number (see **Section 3.6**). Enter the following values for the specified fields, and retain the default values for the remaining fields. Submit these changes.

- **Name:** A descriptive name.
- **Line Coding:** “b8zs”
- **Framing Mode:** “esf”
- **Signaling Mode:** “isdn-pri”
- **Connect:** “pbx”
- **Interface:** “network”
- **Peer Protocol:** “s11”

The **Interface** field must be complementary on both switches. For the sample configuration, Communication Manager must be administered as the *network*, and the CS1000 must be administered as the *user*. Note that the CS1000 can only be administered as *user* for an NI-1 interface.

```
add ds1 1v1                                     Page 1 of 2
                                         DS1 CIRCUIT PACK

      Location: 001V1                          Name: Avaya CS1K
      Bit Rate: 1.544                          Line Coding: b8zs
Line Compensation: 1                          Framing Mode: esf
      Signaling Mode: isdn-pri
      Connect: pbx                              Interface: network
      TN-C7 Long Timers? n                     Country Protocol: s11
Interworking Message: PROGRESS
Interface Companding: mulaw                   CRC? n
      Idle Code: 11111111
                                         DCP/Analog Bearer Capability: 3.1kHz
                                         T303 Timer(sec): 4

Slip Detection? n                            Near-end CSU Type: other
```

3.8 Add PRI NI-1 Signaling Group and Trunk Group

3.8.1 Trunk group

Configure an ISDN trunk group to interface with the CS1000. Use the “add trunk-group n” command, where “n” is an available trunk group number. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Group Type:** “isdn”
- **Group Name:** A descriptive name.
- **TAC:** An available trunk access code.
- **Direction:** “two-way”
- **Carrier Medium:** “PRI/BRI”
- **Service Type:** “tie”

```
add trunk-group 100                                     Page 1 of 21
                                     TRUNK GROUP
Group Number: 100                                     Group Type: isdn          CDR Reports: y
Group Name: Avaya CS1K                               COR: 1                   TN: 1           TAC: 100
Direction: two-way                                   Outgoing Display? n     Carrier Medium: PRI/BRI
Dial Access? n                                       Busy Threshold: 255     Night Service:
Queue Length: 0
Service Type: tie                                     Auth Code? n           TestCall ITC: rest
Far End Test Line No:
TestCall BCC: 4
```

Navigate to **Page 2**. For the **Supplementary Service Protocol** field, enter “a”, and for **Codeset to Send Display**, enter “0”. Retain default values for the remaining fields.

```
add trunk-group 100                                     Page 2 of 21
Group Type: isdn
TRUNK PARAMETERS
Codeset to Send Display: 0                           Codeset to Send National IEs: 6
Max Message Size to Send: 260                       Charge Advice: none
Supplementary Service Protocol: a                   Digit Handling (in/out): enbloc/enbloc
Trunk Hunt: cyclical
Digital Loss Group: 13
Incoming Calling Number - Delete:                    Insert:                  Format:
Bit Rate: 1200                                       Synchronization: async  Duplex: full
Disconnect Supervision - In? y Out? y
Answer Supervision Timeout: 0
Administer Timers? n                                CONNECT Reliable When Call Leaves ISDN? n
```

Navigate to **Page 3**. Enable the **Send Name**, **Send Calling Number**, and **Send Connected Number** fields. For the **Format** field, enter “unk-pvt” to construct the calling and connected numbers using the “private numbering” table, but encode the numbering plan format as “unknown” in the ISDN messages toward the CS1000. Setting the **Internal Alert** field to “y” allows calls arriving from CS1000 users to be treated as internal calls. For example, if a CS1000 telephone dials a Communication Manager telephone, the Communication Manager telephone will ring with the ring pattern for an internal station-station call, internal coverage criteria will apply, and the CS1000 caller will hear tones such as coverage tone, similar to a calls between Communication Manager telephones.

```

add trunk-group 100                                     Page 3 of 21
TRUNK FEATURES
  ACA Assignment? n                                     Measured: none      Wideband Support? n
                                           Internal Alert? y      Maintenance Tests? y
  Data Restriction? n                               NCA-TSC Trunk Member:
                                           Send Name: y          Send Calling Number: y
  Used for DCS? n                                     Send EMU Visitor CPN? n
  Suppress # Outpulsing? n                         Format: unk-pvt
  Outgoing Channel ID Encoding: preferred          UII IE Treatment: service-provider
                                           Replace Restricted Numbers? y
                                           Replace Unavailable Numbers? n
                                           Send Connected Number: y
  Network Call Redirection: none                   Hold/Unhold Notifications? n
  Send UII IE? y                                    Modify Tandem Calling Number? n
  Send UCID? y
  Send Codeset 6/7 LAI IE? y                       Dsl Echo Cancellation? n
  Apply Local Ringback? n                           US NI Delayed Calling Name Update? n
  Show ANSWERED BY on Display? y
                                           Network (Japan) Needs Connect Before Disconnect? n

```

3.8.2 Signaling Group

Configure an ISDN signaling group for the new trunk group. Use the “add signaling-group n” command, where “n” is an available signaling group number. For the **Primary D-Channel** field, enter the slot number for the DS1 module from **Section 3.7** and port “24”.

For the **Group Type**, enter “isdn-pri”. For the **Trunk Group for NCA TSC** and **Trunk Group for Channel Selection** fields, enter the ISDN trunk group number from **Section 3.8.1**. For the **TSC Supplementary Service Protocol** field, enter “a”. Maintain the default values for the remaining fields, and submit these changes.

```

add signaling-group 100                                 Page 1 of 5
                                           SIGNALING GROUP
Group Number: 100                                     Group Type: isdn-pri
  Associated Signaling? y                             Max number of NCA TSC: 10
  Primary D-Channel: 001V124                       Max number of CA TSC: 0
                                           Trunk Group for NCA TSC: 100
  Trunk Group for Channel Selection: 100
  TSC Supplementary Service Protocol: a           Network Call Transfer? n

```

3.8.3 Trunk Group Members

Navigate to **Pages 5 and 6**. Enter all 23 ports of the DS1 module into the **Port** fields, and the corresponding **Code** and **Sfx** fields will be populated automatically. Enter the ISDN signaling group number from **Section 3.8.2** into the **Sig Grp** fields as shown below. Submit these changes.

```
change trunk-group 100                                     Page 5 of 21
                                                           TRUNK GROUP
                                                           Administered Members (min/max): 1/23
GROUP MEMBER ASSIGNMENTS                                Total Administered Members: 23
```

Port	Code	Sfx	Name	Night	Sig Grp
1:	001V101	MM	710		100
2:	001V102	MM	710		100
3:	001V103	MM	710		100
4:	001V104	MM	710		100
5:	001V105	MM	710		100
6:	001V106	MM	710		100
7:	001V107	MM	710		100
8:	001V108	MM	710		100
9:	001V109	MM	710		100
10:	001V110	MM	710		100
11:	001V111	MM	710		100
12:	001V112	MM	710		100
13:	001V113	MM	710		100
14:	001V114	MM	710		100
15:	001V115	MM	710		100

```
change trunk-group 100                                     Page 6 of 21
                                                           TRUNK GROUP
                                                           Administered Members (min/max): 1/23
GROUP MEMBER ASSIGNMENTS                                Total Administered Members: 23
```

Port	Code	Sfx	Name	Night	Sig Grp
16:	001V116	MM	710		100
17:	001V117	MM	710		100
18:	001V118	MM	710		100
19:	001V119	MM	710		100
20:	001V120	MM	710		100
21:	001V121	MM	710		100
22:	001V122	MM	710		100
23:	001V123	MM	710		100

3.9 Configure SIP Signaling Group and Trunk Group

3.9.1 SIP Signaling Group

In the test configuration, trunk group “32” and signaling group “32” were used to reach Session Manager. Use the “add signaling-group n” command, where “n” is an available signaling group number. Enter the following values for the specified fields, and retain the default values for all remaining fields. Submit these changes.

- **Group Type:** “sip”
- **Transport Method:** “tls”
- **Near-end Node Name:** C-LAN node name from **Section 3.3**.
- **Far-end Node Name:** Session Manager node name from **Section 3.3**.
- **Near-end Listen Port:** “5061”
- **Far-end Listen Port:** “5061”
- **Far-end Network Region:** Network region number “1” from **Section 3.5**.
- **Far-end Domain:** SIP domain name from **Section 4.1**.
- **DTMF over IP:** “rtp-payload”

```
add signaling-group 32                                     Page 1 of 1
                                                         SIGNALING GROUP
Group Number: 32                                         Group Type: sip
                                                         Transport Method: tls
IMS Enabled? n
Near-end Node Name: clan1                               Far-end Node Name: sm1
Near-end Listen Port: 5061                             Far-end Listen Port: 5061
                                                         Far-end Network Region: 1
Far-end Domain: avaya.com
                                                         Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload                               Direct IP-IP Audio Connections? y
                                                         IP Audio Hairpinning? n
Enable Layer 3 Test? n                                 Direct IP-IP Early Media? n
Session Establishment Timer(min): 3                    Alternate Route Timer(sec): 6
```

3.9.2 SIP Trunk Group

Use the “add trunk-group n” command, where “n” is an available trunk group number. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Group Type:** “sip”
- **Group Name:** A descriptive name.
- **TAC:** An available trunk access code.
- **Service Type:** “tie”
- **Number of Members:** The number of SIP trunks allocated for calls routed to Session Manager (must be within the limits of the total trunks configured in **Section 3.1**).

```
add trunk-group 32                                     Page 1 of 21
                                     TRUNK GROUP
Group Number: 32                                     Group Type: sip           CDR Reports: y
  Group Name: To SM1                                COR: 1                   TN: 1           TAC: 132
  Direction: two-way                               Outgoing Display? y
  Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: tie                                   Auth Code? n
                                               Signaling Group: 32
                                               Number of Members: 4
```

Navigate to **Page 3**, and enter “public” for the **Numbering Format** field as shown below. Use default values for all other fields. Submit these changes.

```
add trunk-group 32                                     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
```

3.10 Configure Route Patterns

Create a route pattern to use for routing calls to the CS1000 using the PRI NI-1 trunk. Use the “change route-pattern n” command, where “n” is an available route pattern. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Pattern Name:** A descriptive name.
- **Grp No:** The trunk group number from **Section 3.8.2**.
- **FRL:** A level that allows access to this trunk, with 0 being least restrictive.
- **TSC:** “y” (NCA-TSCs will be used)
- **CA-TSC Request:** “none” (since CA-TSC are used for DCS but not for NI-1)
- **Numbering Format:** “unk-unk” (The numbering format and type of number for the Called Party Number will be encoded as “unknown” toward the CS1000).

```

change route-pattern 100                                     Page 1 of 3
                    Pattern Number: 100 Pattern Name: Avaya CS1000
                    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: 100  0
2:
3:
4:
5:
6:

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

Configure a route pattern for routing calls to Session Manager using the SIP trunk group. Use the “change route-pattern n” command, where “n” is an available route pattern. Enter the following values for the specified fields, and retain the default values for the remaining fields. Submit these changes.

- **Pattern Name:** A descriptive name.
- **Grp No:** The SIP trunk group number from **Section 3.9.2**.
- **FRL:** Enter a level that allows access to this trunk, with 0 being least restrictive.

```

change route-pattern 32                                     Page 1 of 3
      Pattern Number: 32  Pattern Name: To SM1
      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: 32    0
2:
3:
4:
5:
6:
      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
  
```

3.11 Configure Location and Public/Private Numbering

Use the “change locations” command to specify the SIP route pattern to be used as a “default SIP route” for the location corresponding to the Main site. In this way, calls to non-numeric users or unknown domains will still be routed to Session Manager. Add an entry for the Main site if one does not exist already, enter the following values for the specified fields, and retain default values for the remaining fields. Submit these changes.

- **Name:** A descriptive name to denote the Main site.
- **Timezone:** An appropriate time zone offset.
- **Rule:** An appropriate daylight savings rule.
- **Proxy Sel. Rte. Pat.:** The SIP route pattern number from the previous section

```

change locations                                     Page 1 of 1
      LOCATIONS
      ARS Prefix 1 Required For 10-Digit NANP Calls? y
  Loc Name          Timezone Rule  NPA          Proxy Sel
  No      Offset          Rte Pat
1: Main          + 00:00  0          32
  
```

Since Communication Manager is configured as an “Access Element” with respect to Session Manager, the SIP trunk is not IMS-enabled (see **Section 3.9.1**). Outbound calls from Communication Manager may go to a public gateway. Therefore, calling parties for calls that

use this trunk should have public numbering treatment. Use the “change public-unknown-numbering 0” command, to define the calling party number to be sent to Session Manager. Add an entry for the trunk group defined in **Section 3.9.2**. In the example shown below, all calls originating from a 5-digit extension beginning with 3 and routed to trunk group 32 will result in a 5-digit calling number. The calling party number will be in the SIP “From” header. Submit these changes.

```

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
5    3         32      5
                                Total Administered: 3
                                Maximum Entries: 9999
  
```

Since the PRI trunk to the CS1000 is used for intra-enterprise calls, the calling parties should have private numbering treatment. Use the “change private-numbering” command to define the calling party number to be sent to the CS1000. Add an entry for the trunk group defined in **Section 3.8.2**. All calls originating from a 5-digit extension beginning with 3 and routed to trunk group 100 will result in the 5-digit calling number to be sent. Submit these changes.

```

change private-numbering 0                                     Page 1 of 2
                                NUMBERING - PRIVATE FORMAT
                                Total
Ext  Ext      Trk      Private  Total
Len  Code     Grp(s)   Prefix   Len
5    3         100     5
                                Total Administered: 2
                                Maximum Entries: 540
  
```

3.12 Configure Dial Plan and AAR Analysis

Configure dial plan and Automatic Alternate Routing (AAR) used for routing calls with dialed digits 53xxx to the CS1000 via the G450 Media Gateway. Use the “change uniform-dialplan 0” command, and add an entry to specify use of AAR for routing of digits 53xxx. Enter the following values for the specified fields, and retain the default values for the remaining fields. This allows callers to use extension dialing without being required to dial an AAR access code.

- **Matching Pattern:** Dialed prefix digits to match on, in this case “53”.
- **Len:** Length of the full dialed number.
- **Del:** Number of digits to delete.
- **Net:** “aar”

Submit these changes.

```

change uniform-dialplan 0                                     Page 1 of 2
                                UNIFORM DIAL PLAN TABLE
                                Percent Full: 0
                                Node
Matching  Insert  Node
Pattern   Digits  Conv  Num
53        aar     n
5         0
  
```

Use the “change aar analysis 0” command, and add corresponding entries to specify use of the PRI NI-1 trunk for calls to the CS1000 (53xxx). Enter the following values for the specified fields, and retain the default values for the remaining fields. Submit these changes.

- **Dialed String:** Dialed prefix digits to match on, in this case “53”.
- **Total Min:** Minimum number of digits.
- **Total Max:** Maximum number of digits.
- **Route Pattern:** The route pattern number from **Section 3.10**.
- **Call Type:** “lev0” for private numbering (PRI NI-1)

```
change aar analysis 0
```

AAR DIGIT ANALYSIS TABLE							Page 1 of 2
Location: all							Percent Full: 1
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Reqd	
53	5	5	100	lev0		n	

Use the “change dialplan analysis” command to define the 3xxxx and 5xxxx extension ranges.

```
change dialplan analysis
```

DIAL PLAN ANALYSIS TABLE									Page 1 of 12
Location: all									Percent Full: 1
	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
1		3	dac						
2		5	ext						
3		5	ext						
5		5	ext						
6		5	ext						
7		5	ext						
8		1	fac						
9		1	fac						

3.13 Save Translations

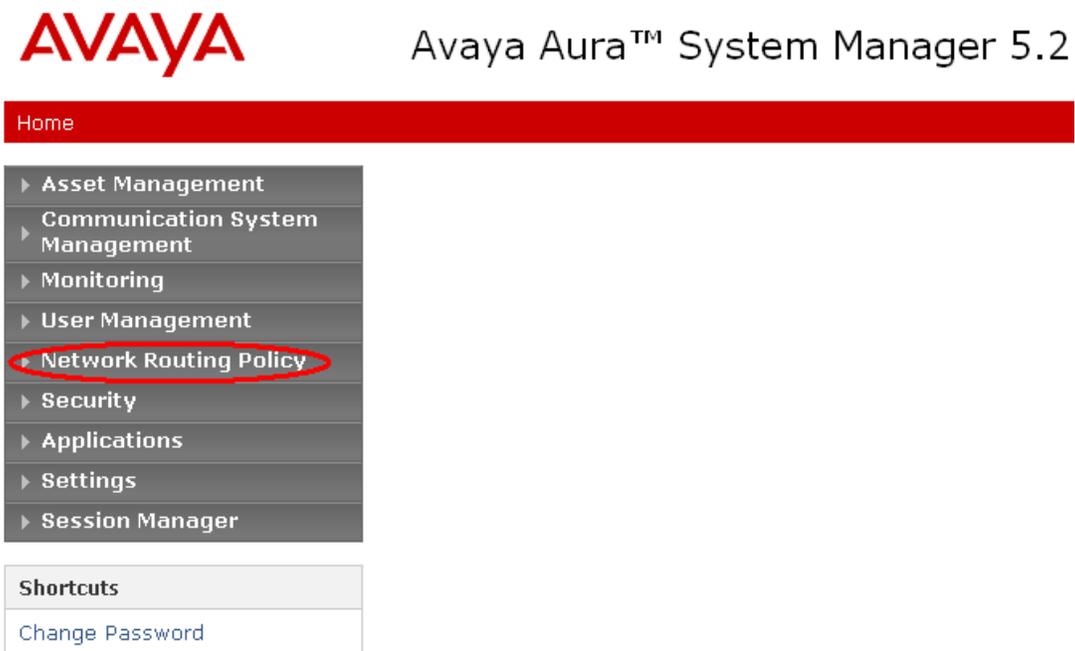
Configuration of Communication Manager is complete. Use the “save translations” command to save these changes.

4 Configure Avaya Aura™ Session Manager

This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain
- Logical/physical Location that can be occupied by SIP Entities
- SIP Entities corresponding to Communication Manager, CS 1000, and Session Manager
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- Routing Policies, which control call routing between the SIP Entities
- Dial Patterns, which govern to which SIP Entity a call is routed
- Session Manager, corresponding to the Session Manager Server to be managed by System Manager.
- Local host name resolution entries corresponding to fully qualified domain names (FQDN's) referenced in the previous steps.

Configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL “https://<ip-address>/SMGR”, where “<ip-address>” is the IP address of System Manager. Log in with the appropriate credentials and click on **OK** in the subsequent confirmation screen. The menu shown below is then displayed. Expand the **Network Routing Policy** Link on the left side as shown. The sub-menus displayed in the left column below will be used to configure all but the last two of the above items (**Sections 4.1** through **4.9**).



4.1 Specify SIP Domain

Add the SIP domain for which the communications infrastructure will be authoritative. Select **SIP Domains** on the left and click the **New** button (not shown) on the right. Fill in the following:

- **Name:** The authoritative domain name (e.g., “avaya.com”)
- **Notes:** Descriptive text (optional).

Click **Commit**.

The screenshot shows the Avaya Aura System Manager 5.2 interface. The top navigation bar includes the Avaya logo, the product name "Avaya Aura™ System Manager 5.2", and a user status message: "Welcome, admin Last Logged on at Jan. 11, 2010". A "Help" link is also present. Below the navigation bar, a red breadcrumb trail reads "Home / Network Routing Policy / SIP Domains". On the left, a sidebar menu lists various management categories, with "SIP Domains" under "Network Routing Policy" circled in red. The main content area is titled "Domain Management" and features a "Commit" button. Below this, there is a table with one row containing the domain "avaya.com", type "sip", and a default checkbox. A "Filter" link is visible on the right. At the bottom of the main area, a red asterisk indicates "* Input Required" with another "Commit" button.

4.2 Add Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. To add a location, select **Locations** on the left and click on the **New** button (not shown) on the right. Under **General**, enter:

- **Name:** A descriptive name.
- **Notes:** Descriptive text (optional).

Under **Location Pattern:**

- **IP Address Pattern:** An IP address pattern used to identify the location.
- **Notes:** Descriptive text (optional).

The screen below shows addition of the Basking Ridge location, which includes Communication Manager, Session Manager, and the CS1000¹ in the 10.1.2.0/24 subnet. Click **Commit** to save the Location definition.

The screenshot displays the Avaya Aura System Manager 5.2 interface. The top navigation bar includes the Avaya logo, the product name 'Avaya Aura™ System Manager 5.2', and a user status message: 'Welcome, admin Last Logged on at Jan. 11, 2011 Help'. Below the navigation bar is a red breadcrumb trail: 'Home / Network Routing Policy / Locations / Location Details'. On the left is a sidebar menu with 'Locations' highlighted in red. The main content area is titled 'Location Details' and contains a 'Commit' button in the top right. The 'General' section has the following fields: '* Name: BaskingRidge', 'Notes: Avaya SM & CM, Nortel CS1000', 'Managed Bandwidth: []', '* Average Bandwidth per Call: 80 Kbit/sec', and '* Time to Live (secs): 3600'. The 'Location Pattern' section has 'Add' and 'Remove' buttons and a table with one row: IP Address Pattern *10.1.2.* and Notes. Below the table is a selection summary: 'Select : All, None (0 of 1 Selected)'.

The fields under *General* can be filled in to specify bandwidth management parameters between Avaya Session Manager and this location. These were not used in the sample configuration, and reflect default values. Note also that although not implemented in the sample configuration, routing policies can be defined based on location.

¹ Note that even though the CS1000 is in a different subnet than 10.1.2.0/24, since the only access to it is via the PRI NI-1 interface on the Communication Manager controlled G450 Media Gateway, from the perspective of Session Manager, routing to the CS1000 is via Communication Manager, which resides in the 10.1.2.0/24 subnet.

4.3 Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system supported by it using SIP trunks. In the sample configuration, this would include the C-LAN board in the Avaya G650 Media Gateway. Select **SIP Entities** on the left and click on the **New** button (not shown) on the right. Under *General*, fill in:

- **Name:** A descriptive name.
- **FQDN or IP Address:** FQDN or IP address of the Session Manager or the signaling interface on the telephony system.
- **Type:** “Session Manager” for Session Manager or “CM” for Communication Manager.
- **Location:** Select one of the locations defined previously.
- **Time Zone:** Time zone for this location.

Under *Port*, click **Add**, and then edit the fields in the resulting new row as shown below:

- **Port:** Port number on which the system listens for SIP requests.
- **Protocol:** Transport protocol to be used to send SIP requests.
- **Default Domain:** The domain used for the enterprise (e.g., “avaya.com”).

Defaults can be used for the remaining fields. Click **Commit** to save each SIP Entity definition.

The following screen shows addition of Session Manager. The IP address of the SM-100 Security Module is entered for **FQDN or IP Address**. Two **Port** entries are shown. The TLS port 5061 is used for communication with other Session Managers and Communication Manager. TCP port 5060 is used for communicating with other SIP entities not addressed in this sample configuration.



- ▶ Asset Management
- ▶ Communication System Management
- ▶ Monitoring
- ▶ User Management
- ▼ Network Routing Policy
 - Adaptations
 - Dial Patterns
 - Entity Links
 - Locations
 - Regular Expressions
 - Routing Policies
 - SIP Domains
 - SIP Entities**
 - Time Ranges
 - Personal Settings
- ▶ Security
- ▶ Applications
- ▶ Settings
- ▶ Session Manager

- Shortcuts**
- Change Password
 - Help for SIP Entity Details fields
 - Help for Committing configuration changes

SIP Entity Details

General

* Name:

* FQDN or IP Address:

Type:

Notes:

Location:

Outbound Proxy:

Time Zone:

Credential name:

SIP Link Monitoring

SIP Link Monitoring:

Entity Links

Entity Links can be modified after SIP Entity is committed.

Port

2 Items | Refresh Filter

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	5060	TCP	avaya.com	<input type="text"/>
<input type="checkbox"/>	5061	TLS	avaya.com	<input type="text"/>

Select : All, None (0 of 2 Selected)

* Input Required

The following screen shows addition of Communication Manager. In this case, **FQDN or IP Address** is the Fully Qualified Domain Name (FQDN) of the C-LAN board in the Avaya G650 Media Gateway. Note that although not shown in the sample configuration, definition of multiple IP addresses (e.g., C-LANs) for the same FQDN (see **Section 4.8**) will cause Session Manager to load balance call traffic among those addresses.

The screenshot displays the Avaya Aura™ System Manager 5.2 interface. The top navigation bar includes the Avaya logo, the product name, and a user status message: "Welcome, admin Last Logged on at Jan. 11, 2011 Help". Below this is a breadcrumb trail: "Home / Network Routing Policy / SIP Entities / SIP Entity Details".

The left sidebar contains a menu with the following items: Asset Management, Communication System Management, Monitoring, User Management, Network Routing Policy (expanded), Adaptations, Dial Patterns, Entity Links, Locations, Regular Expressions, Routing Policies, SIP Domains, SIP Entities (highlighted with a red circle), Time Ranges, Personal Settings, Security, Applications, Settings, and Session Manager.

The main content area is titled "SIP Entity Details" and includes a "Commit" button. Under the "General" tab, the following fields are visible:

- Name:** CallCenter
- * FQDN or IP Address:** callcenter.avaya.com
- Type:** CM
- Notes:** (empty text field)
- Adaptation:** (empty dropdown)
- Location:** BaskingRidge
- Time Zone:** America/New_York
- Override Port & Transport with DNS SRV:**
- * SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text field)
- Call Detail Recording:** none
- SIP Link Monitoring:** Use Session Manager Configuration

4.4 Add Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity link. To add an Entity Link, select **Entity Links** on the left and click on the **New** button (not shown) on the right. Fill in the following fields in the new row that is displayed:

- **Name:** A descriptive name.
- **SIP Entity 1:** Select the Session Manager.
- **Port:** Port number to which the other system sends SIP requests
- **SIP Entity 2:** Select the name of the SIP Entity dedfined in **Section 4.3..**
- **Port:** Port number on which the other system receives SIP requests.
- **Trusted:** Check this box. *Note: If this box is not checked, calls from the associated SIP Entity specified in Section 4.3 will be denied.*

Click **Commit** to save the Entity Link definition. The following screen illustrates adding the Entity Link for Communication Manager.

The screenshot shows the Avaya Aura System Manager 5.2 interface. The header includes the Avaya logo, the system name 'Avaya Aura™ System Manager 5.2', and a user greeting 'Welcome, admin Last Logged on at Feb. 17, 2010 12:13 PM'. The navigation menu on the left is expanded to 'Network Routing Policy', with 'Entity Links' highlighted. The main content area shows the 'Entity Links' configuration page. It includes a 'Commit' and 'Cancel' button at the top right. Below the header, there is a table with the following columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Trusted, and Notes. The table contains one row with the following data: Name: Call Center, SIP Entity 1: SM1, Protocol: TLS, Port: 5061, SIP Entity 2: CallCenter, Port: 5061, Trusted: checked, Notes: CLAN 10.1.2.233. Below the table, there is a 'New' button and a 'Commit' button. The page also includes a 'Filter: Enable' option and a 'Refresh' button.

4.5 Add Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 4.3**. A routing policy must be added for Communication Manager. To add a routing policy, select **Routing Policies** on the left and click on the **New** button (not shown) on the right. The following screen is displayed. Fill in the following:

Under **General**:

Enter a descriptive name in **Name**.

Under **SIP Entity as Destination**:

Click **Select**, and then select the appropriate SIP entity to which this routing policy applies.

Under **Time of Day**:

Select the default time range shown.

Defaults can be used for the remaining fields. Click **Commit** to save each Routing Policy definition. The following screen shows the Routing Policy for users on Communication Manager and the CS1000.

The screenshot shows the Avaya Aura System Manager 5.2 interface. The top navigation bar includes the Avaya logo, the product name 'Avaya Aura™ System Manager 5.2', and a user status message: 'Welcome, admin Last Logged on at Jan. 11, 2010 4:52 PM'. Below the navigation bar is a red breadcrumb trail: 'Home / Network Routing Policy / Routing Policies / Routing Policy Details'. On the left is a vertical navigation menu with categories: Asset Management, Communication System Management, Monitoring, User Management, Network Routing Policy (expanded), Security, Applications, Settings, and Session Manager. Under 'Network Routing Policy', 'Routing Policies' is circled in red. The main content area is titled 'Routing Policy Details' and contains three sections: 'General' with fields for Name (Call Center), Disabled (checkbox), and Notes; 'SIP Entity as Destination' with a 'Select' button and a table listing 'CallCenter' with FQDN 'callcenter.avaya.com' and Type 'CM'; and 'Time of Day' with 'Add', 'Remove', and 'View Gaps/Overlaps' buttons, a table with 1 item (Ranking 0, Name 24/7, Start Time 00:00, End Time 23:59, Notes Time Range 24/7), and a 'Filter: Enable' option.

4.6 Add Dial Patterns

Define dial patterns to direct calls to the appropriate SIP Entity. Calls to 5-digit extensions beginning with “3” (Communication Manager) or “53” (CS1000) should be routed to Communication Manager. To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button (not shown) on the right. Fill in the following, as shown in the screens below:

Under **General**:

- **Pattern:** Dialed number or prefix.
- **Min:** Minimum length of dialed number.
- **Max:** Maximum length of dialed number.
- **SIP Domain:** SIP domain specified in **Section 4.1**
- **Notes:** Comment on purpose of dial pattern.

Under **Originating Locations and Routing Policies**:

Click **Add**, and then select the appropriate location and routing policy from the list.

Default values can be used for the remaining fields. Click **Commit** to save each dial pattern. The following screens show the resulting two dial pattern definitions. Note that similar to Communication Manager, the dial pattern selected will correspond to the longest match of a **Pattern** with the dialed number.

The screenshot shows the Avaya Aura System Manager 5.2 interface. The top navigation bar includes the Avaya logo, the product name "Avaya Aura™ System Manager 5.2", and a user status message: "Welcome, admin Last Logged on at Jan. 11, 2010 4:52 PM". A "Help | Log off" link is also present. The breadcrumb trail reads "Home / Network Routing Policy / Dial Patterns / Dial Pattern Details".

The left sidebar contains a tree view of system management categories. Under "Network Routing Policy", the "Dial Patterns" option is highlighted with a red circle.

The main content area is titled "Dial Pattern Details" and includes "Commit" and "Cancel" buttons. It is divided into two sections:

- General:** Contains input fields for "Pattern" (value: 3), "Min" (value: 5), and "Max" (value: 5). There is a checkbox for "Emergency Call" (unchecked), a dropdown for "SIP Domain" (value: avaya.com), and a text field for "Notes" (value: Call Center ACM CLAN1).
- Originating Locations and Routing Policies:** Includes "Add" and "Remove" buttons. Below is a table with 1 item and a "Refresh" button. A "Filter: Enable" link is also present.

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	Call Center	0	<input type="checkbox"/>	CallCenter	

Select : All, None (0 of 1 Selected)

- ▶ Asset Management
- ▶ Communication System Management
- ▶ Monitoring
- ▶ User Management
- ▼ Network Routing Policy
 - Adaptations
 - Dial Patterns**
 - Entity Links
 - Locations
 - Regular Expressions
 - Routing Policies
 - SIP Domains
 - SIP Entities
 - Time Ranges
 - Personal Settings
- ▶ Security
- ▶ Applications
- ▶ Settings
- ▶ Session Manager

Dial Pattern Details

General

* Pattern:

* Min:

* Max:

Emergency Call:

SIP Domain:

Notes:

Originating Locations and Routing Policies

1 Item | [Refresh](#) Filter: [Enable](#)

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	BaskingRidge	Fred's ACM & ASM's	Call Center	0	<input type="checkbox"/>	CallCenter	

Select : All, None (0 of 1 Selected)

4.7 Add Session Manager

To complete the configuration, adding the Session Manager will provide the linkage between System Manager and Session Manager. Expand the **Session Manager** menu on the left and select **Session Manager Administration**. Then click **Add** (not shown), and fill in the fields as described below and shown in the following screen:

Under **General**:

- **SIP Entity Name:** Select the SIP Entity added for Avaya Session Manager
- **Description:** Descriptive comment (optional)
- **Management Access Point Host Name/IP:** Enter the IP address of the Session Manager management interface.

Under **Security Module**:

- **Network Mask:** Enter the network mask corresponding to the IP address of Session Manager
- **Default Gateway:** Enter the IP address of the default gateway for Session Manager

Use default values for the remaining fields. Click **Save** (not shown) to add this Session Manager. The screen below shows the resulting Session Manager definition.

The screenshot displays the Avaya Aura™ System Manager 5.2 web interface. The top navigation bar includes the Avaya logo, the product name, and a user greeting. A red breadcrumb trail indicates the current path: Home / Session Manager / Session Manager Administration / View Session Manager. On the left, a sidebar menu shows various system management categories, with 'Session Manager Administration' highlighted and circled in red. The main content area is titled 'View Session Manager' and contains two sections: 'General' and 'Security Module'. The 'General' section lists configuration fields: SIP Entity Name (SM1), Description (Session Mgr 1), Management Access Point Host Name/IP (10.1.2.171), and Direct Routing to Endpoints (Enable). The 'Security Module' section lists: SIP Entity IP Address (10.1.2.170), Network Mask (255.255.255.0), Default Gateway (10.1.2.1), Call Control PHB (46), QOS Priority (6), Speed & Duplex (Auto), and VLAN ID.

4.8 Define Local Host Names

Any host names (FQDN's) referenced in SIP Entity definitions must be defined. To do so, Select **Session Manager -> Network Configuration -> Local Host Name Resolution** under the menu on the left. For each host name, click **New** and enter the following:

- **Host Name:** The FQDN used for the host
- **IP Address:** IP address of the host's network interface
- **Port:** Port number to which SIP requests are sent
- **Transport:** Transport to be used for SIP requests

Defaults can be used for the remaining fields. The **Priority** and **Weight** fields are used when multiple IP addresses are defined for the same host. The circled entry in the following screen defines the host name referenced in the SIP Entity configuration for Communication Manager in **Section 4.3**).

The screenshot shows the Avaya Aura System Manager 5.2 interface. The top navigation bar includes the Avaya logo, the product name "Avaya Aura™ System Manager 5.2", and a user status message: "Welcome, admin Last Logged on at Jan. 11, 2010 4:52 PM" with links for "Help" and "Log off". The main content area is titled "Local Host Name Resolution" and includes a sub-header "Local Host Name Entries". Below this, there are buttons for "New", "Edit", "Delete", and "More Actions". A table displays 5 items with columns for Host Name, IP Address, Port, Priority, Weight, and Transport. The entry for "callcenter.avaya.com" is circled in red. The left sidebar shows a navigation menu with "Local Host Name Resolution" highlighted.

Home / Session Manager / Network Configuration / Local Host Name Resolution

Local Host Name Resolution
This page allows you to add, edit, or remove local host name entries. Host name entries on this page will override information provided by DNS.

Local Host Name Entries

New Edit Delete More Actions

5 Items | Refresh Filter: Enable

<input type="checkbox"/>	Host Name	IP Address	Port	Priority	Weight	Transport
<input type="checkbox"/>	allanc-s8300-g350	10.32.2.80	5060	100	100	TCP
<input type="checkbox"/>	alpinemas1	135.8.139.31	5060	100	100	TCP
<input checked="" type="checkbox"/>	callcenter.avaya.com	10.1.2.233	5060	100	100	TCP
<input type="checkbox"/>	m1000.avaya.com	10.1.2.100	5060	100	100	TCP
<input type="checkbox"/>	MikeH-S8300-G450	10.32.2.20	5060	100	100	TCP

Select : All, None (0 of 5 Selected)

5 Configure Avaya Communication Server 1000

This section describes configuration of the CS1000 for call routing using a T1 PRI NI-1 interface to the Avaya G450 Media Gateway. These Application Notes assume that ISDN PRI is not being configured for the first time, so error detection thresholds and clock synchronization control are assumed to be in place. If not, refer to the ISDN Primary Rate Interface document in [7] for detailed descriptions. Furthermore, these Application Notes use the Coordinated Dial Plan (CDP) feature to route calls from the Avaya Communication Server 1000, over the PRI NI-1 trunks to Communication Manager. The CDP feature is assumed to be already enabled on Avaya Communication Server 1000, and therefore will not be described in detail.

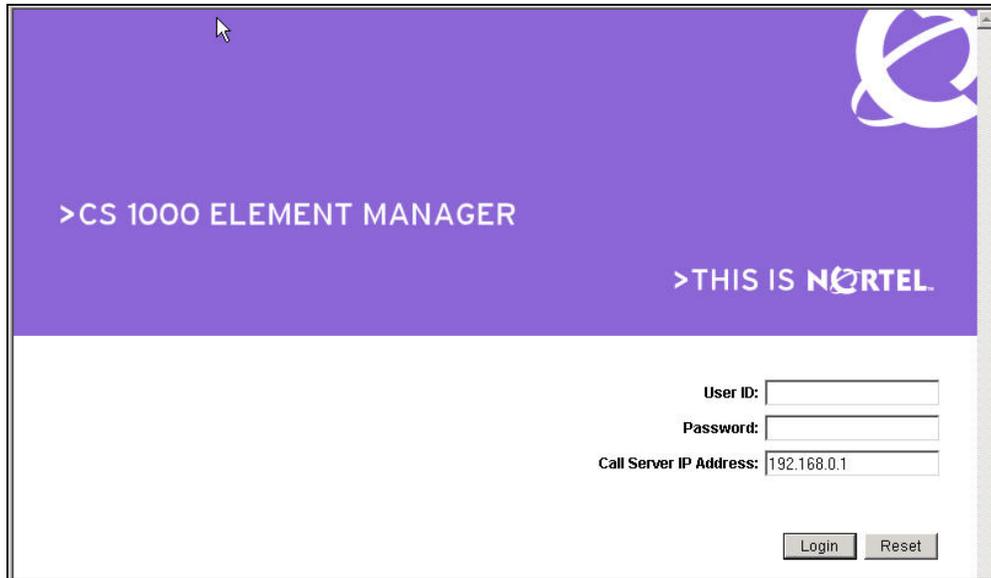
The procedures below describe the details of configuring the CS1000:

- Launch Element Manager
- Verify equipped feature packages
- Administer TMDI card
- Administer D-Channel
- Administer routes and trunks
- Administer route list block
- Administer distant steering code
- Enable TMDI card
- Enable D-Channel automatic establishment
- Enable D-Channel service messages

5.1 Launch Element Manager

Access the CS1000 web based interface Element Manager by using the URL “http://<ip-address>” in an Internet browser window, where “<ip-address>” is the IP address of the Signaling Server. Note that the IP address for the Signaling Server may vary, and in this case “192.168.1.30” is used.

The **CS 1000 ELEMENT MANAGER** screen is displayed. Enter the appropriate credentials, retain the automatically populated value in the **Call Server IP Address** field, and click **Login**.



>CS 1000 ELEMENT MANAGER

>THIS IS NORTEL

User ID:

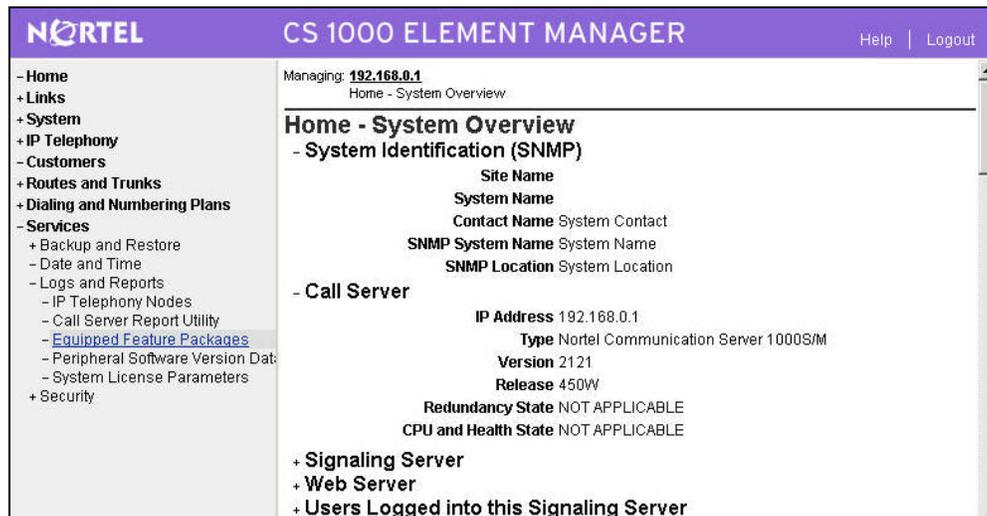
Password:

Call Server IP Address:

Login Reset

5.2 Verify Equipped Feature Packages

The **Home – System Overview** screen is displayed. Select **Services > Logs and Reports > Equipped Feature Packages** in the left pane.



NORTEL CS 1000 ELEMENT MANAGER Help | Logout

Managing: **192.168.0.1**
Home - System Overview

Home - System Overview

- System Identification (SNMP)

- Site Name
- System Name
- Contact Name System Contact
- SNMP System Name System Name
- SNMP Location System Location

- Call Server

- IP Address 192.168.0.1
- Type Nortel Communication Server 1000S/M
- Version 2121
- Release 450W
- Redundancy State NOT APPLICABLE
- CPU and Health State NOT APPLICABLE

+ Signaling Server

+ Web Server

+ Users Logged into this Signaling Server

The **Equipped Feature Packages List** screen is displayed next, and shows a listing of the licensed feature packages in sequential order by package number. Scroll down the right pane as necessary to verify that the following feature packages are equipped:

- 19 Digit Display (DDSP)
- 59 Coordinated Dialing Plan (CDP)
- 95 Calling Party Name Display (CPND)
- 145 Integrated Services Digital Network (ISDN)
- 146 Primary Rate Access (CO) (PRA)
- 154 2.0 Mb/s Primary Rate Interface (PRI2)
- 184 Overlap Signaling (M1 to M1 and M1 to 1TR6 CO) (OVLP)
- 202 International Primary Rate Access (CO) (IPRA)

Package Description	Package Number
Optional Features (OPTF)	1
Multi-Customer Operation (CUST)	2
Call Detail Recording, Teletype Terminal (CDR)	4
Call Detail Recording, Teletype Terminal (CTY)	5
Recorded Announcement (RAN)	7
Time and Date (TAD)	8
Do Not Disturb Individual (DNDI)	9
End-to-End Signaling (EES)	10
Intercept Treatment (INTR)	11
Automatic Number Identification (ANI)	12
Automatic Number Identification, Route Selection (ANIR)	13
Basic Routing (BRTE)	14
Do Not Disturb Group (DNDG)	16
Make Set Busy (MSB)	17
Special Service for 2500 Sets (SS25)	18
Digit Display (DDSP)	19
Office Data Administration System (ODAS)	20

5.3 Administer TMDI Card

Select **System > Loops** from the left pane to display the **Loops (Common Equipment)** screen. In the **Digital Trunk Interface Loop Number (DLOP)** field, click **Add New DLOP** to add a digital trunk interface to the TMDI card.

Managing: 192.168.0.1
System > Loops (Common Equipment)

Loops (Common Equipment)

- Basic Configuration

Input Description	Input Value
Change to Common Equipment parameters (CEOU) (TYPE)	CEOU
Tone and Digit Switch (TDS)	<input type="text"/> Edit
Conference loop (CONF)	029 030 031 062 094 095 Edit

- Digital Trunk Interface Loop Number (DLOP) Add New DLOP

+ Feature Packages

Submit Refresh

The **Add a Digital Trunk Interface** screen is displayed next. For the **Digital Trunk Interface Loop Number (DLOP)** field, select the loop number corresponding to the physical slot location of the TMDI card. In this case, “Loop 13 (13)” is selected from the drop-down list.

For the **Number of voice or data calls (DATA_CALLS_LIMIT)** field, select “23” from the drop-down list, to match the number of trunk members configured in Communication Manager in **Section 3.8.3**. For the **Mode of operation (MODE)** field, select “Primary Rate Interface mode (PRI)” from the drop-down list. For the **Threshold (TRSH)** field, select “0” from the drop-down list. Retain the default values for all remaining fields, and click **Refresh – Digital Trunk Interface Loop Number** at the bottom of the screen.

The screenshot shows the 'Add a Digital Trunk Interface' configuration page in the Nortel CS 1000 Element Manager. The page title is 'Add a Digital Trunk Interface' and the breadcrumb trail is 'System » Loops (Common Equipment) » Add a Digital Trunk Interface'. The configuration fields are as follows:

Input Description	Input Value
- Digital Trunk Interface Loop Number (DLOP)	Loop 13 (13)
- Number of voice or data calls (DATA_CALLS_LIMIT)	23
- Frame format (FRAME_FORMAT)	Extended Super Frame (ESF)
- Mode of operation (MODE)	Primary Rate Interface mode (PRI)
- Line Coding Method (LCMT)	B8ZS Line Coding Method (B8S)
- Yellow Alarm Method (YALM)	Yellow Alarm Method (FDL)
- TMDI Card (TMDI)	<input checked="" type="checkbox"/>
- T1 transmit Equalization (T1TE)	0 - 200 feet (0)
- Threshold (TRSH)	0

At the bottom of the form, there are two buttons: 'Refresh - Digital Trunk Interface Loop Number' and 'Cancel'.

The **Loops (Common Equipment)** screen is displayed again, and updated with values in the **Digital Trunk Interface Loop Number (DLOP)** field. Click **Submit**.

NORTEL CS 1000 ELEMENT MANAGER Help | Logout

Managing: **192.168.0.1**
System » Loops (Common Equipment)

Loops (Common Equipment)

- Basic Configuration

Input Description	Input Value
Change to Common Equipment parameters (CEQU) (TYPE)	CEQU
Tone and Digit Switch (TDS)	<input type="text"/> Edit
Conference loop (CONF)	029 030 031 062 094 095 Edit
Digital Trunk Interface Loop Number (DLOP)	PRI 13 23 ESF YES B8S FDL 0 00 Edit

+ Feature Packages

Submit Refresh

5.4 Administer D-Channel

Select **Routes and Trunks > D-channels** from the left pane to display the **D-Channels** screen. In the **Choose a D-Channel Number** field, select an available D-Channel from the drop-down list (in this case “3”). Click to **Add**.

NORTEL CS 1000 ELEMENT MANAGER Help | Logout

Managing: **192.168.0.1**
Routes and Trunks » D-Channels

D-Channels

Maintenance

- [D-Channel Diagnostics \(LD 96\)](#)
- [Network and Peripheral Equipment \(LD 32, Virtual D-Channels\)](#)
- [MSDL Diagnostics \(LD 96\)](#)
- [TMDI Diagnostics \(LD 96\)](#)
- [D-Channel Expansion Diagnostics \(LD 48\)](#)

Configuration

Choose a D-Channel Number: and type: to Add

The **D-Channels 3 Property Configuration** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **D channel Card Type (CTYP):** “D-Channel on TMDI card (TMDI)”
- **Card number (CDNO):** Select the physical TMDI card location, in this case “13”.
- **Port number (PORT):** “1”
- **Designator (DES):** A descriptive text.
- **User (USR):** “Primary Rate Interface (PRI)”
- **Interface type for D-channel:** “Meridian DMS-100 (D100)”
- **D-Channel PRI loop number:** The digital trunk interface loop number from **Section 5.3**.

Note that the **Meridian 1 node type (SIDE)** field defaults to “Slave to the controller (USR)”, which complements the DS1 interface setting on Avaya Communication Manager in **Section 3.7**.

For the **Release ID of the switch at the far end (RLS)** field, select “36” from the drop-down list. The following screen shows the configured D-Channel. Select **Basic options (BSCOPT)** toward the bottom of the screen to expand it.

Managing: **192.168.0.1**
Routes and Trunks » [D-Channels](#) » D-Channels 3 Property Configuration

D-Channels 3 Property Configuration

- Basic Configuration

Input Description	Input Value
Action Device And Number (ADAN) (TYPE)	DCH
D channel Card Type (CTYP)	TMDI
Card number (CDNO)	13
Port number (PORT)	1
Designator (DES)	AvayaNI1
Recovery to Primary (RCVP)	<input type="checkbox"/>
User (USR)	Primary Rate Interface (PRI)
Interface type for D-channel (IFC)	Meridian DMS-100 (D100)
D-Channel PRI loop number (DCHL)	13
Primary Rate Interface (PRI)	<input type="text"/> more PRI
Secondary PRI2 loops (PRI2)	<input type="text"/>
Meridian 1 node type (SIDE)	Slave to the controller (USR)
Release ID of the switch at the far end (RLS)	36
Central Office switch type (CO_TYPE)	100% compatible with Bellcore standard (STD)
Integrated Services Signaling Link Maximum (ISLM)	200 Range: 1 - 4000

[+ Basic options \(BSCOPT\)](#)
[+ Advanced options \(ADVOPT\)](#)
[+ Feature Packages](#)

For the **D-channel transmission Rate (DRAT)** field, select “64 kb/s clear (64KC)” from the drop-down list.

Retain the default values in the remaining fields, and click **Edit** next to the **Remote Capabilities (RCAP)** field.

- Basic options (BSCOPT)

- Primary D-channel for a backup DCH (PDCH)
- PINX customer number (PINX_CUST)
- Progress signal (PROG)
- Calling Line Identification (CLID)
- Output request Buffers (OTBF) 32
- D-channel transmission Rate (DRAT) 64 kb/s clear (64KC)
- Channel Negotiation option (CNEG) No alternative acceptable, exclusive. (1)
- Remote Capabilities (RCAP)

The **Remote Capabilities Configuration** screen is displayed next. Scroll down the screen as necessary to check the following capability:

- **Network name Display Method 3 (ND3)**

Click **Return – Remote Capabilities** at the bottom of the screen. The **D-Channels 3 Property Configuration** screen is displayed again (not shown below). Click **Submit**.

- Zones
- Network Address Translation
- QoS Thresholds
+ Personal Directories
+ Software
- Customers
- Routes and Trunks
- Routes and Trunks
- **D-Channels**
- Digital Trunk Interface
- Dialing and Numbering Plans
- Electronic Switched Network
- Network Routing Service
- Flexible Code Restriction
- Incoming Digit Conversion
- Services
+ Backup and Restore
- Date and Time
+ Logs and Reports
+ Security

Network name Display method 2 (ND2)
Network name Display method 3 (ND3)
Name display - integer ID coding (NDI)
Name display - object ID coding (NDO)
Path replacement uses integer values (PRI)
Path replacement uses object identifier (PRO)
Remote virtual queuing (RVQ)
Trunk anti-tromboning operation (TAT)
User to user service 1 (UUS1)
NI-2 name display option. (NDS)
Message waiting indication using integer values (QMWI)
Message waiting indication using object identifier (QMWO)
User to user signalling (UUI)

5.5 Administer Routes and Trunks

Select **Routes and Trunks** > **Routes and Trunks** from the left pane to display the **Routes and Trunks** screen. Next to the applicable **Customer** row, click **Add route**.

The screenshot shows the CS 1000 ELEMENT MANAGER interface. The top header is purple with the NORTTEL logo and 'CS 1000 ELEMENT MANAGER'. Below the header, there's a navigation pane on the left with options like Home, Links, System, IP Telephony, Customers, Routes and Trunks, and D-Channels. The main content area shows 'Managing: 192.168.0.1' and 'Routes and Trunks » Routes and Trunks'. The title is 'Routes and Trunks'. Below the title, there's a summary for 'Customer: 0' showing 'Total routes: 28' and 'Total trunks: 29'. An 'Add route' button is located to the right of the summary.

The **Customer 0, New Route Configuration** screen is displayed next. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Route Number (ROUT):** Select an available route number.
- **Designator field for trunk (DES):** A descriptive text.
- **Trunk Type (TKTP):** “TIE trunk data block (TIE)”
- **Incoming and Outgoing trunk (ICOG):** “Incoming and Outgoing (IAO)”
- **Access Code for the trunk route (ACOD):** An available access code.

Verify that **Digital Trunk Route (DTRK)** is checked and the **Digital Trunk Type (DGTP)** field is set to “PRI”. The following screen shows the resulting configuration for the route.

The screenshot shows the CS 1000 ELEMENT MANAGER interface with the configuration for a route. The left navigation pane is expanded to 'Routes and Trunks'. The main content area shows the configuration for 'Route Data Block (RDB) (TYPE)'. The fields and their values are: Customer number (CUST) 00, Route Number (ROUT) 14, Designator field for trunk (DES) AVAYANI1RTE, Trunk Type (TKTP) TIE, Incoming and Outgoing trunk (ICOG) Incoming and Outgoing (IAO), Access Code for the trunk route (ACOD) 510, and Digital Trunk Type (DGTP) PRI. The Digital Trunk Route (DTRK) checkbox is checked. The text 'The route is for a virtual trunk route (VTRK)' is displayed with an unchecked checkbox.

Scroll down the screen, check the **Integrated Services Digital Network option (ISDN)** checkbox to enable additional fields to appear. For the **Mode of operation (MODE)** field, select “ISDN/PRA route, DTRK must be YES (PRA)” from the drop-down list. For the **Interface type for route (IFC)** field, select “Meridian DMS-100 (D100)” from the drop-down list. For the **Call Type for outgoing direct dialed TIE route (CTYP)** field, select “Unknown Call type (UKWN)” from the drop-down list. Check the check boxes **Network Calling Name Allowed (NCNA)** and **Network Call Redirection (NCRD)**. Scroll down to the bottom of the screen, and click **Submit**.

- D-Channels
- Digital Trunk Interface
- **Dialing and Numbering Plans**
 - Electronic Switched Network
 - Network Routing Service
 - Flexible Code Restriction
 - Incoming Digit Conversion
- **Services**
 - + Backup and Restore
 - Date and Time
 - + Logs and Reports
 - + Security

Integrated Services Digital Network option (ISDN)

- **Mode of operation (MODE)** ISDN/PRA route, DTRK must be YES (PRA) ▼

- **Interface type for route (IFC)** Meridian DMS-100 (D100) ▼

- **Send Billing Number (SBN)**

- **Private Network Identifier (PNI)** 00000 Range: 0 - 32700

- **Network Calling Name Allowed (NCNA)**

- **Network Call Redirection (NCRD)**

- **Channel Type (CHTY)** B-channel (BCH) ▼

- **Call Type for outgoing direct dialed TIE route (CTYP)** Unknown Call type (UKWN) ▼

- **Insert ESN Access Code (INAC)**

- **Integrated Service Access Route (ISAR)**

- **Display of Access Prefix on CLID (DAPC)**

- **CLID Public for North American ISDN (CPUB)**

- **B-Channel Overload Control timer (BCOT)** 0 Range: 0 - 4000

+ Basic Route Options

+ Network Options

+ General Options

+ Advanced Configurations

The **Routes and Trunks** screen is displayed again, and updated with the newly added route. Click the **Add trunk** button next to the newly added route.

NORTEL
CS 1000 ELEMENT MANAGER

- Home
- + Links
- + System
- + IP Telephony
- Customers
- **Routes and Trunks**
 - [Routes and Trunks](#)
 - D-Channels

Managing: **192.168.0.1**
Routes and Trunks » Routes and Trunks

Routes and Trunks

- Customer: 0	Total routes: 28	Total trunks: 29	<input type="button" value="Add route"/>
- Route: 12	Type: TIE	Description: IPO	<input type="button" value="Edit"/> <input type="button" value="Add trunk"/>
+ Route: 14	Type: TIE	Description: AVAYAN1ROUTE	<input type="button" value="Edit"/> <input style="border: 2px solid red;" type="button" value="Add trunk"/>

The **Customer 0, Route 14, New Trunk Configuration** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields. Scroll down to the bottom of the screen, and click **Submit**. The **Multiple trunk input number (MTINPUT)** field may be used to add multiple trunks in a single operation, or repeat the operation for each trunk.

- **Multiple trunk input number (MTINPUT):** “23” (must match values in **Sections 5.3 and 3.8.3**)
- **Terminal Number (TN):** The TMDI slot number and port “1”.
- **Designator field for trunk (DES):** A descriptive text.
- **Route number, Member number (RTMB):** Current route number and starting member.
- **Trunk Group Access Restriction (TGAR):** Desired trunk group access restriction level.

NORTEL
CS 1000 ELEMENT MANAGER

- Home
- + Links
- + System
- + IP Telephony
- Customers
- Routes and Trunks
 - Routes and Trunks
 - D-Channels
 - Digital Trunk Interface
- Dialing and Numbering Plans
 - Electronic Switched Network
 - Network Routing Service
 - Flexible Code Restriction
 - Incoming Digit Conversion
- Services
 - + Backup and Restore
 - Date and Time
 - + Logs and Reports
 - + Security

Managing: **192.168.0.1**
Routes and Trunks » [Routes and Trunks](#) » Customer 0, Route 14, New Trunk Configuration

Customer 0, Route 14, New Trunk Configuration

- Basic Configuration

Input Description	Input Value
Multiple trunk input number (MTINPUT)	23
Trunk data block (TYPE)	TIE trunk data block (TIE)
Terminal Number (TN)	13 1 *
Designator field for trunk (DES)	AVAYANI1
Extended Trunk (XTRK)	
Customer number (CUST)	0
Route number, Member number (RTMB)	14 1 *
Level 3 Signaling (SIGL)	
Start arrangement Incoming (STRJ)	
Start arrangement Outgoing (STRO)	
Trunk Group Access Restriction (TGAR)	1
Channel ID for this trunk. (CHID)	
Increase or decrease the member numbers (INC)	Increase channel and member number (YES)
Class of Service (CLS)	Edit

+ Advanced Trunk Configurations

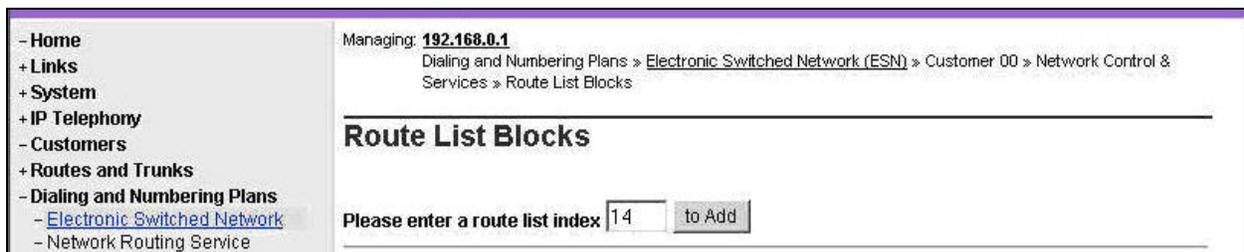
* Mandatory fields of current configuration

5.6 Administer Route List Block

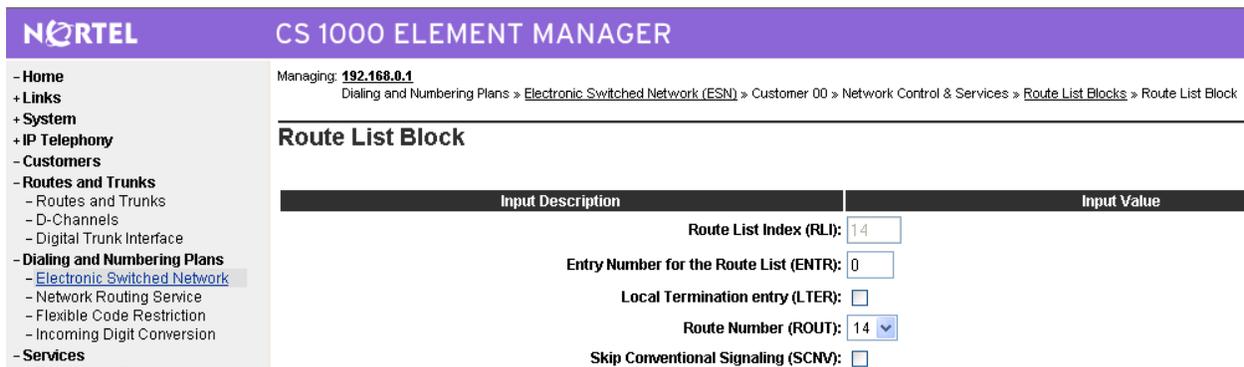
Select **Dialing and Numbering Plans > Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen. Select **Route List Block (RLB)**.



The **Route List Blocks** screen is displayed. In the **Please enter a route list index** field, enter an available route list block number (in this case “14”). Click to **Add**.

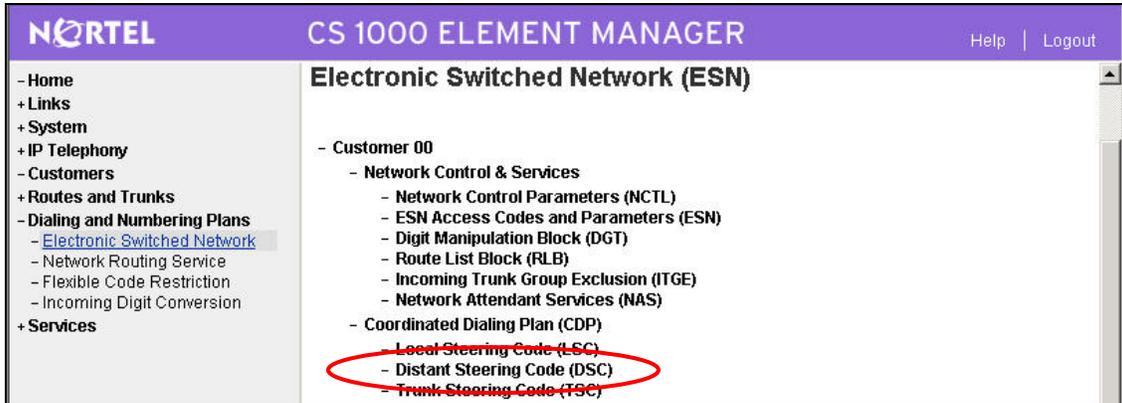


The **Route List Block** screen is updated with a listing of parameters. For the **Route Number (ROUT)** field, select the route number from **Section 5.5**. Retain the default values for the remaining fields, and scroll down to the bottom of the screen and click **Submit** (not shown).



5.7 Administer Distant Steering Code

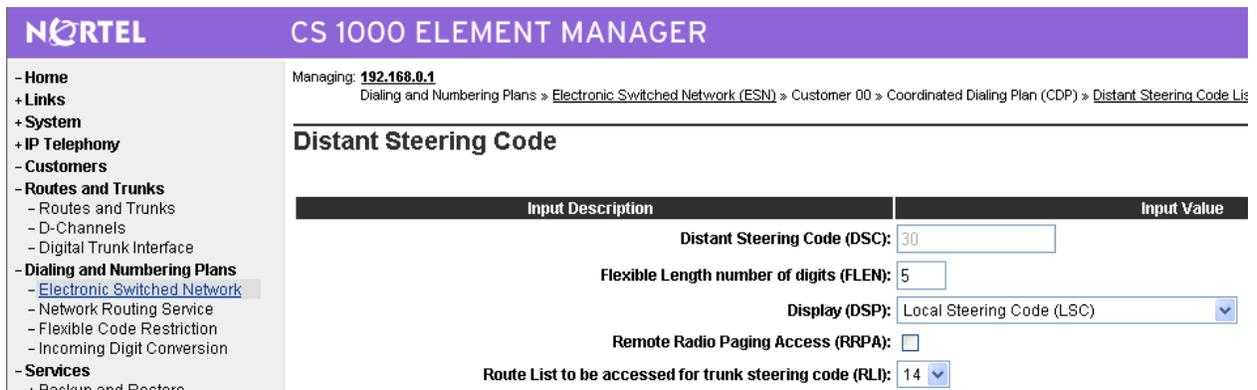
The **Electronic Switched Network (ESN)** screen is displayed again. Select **Distant Steering Code (DSC)** to add an entry to route 30xxx calls to Avaya Communication Manager.



The **Distant Steering Code List** screen is displayed next. In the **Please enter a distant steering code** field, enter the dialed prefix digits to match on (in this case “30”). This specification will match dialed extensions of the form 30xxx. Click to **Add**.



The **Distant Steering Code** screen is displayed. For the **Route List to be accessed for trunk steering code (RLI)** field, select the route list index in **Section 5.6** from the drop-down list. Retain the default values in all remaining fields, and scroll down to the bottom of the screen to click **Submit** (not shown).



5.8 Enable TMDI Card

The remaining steps required to bring the PRI NI-1 trunk into service are best accomplished using the Command Line Interface (CLI) of the CS1000. Access the CLI via a hyper terminal application running on a PC, which has a serial cable connected to the CS1000 serial port, or via *telnet* to the IP address of the CS1000 Signaling Server (192.168.1.30 in the sample configuration).

The CLI is a character-based serial interface to the operating system and overlay programs on each system component. The program issues a prompt for input, and the system administrator enters the appropriate response through the keyboard followed by the **Enter** key. The output from the CS1000 command line interface has been trimmed down in the subsequent sections in order to focus on the key settings for the configuration. Values highlighted in bold represent values entered by the system administrator.

Command	Comment
<pre>> login USERID? xxxxx PASS? yyyyy TTY #00 LOGGED IN xxxxx 16:52 24/5/2010 > ld 96 . enl tmdi 13 all</pre>	<p>Issue the login command. Enter a valid user ID. Enter a valid user password.</p> <p>A sample response indicating successful log in.</p> <p>Use load 96 to enable the TMDI card. Enable the TMDI card with the physical slot number of the TMDI card and the option “all”.</p>

5.9 Enable D-Channel Automatic Establishment

Use the CLI to enable automatic establishment for the administered D-Channel.

Command	Comment
<pre>> ld 96 . enl auto 3</pre>	<p>Use load 96 to enable automatic establishment for the D-Channel. Enable the D-Channel automatic establishment with the D-Channel number, in this case “3”.</p>

5.10 Enable D-Channel Service Messages

Service messages are used to maintain control and obtain status of the PRI trunk. By default, service messages are disabled for PRI interface type “Meridian DMS-100 (D100)”. They must be enabled in this configuration for the individual B channels to come into service. The CLI can be used to enable service messages on the D-Channel. Note that the D-Channel may have to be disabled and enabled before and after enabling service messages.

Command	Comment
> ld 96	Use load 96 to enable service messages for the D-Channel.
. dis dch 3	Disable the D-Channel, in this case “3”.
. enl serv 3	Enable D-Channel service messages.
. enl dch 3	Enable the D-Channel again.

6 Verification Steps

6.1 Verify Avaya Aura™ Communication Manager

Verify the status of the ISDN trunk group to the CS1000 using the “status trunk” command. An example screen is shown below. Idle trunk members should show “in-service/idle”.

```

status trunk 100                                     Page 1

```

TRUNK GROUP STATUS			
Member	Port	Service State	Mtce Connected Ports Busy
0100/001	001V101	in-service/idle	no
0100/002	001V102	in-service/idle	no
0100/003	001V103	in-service/idle	no
0100/004	001V104	in-service/idle	no
0100/005	001V105	in-service/idle	no
0100/006	001V106	in-service/idle	no
0100/007	001V107	in-service/idle	no
0100/008	001V108	in-service/idle	no
0100/009	001V109	in-service/idle	no
0100/010	001V110	in-service/idle	no
0100/011	001V111	in-service/idle	no
0100/012	001V112	in-service/idle	no
0100/013	001V113	in-service/idle	no
0100/014	001V114	in-service/idle	no

If the trunk members show OOS/PINS (out of service, pending in service), verify that service messages have been enabled on the D-Channel in the CS1000 (See **Section 5.10**). If the trunk members are not in-service, check the signaling group status, as shown below, using the “status signaling-group” command. Verify the signaling group is “in-service” as indicated in the **Group State** and **Level 3 State** fields shown below.

```

status signaling-group 100
      STATUS SIGNALING GROUP

      Group ID: 100                      Active NCA-TSC Count: 0
      Group Type: isdn-pri                Active CA-TSC Count: 0
      Signaling Type: facility associated signaling
      Group State: in-service

      Primary D-Channel

      Port: 001V124      Level 3 State: in-service

```

If the signaling group **Level 3 State** is not in service, the health of the physical level can be checked by testing the DS1 board. Abridged output is shown below. While maintenance documentation is beyond the scope of these Application Notes, failure of the initial tests of the DS1 board likely indicate a problem with the physical layer connectivity to the CS1000 (e.g., improper cabling, framing, etc.). If test 144 fails, check that the G450 Media Gateway is deriving clock synchronization properly. One should also verify that the trunk parameters specified for Communication Manager (**Sections 3.7-3.8**) and the CS1000 (**Sections 5.4-5.5**) have been configured correctly.

```

test board lvl                                     Page 1

      TEST RESULTS

Port      Mtce Name   Alt. Name      Test No.  Result      Error Code
001V1     MG-DS1      MG-DS1         138       PASS
001V1     MG-DS1      MG-DS1         139       PASS
001V1     MG-DS1      MG-DS1         140       PASS
001V1     MG-DS1      MG-DS1         141       PASS
001V1     MG-DS1      MG-DS1         142       PASS
001V1     MG-DS1      MG-DS1         143       PASS
001V1     MG-DS1      MG-DS1         144       PASS
001V1     MG-DS1      MG-DS1         145       PASS
001V1     MG-DS1      MG-DS1         146       PASS

```

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 3.9.2**. Verify that all trunks are in the “in-service/idle” state as shown below.

```

status trunk 32

                                TRUNK GROUP STATUS

Member   Port      Service State      Mtce Connected Ports
                                Busy

0032/001 T00226   in-service/idle    no
0032/002 T00227   in-service/idle    no
0032/003 T00228   in-service/idle    no
0032/004 T00229   in-service/idle    no
0032/005 T00230   in-service/idle    no
0032/006 T00231   in-service/idle    no
0032/007 T00232   in-service/idle    no
0032/008 T00233   in-service/idle    no
0032/009 T00234   in-service/idle    no
0032/010 T00235   in-service/idle    no

```

Verify the status of the SIP signaling groups by using the “status signaling-group n” command, where “n” is the signaling group number administered in **Section 3.9.1**. Verify the signaling group is “in-service” as indicated in the **Group State** field shown below.

```

status signaling-group 32

                                STATUS SIGNALING GROUP

Group ID: 32                      Active NCA-TSC Count: 0
Group Type: sip                    Active CA-TSC Count: 0
Signaling Type: facility associated signaling
Group State: in-service

```

Finally, make a call between the Avaya 9600 Series IP Telephone and the Avaya i2004 IP Telephone and verify two-way audio. Verify the status of connected trunks by using the “status trunk” command for the PRI QSIG trunk group (100) to the CS1000. More information can be obtained by using “status trunk 100/x” where x is the trunk member for the in-service/active trunk member for the call.

6.2 Verify Avaya Aura™ Session Manager

Expand the **Session Manager** menu on the left and click **SIP Monitoring**. Verify that none of the links to the defined SIP entities are down, indicating that they are all reachable for call routing. In the sample screen below, the SIP trunk to SM1 has been busied out on Communication Manager, so one of the links is shown as down.

- ▶ Asset Management
- ▶ User Management
- ▶ Monitoring
- ▶ Network Routing Policy
- ▶ Security
- ▶ Applications
- ▶ Settings
- ▼ Session Manager
 - Session Manager Administration
 - System State Administration
 - Security Module Status
 - Data Replication Status
 - Local Host Name Resolution
 - Maintenance Tests
 - SIP Firewall Configuration
 - SIP Monitoring
 - Tracer Configuration
 - Trace Viewer
 - Call Routing Test
 - Managed Bandwidth Usage
- Shortcuts
 - Change Password
 - Help for SIP Monitoring

SIP Entity Link Monitoring Status Summary

This page provides a summary of Session Manager SIP entity link monitoring status.

Entity Link Status for All Session Manager Instances

Session Manager Name	Entity Links Down/Total	Entity Links Partially Down	SIP Entities - Monitoring Not Started	SIP Entities - Not Monitored
SM1	1/13	0	0	0

All Monitored SIP Entities

15 Items Filter: Enable

SIP Entity Name
AcmePacket
AS5400
AudioCodes M1000
Avaya MAS-BR1
Avaya-G430
Avaya-SB500
Avaya_MAS-Br2
Avaya_MAS-HQ
CallCenter

Select the corresponding Session Manager (SM1 in this example) to view the Entity Link that is down and the Reason Code. The Reason Code reflects the result of Session Manager sending a SIP OPTIONS message to that SIP Entity.

- ▶ Asset Management
- ▶ User Management
- ▶ Monitoring
- ▶ Network Routing Policy
- ▶ Security
- ▶ Applications
- ▶ Settings
- ▼ Session Manager
 - Session Manager Administration

Session Manager Entity Link Connection Status

This page displays detailed connection status for all entity links from a Session Manager where at least one connection is currently down.

All Entity Links with Down Connections for Session Manager: SM1

11 Items Filter: Enable

Details	SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
▶ Show	CallCenter	10.1.2.233	5060	TCP	DOWN	408 Request Timeout	DOWN

Once the source of the problem has been located, verify that the link status has changed as shown below. Note that the time period for the status to change is dependent on the SIP Link Monitoring parameter settings defined for the SIP Entity corresponding to Communication Manager. See [2,3] for more information.

- ▶ Asset Management
- ▶ Communication System Management
- ▶ Monitoring
- ▶ User Management
- ▶ Network Routing Policy
- ▶ Security
- ▶ Applications
- ▶ Settings
- ▼ Session Manager

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: CallCenter

1 Item Filter: Enable

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
<input type="checkbox"/> Show	SM1	10.1.2.233	5060	TCP	Up	200 OK	Up

6.3 Verify Nortel Communication Server 1000

Select **Services->Logs and Reports->IP Telephony Nodes** on the left. Click **Status** for the “SS_Node” to verify that the signaling server is enabled and operational.

NORTEL
Help | Logo

Managing: 192.168.0.1
 Services > Logs and Reports > Node Maintenance and Reports

Node Maintenance and Reports

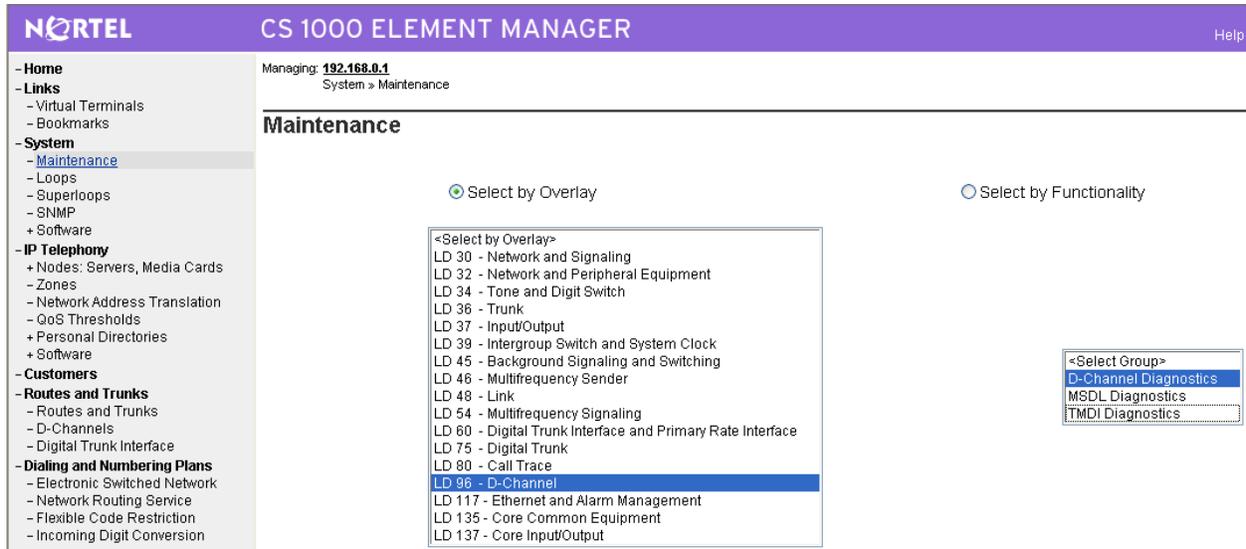
- al Terminals
- emarks
- m
- tenance
- OS
- erloops
- IP
- ware
- ophony
- es: Servers, Media Cards
- ss
- ork Address Translation
- Thresholds
- ional Directories
- ware
- mers
- s and Trunks
- tes and Trunks
- annels
- tal Trunk Interface
- g and Numbering Plans
- ronic Switched Network
- ork Routing Service
- ible Code Restriction
- ming Digit Conversion
- Services
 - + Backup and Restore
 - Date and Time
 - Logs and Reports
 - [IP Telephony Nodes](#)
 - Call Server Report Utility
 - Equipped Feature Packages
 - Peripheral Software Version Data
 - System License Parameters
- + Security

Node ID: 271 Node IP: 192.168.1.33 Total elements: 2

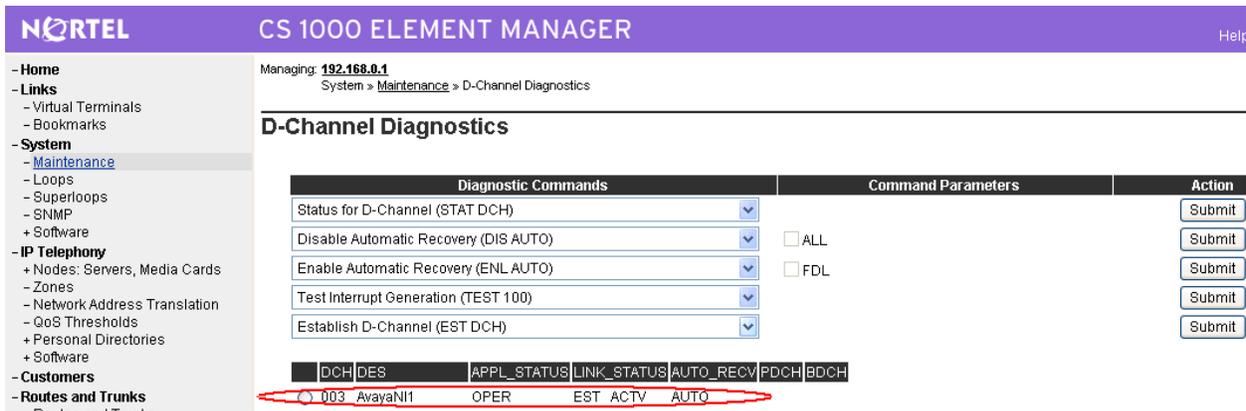
Index	ELAN IP	Type	TN	ELAN			
SS_Node	192.168.0.3	Signalling Server	NO TN	<input type="button" value="GEN CMD"/>	<input type="button" value="RPT LOG"/>	<input type="button" value="OM RPT"/>	<input type="button" value="Reset"/> <input type="button" value="Virtual Terminal"/> <input type="button" value="Status"/>
Media-Card-14	192.168.0.4	Succession Media Card	14 0	<input type="button" value="GEN CMD"/>	<input type="button" value="SYS LOG"/>	<input type="button" value="OM RPT"/>	<input type="button" value="Reset"/> <input type="button" value="Virtual Terminal"/> <input type="button" value="Status"/>

192.168.0.3 : Enabled

Select **System->Maintenance** on the left, and then select **Select by Overlay** and then **LD 96 – D-Channel** in the center window. Select **D-Channel Diagnostics** in the window that appears on the right.



The screen that results, shown below, will indicate the operational state of the D-Channel, in this case “EST ACTV” under the LINK_STATUS column. Other diagnostic tests can be run from this page by selecting the D-Channel, one of the **Diagnostic Commands**, and then clicking on **Submit**.



6.4 Verification Scenarios

Verification scenarios for the configuration described in these Application Notes are listed below. Note that there are some telephone display limitations as described in **Section 6.5**.

- Basic calls between various telephones on the Communication Manager and Avaya Communication Server 1000 can be made in both directions using G.711MU. Proper display of the calling and called party name and number information was verified for all telephones with the basic call scenario.
- Supplementary calling features were verified. The feature scenarios involved additional endpoints on the respective systems, such as performing an unattended transfer to a local endpoint on the same system, and then repeating the scenario to transfer the call to a remote endpoint on the other system. The supplementary calling features verified are shown below.
 - Call hold/unhold
 - Unattended transfer
 - Attended transfer
 - Call forwarding
 - Conference
 - Calling number block

6.5 Telephone Display Limitations

The following are limitations in name and number displays for some of the scenarios verified in the previous section. Unless otherwise specified below, telephone displays will show the correct name and number. Abbreviations are used for brevity (CM = Communication Manager, CS1K = Communication Server 1000).

6.5.1 Basic Calls

When calling from CM to CS1K, the CM telephone shows called number during the ringing phase, and connected name when the call is answered.

When calling from CS1K to CM, the CS1K telephone displays the called number.

6.5.2 Call Hold/Unhold

For a call between CM and CS1K that is held by the CS1K user, when the CS1K user takes the call off hold, the CS1K telephone display changes to the local CS1K PRI trunk designation.

6.5.3 Call Transfer

For a call between CM and CS1K that is transferred to a party on the same PBX as the transferring party, the transferred party's display is not updated (i.e., displays the name of the transferring party).

For a call between CM and CS1K that is transferred to a party that is not on the same PBX as the transferring party, the displays of both the transferred and transfer-to party are not updated (i.e., display the name of the transferring party). Also note that the trunks on the transfer-to party PBX are not released.

6.5.4 Call Forward

For a call from CS1K to CM that is forwarded to another telephone, the CS1K telephone display is not updated (i.e., displays the originally called party).

7 Conclusion

As illustrated in these Application Notes, Avaya Communication Server 1000 front-ended by an Avaya G450 Media Gateway via a PRI NI-1 trunk can be integrated with Session Manager and Communication Manager.

8 Additional References

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

Avaya Aura™ Session Manager:

- [1] *Avaya Aura™ Session Manager Overview*, Doc ID 03-603323, available at <http://support.avaya.com>.
- [2] *Administering Avaya Aura™ Session Manager*, Release 5.2, Issue 2.0, November 2009, Document Number 03-603324, available at <http://support.avaya.com>.
- [3] *Maintaining and Troubleshooting Avaya Aura™ Session Manager*, Doc ID 03-603325, available at <http://support.avaya.com>.

Avaya Aura™ Communication Manager 5.2.1:

- [4] *SIP Support in Avaya Aura™ Communication Manager Running on Avaya S8xxx Servers*, Doc ID 555-245-206, May, 2009, available at <http://support.avaya.com>.
- [5] *Administering Avaya Aura™ Session Manager*, Release 5.2, Issue 2.0, November 2009, Document Number 03-603324, available at <http://support.avaya.com>.
- [6] *Upgrading, Migrating, and Converting Avaya Servers and Gateways, Release 5.0*, Doc ID 03-300412, January 2008, available at <http://support.avaya.com>.

Avaya Communication Server 1000 4.5:

- [7] *ISDN Primary Rate Interface Installation and Configuration*, Nortel Communication Server 1000 Release 4.5, Document Number 553-3001-201, available on the Nortel Communication Server Electronic Reference Library CD.

Avaya Application Notes:

- [8] *Configuring SIP Trunks among Avaya Aura™ Session Manager, Avaya Aura™ Communication Manager 5.2, and Nortel Communication Server 1000 – Issue 1.1*, available at <http://www.avaya.com>.
- [9] *Front-Ending Nortel Communication Server 1000 with an AudioCodes Mediant 1000 Modular Media Gateway to Support SIP Trunks to Avaya Aura™ Session Manager with*

Avaya Aura™ Communication Manager 5.2 as an Access Element – Issue 1.1, available at <http://www.avaya.com>.

- [10] *Front-Ending Avaya Communication Server 1000 R4.5 with an Avaya G450 Media Gateway Controlled by Avaya Aura™ Communication Manager 5.2.1 to Support SIP Trunks to Avaya Aura™ Session Manager 5.2 and Avaya Modular Messaging 5.2 – Issue 1.0*, available at <http://www.avaya.com>.

©2010 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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 Solution & Interoperability Test Lab at interoplabnotes@list.avaya.com