



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for HP Networking Multi Service Router 30 Series PSTN Gateway in an Avaya Telephony Environment that includes Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and various Avaya Telephones – Issue 1.0**

## **Abstract**

These Application Notes describe the steps for configuring HP Multi Service Router 30 series PSTN Gateway in an Avaya Telephony Environment that includes Avaya Aura® Communication Manager, Avaya Aura® Session Manager and various Avaya telephones.

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

# 1. Introduction

These Application Notes describe a solution for configuring a HP Networking Multi-Service Router 30 series PSTN Gateway (herein referred to as MSR30) in an Avaya telephony environment.

The MSR30 product line is a configurable set of chassis and modules that meet a wide variety of customer demands. Modules include analog and digital voice, WAN data, VPN and Power over Ethernet (PoE) Networking.

Customers who use Avaya Unified Communications products with HP hardware, such as the ProLiant servers, often require Gateways to interoperate with traditional telephone equipment.

## 2. General Test Approach and Test Results

All test cases were performed manually. The general approach was to place various types of calls to and from the simulated PSTN. Feature testing included inbound and outbound calls, transfers, conference calls, Message Waiting Indicator (MWI), FAX and voicemail. For serviceability testing, failures such as cable pulls and resets were applied. All test cases passed, except the following anomalies:

The MSR30 does not support PSTN-side hold.
--

### 2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. The feature testing evaluated the SIP trunk between Session Manager and MSR30 with inbound, outbound, transfer, conference, MWI, FAX, and voicemail. The serviceability testing introduced failure scenarios to see if the MSR30 could resume after failure.

### 2.2. Support

Technical support on HP Networking MSR30 series can be obtained through the following:

HP Contract Holders in the Americas	Use the generic HP Technical Support number 1-800-633-3600.
Warranty issues in the Americas	Call 1-800-334-5144. When prompted, say Networking then 3Com, or H3C or A Series.
All other Worldwide regions	Please use the following: HP Networking telephone contact link: <a href="http://www.hp.com/go/telephone">www.hp.com/go/telephone</a> HP Networking product support link: <a href="http://www.hp.com/networking/support">www.hp.com/networking/support</a>

### 3. Reference Configuration

Figure 1 provides the test configuration used for the compliance testing.

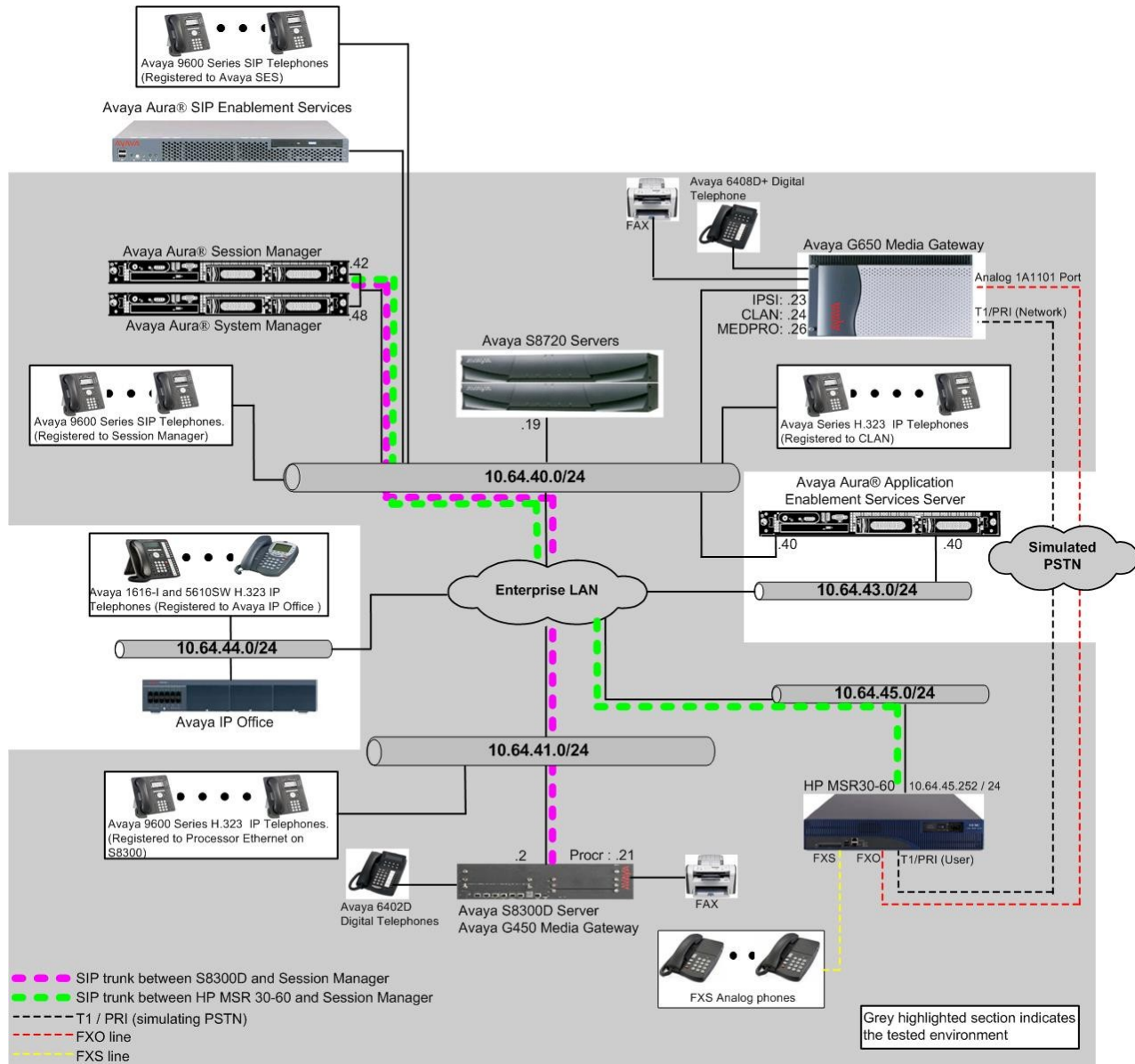


Figure 1: The HP Networking MSR30 in the Avaya Telephony environment

## 4. Equipment and Software Validated

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

Equipment		Software/Firmware
Avaya S8300D Server with Avaya G450 Media Gateway		6.0.1(R016x.00.1.510.1) w/ patch 00.1.510.1-18860
Avaya Aura® System Manager		6.1 (R6-1-0-20-0)
Avaya Aura® Session Manager		6.1
Avaya S8720 Servers with Avaya G650 Media Gateway		Avaya Communication Manager 5.2.1 (R015x.02.1.016.4)
Avaya 9600 Series IP Telephones		
	9620 (H.323)	3.1
	9630 (H.323)	3.1
Avaya 9600 Series SIP Telephones		
	9630 (SIP)	2.6.4
	9640 (SIP)	2.6.4
	9650 (SIP)	2.6.4
Avaya 6400 Series Digital Telephones		N/A
Avaya C363T-PWR Converged Stackable Switch		4.5.14
HP Networking 2910al-48G-PoE Switch		W.14.30
HP Networking Multi-Service Router 30-60 Series PSTN Gateway		R2207P38
HP 1-Port T1-Voice SIC A-MSR Module HP 2-Port FXO SIC A-MSR Module HP 4-Port FXO MIM A-MSR Module HP 16-port FXS Voice Interface MIM Module HP 16-Port 10/100 POE MIM A-MSR Module HP Voice Co-Processor Module A-MSR Module HP 24-Channel Voice Processor A-MSR Module		

## 5. Configure Avaya Testing Environment

This section describes the configuration for the Avaya telephony testing environment, shown in **Figure 1**. Telephones in the Enterprise side use a 72xxx dial plan and telephones on the PSTN side use a 2xxxx dial plan.

### 5.1. Configure Avaya Aura® Communication Manager on Enterprise side

This section describes the procedure for setting up a SIP trunk between Communication Manager and Session Manager. The steps include setting up an IP codec set, an IP network region, IP node name, a signaling group, and a trunk group. The highlights in the following screens indicate the values used during the compliance test. Default values may be used for all other fields.

These steps are performed from the Communication Manager System Access Terminal (SAT) interface. All SIP telephones are configured as off-PBX telephones in Communication Manager.

### 5.1.1. Capacity Verification

Enter the **display system-parameters customer-options** command. Verify that there are sufficient Maximum Off-PBX Telephones – OPS licenses. If not, contact an authorized Avaya account representative to obtain additional licenses.

display system-parameters customer-options		Page 1 of 11
OPTIONAL FEATURES		
G3 Version: V16	Software Package: Enterprise	
Location: 2	System ID (SID): 1	
Platform: 28	Module ID (MID): 1	
		USED
Platform Maximum Ports:	6400	211
Maximum Stations:	2400	35
Maximum XMOBILE Stations:	2400	0
Maximum Off-PBX Telephones - EC500:	9600	0
Maximum Off-PBX Telephones - OPS:	9600	18
Maximum Off-PBX Telephones - PBFMC:	9600	0
Maximum Off-PBX Telephones - PVFMC:	9600	0
Maximum Off-PBX Telephones - SCCAN:	0	0
Maximum Survivable Processors:	313	1

On **Page 2** of the form, verify that the number of SIP trunks supported by the system is sufficient for the number of SIP trunks needed. If not, contact an authorized Avaya account representative to obtain additional licenses.

display system-parameters customer-options		Page 2 of 11
OPTIONAL FEATURES		
IP PORT CAPACITIES		USED
Maximum Administered H.323 Trunks:	4000	30
Maximum Concurrently Registered IP Stations:	2400	5
Maximum Administered Remote Office Trunks:	4000	0
Maximum Concurrently Registered Remote Office Stations:	2400	0
Maximum Concurrently Registered IP eCons:	68	0
Max Concur Registered Unauthenticated H.323 Stations:	100	0
Maximum Video Capable Stations:	2400	0
Maximum Video Capable IP Softphones:	2400	0
Maximum Administered SIP Trunks:	4000	110
Maximum Administered Ad-hoc Video Conferencing Ports:	4000	0
Maximum Number of DS1 Boards with Echo Cancellation:	80	0
Maximum TN2501 VAL Boards:	10	0
Maximum Media Gateway VAL Sources:	50	1
Maximum TN2602 Boards with 80 VoIP Channels:	128	0
Maximum TN2602 Boards with 320 VoIP Channels:	128	0
Maximum Number of Expanded Meet-me Conference Ports:	300	0

### 5.1.2. IP Codec Set

This section describes the steps for administering a codec set in Communication Manager. This codec set is used in the IP network region for communications between Communication Manager and Session Manager. Enter the **change ip-codec-set <c>** command, where **c** is a number between **1** and **7**, inclusive. IP codec sets are used in **Section 5.1.3** for configuring an IP network region to specify which codec sets may be used within and between network regions. The compliance test used G.711MU.

change ip-codec-set 1

Page1 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:			

On **Page 2**, set **FAX Mode** to **t.38-standard** for FAXing through the SIP trunk via the MSR30.

change ip-codec-set 1				Page	2 of	2
IP Codec Set						
Allow Direct-IP Multimedia? y						
Maximum Call Rate for Direct-IP Multimedia: 4096:Kbits						
Maximum Call Rate for Priority Direct-IP Multimedia: 4096:Kbits						
	Mode	Redundancy				
FAX	t.38-standard	3				
Modem	off	0				
TDD/TTY	US	3				
Clear-channel	n	0				

### 5.1.3. Configure IP Network Region

This section describes the steps for configuring an IP network region in Communication Manager in order to work with Session Manager. Enter the **change ip-network-region** <n>command, where **n** is a number between **1** and **250** inclusive and configure the following:

- **Authoritative Domain**—Set to the appropriate domain. During the compliance test, the authoritative domain is set to **avaya.com**. This should match the SIP Domain value on Session Manager in **Section 5.3.1**
- **Intra-region IP-IP Direct Audio**— Set to **yes** to allow direct IP-to-IP audio connectivity between endpoints registered to Communication Manager or Session Manager in the same IP network region. The default value for this field is **yes**.
- **Codec Set**— Set the codec set number as provisioned in **Section 5.1.2**.
- **Inter-region IP-IP Direct Audio**— Set to **yes** to allow direct IP-to-IP audio connectivity between endpoints registered to Communication Manager or Session Manager in different IP network regions. The default value for this field is **yes**.

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

### 5.1.4. Configure IP Node Name

This section describes the steps for setting an IP node name for Session Manager. Enter the **change node-names ip** command and add a node name for Session Manager with its IP address.

```
change node-names ip                                         Page 1 of 2
                                                                IP NODE NAMES
    Name      IP Address
    SM-1      10.64.40.42
    default   0.0.0.0
    msgserver-ip 10.64.41.21
    msgserver-sip 10.64.41.21
    procr     10.64.41.21
    procr6    ::
```

### 5.1.5. Configure SIP Signaling

This section describes the steps for administering a signaling group for communication between Communication Manager and Session Manager. Enter the **add signaling-group <s>** command, where **s** is an available signaling group and configure the following:

- Group Type– Set to **sip**.
- IMS Enabled – Verify the field is set to **n**. This configures the Communication Manager to function as an Evolution Server. Setting this field to **y** causes Communication Manager to function as a Feature Server.
- Near-end Node Name- Set to **procr** as shown in **Section 5.1.4**.
- Far-end Node Name - Set to **SM-1** (Session Manager) as shown in **Section 5.1.4**.
- Far-end Network Region - Set to the region configured in **Section 5.1.3**.
- Far-end Domain- Set to **avaya.com**, matching the SIP Domain in **Section 5.3.1**.

Take note of the Group Number value as it will be needed in **Section 5.1.6**.

add signaling-group 92		Page 1 of 1
SIGNALING GROUP		
Group Number: 92	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		SIP Enabled LSP? n
IP Video? n		Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y	Peer Server: SM	
Near-end Node Name: procr	Far-end Node Name: SM-1	
Near-end Listen Port: 5061	Far-end Listen Port: 5061	
	Far-end Network Region: 1	
Far-end Domain: avaya.com		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Initial IP-IP Direct Media? n	
	Alternate Route Timer(sec): 6	



### 5.1.6. Configure SIP Trunk

This section describes the steps for administering a trunk group for communication between Communication Manager and Session Manager. Enter the **add trunk-group <t>** command, where **t** is an unallocated trunk group and configure the following:

- **Group Type**– Set to **sip**.
- **Group Name**– Enter a descriptive name.
- **TAC (Trunk Access Code)** – Set to any available trunk access code.
- **Signaling Group**– Set to the Group Number field value configured in **Section 5.1.5**.
- **Number of Members**– Allowed values are between 0 and 255. Set to a value large enough to accommodate the number of SIP telephone extensions being used.

```
add trunk-group 92                                     Page 1 of 21
                                     TRUNK GROUP
Group Number: 92                                     Group Type: sip          CDR Reports: y
Group Name: No IMS SIP trk                          COR: 1          TN: 1          TAC: 1092
  Direction: two-way      Outgoing Display? n
  Dial Access? n          Night Service:
Queue Length: 0
Service Type: tie        Auth Code? n
                                     Member Assignment Method: auto
                                     Signaling Group: 92
                                     Number of Members: 10
```

## 5.2. Configure Avaya Aura® Communication Manager on PSTN side

This section describes the procedure for setting up a T1/PRI trunk between Communication Manager and the MSR30. The steps include setting up a DS1 card, a signaling group, and a trunk group. The highlights in the following screens indicate the values used during the compliance test. Default values may be used for all other fields.

These steps are performed from the Communication Manager System Access Terminal (SAT) interface.

### 5.2.1. Configure DS1 card for T1

Enter the **add ds1 x** command, where **x** is the board number of the DS1 circuit pack. Enter a descriptive Name and set the other highlighted fields to the values indicated. Provide the following information:

- Name – A descriptive name.
- Line Coding– Select **b8zs**. This value should match the MSR30's configuration.
- Framing Mode - Select **esf**. This value should match the MSR30's configuration.
- Signaling Mode –Select **isdn-pri**.
- Connect – Select **pbx**.
- Interface – Select **network**.

*Note: Communication Manager was set to **network** on the Interface field. This means the MSR30 should be set to **user** mode.*

```

add ds1 1a09                                     Page 1 of 2
                                         DS1 CIRCUIT PACK

Location: 01A09                                Name: Temp-HP
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: 1
Interworking Message: PROGress                 Protocol Version: b
Interface Companding: mulaw                    CRC? n
Idle Code: 11111111                           DCP/Analog Bearer Capability: 3.1kHz

T303 Timer(sec): 4

Slip Detection? y                             Near-end CSU Type: other

Block Progress Indicator? n

```

### 5.2.2. Configure Signaling Group

Enter the **add signaling-group s** command, where **s** is an unused signaling group number. Set the highlighted fields below to the values indicated.

```

add signaling-group 80                           Page 1 of 5
                                         SIGNALING GROUP

Group Number: 80                                Group Type: isdn-pri
Associated Signaling? y                        Max number of NCA TSC: 0
Primary D-Channel: 01A0924                   Max number of CA TSC: 0
Trunk Group for Channel Selection: 80         Trunk Group for NCA TSC:
TSC Supplementary Service Protocol: a         Network Call Transfer? n

```

### 5.2.3. Configure Trunk Group

Enter the **add trunk-group t** command, where **t** is an unused trunk group number. Set the highlighted fields below to the values indicated.

```
add trunk-group 80                                     Page 1 of 21
                                     TRUNK GROUP
Group Number: 80                                     Group Type: isdn       CDR Reports: r
Group Name: Temp-HP                                COR: 1              TN: 1          TAC: 113
  Direction: two-way                               Outgoing Display? y  Carrier Medium: PRI/BRI
  Dial Access? y                                   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
```

On **Page 5**, add trunk group members.

```
display trunk-group 80                               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: 01A0901 TN464 G          .          80
2: 01A0902 TN464 G          .          80
.
.
.
.
22: 01A0922 TN464 G          .          80
23: 01A0923 TN464 G          .          80
```

### 5.2.4. Configure UDP and AAR

During the compliance test, Automatic Alternate Routing (AAR) and Uniform Dial Plan (UDP) were utilized between Communication Manager and the MSR30 via the T1/PRI trunk. The following displays the sample UDP and AAR configuration used during the test.

Enter the **change uniform-dialplan d** command, where **d** is any digit that is valid under the provisioned dial plan. Enter the whole or a partial extension on enterprise side for the Matching Pattern field. Enter the length of the extension for the Len field. Set the Del field to **0**, and the Net field is set to **aar**.

```
change uniform-dialplan 7                             Page 1 of 2
                                     UNIFORM DIAL PLAN TABLE
                                     Percent Full: 0

   Matching      Insert      Node
   Pattern      LenDel      Digits      Net ConvNum
720             5 0             aar n
```

Enter the **change aar analysis d** command, where **d** is any digit that is valid under the provisioned dial plan. Enter the whole or a partial extension on enterprise side for the Matching Pattern field. Enter the number of an unused route pattern for the Route Pattern field. The Call Type field is set to **aar**.

change aar analysis 7							Page	1 of	2
AAR DIGIT ANALYSIS TABLE									
Location: all					Percent Full: 2				
Dialed String	Total Min Max		Route Pattern	Call Type	Node Num	ANI Reqd			
720	5	5	80	aar		n			

### 5.2.5. Configure Route Pattern

Enter the **change route-pattern r** command, where **r** is the number of the route pattern specified in previous section. Enter the number of the trunk group configured for the Grp No field. Assign a Facility Restriction Level to this routing preference for the FRL field. The FRL value **0** is the least restrictive.

change route-pattern 80												Page	1 of	3
Pattern Number: 80						Pattern Name: To PSTN via G3r								
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: 80 0												n	user	
BCC VALUE		TSC	CA-TSC	ITC BCIE		Service/Feature			PARM	No.	Numbering	LAR		
0	1	2	M	4	W	Request					Dgts Format			
								Subaddress						
1: y		y	y	y	y	n	n	rest			none			

### 5.3. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. All SIP call provisioning for Session Manager is performed through the System Manager Web interface and is then downloaded into Session Manager.

This section assumes that Session Manager and System Manager have been installed, network connectivity exists between the two platforms, and the basic configuration is performed.

The following list outlines the steps for configuring Session Manager.

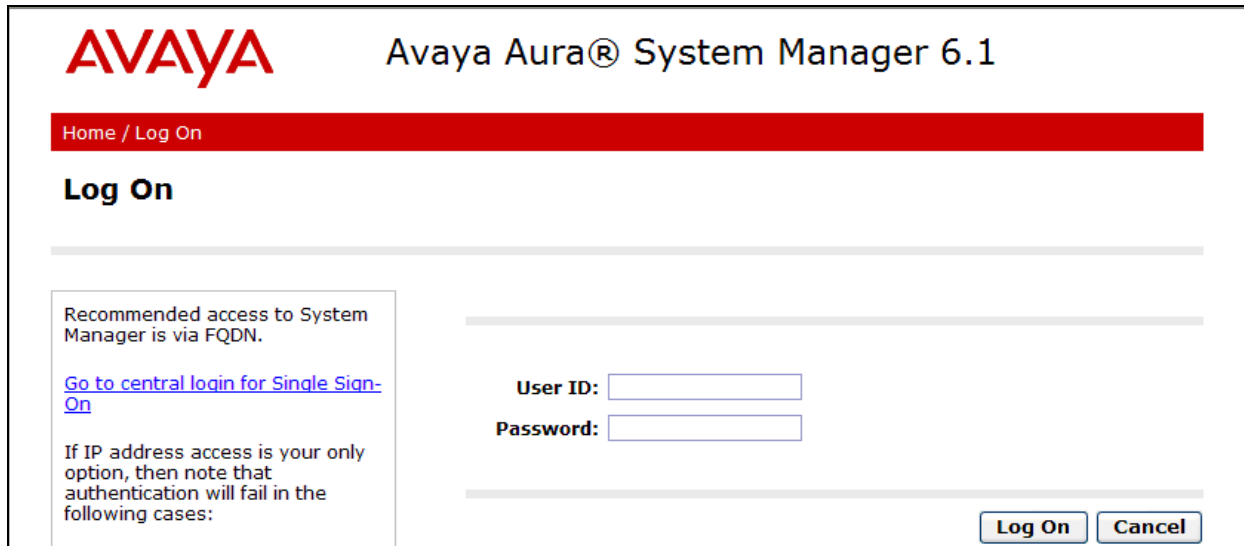
- SIP Domains
- Locations
- SIP Entities
- Entity Links
- Time Ranges
- Routing Policy
- Dial Patterns
- Manage Element
- Applications
- Application Sequence
- User Management

For a SIP trunk between Session Manager and the MSR30, the following sections need to be configured:

- **SIP Entity**
- **Entity Link**
- **Routing Policy**
- **Dial Patterns**

### 5.3.1. Configure SIP Domain

Launch a web browser, enter <https://<IP address of System Manager>/SMGR> in the URL, and log in with the appropriate credentials.

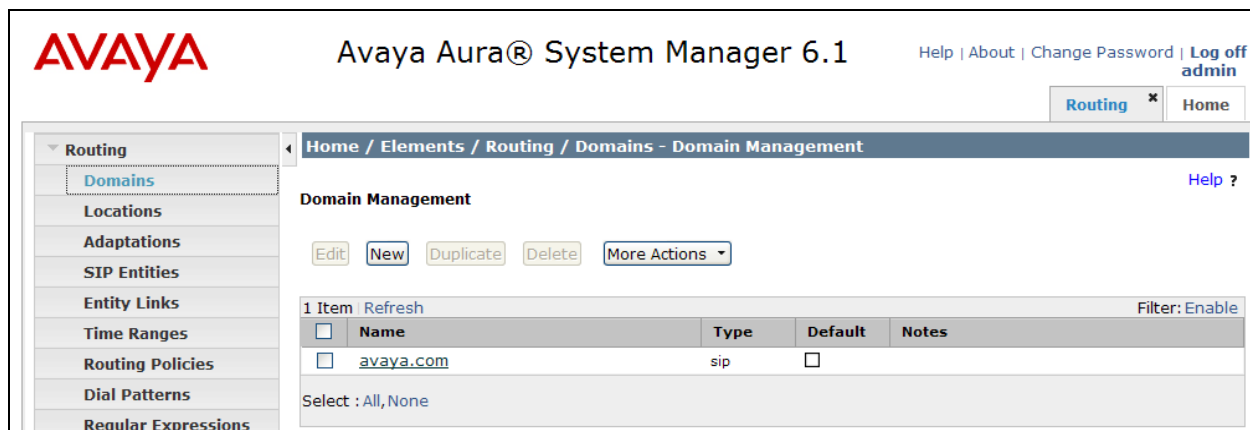


The screenshot shows the Avaya Aura® System Manager 6.1 login page. At the top is the Avaya logo and the title 'Avaya Aura® System Manager 6.1'. Below this is a red navigation bar with 'Home / Log On'. The main heading is 'Log On'. On the left, a box contains text: 'Recommended access to System Manager is via FQDN. Go to central login for Single Sign-On. If IP address access is your only option, then note that authentication will fail in the following cases:'. To the right of this box are two input fields: 'User ID:' and 'Password:'. At the bottom right are 'Log On' and 'Cancel' buttons.

Navigate to **Elements→Routing→Domains** and click on the **New** button to create a new SIP Domain (screen not shown). Enter the following values and use defaults for the remaining fields:

- **Name** –Enter the Authoritative Domain name specified in **Section 5.1.3**, which is **avaya.com**.
- **Type** – Select **SIP**

Click **Commit** to save. The following screen shows the Domains page used during the compliance test.



The screenshot shows the 'Domains - Domain Management' page in Avaya Aura® System Manager 6.1. The top navigation bar includes 'Help | About | Change Password | Log off admin'. Below this is a breadcrumb trail: 'Home / Elements / Routing / Domains - Domain Management'. The left sidebar shows a tree view with 'Routing' expanded and 'Domains' selected. The main content area has a 'Domain Management' heading and buttons for 'Edit', 'New', 'Duplicate', 'Delete', and 'More Actions'. Below these is a table with one item: 'avaya.com' of type 'sip'. The table has columns for 'Name', 'Type', 'Default', and 'Notes'. At the bottom, there is a 'Select : All, None' option and a 'Filter: Enable' link.

Name	Type	Default	Notes
avaya.com	sip	<input type="checkbox"/>	

### 5.3.2. Configure Locations

Locations are used to identify logical and/or physical locations where SIP Entities reside. This is used for bandwidth management or location-based routing.

Navigate to **Routing→Locations**, and click on the **New** button to create a new location (screen not shown).

#### General section

Enter the following values and use default values for the remaining fields.

- Enter a descriptive Location in the **Name** field (e.g. **.41 Subnet**).
- Enter a description in the **Notes** field if desired.

#### Location Pattern section

Click **Add** and enter the following values:

- The IP address information for the **IP address Pattern** (e.g. **10.64.41.\***).
- A description in the **Notes** field if desired.

Repeat these steps in the Location Pattern section if the Location has multiple IP segments. Modify the remaining values on the form, if necessary; otherwise, use all the default values. Click on the **Commit** button.

Repeat all the steps for each new Location. The following screen shows the Location page used during the compliance test.

The screenshot shows the Avaya Aura® System Manager 6.1 interface. The top navigation bar includes the Avaya logo, the title 'Avaya Aura® System Manager 6.1', and links for 'Help', 'About', 'Change Password', and 'Log off admin'. Below the navigation bar, there are tabs for 'Routing' and 'Home'. The main content area is titled 'Locations - Location' and includes a 'Location' section with buttons for 'Edit', 'New', 'Duplicate', 'Delete', and 'More Actions'. A table lists two locations: '.41 Subnet' and '.45 subnet'. The table has columns for 'Name' and 'Notes'. The 'Name' column contains the location names, and the 'Notes' column is empty. The table also includes a 'Select' dropdown menu with options 'All', 'None', and 'Filter: Enable'.

### 5.3.3. Configure SIP Entities

A SIP Entity must be added for Session Manager and for each network component that has a SIP trunk. During the compliance test the following SIP Entities were configured:

- Session Manager itself
- Communication Manager (Avaya S8300D Server)
- Communication Manager (Avaya S8720 Servers – not shown)
- HP MSR

Navigate to **Routing → SIP Entities** and click on the **New** button to create a new SIP entity (screen not shown). Provide the following information:

#### General section

Enter the following and use default values for the remaining fields:

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the IP address of the signaling interface on each:
  - Communication Manager
  - Session Manager virtual SM-100
  - HP MSR
- From the **Type** drop down menu, select a type that best matches the SIP Entity:
  - For Communication Manager, select **CM**
  - For Session Manager, select **Session Manager**
  - For the MSR, select **gateway**
- Enter a description in the **Notes** field if desired.
- Select a location from **Section 5.3.2**.
- Select the appropriate time zone.
- Accept the other default values.

Click on the **Commit** button to save each SIP entity. The following screen shows the SIP Entities page used during the compliance test.

Repeat all the steps for each new entity.

The screenshot shows the Avaya Aura System Manager 6.1 interface. The top navigation bar includes the Avaya logo, the title 'Avaya Aura® System Manager 6.1', and links for 'Help | About | Change Password | Log off admin'. Below the navigation bar, there is a breadcrumb trail: 'Home / Elements / Routing / SIP Entities - SIP Entities'. The main content area is titled 'SIP Entities' and includes a 'Help ?' link. Below the title, there are buttons for 'Edit', 'New', 'Duplicate', 'Delete', and 'More Actions'. A table displays 4 items with columns for 'Name', 'FQDN or IP Address', 'Type', and 'Notes'. The table contains the following data:

Name	FQDN or IP Address	Type	Notes
HP MSR	10.64.45.252	Gateway	
S8300D	10.64.41.21	CM	
SessionManager	10.64.40.42	Session Manager	SessionManager in D4H26

Below the table, there is a 'Select : All, None' option.



### 5.3.4. Configure Entity Links

Entity Links define the connections between the SIP Entities and Session Manager. In the compliance test, the following entity links are defined from Session Manager.

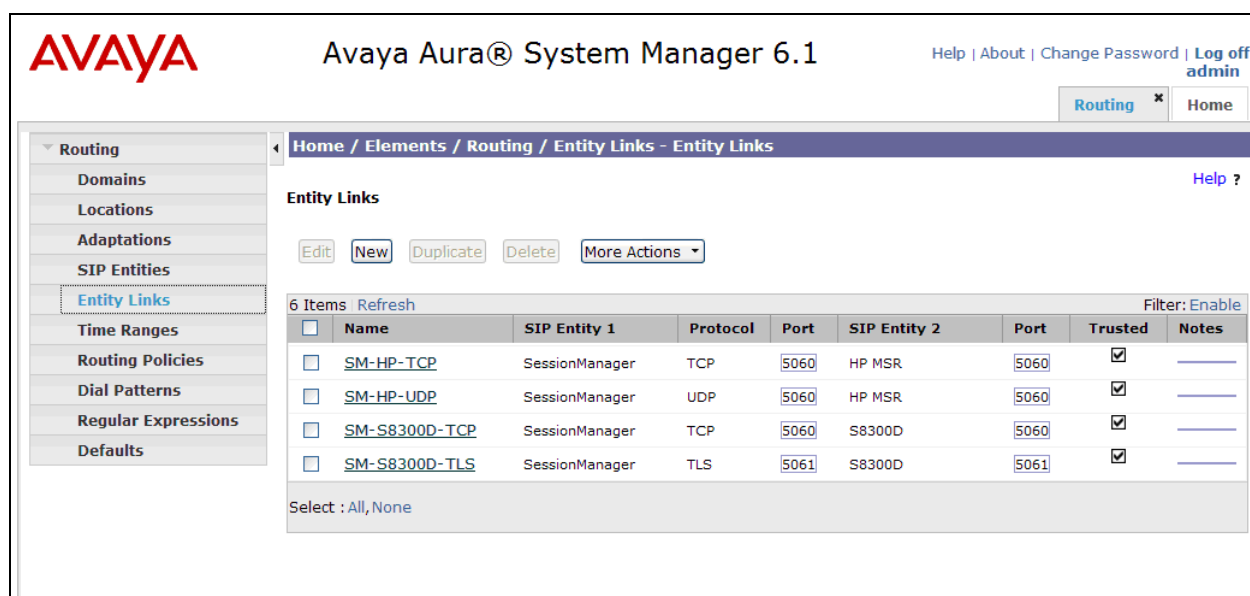
- Session Manager ⇔ Communication Manager (Avaya S8300D Server)
- Session Manager ⇔ MSR30

Navigate to **Routing → Entity Links** and click on the **New** button to create a new entity link (screen not shown). Provide the following information:

- **Name:** Enter a descriptive name.
- In the **SIP Entity 1** drop down menu, select the Session Manager SIP Entity created in **Section 5.3.3** (e.g. **SessionManager**).
- In the **Protocol** drop down menu, select the protocol to be used.
- In the **Port** field, enter the port to be used (e.g. **5060** or **5061**).
  - TLS – 5061
  - UDP or TCP – 5060
- In the **SIP Entity 2** drop down menu, select one of the two entities in the bullet list above (which were created in **Section 5.3.3**). In the compliance test **HP MSR** was selected.
- In the **Port** field, enter the port to be used (e.g. **5060** or **5061**).
- Check the **Trusted** box.
- Enter a description in the **Notes** field if desired.

Click on the **Commit** button to save each Entity Link definition. The following screen shows an Entity Links page used during the compliance test.

Repeat all the steps for each new SIP Entity Link.



The screenshot shows the Avaya Aura System Manager 6.1 interface. The left sidebar contains a navigation menu with options like Domains, Locations, Adaptations, SIP Entities, Entity Links (selected), Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Entity Links' and includes a breadcrumb trail: 'Home / Elements / Routing / Entity Links - Entity Links'. Below the title, there are buttons for 'Edit', 'New', 'Duplicate', 'Delete', and 'More Actions'. A table lists 6 items, each with a checkbox, a name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Trusted status, and Notes. The table data is as follows:

	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
<input type="checkbox"/>	SM-HP-TCP	SessionManager	TCP	5060	HP MSR	5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	SM-HP-UDP	SessionManager	UDP	5060	HP MSR	5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	SM-S8300D-TCP	SessionManager	TCP	5060	S8300D	5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	SM-S8300D-TLS	SessionManager	TLS	5061	S8300D	5061	<input checked="" type="checkbox"/>	

At the bottom of the table, there is a 'Select' dropdown menu with options 'All' and 'None'.

### 5.3.5. Time Ranges

Time Ranges define admission control criteria to be specified for Routing Policies (Section 5.3.6). In the reference configuration, no restrictions were used.

To add a Time Range, navigate to **Routing→Time Ranges**, and click on the **New** button (not shown). Provide the following information:

- Enter a descriptive name in the **Name** field (e.g. **24/7**).
- Check each day of the week.
- In the **Start Time** field, enter **00:00**.
- In the **End Time** field, enter **23:59**.
- Enter a description in the **Notes** field if desired.

Click the **Commit** button. The following screen shows the Time Range page used during the compliance test.

AVAYA Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing \* Home

Home / Elements / Routing / Time Ranges - Time Ranges

Time Ranges

Help ?

Commit Cancel

1 Item Refresh Filter: Enable

Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
* 24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	* 00:00	* 23:59	

\* Input Required

Commit Cancel

### 5.3.6. Configure Routing Policy

Routing Policies associate destination SIP Entities (**Section 5.3.3**) with Time of Day admission control parameters (**Section 5.3.5**) and Dial Patterns (**Section 5.3.7**). In the reference configuration, Routing Policies are defined for:

- Inbound calls to Communication Manager.
- Inbound calls to MSR30.

To add a Routing Policy, navigate to **Routing → Routing Policies** and click on the **New** button on the right (screen not shown). Provide the following information:

#### General section

- Enter a descriptive name in the **Name** field.
- Enter a description in the **Notes** field if desired.

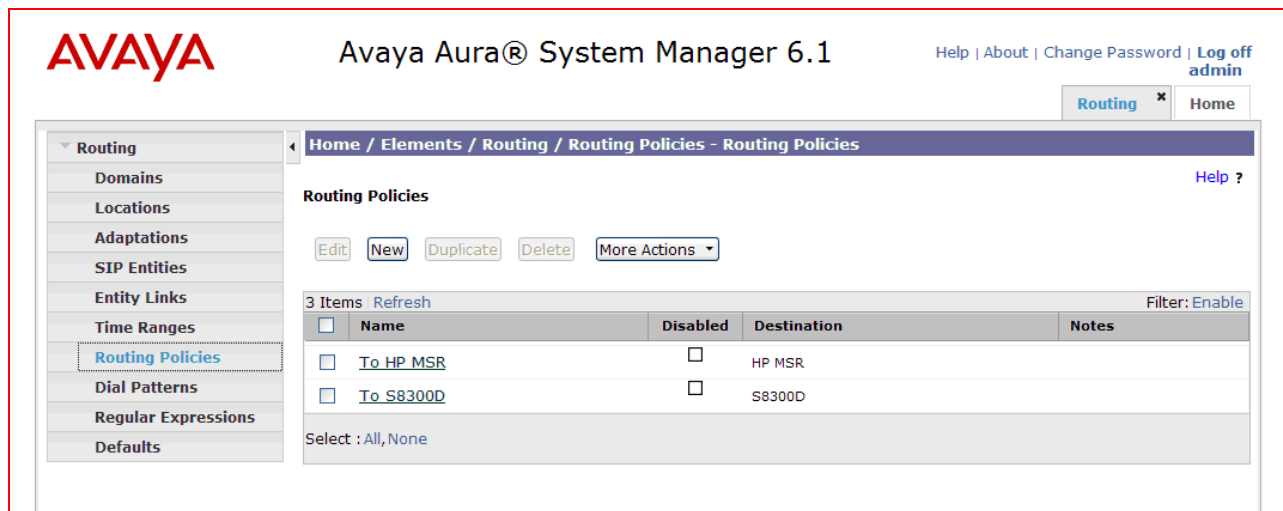
#### SIP Entity as Destination section

- Click the **Select** button.
- Select a SIP Entity that will be the destination for this call.
- Click the **Select** button and return to the Routing Policy Details form.

#### Time of Day section

- Leave default values.

Click **Commit** to save Routing Policy definition. Repeat the steps for each new Routing Policy. The following screen shows the Routing Policy used for Communication Manager during the compliance test.



The screenshot shows the Avaya Aura System Manager 6.1 interface. The top navigation bar includes the Avaya logo, the title 'Avaya Aura® System Manager 6.1', and links for 'Help', 'About', 'Change Password', and 'Log off admin'. The main content area is titled 'Routing Policies' and includes a breadcrumb trail 'Home / Elements / Routing / Routing Policies - Routing Policies'. A sidebar on the left lists various configuration categories, with 'Routing Policies' highlighted. The main area contains a table of routing policies with columns for 'Name', 'Disabled', 'Destination', and 'Notes'. Two policies are listed: 'To HP MSR' and 'To S8300D', both with the 'Disabled' checkbox checked. Below the table, there is a 'Select' dropdown menu set to 'All, None'.

<input type="checkbox"/>	Name	Disabled	Destination	Notes
<input checked="" type="checkbox"/>	To HP MSR	<input checked="" type="checkbox"/>	HP MSR	
<input checked="" type="checkbox"/>	To S8300D	<input checked="" type="checkbox"/>	S8300D	

### 5.3.7. Dial Patterns

Dial Patterns define digit strings to be matched for inbound and outbound calls. In the compliance test, the following dial patterns are defined from Session Manager.

- 720 –Endpoints in the Avaya S8300D Server
- 2 – 2xxxx extensions in the simulated PSTN side

To add a Dial Pattern, select **Routing → Dial Patterns** and click on the **New** button (not shown) on the right pane. Provide the following information:

#### General section

- Enter a unique pattern in the **Pattern** field (e.g. 2).
- In the **Min** field enter the minimum number of digits (e.g. 5).
- In the **Max** field enter the maximum number of digits (e.g. 5).
- In the **SIP Domain** drop down menu select the domain that will be contained in the Request URI *received* by Session Manager from Communication Manager.

#### Originating Locations and Routing Policies section

- Click on the **Add** button and a window will open (not shown).
- Click on the box for the appropriate Originating Locations, and Routing Policies (see **Section 5.3.6**) that pertain to this Dial Pattern.
  - Select the Originating Location to apply the selected routing policies to **All**.
  - Select Routing Policies to **HP MSR**.
  - Click on the **Select** button and return to the Dial Pattern window.

Click the **Commit** button to save the new definition. The following screen shows the dial pattern used for 2xxxx during the compliance test. Repeat steps for the remaining Dial Patterns.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing \* Home

Home / Elements / Routing / Dial Patterns - Dial Pattern Details

Dial Pattern Details

Help ?

Commit Cancel

General

\* Pattern: 2

\* Min: 5

\* Max: 5

Emergency Call: ☐

SIP Domain: avaya.com

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Refresh

<input type="checkbox"/>	Originating Location Name <sup>1</sup>	Originating Location Notes	Routing Policy Name	Rank <sup>2</sup>	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	To HP MSR	0	<input type="checkbox"/>	HP MSR	HP MSR

Filter: Enable

### 5.3.8. Configure Managed Elements

To define a new Managed Element, navigate to **Elements → Inventory → Manage Elements**. Click on the **New** button (not shown) to open the **New Entities Instance** page.

In the **New Entities Instance** Page

- In the **Type** field, select **CM** using the drop-down menu and the **New CM Instance** page opens (not shown).

In the **New CM Instance Page**, provide the following information:

- Application section
  - **Name** – Enter name for Communication Manager (Evolution Server).
  - **Description** - Enter description if desired.
  - **Node** – Enter IP address of the administration interface. During the compliance test, the **procr** IP address (10.64.41.21) was utilized.

The screenshot shows a web interface for configuring a Managed Element. At the top, there are two tabs: 'Application' and 'Attributes'. The 'Application' tab is selected. Below the tabs, there is a section titled 'Application' with a dropdown arrow. Below this, there are four input fields: '\* Name' with the value 'Element-S8300D', '\* Type' with a dropdown menu showing 'CM', 'Description' with the value 'S8300D in D4H26', and '\* Node' with the value '10.64.41.21'.

- Attributes section

System Manager uses the information entered in this section to log into Communication Manager using its administration interface. Enter the following values and use default values for remaining fields.

  - **Login** – Enter login used for administration access
  - **Password** – Enter password used for administration access
  - **Confirm Password** – Repeat value entered in above field
  - **Is SSH Connection** – Check the box
  - **Port** – Verify **5022** is set

Application \*

Attributes \*

SNMP Attributes ▾

\* Version ☒ None ☐ V1 ☐ V3

Attributes ▾

\* Login

Password

Confirm Password

Is SSH Connection ☒

\* Port

Alternate IP Address

RSA SSH Fingerprint (Primary IP)

RSA SSH Fingerprint (Alternate IP)

Is ASG Enabled ☐

ASG Key

Confirm ASG Key

Location

Click **Commit** (not shown) to save the element. The following screen shows the element created, **Element-S8300D**, during the compliance test.

AVAYA

Avaya Aura® System Manager 6.1

[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Inventory](#) ✕ [Routing](#) ✕ [Home](#)

▼ Inventory

Manage Elements

Discovered Inventory

► Discovery Management

► Synchronization

Home / Elements / Inventory / Manage Elements - Manage Elements

Manage Elements [Help ?](#)

Entities

View Edit New Delete More Actions ▾

3 Items Refresh Show ALL ▾ Filter: Enable

<input type="checkbox"/>	Name	Node	Type	Version	Description
<input type="checkbox"/>	Element-DellCM	10.64.40.24	CM		DellCM in D4H26
<input type="checkbox"/>	Element-S8300D	10.64.41.21	CM		S8300D in D4H26
<input type="checkbox"/>	Element-SessionManager	10.64.40.43	Session Manager		SessionManager in D4H26

Select : All, None

### 5.3.9. Configure Applications

To define a new Application, navigate to **Elements → Session Manager → Application Configuration → Applications**. Click **New** (not shown) to open the Applications Editor page:

- Application Editor section
  - **Name** – Enter name for the application.
  - **SIP Entity**–Select the SIP Entity for Communication Manager defined in **Section 5.3.3**.
  - **CM System for SIP Entity** –Select the name of the Managed Element defined for Communication Manager in **Section 5.3.8**.
  - **Description**– Enter description if desired.

### Application

**\*Name**

**\*SIP Entity**

**\*CM System for SIP Entity**   [View/Add CM Systems](#)

**Description**

- Leave the fields in the Application Attributes (optional) section blank.

Click the **Commit** button (not shown) to save the Application. The screen below shows the Application, **S8300D-App**, defined for Communication Manager.

Avaya Aura® System Manager 6.1

[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Session Manager

Inventory

Routing

Home

Session Manager

Inventory

Routing

Home

Session Manager

Dashboard

Session Manager

Administration

Communication Profile Editor

Network Configuration

Device and Location Configuration

Application Configuration

Applications

Home / Elements / Session Manager / Application Configuration / Applications - Applications

Applications

This page allows you to add, edit, or remove applications for available SIP Entities.

Application Entries

New

Edit

Delete

2 Items

Refresh

Filter: Enable

<input type="checkbox"/>	Application Name	SIP Entity	Description
<input type="checkbox"/>	<a href="#">DellCM-App</a>	DellCM	
<input type="checkbox"/>	<a href="#">S8300D-App</a>	S8300D	

Select : All, None

### 5.3.10. Define Application Sequence


Navigate to **Elements → Session Manager → Application Configuration → Application Sequences**. Click **New** (not shown) and provide the following information:

- Sequence Name section
  - **Name** – The name for the application.
  - **Description** – Enter description, if desired.

### Application Sequence

\*Name

Description

- Available Applications section
  - Click  icon associated with the Application for Communication Manager defined in **Section 5.3.9** to select this application.
  - Verify a new entry is added to the Applications in this Sequence table as shown below.

Click the **Commit** button (not shown) to save the new Application Sequence.

### Applications in this Sequence

1 Item					
<input type="checkbox"/>	Sequence Order (first to last)	Name	SIP Entity	Mandatory	Description
<input type="checkbox"/>		<a href="#">S8300D-App</a>	S8300D	<input checked="" type="checkbox"/>	

Select : All, None

The screen below shows the Application Sequence, **S8300D-AppSeq**, defined during the compliance test.

Avaya Aura® System Manager 6.1

[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Session Manager

Dashboard

Session Manager

Administration

Communication Profile Editor

Network Configuration

Device and Location Configuration

Application Configuration

Applications

Application Sequences

Session Manager

Inventory

Routing

Home

Home / Elements / Session Manager / Application Configuration / Application Sequences - Application Sequences

### Application Sequences

This page allows you to add, edit, or remove sequences of applications.

Application Sequences

2 Items		<a href="#">Refresh</a>	Filter: Enable
<input type="checkbox"/>	Name	Description	
<input type="checkbox"/>	<a href="#">DellCM-AppSeq</a>		
<input type="checkbox"/>	<a href="#">S8300D-AppSeq</a>		

Select : All, None



## 6. Configure HP Networking MSR PSTN Gateway

This section describes the configuration for the MSR30 in **Figure 1**. It is assumed that basic configuration has been performed to allow for IP and WebUI connectivity into MSR30. All steps in this section are performed using the WebUI.

Using a web browser, go to <http://<IP address of MSR30>> and log in with the appropriate credentials.



### 6.1. Introduction to the MSR Product Line

This section describes the high level features of the MSR product line. Further details can be found on the HP website.

The HP Multiple Services Router (MSR) Series is a family of modular devices with a full range of models for requirements from small offices to large data centers. The MSR product line delivers high performance, secure, integrated services on a single platform.

The MSR product line enhances network functionality, reduces complexity and simplifies management. The product line includes a variety of chassis that run Comware – the management software. Comware supports the centralized management suite IMC (Intelligent Management Center) and a comprehensive integrated security service. Additional benefits of the MSR Series include:

- Convergence of routing, switching, security and voice
- Modular, multi-bus architecture with high reliability and high performance
- Embedded encryption, quality of service, firewall, security features
- Redundant power supply and hot swapping available on select models
- Unified management platform
- Common modules across many platforms
- Open application architecture enabled
- No extra license cost for features

The HP MSR product line includes the following chassis:

MSR50 Series	High performance, reliable, scalable, available in PoE and DC models
MSR30 Series	Medium branch office routers available in PoE and DC models. Supports external Redundant Power Supply and 1GB WAN interfaces
MSR20 Series	Small branch office routers
MSR20-1x Series	Fixed WAN interface connectivity with WLAN models
MSR900 Series	Ethernet 10/100 WAN connectivity with WLAN models and 4 or 8 Ethernet ports

Power supply options for the MSR product line include:

- All MSR routers (except the MSR900) use 100~240V 50/60Hz
- MSR50 Series supports optional built-in dual Power Supply Unit and hot-swap
- MSR30 Series (starting with MSR30-16-POE) have a connector to a redundant power supply
- MSR900 Series routers use 12V input

MSR30-16, -20, -40, -60 Series and MSR50 Series support PoE:

- Standard 802.3af PoE Ethernet Switching interfaces
- MSR50 Series requires a PoE module
- MSR30 Series requires separately ordered PoE chassis

The MSR Series has a modular N-Bus architecture that provides high performance and flexibility that support a variety of interchangeable modules:

- WAN-data including MPLS, DSL, Cellular-3G, ATM, SONET, OC-3 POS, OC-3/T3/E3 and others
- Voice (T1, E1, J1, BRI)
- VPN
- Wi-Fi Access Point (b/g)
- Additional Ethernet ports
- Analog modems

Finally, the MSR product line includes features such as:

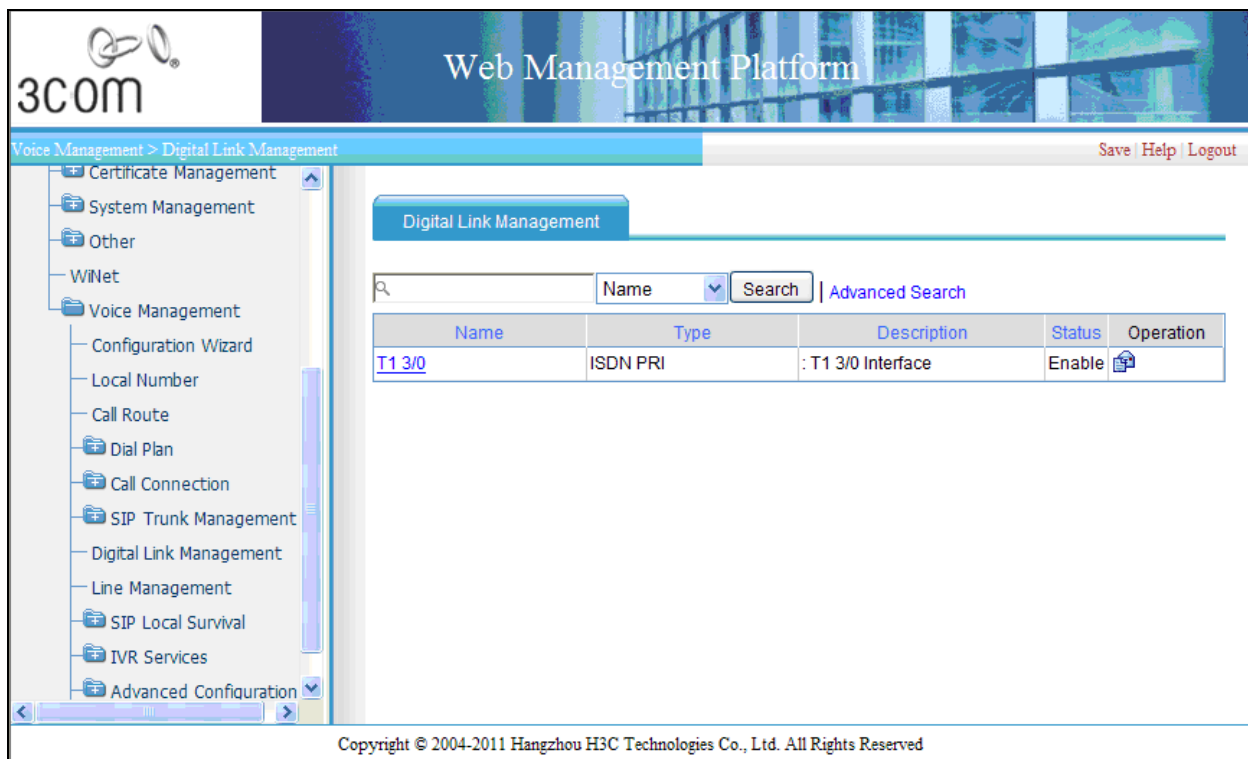
- Standards based routing, switching and wireless access
- Support for IPv4/IPv6, RIP, MPLS, IS-IS, BGP, OSPF, L2TP, GRE, PPP
- Support for IPSec, SSL, VPN, status based ASPF Firewall
- Power over Ethernet
- Support for QoS, security and VLANs

### 6.1.1. Introduction to the MSR30

The MSR30 Series are targeted for enterprise branch office or small to medium business core router applications. MSR30s have higher performance than the MSR20s and support both SIC and MIM interface modules. The MSR 30 series has 6 different models for various density and scalability requirements and has options for DC power supply and Power over Ethernet on some models.

### 6.2. Configure T1/PRI

Navigate to **Voice Management**→**Digital Link Management** and click the  icon under Operation.




Web Management Platform

Voice Management > Digital Link Management

Save | Help | Logout

Digital Link Management

Search [Name] [Type] [Description] [Status] [Operation]

Name	Type	Description	Status	Operation
<a href="#">T1 3/0</a>	ISDN PRI	: T1 3/0 Interface	Enable	

Copyright © 2004-2011 Hangzhou H3C Technologies Co., Ltd. All Rights Reserved

In the T1 Parameters Configuration page, provide the following information:

- **Working Mode** – Select **PRI Trunk Signaling**
- **Bound Timeslot Number** – Enter **1-24**
- **Frame Check Node** – Select **ESF**
- **Line Coding** – Select **B8ZS**
- **ISDN Protocol Mode** – Select **User Side Mode**

Click the **Apply** button at the bottom (Not shown)

H3C

- Device Info
- Wizard
- Interface Setup
- 3G
- NAT Configuration
- Security Setup
- Advanced
- VPN
- Certificate Management
- System Management
- Other
- WiNet
- Voice Management
  - Configuration Wizard
  - Local Number
  - Call Route
  - Dial Plan
  - Call Connection
  - SIP Trunk Management
  - Digital Link Management
  - Line Management
  - SIP Local Survival
  - IVR Services
  - Advanced Configuration
  - States and Statistics

## T1 Parameters Configuration

### Physical Parameters Configuration

Working Mode	<input type="radio"/> None	<input checked="" type="radio"/> PRI Trunk Signaling
Bound Timeslot Number	<input type="text" value="1-24"/>	(1-24)
Frame Check Mode	<input checked="" type="radio"/> ESF	<input type="radio"/> SF
Line Coding	<input checked="" type="radio"/> B8ZS	<input type="radio"/> AMI
TDM Clock Source	<input type="radio"/> Internal	<input checked="" type="radio"/> Line <input type="radio"/> Line primary
Status	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable

### ISDN Parameters Configuration

ISDN Protocol Type	<input type="text" value="DSS1(default)"/>		
ISDN Protocol Mode	<input checked="" type="radio"/> User Side Mode	<input type="radio"/> Network Side Mode	
ISDN Timeslot Management	<input checked="" type="radio"/> Disable	<input type="radio"/> Common Management	<input type="radio"/> Forced Management
ISDN Timeslot Order	<input checked="" type="radio"/> Ascending Order	<input type="radio"/> Descending Order	
ISDN Overlap-Sending	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable	Max Number of Digits that Can Be Sent Each Time <input type="text" value="10"/> (1-15, default=10)
Convert Received Progress Messages into Alerting Messages	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
Switch to ACTIVE State Without Receiving a Connect-Ack Message	<input type="text" value="Disable (default)"/>		
Carry High Layer Compatibility Information	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
Carry Low Layer Compatibility Information	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
Ignore the Sending-Complete Information Element in Setup Messages	<input type="text" value="Disable (default)"/>		

## 6.3. Configure Call Route

Two routes are used during the compliance test:

- Route to PSTN
- Route to Session Manager using a SIP trunk

### 6.3.1. Configure route to PSTN

Navigate to **Voice Management**→**Call Route**. To add a route, click the **Add** button (not shown) and provide the following information:

- **Call Route ID** – Enter a value within the ID range.
- **Destination Number** – Enter **.T**. Any extension other than specified in the call route will use this call route.
- **Route Description** – Enter a descriptive name.
- **Call Route Type** – Select **Trunk**.
- **Trunk Route Line** – Using the drop down list, select **subscriber-line3/0-23**.
- **Register Function** – Select **Disable**.

Click the **Apply** button.

The screenshot displays the 'Configure Route' configuration page in the H3C Voice Management interface. The left sidebar shows the navigation tree with 'Voice Management' expanded. The main configuration area contains the following fields and options:

- Call Route ID:** 10000 (Range: \*(10000-19999))
- Destination Number:** .T (Range: \*A string of 1 to 31 characters, supporting regular expressions.)
- Route Description:** to\_8720\_pstn (Range: A string of 1 to 80 characters)
- Call Route Type:** ☒ Trunk (Other options: SIP)
- SIP Routing:** ☒ Proxy Server (Other options: IP Routing, Binding Server Group)
- Transport Layer Protocol for Call Route:** ☒ UDP (Other options: TCP, TLS)
- URL Scheme for Call Route:** ☒ SIP (Other option: SIPS)
- Destination Address:** (Empty field) (Range: IPv4 address or domain name with 1 to 255 Characters)
- Port:** 65535 (Range: 1-65535. System assigned by default)
- Server Group:** (Empty dropdown)
- Trunk Route Line:** subscriber-line3/0:23 (Dropdown menu)
- Register Function:** ☒ Disable (Other option: Enable)
- Register Username:** (Empty field) (Range: A string of 1 to 63 characters, case sensitive.)
- Register Password:** (Empty field) (Range: A string of 1 to 16 characters, case sensitive.)
- Cnonce Name:** (Empty field) (Range: A string of 1 to 50 characters, case sensitive, must be set together with username and password.)
- Realm Name:** (Empty field) (Range: A string of 1 to 50 characters, case sensitive, must be set together with username and password.)
- Status:** ☒ Enable (Other option: Disable)

### 6.3.2. Configure route to Session Manager

Navigate to **Voice Management**→**Call Route**. To add a route, click the **Add** button (not shown) and provide the following information:

- **Call Route ID** – Enter a value within the ID range.
- **Destination Number** – Enter 7.... Any 5 digit extension starting with 7 will use this route.
- **Route Description** – Enter a descriptive name.
- **Call Route Type** – Select **SIP**.
- **SIP Routing** – Select **IP Routing**.
- **Transport Layer Protocol for Call Route** – Select **TCP**.
- **Destination Address** – Enter the Session Manager Security Module IP address.

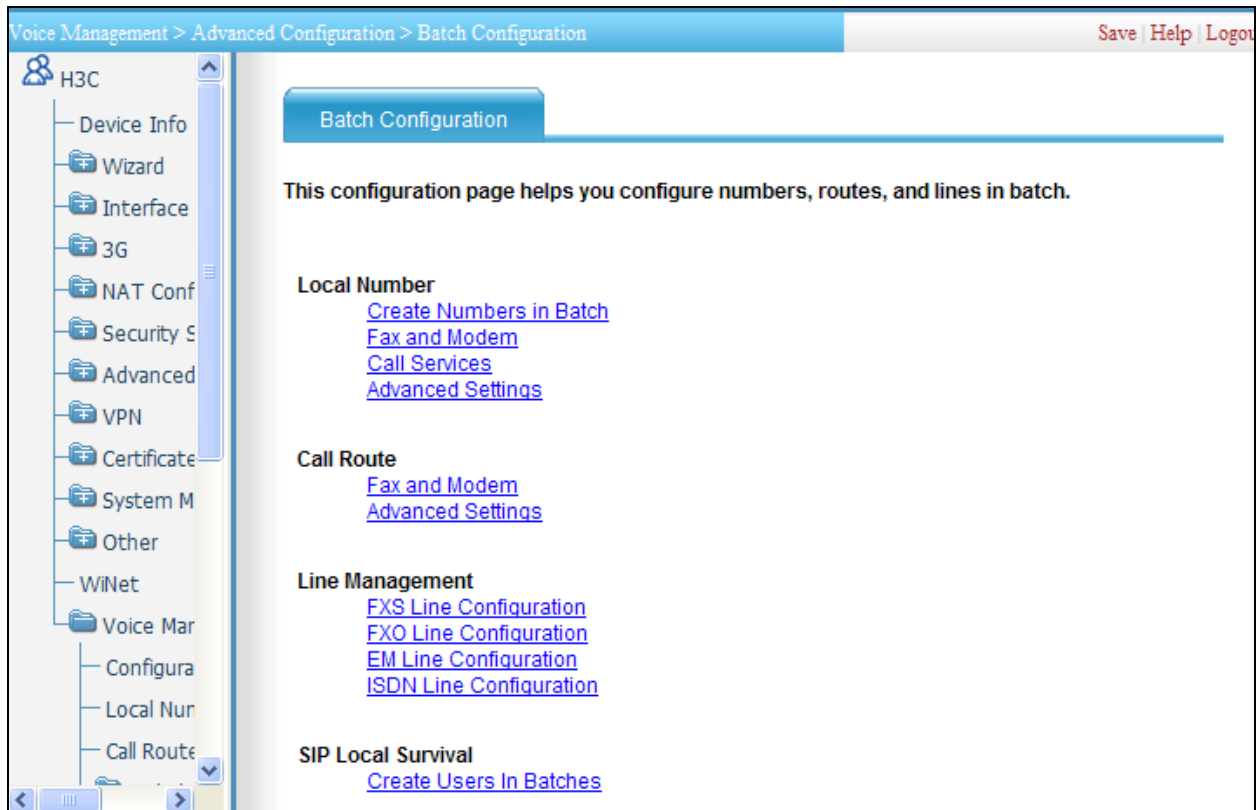
Click the **Apply** button.

The screenshot displays the 'Configure Route' configuration page in the H3C Voice Management interface. The left sidebar shows the navigation tree with 'Voice Management' expanded. The main content area contains the following fields and options:

- Call Route ID:** 10001 (Range: \*(10000-19999))
- Destination Number:** 7.... (Range: \*A string of 1 to 31 characters, supporting regular expressions.)
- Route Description:** to\_sip (Range: A string of 1 to 80 characters)
- Call Route Type:** ☒ SIP, ☐ Trunk
- SIP Routing:** ☐ Proxy Server, ☒ IP Routing, ☐ Binding Server Group
- Transport Layer Protocol for Call Route:** ☐ UDP, ☒ TCP, ☐ TLS
- URL Scheme for Call Route:** ☒ SIP, ☐ SIPS
- Destination Address:** 10.64.40.42 (IPv4 address or domain name with 1 to 255 Characters)
- Port:** 5060 (Range: 1-65535, System assigned by default)
- Server Group:** (Dropdown menu)
- Trunk Route Line:** (Dropdown menu)
- Register Function:** ☒ Enable, ☐ Disable
- Register Username:** (Text field) (Range: A string of 1 to 63 characters, case sensitive.)
- Register Password:** (Text field) (Range: A string of 1 to 16 characters, case sensitive.)
- Cnonce Name:** (Text field) (Range: A string of 1 to 50 characters, case sensitive, must be set together with username and password.)
- Realm Name:** (Text field) (Range: A string of 1 to 50 characters, case sensitive, must be set together with username and password.)
- Status:** ☒ Enable, ☐ Disable

## 6.4. Configure FXS Line

Navigate to **Voice Management** → **Advanced Configuration** → **Batch Configuration**. Select **Create Numbers in Batch** under the Local Number section.



Provide the following information:

- **Start Number** – Enter a unique extension.
- **Register Mode** – Select **No Username and No Password**.
- Move FXS lines from the **Available FXS Lines** folder to the **Selected FXS Lines** folder.

Click the **Apply** button.

Voice Management > Advanced Configuration > Batch Configuration Save Help Logout

**H3C**

- Device Info
- Wizard
- Interface Setup
- 3G
- NAT Configuration
- Security Setup
- Advanced
- VPN
- Certificate Management
- System Management
- Other
- WiNet
- Voice Management
  - Configuration Wizard
  - Local Number
  - Call Route
  - Dial Plan
  - Call Connection

**Create Numbers In Batch**

Start Number:  \*Chars.(1-31), which can only include digits in the range 0 to 9.

Register Mode:
 ☐ Username and Password are the Same as Number
 ☒ No Username and No Password
 ☐ Username and Password are Specified Uniformly

Register Username:  A string of 1 to 63 characters, case sensitive.

Register Password:  A string of 1 to 16 characters, case sensitive.

-----Selected FXS Lines-----

line8/0  
line8/1  
line8/2  
line8/3  
line8/4  
line8/5  
line8/6  
line8/7

<  
<<  
>  
>>

-----Available FXS Lines-----

Items marked with an asterisk(\*) are required

Apply Cancel

## 6.5. Configure FXO Line

In the MSR30, the FXO Subscriber Line 1/0<sup>1</sup> was connected to an FXS Analog circuit pack port (1A1101) in the Avaya G650 Media Gateway. The port **1A1101** is configured as type**2500** and used extension **22006**. All other values are default.

```

change station 22006                                     Page 1 of 4
                                STATION
Extension: 22006                                Lock Messages? n                BCC: 0
Type: 2500                                Security Code:                TN: 1
Port: 01A1101                                Coverage Path 1:            COR: 1
Name: FXS-1                                Coverage Path 2:            COS: 1
                                Hunt-to Station:            Tests? y

STATION OPTIONS
  XOIP Endpoint type: auto                Time of Day Lock Table:
  Loss Group: 1                            Message Waiting Indicator: none
  Off Premises Station? n

  Survivable COR: internal
  Survivable Trunk Dest? y
  
```

The following is the test scenario:

When a call comes into extension 22006, the analog (FXS) port sends battery current and ring voltage to the MSR30's FXO port. The FXO port then goes

<sup>1</sup> The MSR uses the following convention to identify ports: <Module Identifier>/<Port Identifier>. So Subscriber Line 1/0 refers to the module in slot 1 of the chassis and port 0 on the chassis. Users can refer to the HP chassis and module documentation (see References) in order to locate the physical port.



off-hook (loop closure). When the FXO port goes off-hook, it starts to listen for DTMF digits. After a pause, the FXS port starts sending the dialed extension as DTMF digits. The MSR30 utilizes call route table to connect to the destination's extension.

To check the status of all lines, navigate to **Voice Management → States and Statistics → Line States**.

Voice Management > States and Statistics > Line States

Save Help Logout

H3C

- Device Info
- Wizard
- Interface Setup
- 3G
- NAT Configuration
- Security Setup
- Advanced
- VPN
- Certificate Management
- System Management
- Other
- WiNet
- Voice Management
  - Configuration Wizard
  - Local Number
  - Call Route
  - Dial Plan
  - Call Connection
  - SIP Trunk Management
  - Digital Link Management
  - Line Management
  - SIP Local Survival
  - IVR Services
  - Advanced Configuration
  - States and Statistics
    - Line States

Line State Information

Search Name Search Advanced Search

Name	Type	Description	Subscriber Line Status	Details
subscriber-line1/0	FXO	subscriber-line1/0 Interface	UP	<a href="#">Details</a>
subscriber-line1/1	FXO	subscriber-line1/1 Interface	Physical Down	<a href="#">Details</a>
subscriber-line3/0:23	ISDN PRI	subscriber-line3/0:23 Interface	UP	<a href="#">Details</a>
subscriber-line5/0	FXO	subscriber-line5/0 Interface	Physical Down	<a href="#">Details</a>
subscriber-line5/1	FXO	subscriber-line5/1 Interface	Physical Down	<a href="#">Details</a>
subscriber-line5/2	FXO	subscriber-line5/2 Interface	Physical Down	<a href="#">Details</a>
subscriber-line5/3	FXO	subscriber-line5/3 Interface	Physical Down	<a href="#">Details</a>
subscriber-line8/0	FXS	subscriber-line8/0 Interface	UP	<a href="#">Details</a>
subscriber-line8/1	FXS	subscriber-line8/1 Interface	UP	<a href="#">Details</a>
subscriber-line8/2	FXS	subscriber-line8/2 Interface	UP	<a href="#">Details</a>
subscriber-line8/3	FXS	subscriber-line8/3 Interface	UP	<a href="#">Details</a>
subscriber-line8/4	FXS	subscriber-line8/4 Interface	UP	<a href="#">Details</a>
subscriber-line8/5	FXS	subscriber-line8/5 Interface	UP	<a href="#">Details</a>
subscriber-line8/6	FXS	subscriber-line8/6 Interface	UP	<a href="#">Details</a>
subscriber-line8/7	FXS	subscriber-line8/7 Interface	UP	<a href="#">Details</a>

## 7. Verification Steps

### 7.1. Capturing the MSR30's configuration and call debug logs

Use the following commands to document the current MSR30 configuration and develop data for troubleshooting:

- Access the MSR's command line
- Using your terminal application, log all information to a file. (Or, be prepared to copy a lot of data in the screen buffer)
- Type **"screen-length disable"** to disable paging
- Type **"display current-configuration"** and **"display voice entity all"** to capture the current configuration
- Type **"debug voice sip all"** to capture log information
- Enable sending debug messages to console, type: **"terminal debugging"** and **"terminal monitor"**
- Confirm that debug is on by typing: **"display debug"**... and you'll see that several SIP switches are on
- Place a call
- Capture all log data printed to the console window
- To return to normal operating mode, type **"undo debug voice sip all"**
- Re-Enable paging: **"undo screen-length disable"**

### 7.2. Verification from Avaya Aura® Communication Manager on PSTN side

The following commands can be used to check the status of the T1/PRI trunk:

- **"status trunk xx"**, where xx is a trunk group number. Ensure the trunk is **up**.
- **"list trace tac yy"**, where yy is a unique trunk access code.

## 7.3. Verification from Avaya Aura® Session Manager on Enterprise side

During the compliance test, the **traceSM** tool in Session Manager was utilized to capture the SIP signaling between Communication Manager (10.64.41.21), Session Manager (SM100) and the MSR30 (10.64.45.252). The following is a sample of the trace tool:

10.64.41.21	SM100	10.64.45.252
11:10:16,190	→PUBLISH→	(1) sips:72026@avaya.com
11:10:16,197	←200 OK←	(1) 200 OK (PUBLISH)
11:10:26,450	←INVITE←	(3) T:72001 F:22002 U:72001
11:10:26,452	→Trying→	(3) 100 Trying
11:10:26,462	←INVITE←	(3) T:72001 F:22002 U:72001 P:terminating
11:10:26,467	→Trying→	(3) 100 Trying
11:10:26,471	→Ringing→	(3) 180 Ringing
11:10:26,476	←Ringing←	(3) 180 Ringing
11:10:26,582	←PRACK←	(3) sip:72001@10.64.41.21
11:10:26,585	→200 OK→	(3) sip:72001@10.64.41.21
11:10:26,588	←200 OK←	(3) 200 OK (PRACK)
11:10:26,591	→200 OK→	(3) 200 OK (PRACK)
11:10:29,852	←200 OK←	(3) 200 OK (INVITE)
11:10:29,858	→200 OK→	(3) 200 OK (INVITE)
11:10:29,862	←ACK←	(3) sip:72001@10.64.41.21
11:10:29,865	→reINVIT→	(3) sip:72001@10.64.41.21
11:10:29,870	←Trying←	(3) sip:22002@10.64.45.252 F:72001 U:22002
11:10:29,871	→reINVIT→	(3) 100 Trying
11:10:29,875	←Trying←	(3) sip:22002@10.64.45.252 F:72001 U:22002
11:10:29,877	→200 OK→	(3) 100 Trying
11:10:29,879	←200 OK←	(3) 200 OK (INVITE)
11:10:29,882	→ACK→	(3) 200 OK (INVITE)
11:10:29,888	←ACK←	(3) sip:22002@10.64.45.252
11:10:29,891	→BYE→	(3) sip:22002@10.64.45.252
11:10:34,292	←BYE←	(3) sip:22002@10.64.45.252
11:10:34,295	→200 OK→	(3) sip:22002@10.64.45.252
11:10:34,298	←200 OK←	(3) 200 OK (BYE)
11:10:34,301	→200 OK→	(3) 200 OK (BYE)

## 8. Conclusion

These Application Notes describe the procedures required to configure an HP Networking Multi-Service Router 30 Series PSTN Gateway in an Avaya Telephony environment. The HP Networking Multi-Service Router 30 Series PSTN Gateway successfully passed compliance testing.

### Anomalies

The MSR30 does not support PSTN-side hold.
--

## 9. Additional References

Product documentation for Avaya products may be found at <http://support.avaya.com>

- [1] *Administering Avaya Aura™ Communication Manager*, Release 6.0, June 2010, Issue 6.0, Document Number 03-300509
- [2] *Administering Avaya Aura® Session Manager*, Release 6.1, November 2010, Issue 1.1, Document Number 03-603324
- [3] *Administering Avaya Aura® System Manager*, Release 6.1, November 2010

Product documentation for HP products may be found at <http://www.hp.com/networking>

- [4] *MSR Series Routers Web-Based Configuration Guide-Release 2207(V1.05)*[http://h3c.com/portal/Technical\\_Support\\_Documents/Technical\\_Documents/Routers/H3C\\_MSR\\_50\\_Series\\_Routers/Configuration/User\\_Manual/H3C\\_MSR\\_WCG-Release\\_2207\(V1.05\)](http://h3c.com/portal/Technical_Support_Documents/Technical_Documents/Routers/H3C_MSR_50_Series_Routers/Configuration/User_Manual/H3C_MSR_WCG-Release_2207(V1.05))
- [5] *MSR Series Routers Interface Module Manual(V1.07)*[http://h3c.com/portal/Technical\\_Support\\_Documents/Technical\\_Documents/Routers/H3C\\_MSR\\_50\\_Series\\_Routers/Installation/Installation\\_Manual/H3C\\_MSR\\_IMM\(V1.07\)](http://h3c.com/portal/Technical_Support_Documents/Technical_Documents/Routers/H3C_MSR_50_Series_Routers/Installation/Installation_Manual/H3C_MSR_IMM(V1.07))
- [6] *MSR 30 Routers Installation Guide(V1.05)*[http://h3c.com/portal/Technical\\_Support\\_Documents/Technical\\_Documents/Routers/H3C\\_MSR\\_30\\_Series\\_Routers/Installation/Installation\\_Manual/H3C\\_MSR\\_30\\_Routers\\_IG\(V1.05\)](http://h3c.com/portal/Technical_Support_Documents/Technical_Documents/Routers/H3C_MSR_30_Series_Routers/Installation/Installation_Manual/H3C_MSR_30_Routers_IG(V1.05))

---

**©2011 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 DevConnect Program at [devconnect@avaya.com](mailto:devconnect@avaya.com).