

Avaya Solution & Interoperability Test Lab

Configuring Avaya SIP Telephony with Cisco SIP Network Devices – Issue 2.0

Abstract

These Application Notes describe the administrative steps required to support Session Initiation Protocol (SIP) telephony using Avaya SIP Enablement Services and Avaya Communication Manager with Cisco SIP proxy, Network Address Translation (NAT), and PSTN gateway products. The sample network supports on-net (all SIP) and off-net (SIP/PSTN) calling.

These Application Notes are an updated and expanded version of the Application Notes entitled *Configuring SIP Call Routing among Avaya Converged Communications Server (CCS) and Cisco SIP Telephony Network Devices – Issue 1.0*.

©2006 Avaya Inc. All Rights Reserved.

1. Introduction

Enterprises and Service Providers are using the Session Initiation Protocol (SIP) protocol for telephony and other IP based services. Customers can also use SIP to interconnect their communication systems among multiple locations. Since many communications equipment manufacturers are now offering SIP compatible products, it is important to understand the functionality and configuration considerations involved in integrating various SIP-based products in the enterprise.

The Avaya SIP offer includes Avaya SIP Enablement Services (proxy, registrar, presence), a SIP-enabled Avaya Communication Manager (feature server, gateway), and Avaya 4600 Series IP Telephones. These Application Notes focus on using this subset of the Avaya SIP telephony offer with Cisco SIP infrastructure products that perform the following functions:

- Call routing to SIP telephones and T1 PRI gateways in a foreign domain.
- NAT by edge routers and firewalls.
- Call routing to a local T1 PRI gateway supported by the edge router.

The sample configuration used is shown in **Figure 1**. An enterprise with domain *companyx.com* contains a multi-home configuration of Avaya SIP Enablement Services, to which Avaya 4600 Series IP Telephones (SIP) and Cisco 7960 SIP telephones are registered. SIP trunks are configured between each home server and the Avaya S8300 Media Server with G700 Media Gateway. The Avaya S8300 Media Server with G700 Media Gateway also supports an Avaya 6408 Digital Telephone and an Avaya 4610 IP Telephone (H.323). An Avaya C363T-PWR Converged Stackable Switch provides all LAN connectivity. The Cisco 3825 router provides IP network connectivity to a simulated SIP service provider "cloud" with domain *sipsp.com*. This domain contains a Cisco SIP Proxy Server (CSPS) supporting Cisco SIP telephones. The Cisco AS5350 Voice Gateway is used for connectivity to the PSTN via a T1 PRI trunk to an Avaya DEFINITY® Server R. The Cisco 3825 router in *companyx.com* also provides local PSTN service via a T1 PRI trunk to the Avaya DEFINITY® Server R. Static and dynamic (Port) NAT are configured in the Cisco 3825 router and the Cisco PIX-515E firewall, resulting in the private/public address maps shown in **Table 1**.

These Application Notes focus on the administrative steps needed to configure the above SIP network elements to support the following types of calls in either direction:

- On-net calls between telephones in *companyx.com* and *sipsp.com.*
- Off-net calls between a telephone in *companyx.com* and the PSTN via *sipsp.com*.
- Off-net calls between a telephone in *companyx.com* and the PSTN via the local Cisco 3825 router.

©2006 Avaya Inc. All Rights Reserved.

Table 2 shows the network flow for these calls. The sample configuration also supports the following call features among combinations of the endpoints shown in **Figure 1**: hold, attended and unattended transfer, conference, and call forward. Refer to the appropriate Avaya product documentation for general telephone and server administration details (References [1-4]). See Reference [5] for Application Notes describing administration to support Cisco 7940/7960 SIP telephones in an Avaya SIP environment.

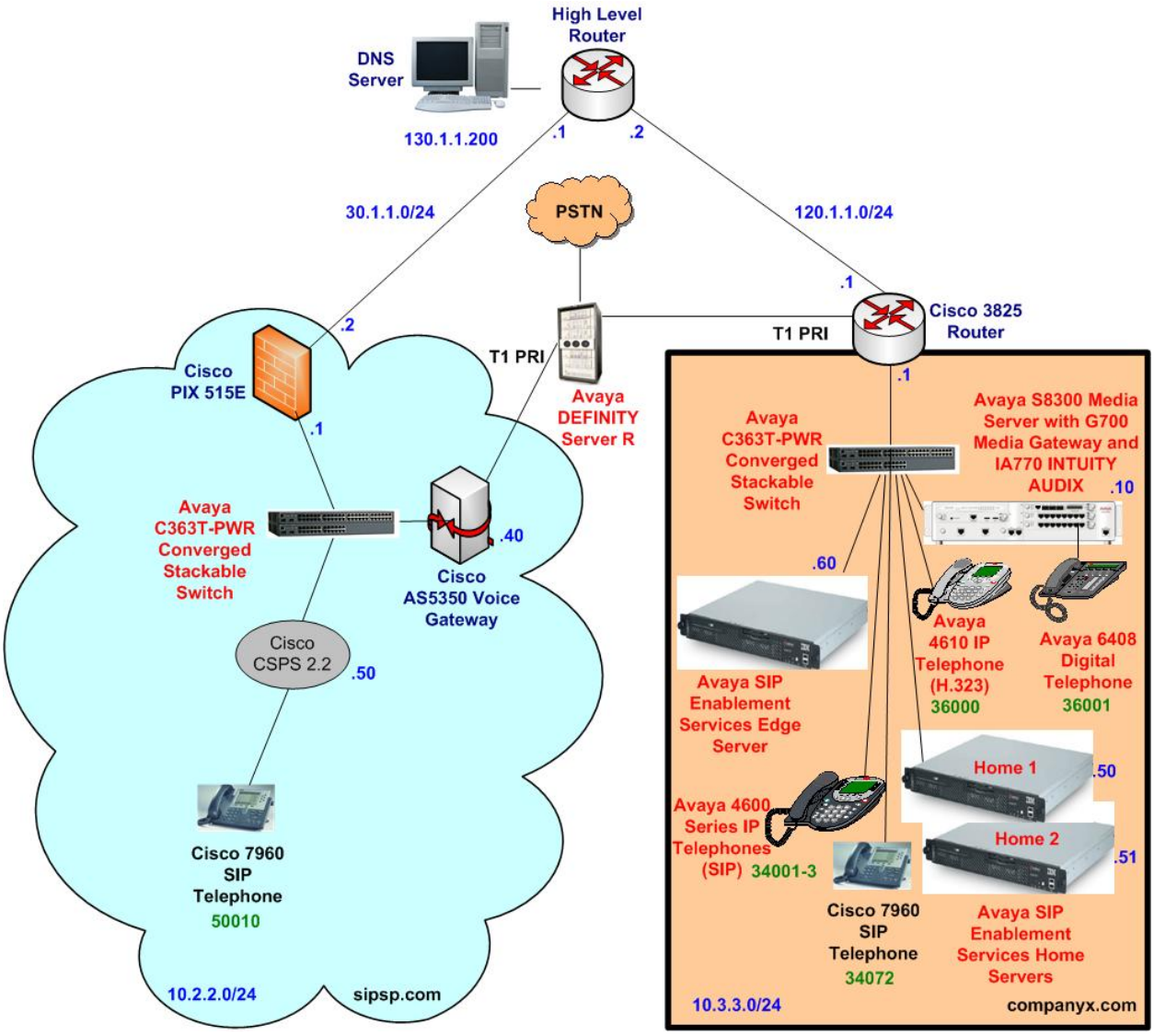


Figure 1: Sample Configuration for Avaya/Cisco SIP Call Routing

©2006 Avaya Inc. All Rights Reserved.

***Domain*/NAT Device**	**Device**	**Public**	**Private**	**NAT Type**
companyx.com/ Cisco 3825	IP telephones, Avaya G700 Media Gateway VoIP Engine (media)	120.1.1.3	10.3.3.x	Dynamic (PNAT)
	Avaya SIP Enablement Services Edge	120.1.1.4	10.3.3.60	Static
	Avaya SIP Enablement Services Home 1	120.1.1.5	10.3.3.50	Static
	Avaya SIP Enablement Services Home 2	120.1.1.6	10.3.3.51	Static
	Avaya S8300 Media Server (signaling)	120.1.1.7	10.3.3.10	Static
sipsp.com/ Cisco PIX-515E	IP telephones, Cisco AS5350 Voice Gateway (media)	30.1.1.5	10.2.2.x	Dynamic (PNAT)
	Cisco SIP Proxy Server	30.1.1.6	10.2.2.50	Static
	Cisco AS5350 Voice Gateway (signaling)	30.1.1.7	10.2.2.40	Static

Table 1: Public/Private Network Address Translation Mapping in Cisco

Destination Number	**Network Path →**								
From companyx.com									
5XXXX	Avaya SIP Enablement Services Home 2[1]	Cisco 3825 (router)	High Level Router	Cisco PIX	Cisco CSPS	SIP Telephones Registered to CSPS			
91733NNNXXXX	Avaya SIP Enablement Services Home 2[1,2]	Cisco 3825 (router)	High Level Router	Cisco PIX	Cisco CSPS	Cisco AS5350	Avaya Server R	PSTN	
91732NNNXXXX	Avaya SIP Enablement Services Home 1[1,2]	Cisco 3825 (router & gateway)	Avaya Server R	PSTN					
From sipsp.com									
3XXXX	Cisco CSPS	Cisco PIX	High Level Router	Cisco 3825	Avaya SIP Enablement Services Edge	Avaya SIP Enablement Services Home 1 or 2[1]	*companyx* Telephones		
From PSTN									
AAANN21234	Avaya Server R (digits sent: 21234)	Cisco 3825 (router & gateway)	Avaya SIP Enablement Services Edge	Avaya SIP Enablement Services Home 1[1]	Avaya 4600 Series IP Telephone (SIP) X.34001				
AAANN25678	Avaya Server R (digits sent: 25678)	Cisco AS5350	Cisco CSPS	Cisco PIX	High Level Router	Cisco 3825 (router)	Avaya SIP Enablement Services Edge	Avaya SIP Enablement Services Home 1[1]	Avaya 4600 Series IP Telephone (SIP) X.34002

Table 2: Network Flow for Off-Premises Calls To/From *companyx.com*

[1] For brevity, the standard SIP signaling between Avaya SIP Enablement Services home servers and Avaya Communication Manager running on the Avaya S8300 Media Server are not shown. See Section 3.2 for details.
[2] The "91" is removed by Avaya Communication Manager before routing to the next hop

©2006 Avaya Inc. All Rights Reserved.

2. Equipment and Software Validated

The equipment and software used for the sample configuration are show below in **Table 3**.

Equipment	Software
Avaya S8300 Media Server with G700 Media Gateway and IA770 INTUITY™ AUDIX®	Avaya Communication Manager 3.1 Load 628.6
Avaya SIP Enablement Services	3.1 (Load 18)
Avaya C363T-PWR Converged Stackable Switch	4.5.14
Avaya 4600 Series IP telephones (SIP)	2.2.2
Avaya 4610 IP telephone (H.323)	2.3
Avaya DEFINITY® Server R	Avaya Communication Manager 1.3
Cisco AS5350 Voice Gateway	IOS 12.4(7)
Cisco 7960 SIP Telephone	POS3-08-2-00
Cisco SIP Proxy Server (CSPS)	2.2.1.1
Cisco PIX 515E Firewall/NAT	IOS 7.1(2)
Cisco 3825 Router/Gateway/NAT ALG	C3825-IPVOICE-M, IOS 12.3(14)T7
PC (DNS server)	Microsoft Advanced Server 5.00.2195 SP 4

Table 3: Equipment and Software Versions

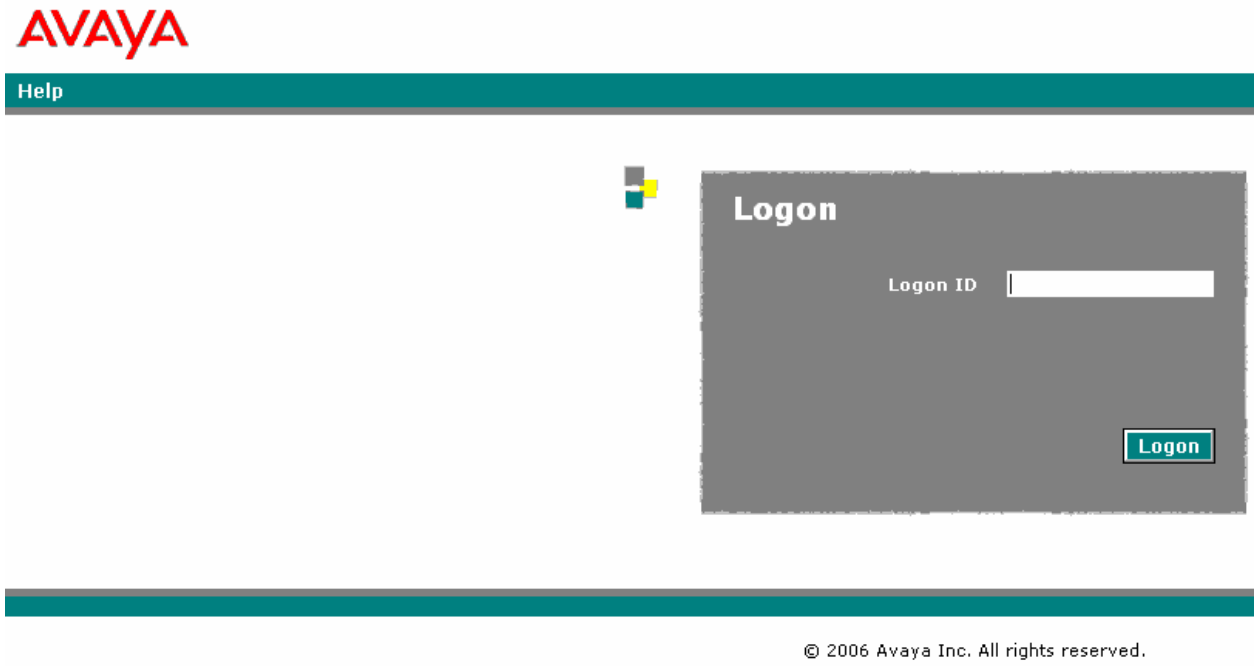
3. Configure Avaya SIP Enablement Services

3.1. Configure SIP Trunks

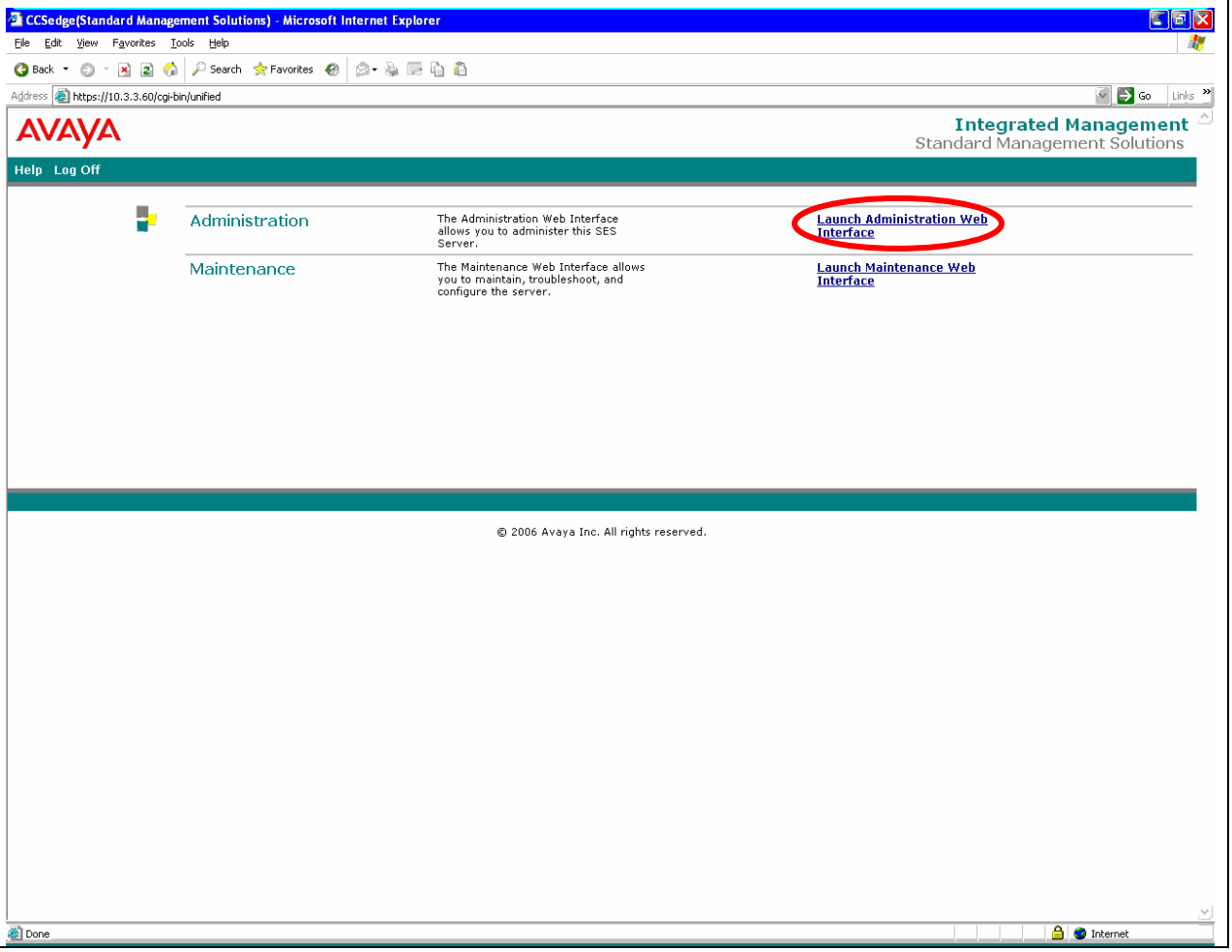
For Avaya Communication Manager to provide calling features to SIP telephones registered to Avaya SIP Enablement Services homes 1 and 2, SIP trunks must be configured between the S8300 Media Server with G700 Media Gateway and each home. The following shows the configuration steps for Avaya SIP Enablement Services. See Section 4 for configuration steps in Avaya Communication Manager.

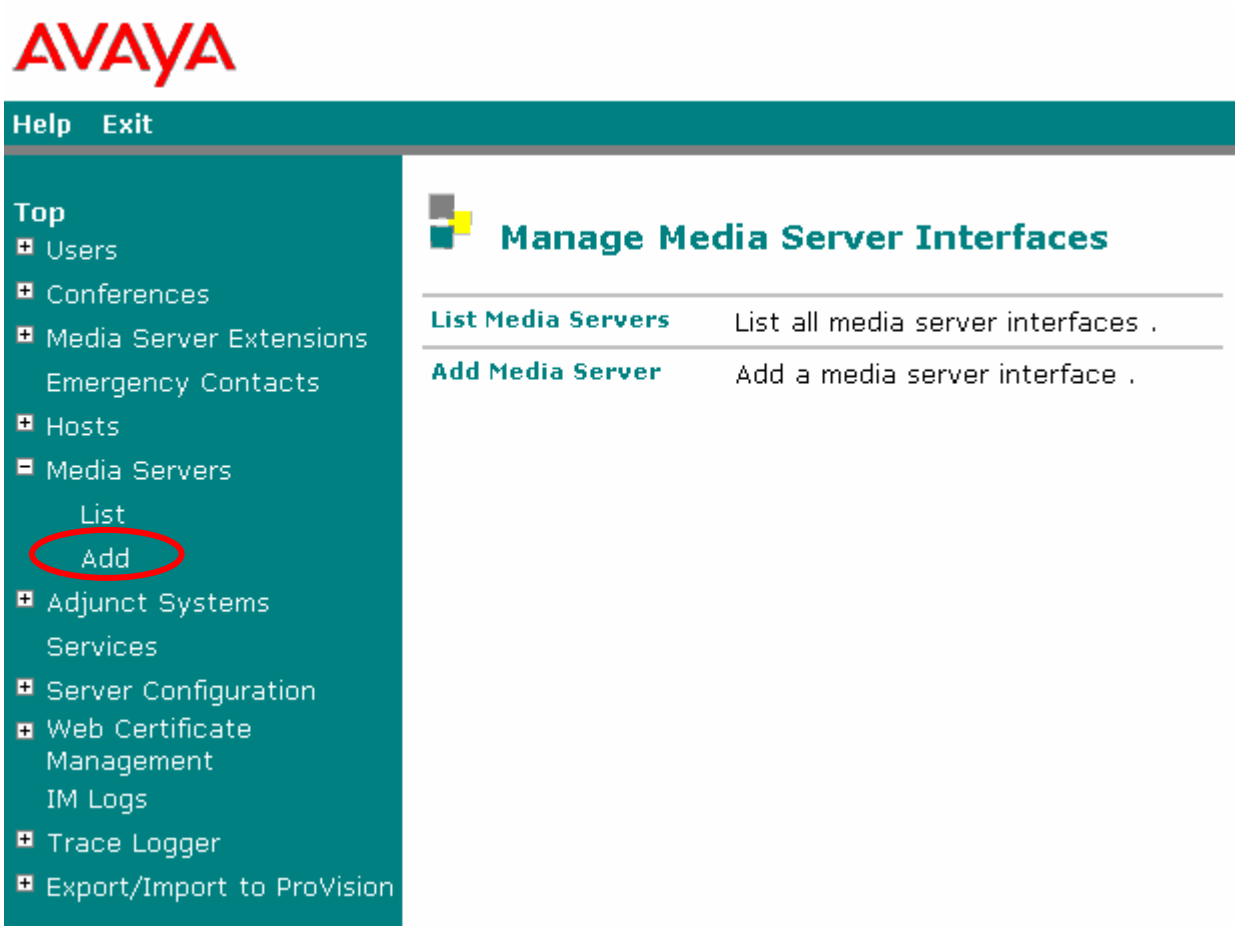
.

©2006 Avaya Inc. All Rights Reserved.

Steps	Description
1.	Avaya SIP Enablement Services is configured using a web browser. Set the URL of the browser to http://IP-address/admin, where *IP-address* is the IP address of the Avaya SIP Enablement Services Master Administrator server (the edge server in multi-home configurations), and log in with the proper credentials. 

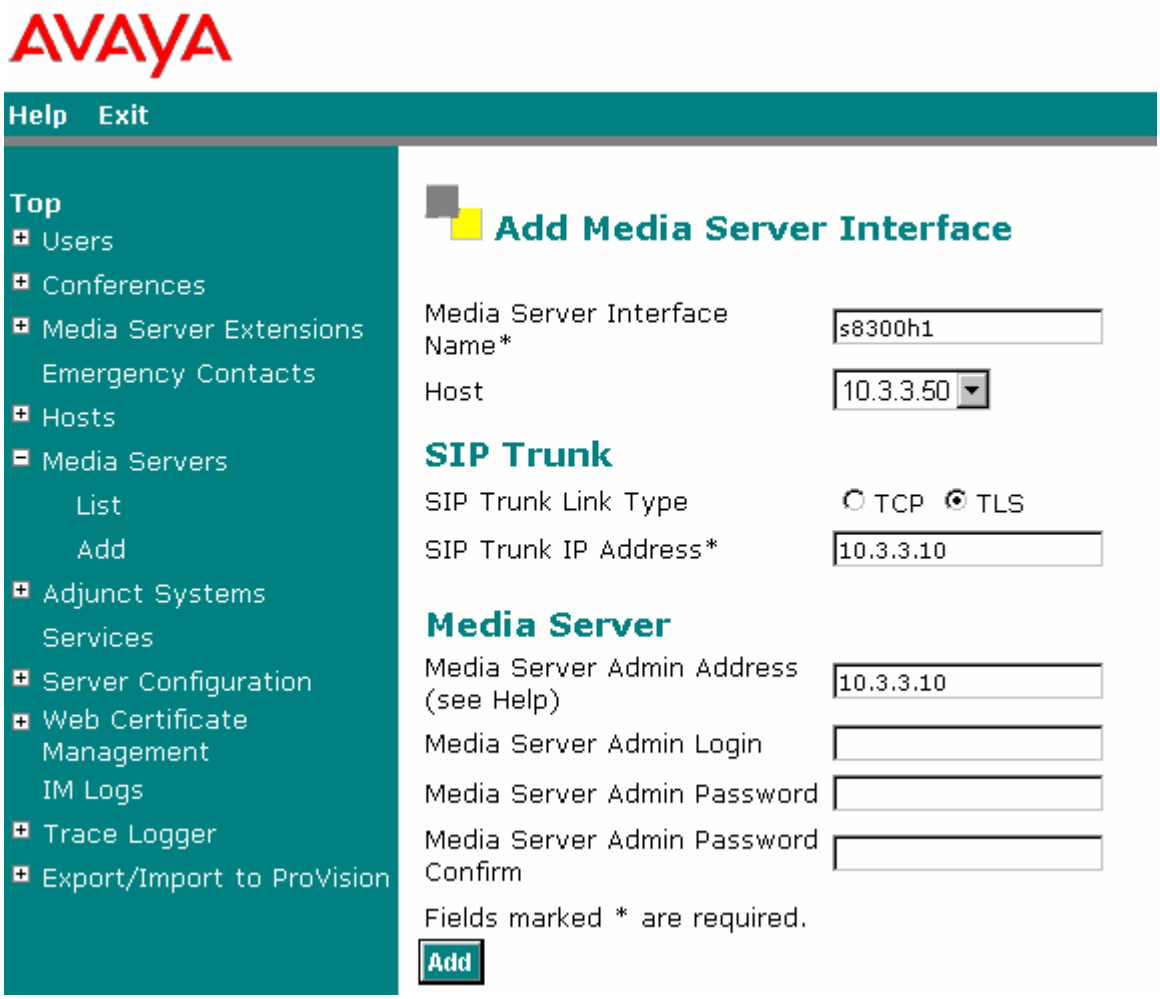
©2006 Avaya Inc. All Rights Reserved.

Steps	Description
2.	The main administration screen will be displayed after logging in. Click on **Launch Administration Web Interface.** 

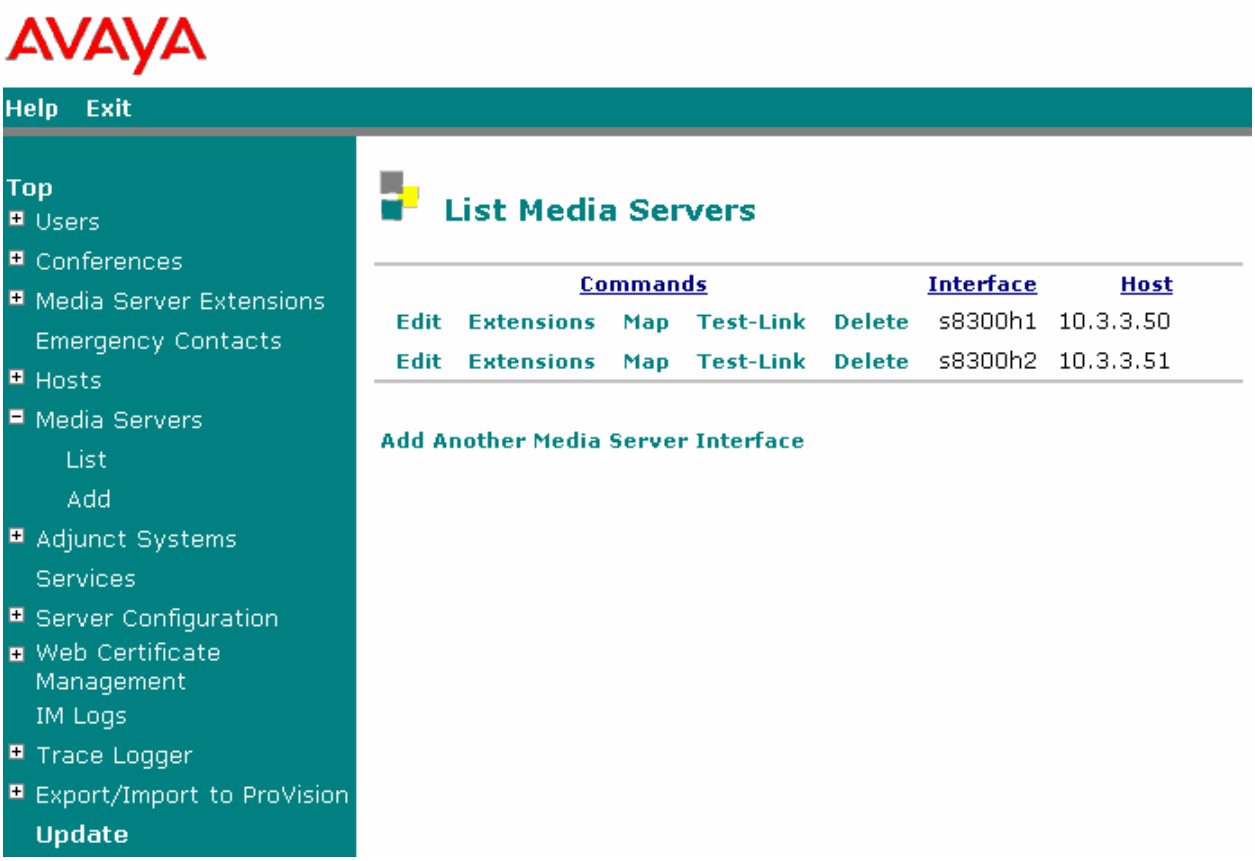
Steps	Description
3.	The Avaya SIP Enablement Services administration web interface will be displayed. Expand the **Media Servers** link on the left side of the page, and click on **Add**. 

©2006 Avaya Inc. All Rights Reserved.

Steps	Description
4.	On the *Add Media Server Interface* page, fill in the fields as shown. Create a **Media Server Interface Name** and select the **Host** IP address corresponding to the Avaya SIP Enablement Services home, in this case home 1. **SIP Trunk Link Type** is defaulted to *TLS*. For the sample configuration, the SIP trunk is connected to an Avaya S8300 Media Server, so the **SIP Trunk IP Address** and **Media Server Admin Address** will be the same. Enter the appropriate login and password credentials used for System Access Terminal administration sessions with Avaya Communication Manager. Click on **Add**. Then click **Continue** on the confirmation page.



©2006 Avaya Inc. All Rights Reserved.

Steps	Description
5.	Repeat the previous step to administer another SIP trunk from home 2 to Avaya Communication Manager. The SIP trunks should be displayed as shown below: 
6.	To apply the administration in the above steps, click on **Update** on the left side of the page. This link appears on the current page whenever updates are outstanding, and can be used at any time to save the administration performed to that point.

3.2. Configure Call Routing

3.2.1. Outbound Calls

See **Figure 2** for a high level view of the call routing process for SIP calls to remote destinations. Avaya SIP Enablement Services will always route call requests (INVITEs) from registered SIP telephones to Avaya Communication Manager for dial plan analysis and origination/termination services[3]. Avaya Communication Manager then routes the INVITE back to Avaya SIP Enablement Services for further routing to the next hop. Next hop routing can be administered

[3]To obtain these services, a Media Server Extension should always be defined for a SIP telephone user in Avaya SIP Enablement Services. See References [1] and [5].

©2006 Avaya Inc. All Rights Reserved.

in two ways. If the domain supplied in the request URI of the INVITE message sent by Avaya Communication Manager is the home domain (*companyx.com* in this case), routing must be based on the dialed number and is configured via address maps. If the supplied domain is a foreign SIP domain, next hop routing will be based on a DNS lookup of the foreign domain name. Avaya Communication Manager can be administered to determine the domain based on dial plan and routing rules.

In the sample configuration, remote destinations include SIP telephones hosted by the Cisco CSPS proxy in *sipsp.com*, PSTN destinations accessed via the Cisco CSPS and AS5350 Voice Gateway in *sipsp.com*, and PSTN destinations accessed via the local Cisco 3825 router/gateway in *companyx.com*. Calls for the first two cases are routed to the next hop by Avaya SIP Enablement Services based on DNS lookup for the host associated with domain *sipsp.com*[4], so no further configuration is necessary. Since calls for the third case are within the same *companyx.com* domain, next hop routing is via an address map based on the dialed number[5]. This section describes administration of the address map. See Section 4 for how to administer Avaya Communication Manager to use foreign domain routing.

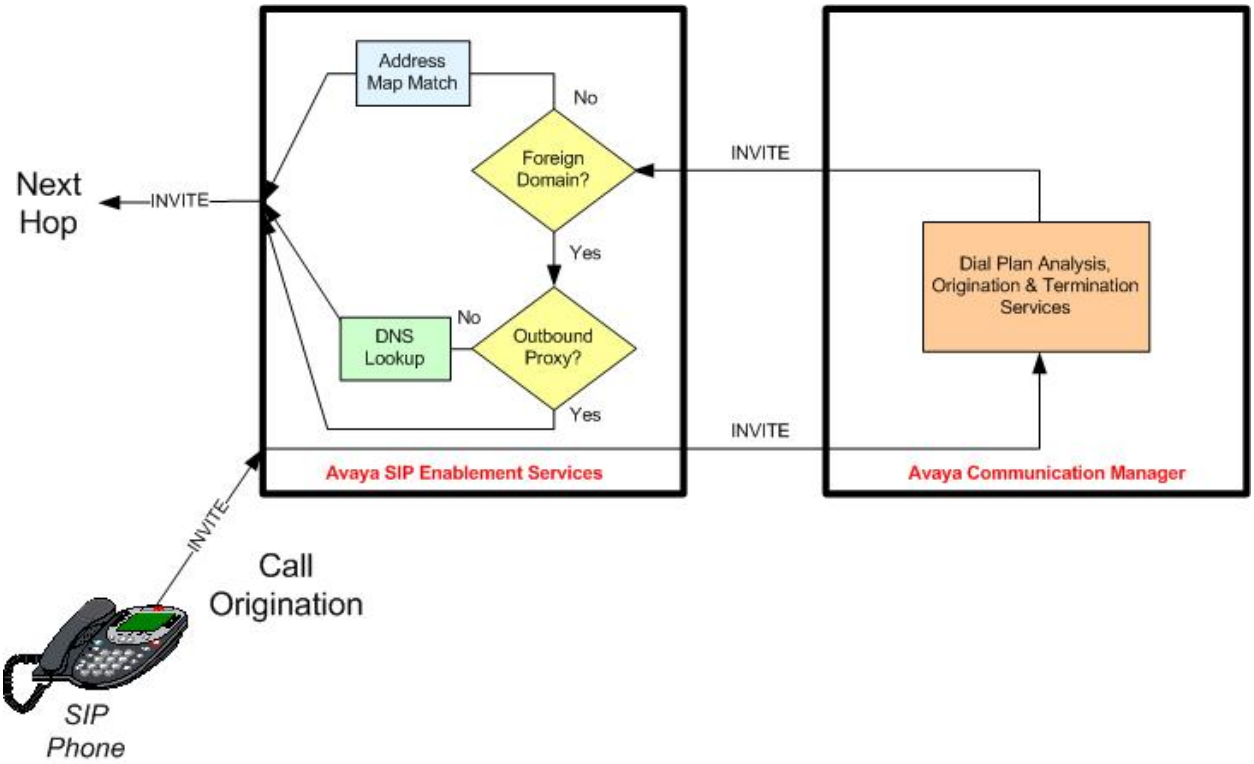


Figure 2 – High Level View of SIP Call Routing for Remote Destinations

[4] If an Outbound Proxy is configured in Avaya SIP Enablement Services, the DNS lookup step is skipped and the INVITE is routed directly to that proxy.

[5] Foreign domain routing could also be implemented based on dialed number, but the domain lookup method permits dial plan information to be centralized in Avaya Communication Manager rather than distributed in both Avaya Communication Manager and Avaya SIP Enablement Services.

©2006 Avaya Inc. All Rights Reserved.

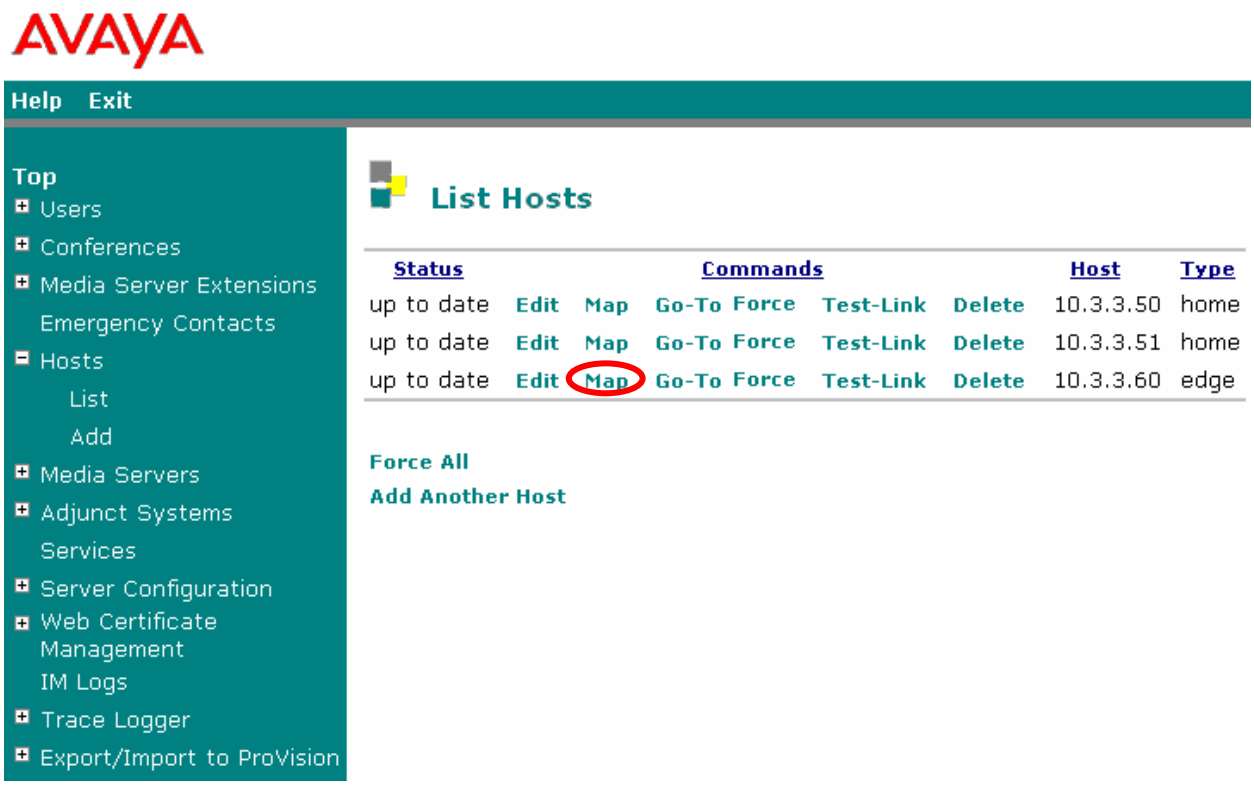
Call routing to the PSTN via the Cisco 3825 is configured on Avaya SIP Enablement Services by means of an *address map*, which specifies one or more dial strings to be matched and the SIP destination to which the call is to be routed if a match is found. In the sample configuration, PSTN numbers with area code 732 will be routed to the Cisco 3825 router/gateway.

Steps	Description
1.	Expand the **Hosts** link on the left side of the main administration page, and then click on **List**.

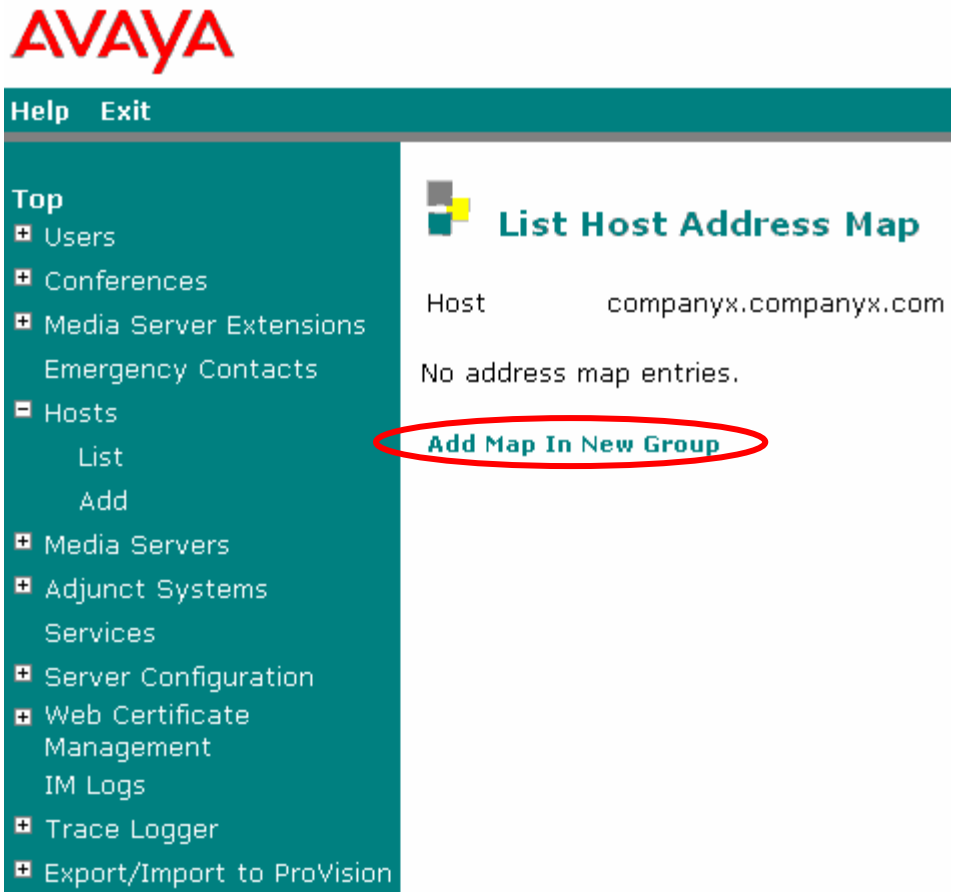


©2006 Avaya Inc. All Rights Reserved.

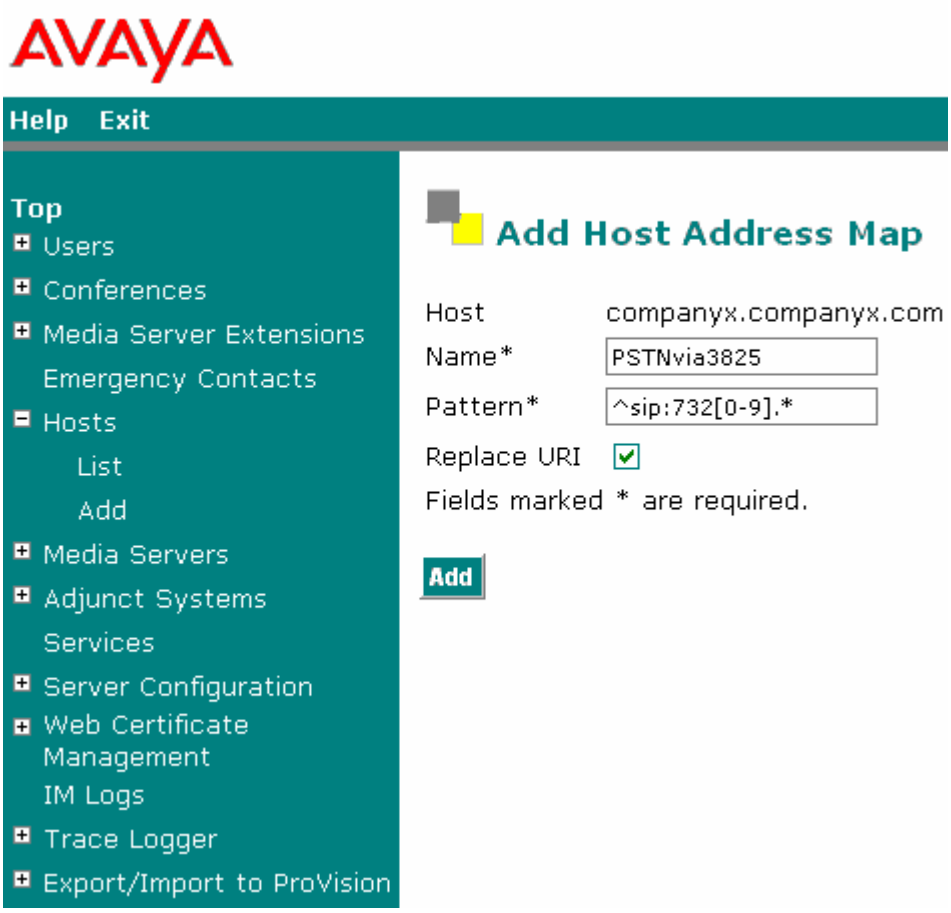
Steps	Description
2.	The existing home and edge servers will be displayed. The address map will be defined once for the edge server, and will be active in all home servers when they route calls. In the row corresponding to the edge server, click on **Map** under *Commands*.



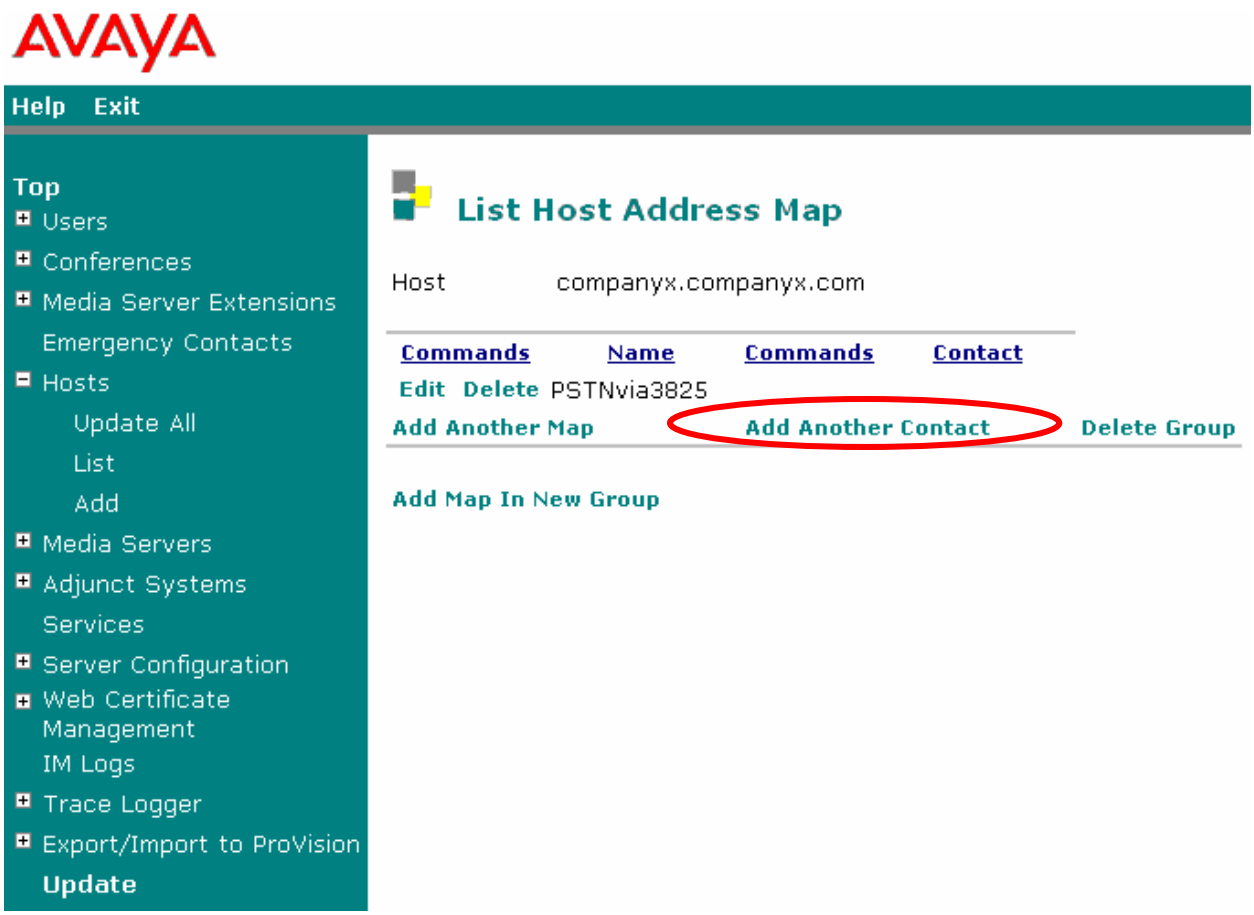
©2006 Avaya Inc. All Rights Reserved.

Steps	Description
3.	The *List Host Address Map* page is displayed. Click on **Add Map in New Group**. 

©2006 Avaya Inc. All Rights Reserved.

Steps	Description
4.	The *Add Host Address Map* page will be displayed. Specify a **Name** for the address map, and the **Pattern** match specification. In the sample configuration, PSTN telephone numbers with area code 732 are to be routed to the local Cisco 3825 router/gateway. The pattern match specification is applied to the Uniform Resource Identifier (URI) field of incoming INVITE messages. The URI usually takes the form sip:user@domain, where *domain* can be a domain name or an IP address. In the sample configuration, *user* is actually the telephone number of the phone. An example of a URI sent by a local SIP telephone would be sip:7321234567@companyx.com. The specification below means "match on the characters 'sip:732' if they occur at the beginning of the URI, followed by any number of characters in the range 0 through 9." See Section 13 for a more detailed description of the syntax for address map patterns. Check **Replace URI** (default). When routing the incoming INVITE, Avaya SIP Enablement Services will replace the URI with the URI specified in the contact (see Step 6). Click on **Add**; then click on **Continue** on the confirmation page. 

©2006 Avaya Inc. All Rights Reserved.

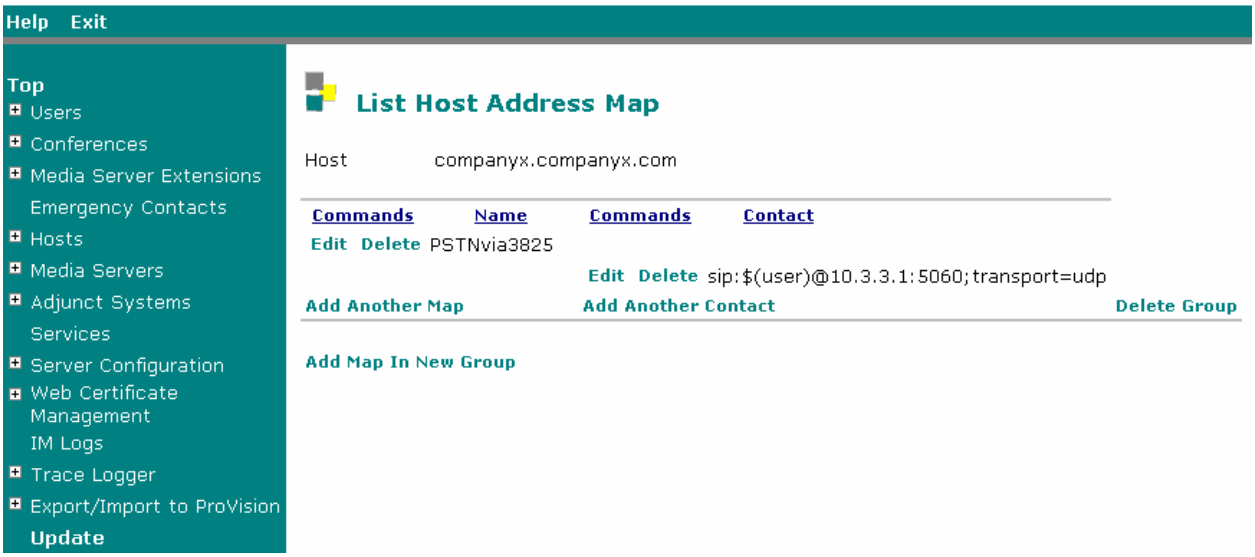
Steps	Description
5.	The current host address map list is displayed. To specify the routing for the address map just defined, click on **Add Another Contact**. 

©2006 Avaya Inc. All Rights Reserved.

Steps	Description
6.	Fill in the **Contact** field as shown. In this case, the IP address and port number used by the Cisco 3825 router/gateway are specified, as well as the transport protocol used to send SIP signaling messages.[6] Avaya SIP Enablement Services will substitute "$(user)" with the user field (i.e., the dialed number) in the incoming INVITE message. Click on **Add**; then click on **Continue** on the confirmation page. 

[6] If DNS is configured for the system with the port number and transport protocol of the destination proxy, Avaya SIP Enablement Services will automatically retrieve this information based on the domain name, and these fields need not be included. In this case, the contact would be "sip:$(user)@proxydomain".

©2006 Avaya Inc. All Rights Reserved.

Steps	Description
7.	The *List Host Address Map* page is then displayed with the updated contact information. This completes configuration of the host address map for routing calls to the Cisco 3825 router/gateway. 

8.	All SIP proxies/gateways to which calls can be routed should be administered as *trusted hosts* in each of the Avaya SIP Enablement Services servers. This will permit far-end call clearing and other supplementary call service requests by remote parties to be handled without authentication challenges. This is performed at the Linux Command Line Interface (CLI) of the edge server (or edge/home if only one server is used). Use the standard methods to telnet to the edge server, and log in with the proper credentials. The format of the **`trustedhost`** command is:
	
	`trustedhost –a host –n server –c comment`
	
	For the sample configuration, the following **`trustedhost`** commands are executed:
	
	`trustedhost –a 10.3.3.1 –n 10.3.3.60 –c Cisco 3825 (Edge)`
	`trustedhost –a 10.3.3.1 –n 10.3.3.50 –c Cisco 3825 (Home 1)`
	`trustedhost –a 10.3.3.1 –n 10.3.3.51 –c Cisco 3825 (Home 2)`
	`trustedhost –a 30.1.1.6 –n 10.3.3.60 –c Cisco Proxy (Edge)`
	`trustedhost –a 30.1.1.6 –n 10.3.3.50 –c Cisco Proxy (Home 1)`
	`trustedhost –a 30.1.1.6 –n 10.3.3.51 –c Cisco Proxy (Home 2)`
	`trustedhost –a 30.1.1.7 –n 10.3.3.60 –c Cisco AS5350 (Edge)`
	`trustedhost –a 30.1.1.7 –n 10.3.3.50 –c Cisco AS5350 (Home 1)`
	`trustedhost –a 30.1.1.7 –n 10.3.3.51 –c Cisco AS5350 (Home 2)`

©2006 Avaya Inc. All Rights Reserved.

Steps	Description
9.	To apply the administration in the above steps, *including Step 8*, click on **Update** on the left side of the page on the web browser interface. This link appears on the current page whenever updates are outstanding, and can be used at any time to save the administration performed to that point.

3.2.2. Inbound Calls

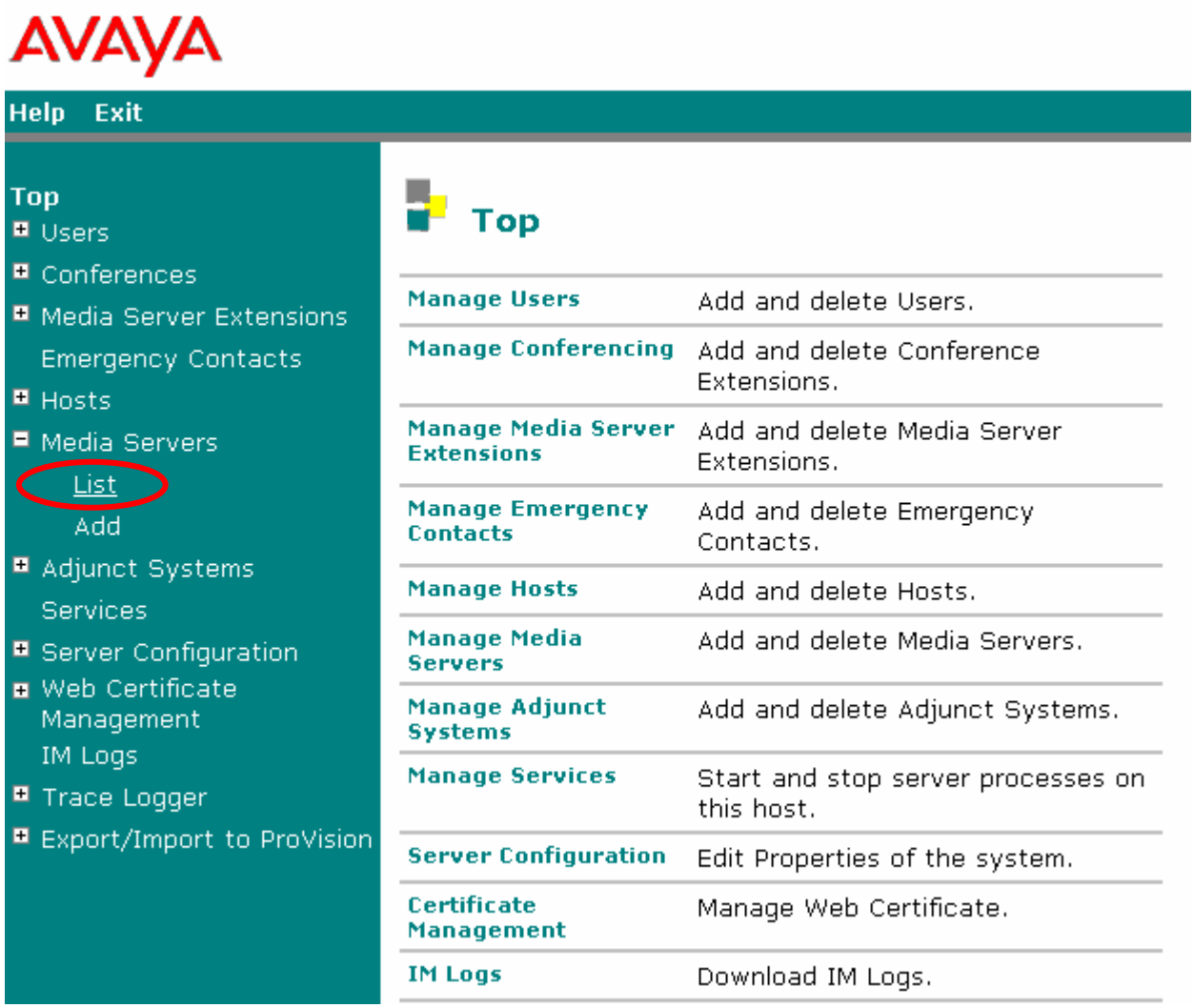
Inbound calls to *companyx.com* users who have been administered in Avaya SIP Enablement Services are automatically routed to Avaya Communication Manager for call termination services. There are however two cases in which users may not be defined in Avaya SIP Enablement Services:

1. Based on the DID number dialed, calls from remote PSTN destinations to telephones within *companyx.com* are routed through the Cisco AS5350 or 3825 PSTN/SIP gateways, Avaya SIP Enablement Services, and Avaya Communication Manager, in that order. In the sample configuration, two DID numbers are mapped to specific SIP extensions in *companyx*.com. The gateways receive the last 5 digits of the DID number (2xxxx) from the Avaya DEFINITY® Server R on the T1 PRI interface, and send them in the SIP INVITE message to the Avaya SIP Enablement Services edge server. By means of a media server address map defined for one of the home servers, the INVITE is then routed to that home server and then over the SIP trunk to Avaya Communication Manager, where the digits are mapped to a specific SIP extension (see Section 4.2.2).
2. Extension-to-extension calls from SIP telephones in *sipsp.com* to non-SIP telephones in *companyx.com* must be routed to Avaya Communication Manager. This can be achieved by the normal user and media server extension administration documented in Reference [1]. For large numbers of such non-SIP telephone users, a media server address map is a more efficient way to configure this routing.

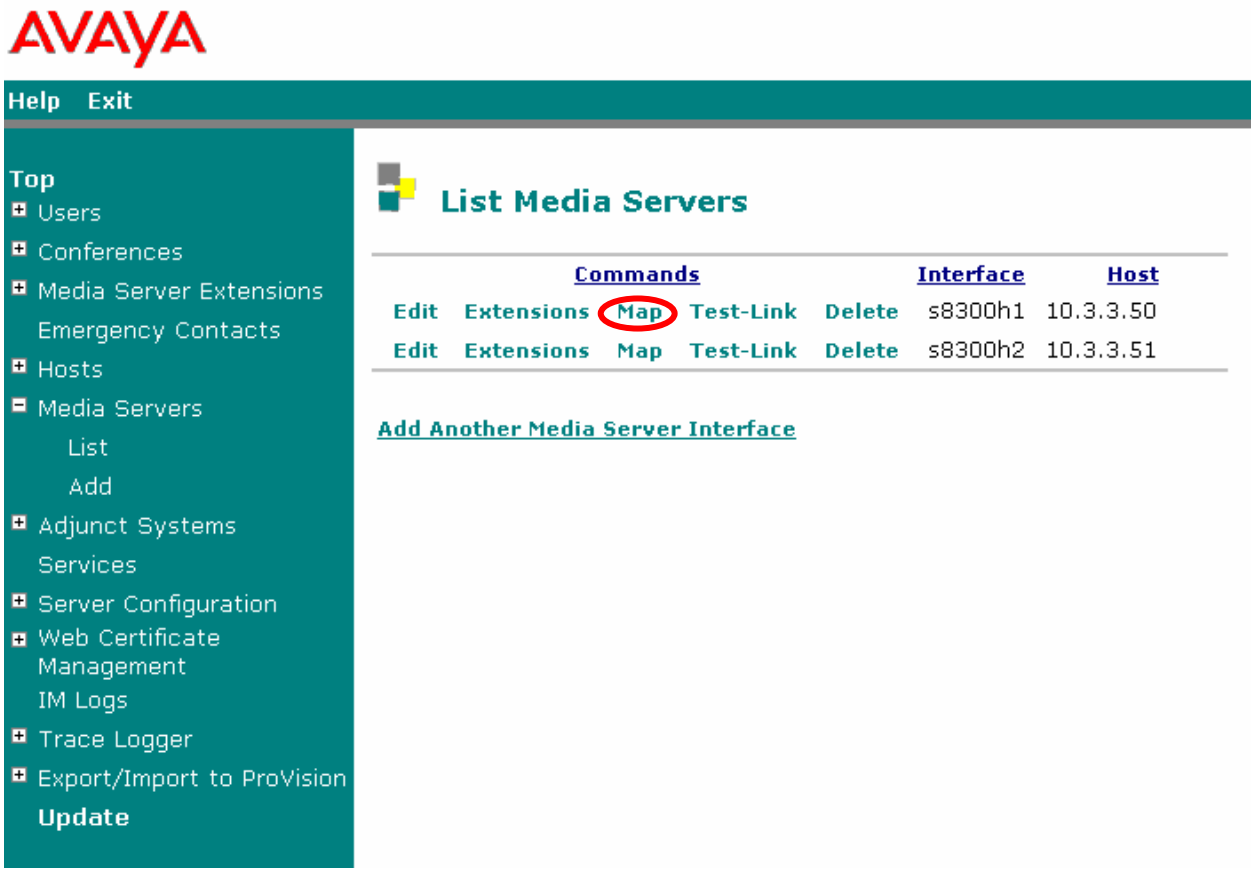
This section describes the steps for creating a media server address map in Avaya SIP Enablement Services to implement routing for the above two cases.

©2006 Avaya Inc. All Rights Reserved.

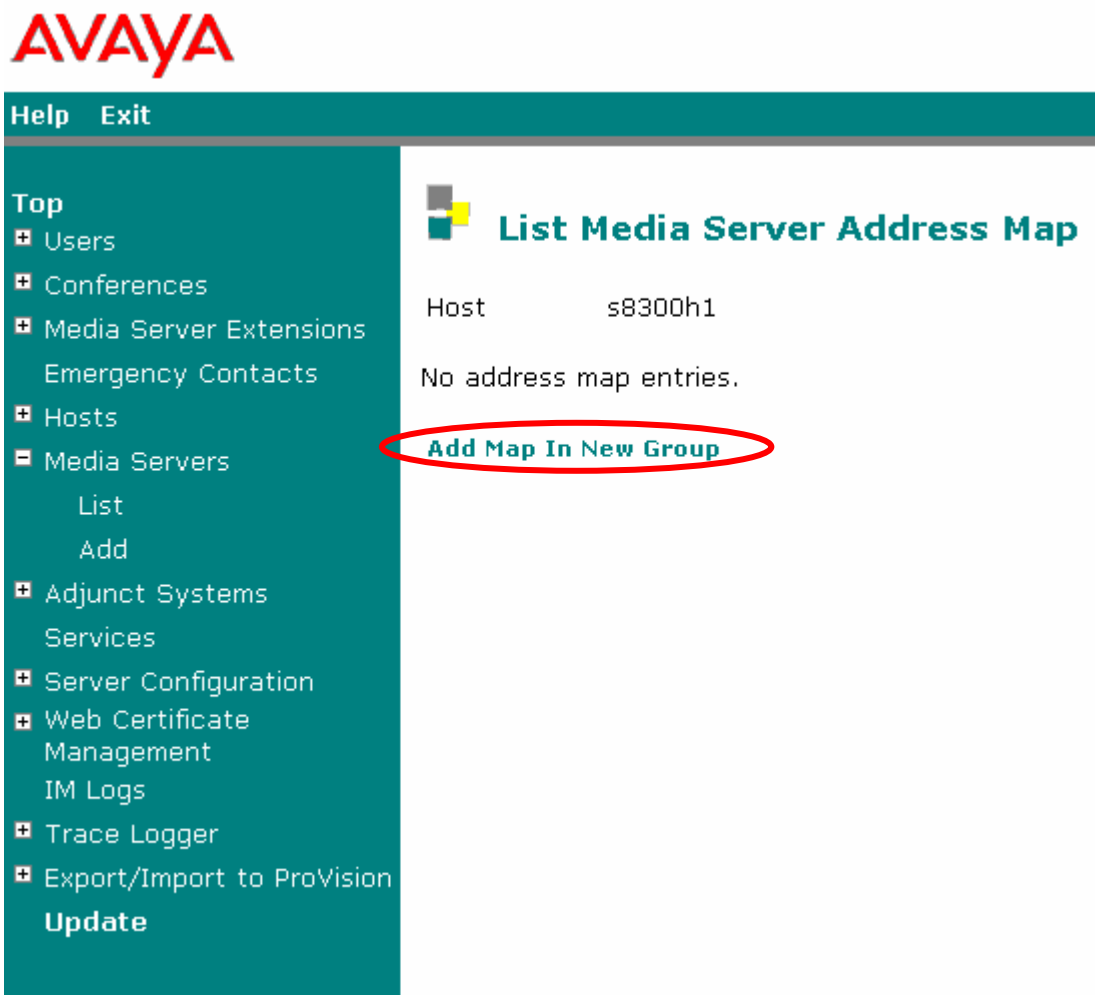
Steps	Description
1.	Expand the **Media Servers** link on the left side of the main administration page, and select **List**.



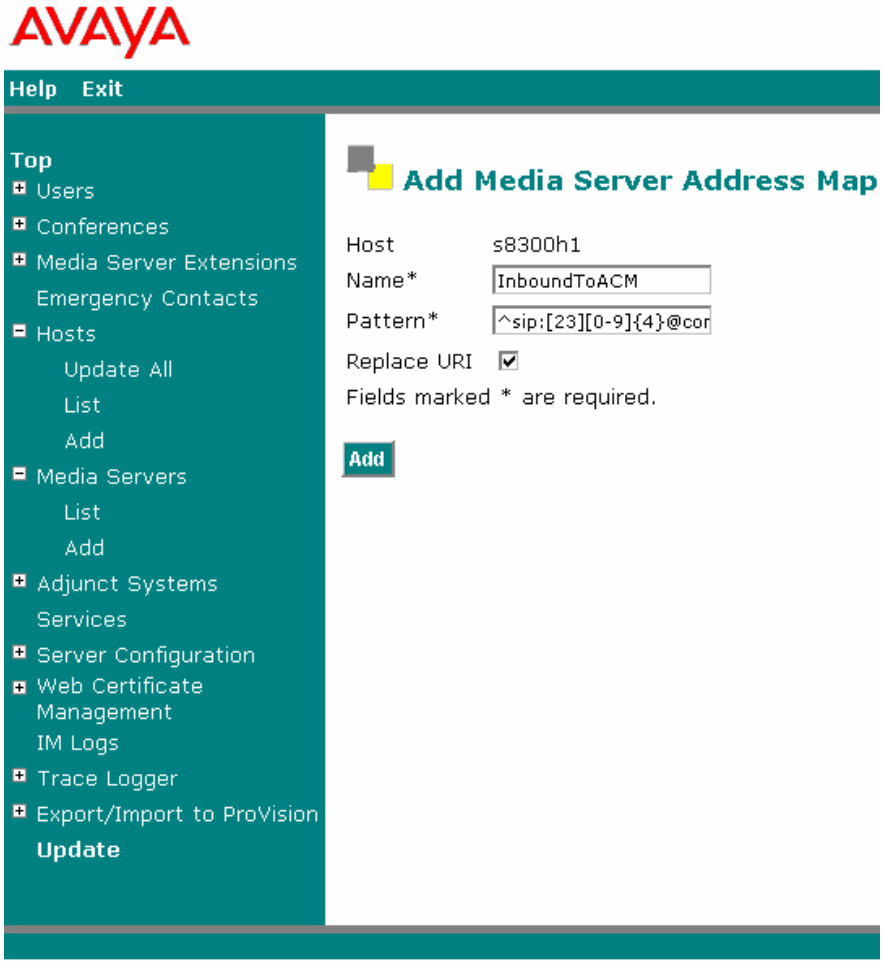
©2006 Avaya Inc. All Rights Reserved.

Steps	Description
2.	The existing media servers will be displayed. In the row corresponding to either one of the media servers, click on **Map** under *Commands*. Inbound calls to non-SIP telephone extensions will be directed to the SIP trunk corresponding to the media server for which the address map is defined. In the sample configuration, since the media servers define SIP trunks from each home to the same Avaya Communication Manager, the address map can be defined under either media server. If each home had a SIP trunk to a different Avaya Communication Manager, then two separate address maps (one per media server) would be required to cover the routing. 

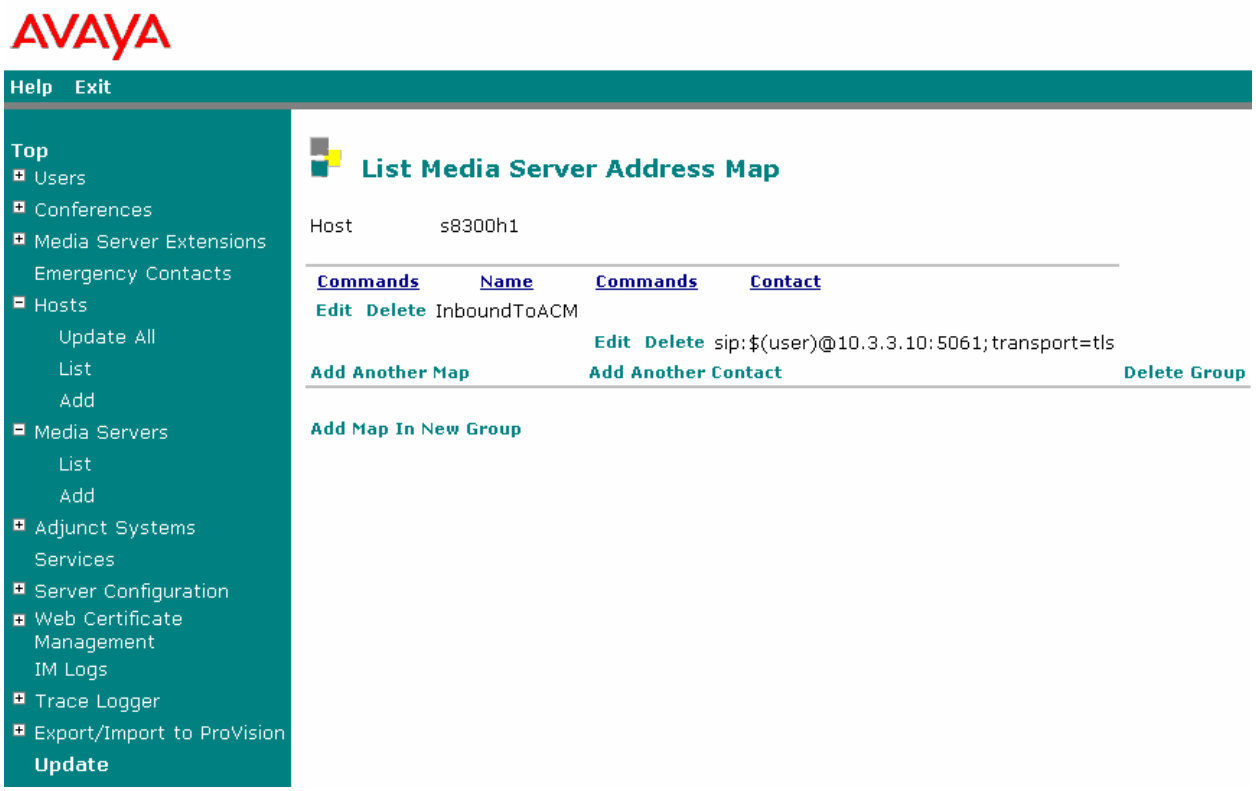
©2006 Avaya Inc. All Rights Reserved.

Steps	Description
3.	The *List Media Server Address Map* page is displayed for that media server. Click on **Add Map in New Group**. 

©2006 Avaya Inc. All Rights Reserved.

Steps	Description
4.	The *Add Media Server Address Map* page will be displayed. Specify a **Name** for the address map, and the **Pattern** match specification. The pattern match specification is applied to the Uniform Resource Identifier (URI) field of incoming INVITE messages. The URI usually takes the form sip:user@domain, where *domain* can be a domain name or an IP address. In the sample configuration, *user* is the telephone number. Examples of the URIs for a Type 1 call would be sip:21234@companyx.com (via the Cisco 3825) and sip:25678@companyx.com (via the Cisco AS5350). An example of a Type 2 call would be sip:36001@companyx.com, where extension 36001 is the Avaya 6408 Digital Telephone. The specification below covers both call types, and means "match on the characters 'sip:' if they occur at the beginning of the URI, followed by either a 2 or a 3, followed by 4 characters in the range 0 through 9, followed by '@companyx.com'". See Section 13 for a more detailed description of the syntax for address map patterns. Check **Replace URI** (default). When routing the incoming INVITE, Avaya SIP Enablement Services will replace the URI with the URI specified in the contact (see Step 5). Click on **Add**, then **Continue** on the confirmation page. 

©2006 Avaya Inc. All Rights Reserved.

Steps	Description
5.	The new media server address map list is displayed. The contact for the media server is automatically added. 
6.	To apply the administration in the above steps, click on **Update** on the left side of the page. This link appears on the current page whenever updates are outstanding, and can be used at any time to save the administration performed to that point.

4. Configure Avaya Communication Manager

The following sections describe how to configure call routing in Avaya Communication Manager for the sample configuration. Other aspects of SIP administration can be found in Reference [2].

4.1. Configure SIP trunks

This section describes how to configure the SIP trunks that communicate with those defined for Avaya SIP Enablement Services in Section 3. It also shows how to configure a SIP trunk that will use a foreign domain when routing outbound calls. The following commands are to be executed at the System Access Terminal.

©2006 Avaya Inc. All Rights Reserved.

4.1.1. Verify System Capacity

First, verify that an adequate number of SIP trunk members are administered for the system using the **change system-parameters customer-options** command. Note that one trunk group member is consumed for each SIP endpoint on a call, so that the maximum number of simultaneous SIP-SIP calls supported is equal to half the total number of members (two members per call), whereas SIP-H.323 or SIP-digital calls only consume one trunk member per call.

```
change system-parameters customer-options                       Page   2 of  10
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                              USED
                     Maximum Administered H.323 Trunks: 5       0
           Maximum Concurrently Registered IP Stations: 5       1
             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: 5       0
                 Maximum Video Capable H.323 Stations: 0       0
                  Maximum Video Capable IP Softphones: 5       0
                      Maximum Administered SIP Trunks: 100     0

   Maximum Number of DS1 Boards with Echo Cancellation: 0       0
                            Maximum TN2501 VAL Boards: 0       0
                    Maximum G250/G350/G700 VAL Sources: 5       1
           Maximum TN2602 Boards with 80 VoIP Channels: 0       0
          Maximum TN2602 Boards with 320 VoIP Channels: 0       0
   Maximum Number of Expanded Meet-me Conference Ports: 0       0

         (NOTE: You must logoff & login to effect the permission changes.)
```

4.1.2. Define Codec Sets

Define the audio codec sets to be used for calls within and outside *companyx.com*. In the sample configuration, local calls and outbound calls that use the local Cisco 3825 router as a PSTN gateway will use G.711 mu-law. Codec set 1 will be defined for this purpose. It is assumed that there are bandwidth limitations for calls to the *sipsp.com* domain. Such calls should attempt to use G.729, with G.711 as a secondary choice, comprising codec set 2. Use the **change ip-codec-set** command to define these two codec sets. Default values can be used for Page 2.

©2006 Avaya Inc. All Rights Reserved.

```
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:
```

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

                         IP Codec Set

   Codec Set: 2

   Audio        Silence      Frames   Packet
   Codec        Suppression  Per Pkt  Size(ms)
 1: G.729            n          2        20
 2: G.711MU          n          2        20
 3:
```

4.1.3. Verify Near End IP Network Region

Use the **change ip-interface procr** command to verify/set the IP network region of the S8300 Media Server. This can be viewed as the near-end network region, and is usually defaulted to region 1. This region will be used for all local calls within *companyx.com*.

```
change ip-interface procr                                      Page   1 of   1
                                 IP INTERFACES

                  Type: PROCR

             Node Name: procr
            IP Address: 10 .3  .3  .10
           Subnet Mask: 255.255.255.0

  Enable Ethernet Port? y                       Allow H.323 Endpoints? y
        Network Region: 1                        Allow H.248 Gateways? y
                                                   Gatekeeper Priority: 5

                    Target socket load: 1700
```

4.1.4. Define IP Network Regions

Define IP network region 1 using the **change ip-network-region** command. On Page 1, set the **Authoritative Domain** to be the same as that administered in Avaya SIP Enablement Services. The **Name** field can be set to a meaningful value. On Page 3, enter the codec sets to be used for local calls within region 1, and for calls to region 2. Although not

©2006 Avaya Inc. All Rights Reserved.

shown here, note that specific call access control limits can be imposed on inter-region calling, and can enforce bandwidth limitations. See Reference [3] for more details. IP network region 2 will be used as the far end network region for calls to *sipsp.com*, and so codec set 2 should be used, as described earlier in Section 4.1.2.

```
change ip-network-region 1                                    Page   1 of  19
                              IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: companyx.com
    Name: Company X
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 5000                      IP Audio Hairpinning? y
   UDP Port Max: 6001
DIFFSERV/TOS PARAMETERS                 RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                     RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

```
change ip-network-region 1                                    Page   3 of  19

                   Inter Network Region Connection Management

 src dst codec direct   Total           Video                              Dyn
 rgn rgn  set   WAN  WAN-BW-limits  WAN-BW-limits  Intervening-regions  CAC IGAR
 1   1    1
 1   2    2     y        :NoLimit       :NoLimit
```


©2006 Avaya Inc. All Rights Reserved.

```
 change ip-network-region 2                                    Page   1 of  19
                              IP NETWORK REGION
  Region: 2
Location: 1       Authoritative Domain: sipsp.com
    Name: PSTN via sipsp
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 2              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                     IP Audio Hairpinning? y
   UDP Port Max: 3029
DIFFSERV/TOS PARAMETERS                 RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

```
change ip-network-region 2                                    Page   3 of  19

                   Inter Network Region Connection Management

 src dst codec direct   Total           Video                              Dyn
 rgn rgn  set   WAN  WAN-BW-limits  WAN-BW-limits  Intervening-regions  CAC IGAR
 2   1    2     y        :NoLimit       :NoLimit                           n
 2   2    2
```

4.1.5. Define IP Node Names

Define the IP addresses of the Avaya SIP Enablement Services home servers using the **change node-names ip** command.

```
change node-names ip                                          Page   1 of   1
                                  IP NODE NAMES
    Name              IP Address          Name              IP Address
Home1                10 .3  .3  .50                          .   .   .
Home2                10 .3  .3  .51                          .   .   .
default              0  .0  .0  .0                          .   .   .
procr                10 .3  .3  .10                          .   .   .
                        .   .   .                           .   .   .
```

4.1.6. Define SIP trunks

Add a signaling group for the SIP trunk to Avaya SIP Enablement Services home 1, using the **add signaling-group** command, and fill in the indicated fields. Default values can be used for the remaining fields. The **Far-end Domain** should be the same as that administered in Avaya SIP Enablement Services. The administration of this SIP trunk (trunk 10) supports that performed in SIP Enablement Services in Section 3.1.

©2006 Avaya Inc. All Rights Reserved.

```
add signaling-group 10                                          Page   1 of   1
                              SIGNALING GROUP

 Group Number: 10             Group Type: sip
                         Transport Method: tls




   Near-end Node Name: procr                 Far-end Node Name: Home1
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                         Far-end Network Region: 1
       Far-end Domain: companyx.com

                                              Bypass If IP Threshold Exceeded? n

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

Add the corresponding trunk group controlled by this signaling group via the **add trunk-group** command. Be sure to enter the signaling group number in **Signaling Group** and the number of members desired in **Number of Members**.

```
add trunk-group 10                                              Page   1 of  21
                                TRUNK GROUP

Group Number: 10                    Group Type: sip           CDR Reports: y
  Group Name: Home 1                        COR: 1        TN: 1        TAC: *010
   Direction: two-way         Outgoing Display? y
 Dial Access? n                                          Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n

                                                      Signaling Group: 10
                                                    Number of Members: 50
```

On Page 2, change the **Preferred Minimum Session Refresh Interval** field to a value compatible with far-end SIP proxies and gateways that the configuration will use[7]. This field controls the value of the minimum session interval (Min-SE) header in SIP messages such as INVITE that are sent by Avaya Communication Manager. Since refresh messages are sent when half the session interval has expired, the value of Min-SE sent is twice the value

[7] Although the default value of 120 seconds can be used, it has been found that some SIP network elements require a larger value to support certain calling scenarios. A SIP STATUS message "422 Session Timer Too Small" returned from the network is an indication that the value should be adjusted to one-half the Min-SE value indicated in the message.

©2006 Avaya Inc. All Rights Reserved.

administered in **Preferred Minimum Session Refresh Interval**. In the sample configuration, Cisco SIP network components such as the Cisco 3825 router and AS5350 Voice Gateway require a Min-SE value of 1800.

```
add trunk-group 10                                              Page   2 of  21
      Group Type: sip

TRUNK PARAMETERS

     Unicode Name? y

                                        Redirect On OPTIM Failure: 5000

            SCCAN? n                                Digital Loss Group: 18
                     Preferred Minimum Session Refresh Interval(sec): 900
```

On Page 3, set **Numbering Format** to be *public*. Subsequent pages need not be changed. The trunk members will be automatically generated based on the value of **Number of Members** on Page 1.

```
add trunk-group 10                                              Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                        Maintenance Tests? y



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


                                              Replace Unavailable Numbers? n
```

Similarly, define the signaling and trunk groups for the SIP trunk to home 2, as shown below. In the sample configuration, signaling and trunk groups 12 are defined.

©2006 Avaya Inc. All Rights Reserved.

```
add signaling-group 12                                          Page   1 of   1
                                SIGNALING GROUP

 Group Number: 12              Group Type: sip
                         Transport Method: tls




   Near-end Node Name: procr                 Far-end Node Name: Home2
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                         Far-end Network Region: 1
       Far-end Domain: companyx.com

                                              Bypass If IP Threshold Exceeded? n

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

```
add trunk-group 12                                              Page   1 of  21
                                TRUNK GROUP

Group Number: 12                    Group Type: sip           CDR Reports: y
  Group Name: Home 2                        COR: 1        TN: 1        TAC: *012
   Direction: two-way         Outgoing Display? y
 Dial Access? n                                          Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n

                                                      Signaling Group: 12
                                                    Number of Members: 24
```

```
add trunk-group 12                                              Page   2 of  21
      Group Type: sip

TRUNK PARAMETERS

     Unicode Name? y

                                          Redirect On OPTIM Failure: 5000

            SCCAN? n                                 Digital Loss Group: 18
                      Preferred Minimum Session Refresh Interval(sec): 900
```


©2006 Avaya Inc. All Rights Reserved.

```
add trunk-group 12                                          Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                      Maintenance Tests? y



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


                                              Replace Unavailable Numbers? n
```

So far, the SIP trunk administration in this section covers all local SIP calls within the domain *companyx.com*, as well as calls to the PSTN via the local Cisco 3825 router. For calls to *sipsp.com*, the sample configuration will use foreign domain routing as described in Section 3.2.1. To route calls to a foreign domain, another SIP trunk is defined that shares the same *signaling connection* as one of the SIP trunks just defined. A signaling connection is a collection of SIP trunks that are defined with and share the same near-end and far-end IP addresses and port numbers. Its capacity is the sum of the capacities of these trunks[8]. In the sample configuration, another SIP trunk (trunk 11) will be defined that shares the same signaling connection as the trunk to home 2 (trunk 12). As shown below, the only difference between this trunk group and trunk group 12 is the different value of **Far-end Domain**. When this trunk group is selected as a result of the call routing rules described in the next section, the INVITE for that call will contain the foreign domain (*sipsp.com*) in the request URI.

```
add signaling-group 11                                      Page   1 of   1
                              SIGNALING GROUP

 Group Number: 11             Group Type: sip
                        Transport Method: tls




   Near-end Node Name: procr                Far-end Node Name: Home2
 Near-end Listen Port: 5061               Far-end Listen Port: 5061
                                       Far-end Network Region: 1
       Far-end Domain: sipsp.com

                                            Bypass If IP Threshold Exceeded? n

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

[8] This allows Avaya Communication Manager to support signaling to another proxy with higher capacity than a single trunk group, which is limited to 255 members.

©2006 Avaya Inc. All Rights Reserved.

```
add trunk-group 11                                          Page   1 of  21
                              TRUNK GROUP

Group Number: 11                  Group Type: sip           CDR Reports: y
  Group Name: To sipsp.com                     COR: 1       TN: 1  TAC: *011
   Direction: two-way       Outgoing Display? y
 Dial Access? n                                        Night Service:
Queue Length: 0
Service Type: tie                  Auth Code? n

                                                     Signaling Group: 11
                                                   Number of Members: 24
```

```
add trunk-group 11                                          Page   2 of  21
      Group Type: sip

TRUNK PARAMETERS

     Unicode Name? y

                                          Redirect On OPTIM Failure: 5000

           SCCAN? n                                 Digital Loss Group: 18
                     Preferred Minimum Session Refresh Interval(sec): 900
```

```
add trunk-group 11                                          Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                       Maintenance Tests? y



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


                                             Replace Unavailable Numbers? n
```

4.1.7. Define Public Numbering Format

Together with the **Numbering Format** field in the trunk group administration of the previous section, the **change public-unknown-numbering** command will enable Avaya Communication Manager to provide the proper calling number when calls are placed over the SIP trunks from telephones in *companyx.com*. The first two entries below indicate that the 5-digit calling extension will be passed for calls within *companyx.com* placed from stations whose extensions begin with 3. This covers all extensions in the sample configuration. The last entry specifies a full 10-digit number (*CPN Prefix* plus 5-digit extension) to be provided for foreign domain calls to the foreign domain *sipsp.com*.

©2006 Avaya Inc. All Rights Reserved.

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

 5 3       10                        5
 5 3       12                        5
 5 3       11        73212           10
```

4.2. Configure Call Routing

4.2.1. Outbound Calls

Avaya SIP Enablement Services always routes calls from *companyx.com* SIP telephones to Avaya Communication Manager, where dial plan and routing rules will be applied to determine where the call should be routed next. In the sample configuration, Automatic Route Selection (ARS) will be configured for calls outside the enterprise. Calls for the local area code (732) will use the integrated PSTN gateway in the local Cisco 3825 router. Calls for area code 733 will be routed to *sipsp.com*, where they will be routed to the Cisco AS5350 Voice Gateway. The following configuration steps support these routing rules.

©2006 Avaya Inc. All Rights Reserved.

Use the **change dialplan analysis** command to add the feature access code for outside dialing.

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

      Dialed  Total  Call      Dialed  Total  Call      Dialed  Total  Call
      String  Length Type      String  Length Type      String  Length Type
        0       3    fac
        1       3    fac
        3       5    ext
        4       5    ext
        5       5    ext
        7       5    ext
        9       1    fac
        *       2    fac
        *       3    fac
        *       4    dac
        #       2    fac
        #       3    fac
```

Use the **change feature-access-codes** command to specify 9 as the access code for outside dialing.

```
change feature-access-codes                                     Page   1 of   5
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code: 101
         Abbreviated Dialing List2 Access Code: 102
         Abbreviated Dialing List3 Access Code: 103
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code: 106
                       Answer Back Access Code: 105
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code:
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                  Automatic Callback Activation: *5     Deactivation: #5
Call Forwarding Activation Busy/DA: *2     All: 112    Deactivation: #2
                        Call Park Access Code: 104
                      Call Pickup Access Code: *6
CAS Remote Hold/Answer Hold-Unhold Access Code: #6
                   CDR Account Code Access Code:
                         Change COR Access Code:
                    Change Coverage Access Code:
                    Contact Closure   Open Code:          Close Code:
                    Contact Closure  Pulse Code:
```

Now use the **change ars analysis** command to configure the route selection, based on the number dialed following the "9". In the sample configuration, PSTN destinations are dialed in the form 1AAANNNXXXX, or AAANNNXXXX if the area code is local. If the area code

©2006 Avaya Inc. All Rights Reserved.

(AAA) is 732, the call is to be routed by SES via address map to the local Cisco 3825 router. If it is 733, the call is to be routed by Avaya SIP Enablement Services via foreign domain routing to *sipsp.com*. On-net calls to extensions beginning with 5 are also routed via foreign domain routing to SIP telephones supported by the Cisco SIP Proxy in *sipsp.com*. The entries below define the number format to be matched and the routing patterns selected. In the sample configuration, the route pattern numbers correspond to the trunk groups they select. For numbers beginning with 1732 or 732, trunk group 10 is used, although trunk group 12 could have been used just as well. To ensure foreign domain routing for 1733NNNXXXX or 5XXXX calls, trunk group 11 must be used as opposed to 12, even though they make up the same signaling connection.

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

         Dialed           Total     Route    Call   Node  ANI
         String          Min  Max  Pattern   Type   Num   Reqd
   1732                  11   11    10       fnpa         n
   1733                  11   11    11       fnpa         n
   5xxxx                 5    5     11       locl         n
   732                   10   10    10       fnpa         n
```

Use the **`change route-pattern`** command to define the SIP trunk group to be selected for the corresponding route patterns, as shown below.

```
change route-pattern 10                                        Page   1 of   3
                  Pattern Number: 10  Pattern Name: PSTN via 3825
                           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: 10   0                                                             n   user
 2:                                                                    n   user
 3:                                                                    n   user
 4:                                                                    n   user
 5:                                                                    n   user
 6:                                                                    n   user

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


©2006 Avaya Inc. All Rights Reserved.

```
change route-pattern 11                                          Page   1 of   3
                    Pattern Number: 10  Pattern Name: PSTN via 3825
                                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: 11   0                                                           n   user
 2:                                                                  n   user
 3:                                                                  n   user
 4:                                                                  n   user
 5:                                                                  n   user
 6:                                                                  n   user

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

Use the **`change locations`** command to designate any one of the SIP trunk routing patterns defined above in the **`Proxy Sel. Rte. Pat.`** field. This provides support for features such as call transfer and URI dialing.

```
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                                 10
```

4.2.2. Inbound Calls

In the sample configuration, two DID numbers assigned by the local PSTN network provider, one assigned to each of the two Cisco gateways (see **Figure 1** and **Table 2**), will be mapped directly to two SIP extensions in *companyx.com*. The incoming numbers presented by the Cisco gateways will be in the form 2xxxx, the least significant 5 digits in the DID number. The address map defined in Avaya SIP Enablement Services in Section 3.2.2 will cause inbound calls from the gateways to be routed from home 1 into Avaya Communication Manager on SIP trunk group 10. The **`change inc-call-handling-trmt trunk-group`** command can be used to map the dialed number to a local extension. As shown, below, incoming digits 21234 from the Cisco 3825 will cause the call to terminate on SIP telephone extension 34001, and 25678 from the Cisco AS5350 will terminate on 34002.

©2006 Avaya Inc. All Rights Reserved.

```
change inc-call-handling-trmt trunk-group 10                    Page   1 of   3
                        INCOMING CALL HANDLING TREATMENT
 Service/       Called    Called        Del  Insert
 Feature         Len      Number
 tie              5   21234             5    34001
 tie              5   25678             5    34002
 tie
```

5. Configure Cisco 3825 Router/Gateway

The following sections provide annotated configurations for supporting SIP-aware Network Address Translation (NAT), Port Network Address Translation (PNAT), and PSTN gateway functions in the Cisco 3825 router. They are not complete configurations for the router - only configuration commands relative to the above functions are shown.

5.1. Configure NAT and PNAT

The following configuration steps implement the NAT address mapping by the 3825 router as shown in **Table 1.** Note that in situations where the router is expected to re-fragment large packets bearing SIP messaging (e.g., INVITEs resulting from forwarded calls over multiple systems), Cisco requires use of the Advanced IP Services or Advanced Enterprise package as opposed to the IP Voice package, since they contain the Virtual Fragmentation Reassembly (VFR) feature required for proper fragmentation of the packets during the NAT process.

! interface GigabitEthernet0/0 description Outside interface ip address 120.1.1.1 255.255.255.0 ip nat outside duplex auto speed auto media-type rj45 negotiation auto !	Outside interface of router Designate this interface as using NAT (public side)
! interface FastEthernet1/0 ! interface FastEthernet1/1 ! interface FastEthernet1/2 ! interface FastEthernet1/3 ! interface FastEthernet1/4 ! interface FastEthernet1/5 ! interface FastEthernet1/6	Ethernet Interface Module ports

©2006 Avaya Inc. All Rights Reserved.

! interface FastEthernet1/7 ! interface FastEthernet1/8 ! interface FastEthernet1/9 ! interface FastEthernet1/10 ! interface FastEthernet1/11 ! interface FastEthernet1/12 ! interface FastEthernet1/13 ! interface FastEthernet1/14 ! interface FastEthernet1/15 ! !	Above Ethernet ports are all on default Vlan (Vlan1)
interface Vlan1 ip address 10.3.3.1 255.255.255.0 ip nat inside ! !	Gateway IP address Designate as using NAT (private side)
1 ip nat pool sip 120.1.1.3 120.1.1.3 prefix-length 24 ip nat inside source list 1 pool sip overload ! ! ! ! ! ! !	Define IP address pool (sip) used for PNAT (120.1.1.3) “overload” => PNAT; see access list 1 below for PNAT-able private addresses Establish static NAT for Avaya servers, since well-known port numbers must be used.
ip nat inside source static 10.3.3.60 120.1.1.4 extendable ip nat inside source static 10.3.3.50 120.1.1.5 extendable ip nat inside source static 10.3.3.51 120.1.1.6 extendable ip nat inside source static 10.3.3.10 120.1.1.7 extendable !	Avaya SIP Enablement Services edge Avaya SIP Enablement Services Home 1 Avaya SIP Enablement Services Home 2 Avaya S8300 Media Server “procr” interface

©2006 Avaya Inc. All Rights Reserved.

access-list 1 deny 10.3.3.10 access-list 1 deny 10.3.3.60 access-list 1 deny 10.3.3.50 access-list 1 deny 10.3.3.51 access-list 1 permit 10.3.3.0 0.0.0.255 !	This access list is used by PNAT. Don't PNAT for statically NAT'd addresses Allow all other private addresses to be PNAT'd

5.2. Configure the T1/PRI Interface

PSTN connectivity uses a T1 PRI link to a DS1 interface on the Avaya DEFINITY® Server R. The configuration screens for the Server R side of the T1 interface are provided in Section 9.

! isdn switch-type primary-ni ! !	Set ISDN PRI switch protocol
voice-card 0 dspfarm !	Using default DSP card config
voice call send-alert ! ! !	Send ALERT message (rather than PROGRESS) back to Avaya DEFINITY Server R on receipt of SETUP message.
voice class codec 1 codec preference 1 g711ulaw ! !	Set the codec for packetized voice
controller T1 0/0/0 framing esf linecode b8zs pri-group timeslots 1-24 !	Configure T1 controller 0 Use all 23 bearer channels
network-clock-participate wic 0 !	Get DS1 clock from far end
interface Serial0:23 no ip address isdn T309-enable isdn T306 30000 isdn T310 40000 no cdp enable no clns route-cache !	Define the PRI signaling Channel (last channel) Enable call clearing timer DISCONNECT timer CALL PROCEEDING timer No Cisco Discovery Protocol Switch to voice-port config mode using PRI D channel on T1 controller 0
voice-port 0/0/0:23 !	

©2006 Avaya Inc. All Rights Reserved.

5.3. Configure Call Routing

These configuration steps implement call routing by the 3825 router between its Ethernet/SIP and T1/PRI interfaces. The configuration of dial peers is analogous to ARS and route pattern configuration in Avaya Communication Manager or address maps in Avaya SIP Enablement Services.

sip-ua	Enable SIP user agent
dial-peer cor custom	Any named class of
!	restrictions will apply to
!	dial peers
dial-peer voice 732 pots	Define dial peer for SIP-to-
application session	PSTN calls
destination-pattern 732.......	Match on area code 732
direct-inward-dial	
port 0/0/0:23	Use D-channel on T1
forward-digits all	Send all dialed digits
prefix *9	Avaya DEFINITY Server R uses
!	“*9” feature access code for
!	outbound calls
!	
dial-peer voice 20000 voip	Define dial peer for PSTN to
service session	SIP calls
destination-pattern 2....	Match on 2xxxx passed from
progress_ind setup enable 1	Avaya DEFINITY Server R
session protocol sipv2	
session target ipv4:10.3.3.60	Send INVITE to Avaya SIP
session transport udp	Enablement Services edge
dtmf-relay rtp-nte	Use RFC2833 (out-of-band)
codec g711ulaw	Use G.711 (local to
!	*companyx.com*)

6. Configure NAT in Cisco PIX 515E Firewall

The following commands configure IP routing, NAT, and PNAT for the Cisco PIX 515E, which serves as the gateway for *sipsp.com*. No security configuration has been included.

!	
interface Ethernet0	
nameif outside	Outside (public) interface
security-level 0	for NAT
ip address 30.1.1.2 255.255.255.0	
!	
interface Ethernet1	
nameif inside	Inside (private) interface
security-level 100	for NAT

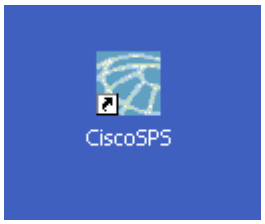
©2006 Avaya Inc. All Rights Reserved.

ip address 10.2.2.1 255.255.255.0 ! nat-control ! global (outside) 1 30.1.1.5 nat (inside) 1 10.2.2.0 255.255.255.0 static (inside,outside) 30.1.1.6 10.2.2.50 netmask 255.255.255.255 static (inside,outside) 30.1.1.7 10.2.2.40 netmask 255.255.255.255 ! route outside 0.0.0.0 0.0.0.0 30.1.1.1 1 !	 Enable NAT Define public/private IP address ranges (PNAT on 30.1.1.5) Define static NAT for Cisco CSPS and AS5350, since well-known ports must be used Default route to High Level Router

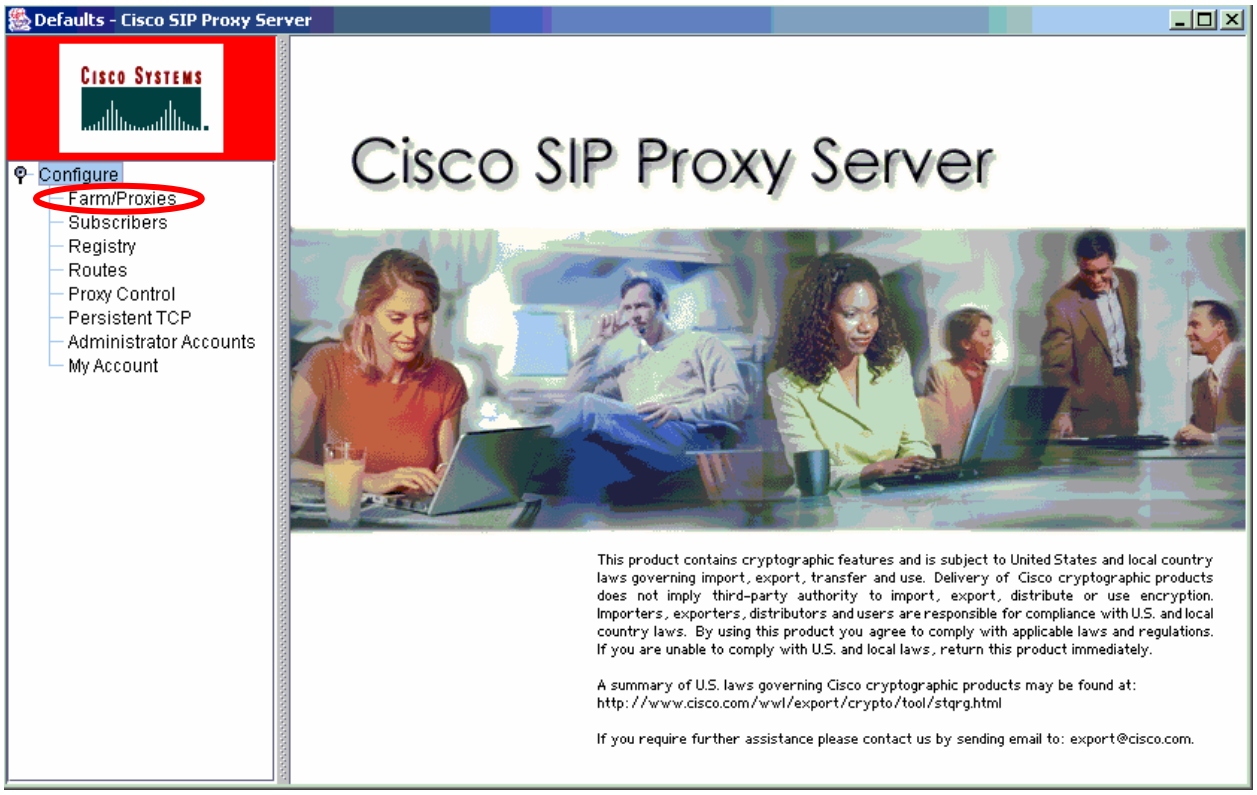
7. Configure the Cisco SIP Proxy Server (CSPS)

The following sections describe the steps for configuring the core proxy parameters, users, and call routing for the Cisco SIP Proxy. Configuration is performed using the GUI-based provisioning system, which can be installed on Linux or Microsoft Windows. It is assumed that the CSPS has been installed and running, and is configured with an IP address (10.2.2.50) and authoritative SIP domain (*sipsp.com*). All steps are executed using the Microsoft Windows version of the GUI provisioning system.

7.1. Configure Core Proxy Parameters

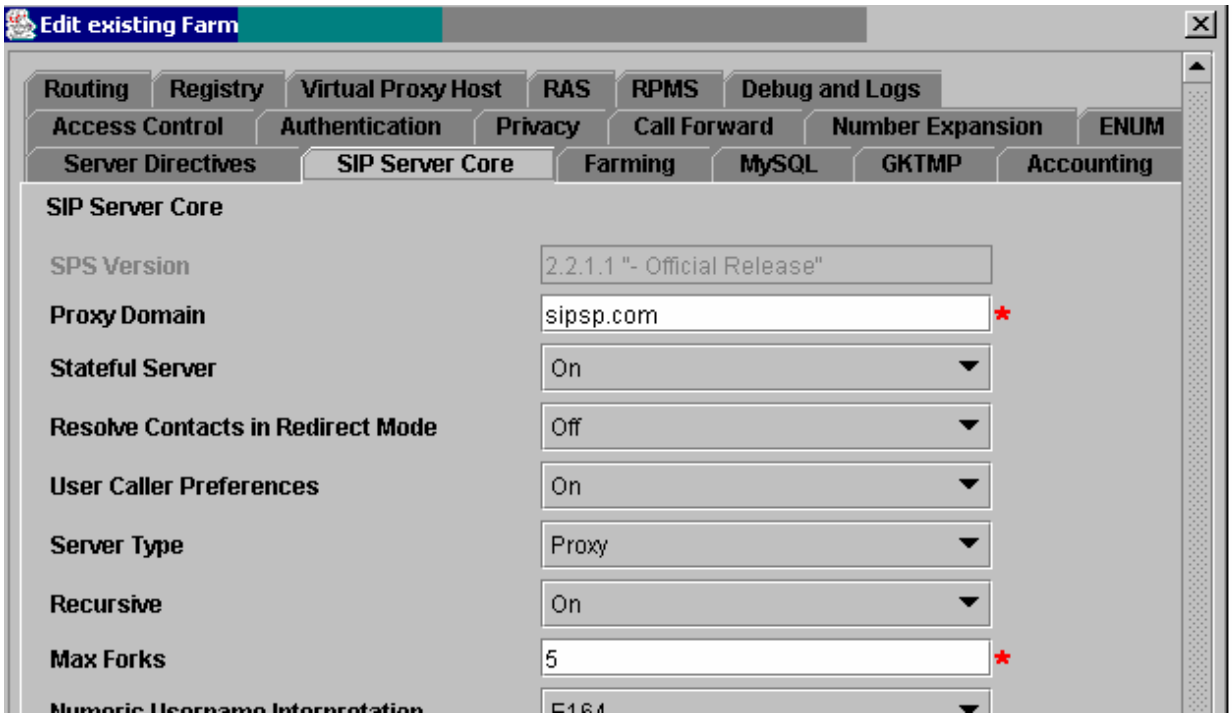
Steps	Description
1.	Invoke the GUI provisioning system from the Microsoft Windows client PC by double-clicking the desktop icon as shown below: 

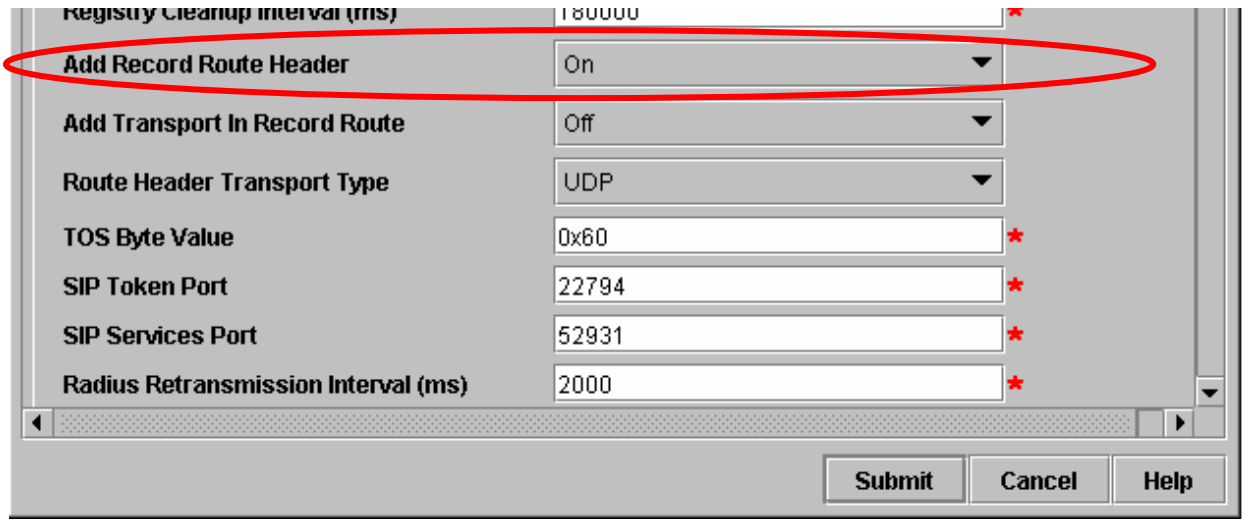
©2006 Avaya Inc. All Rights Reserved.

Steps	Description
2.	The main GUI provisioning screen will be displayed. Click on **Farm/Proxies.** 

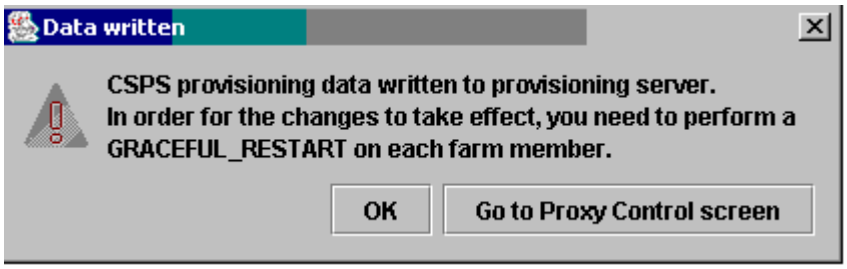
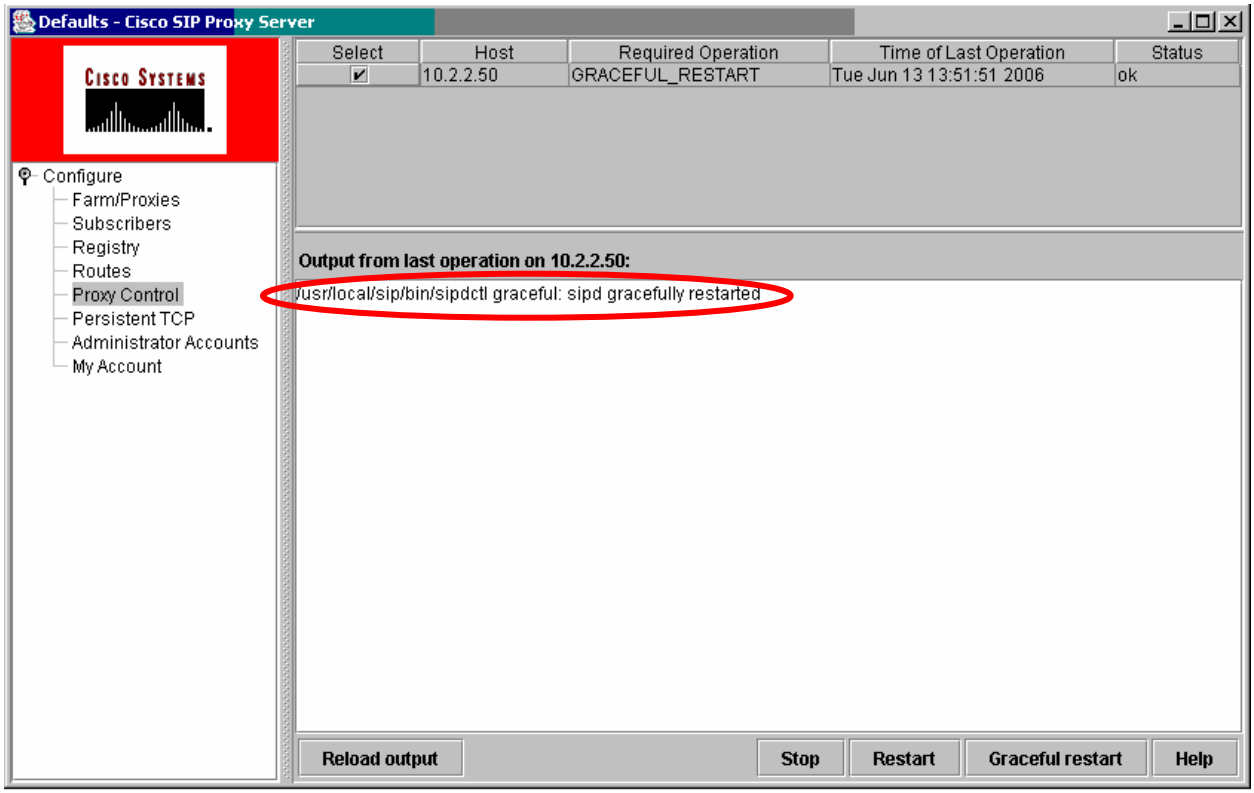
©2006 Avaya Inc. All Rights Reserved.

Steps	Description
3.	The main proxy administration screen will be displayed, shown here in abbreviated form. Click on the **SIP Server Core** tab, shown in abbreviated form below. Set the **Add Record Route Header** option to *On*. Click on **Submit**.



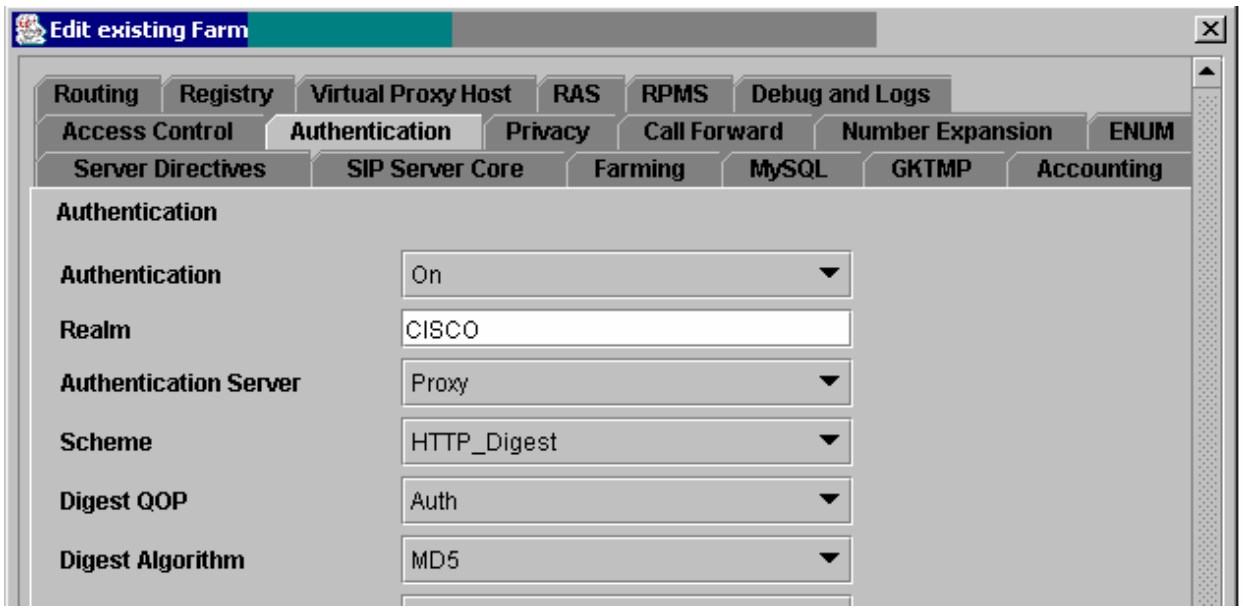


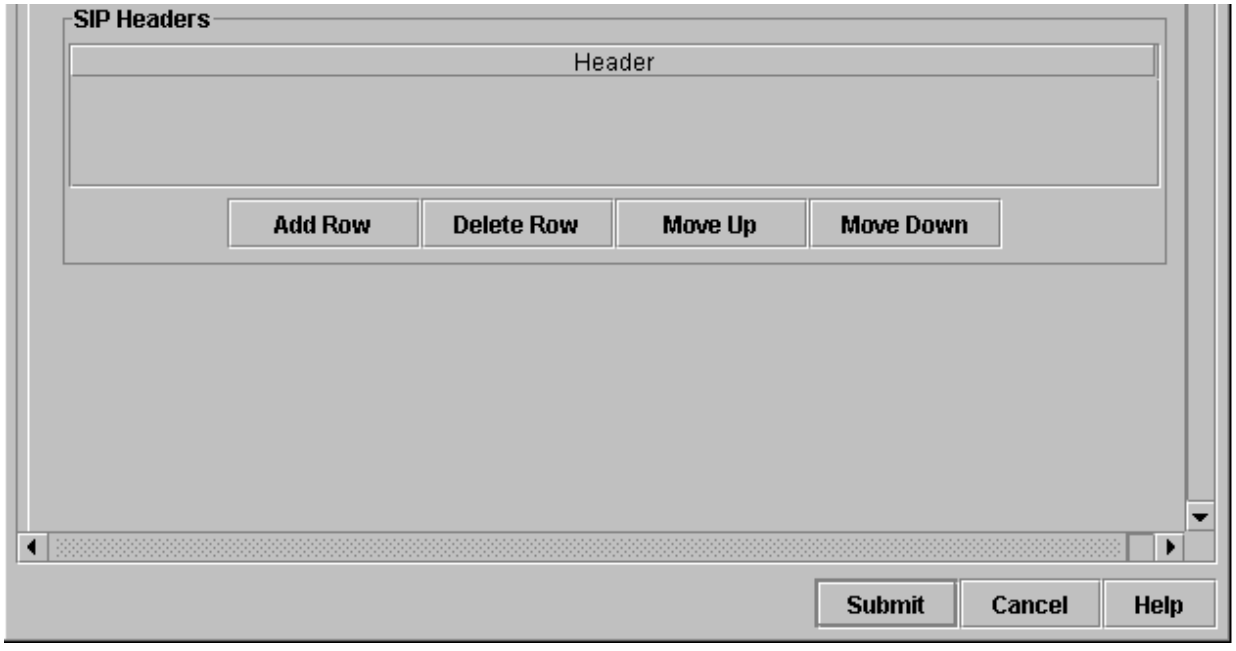
©2006 Avaya Inc. All Rights Reserved.

Steps	Description
4.	Click on **Go to Proxy Control screen** when the dialog box shown below is displayed. Or, if the authentication configuration in Step 6 will be performed, the restart can be postponed until then by clicking on **OK**. 
5.	If **Go to Proxy Control screen** was selected, the Proxy control screen will be displayed, with the box for the proxy in the *Select* column already checked. Click on **Graceful restart**. The status message in the middle of the screen should indicate a successful restart. 

©2006 Avaya Inc. All Rights Reserved.

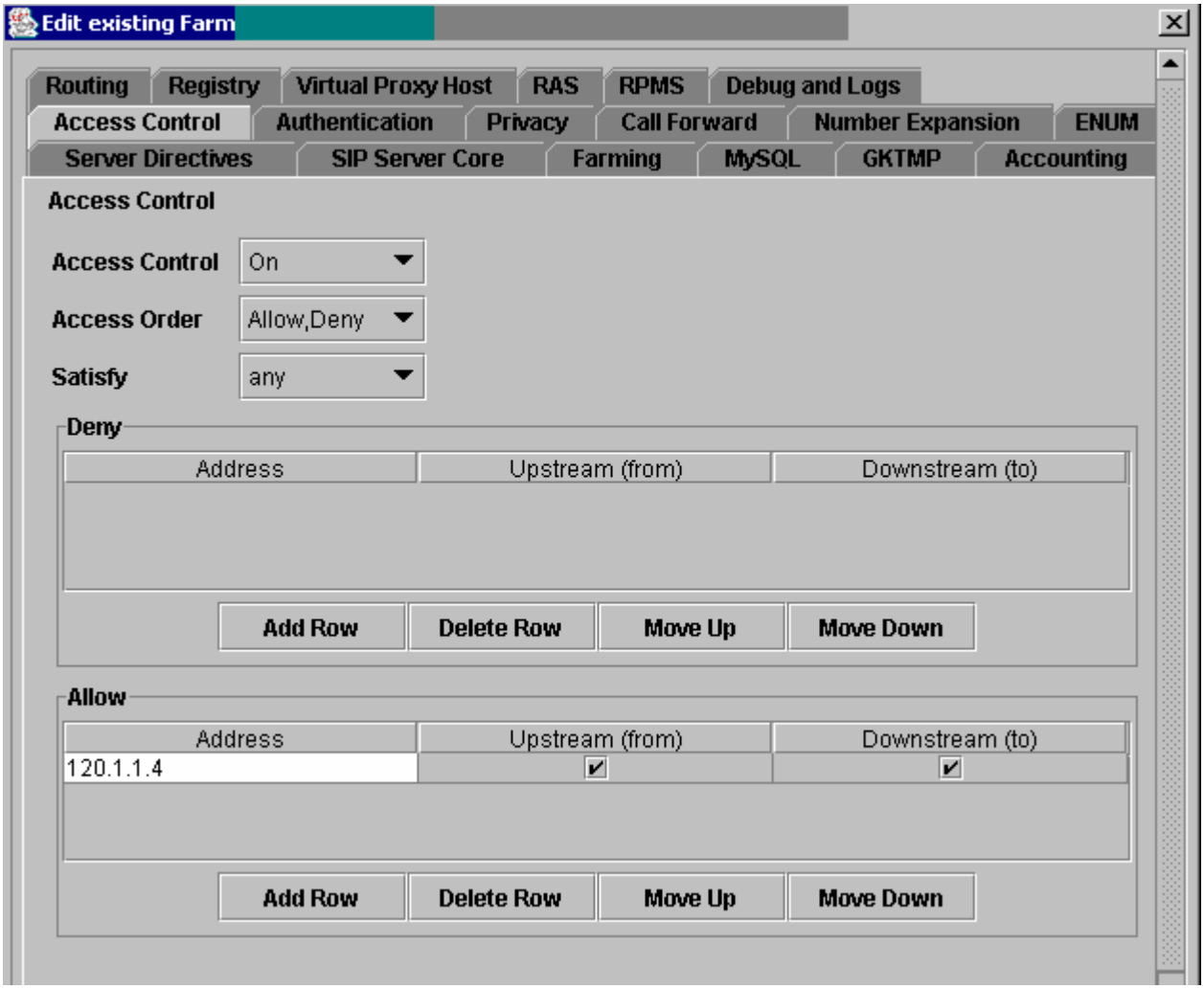
Steps	Description
6.	To enable authentication of all SIP requests by users and other proxies, select the **Authentication** tab, shown below in abbreviated form. Set the **Authentication** option to *On*. Default values for the remaining fields can be used. Click on **Submit**. See Steps 4 and 5 for instructions on gracefully restarting the proxy.





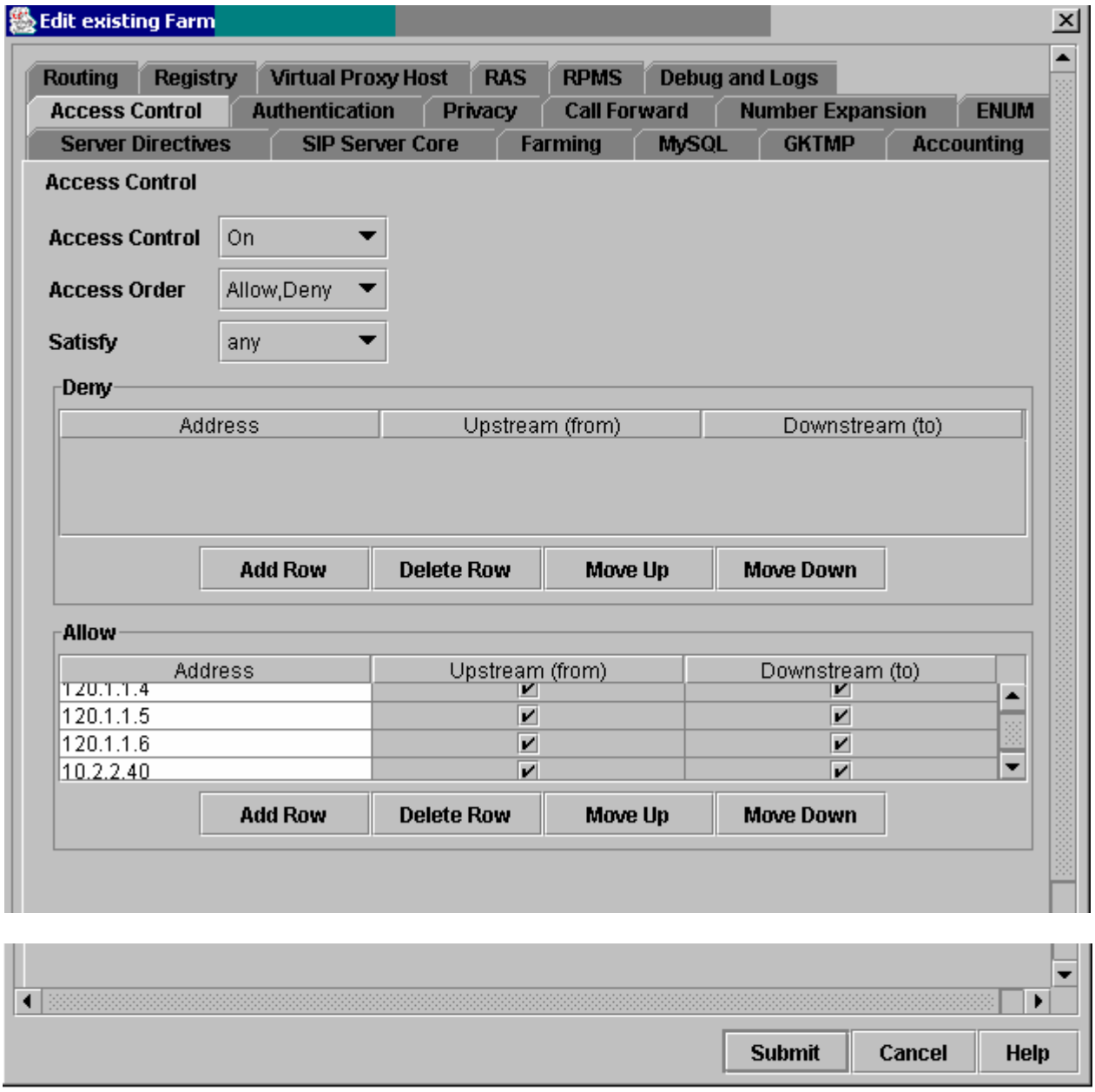
©2006 Avaya Inc. All Rights Reserved.

Steps	Description
7.	Similar to the *trustedhost* capability in Avaya SIP Enablement Services, Cisco CSPS supports identifying specific proxies and gateways in the network that need not be authenticated when they request SIP call services. Select the **Access Control** tab, shown below in abbreviated form. Set the **Access Control** option to *On*, and the **Access Order** and **Satisfy** options as shown. Then Select **Add Row** under *Allow*, and fill in the IP address of one of the proxies/gateways to be granted access. The IP address below is the public address of the Avaya SIP Enablement Services edge. Check both **Upstream (from)** and **Downstream (to)**.



©2006 Avaya Inc. All Rights Reserved.

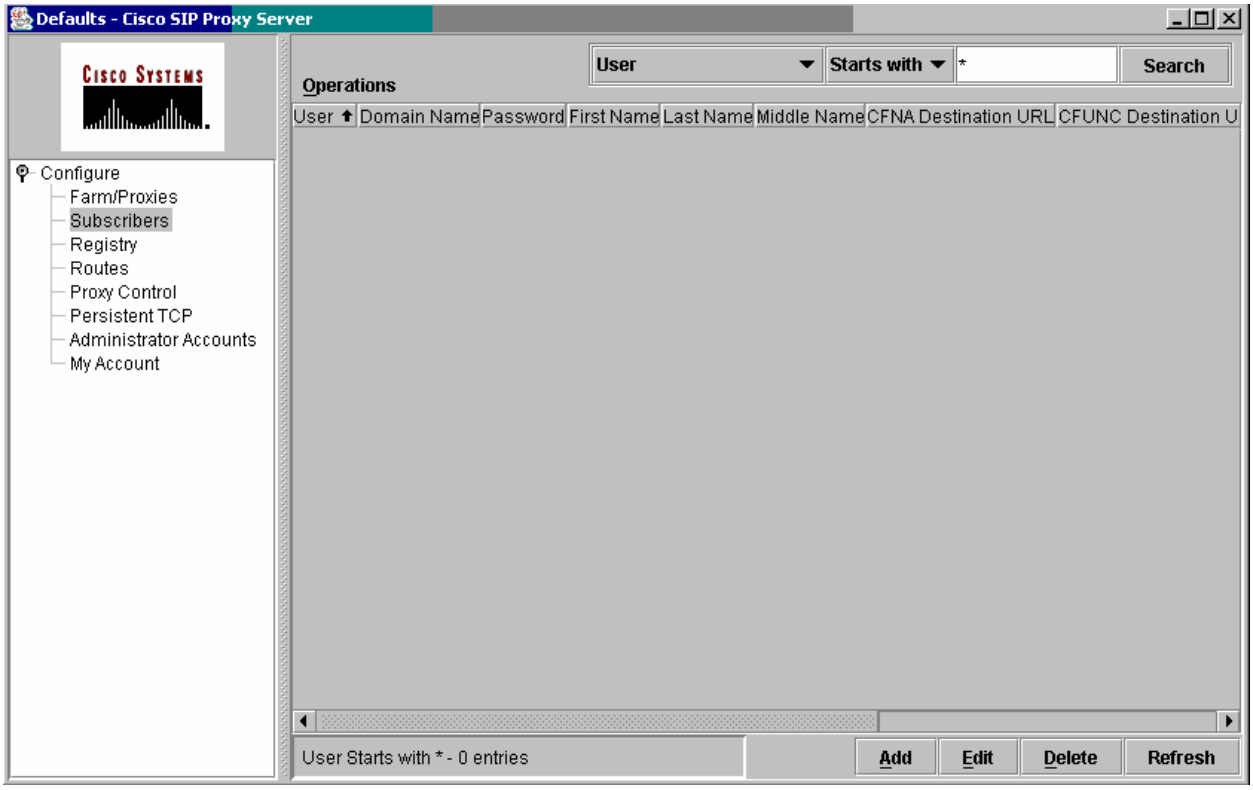
Steps	Description
8.	Continue selecting **Add Row** for each proxy/gateway to be granted access. Shown below are entries for the Avaya SIP Enablement Services edge and home servers and the Cisco AS5350 Voice Gateway. Click on **Submit**. See Steps 4 and 5 for instructions on gracefully restarting the proxy.



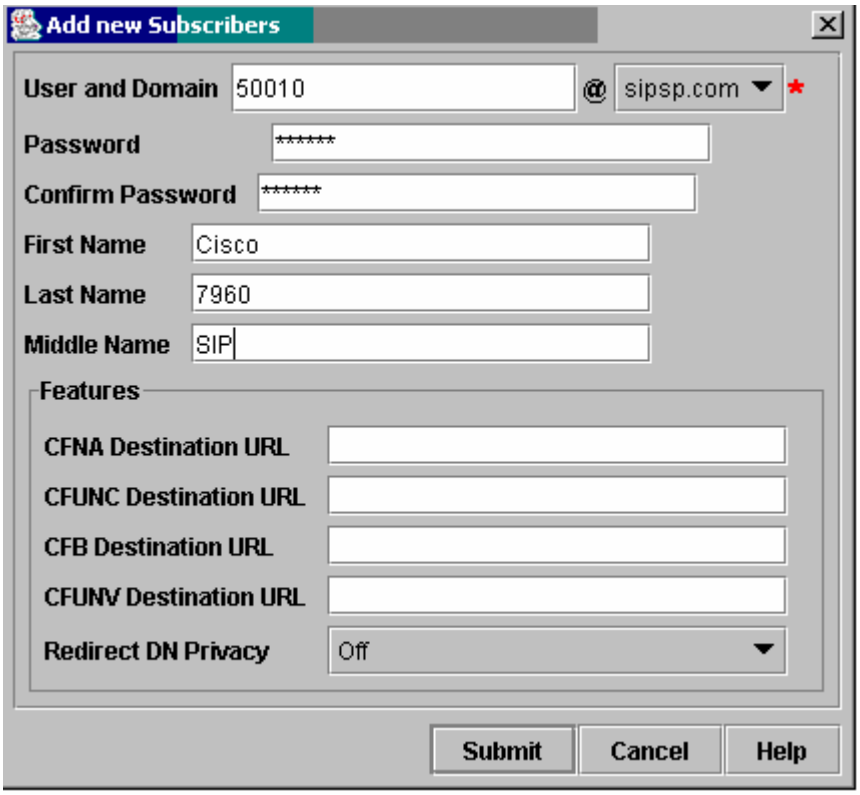
©2006 Avaya Inc. All Rights Reserved.

7.2. Configure SIP Users

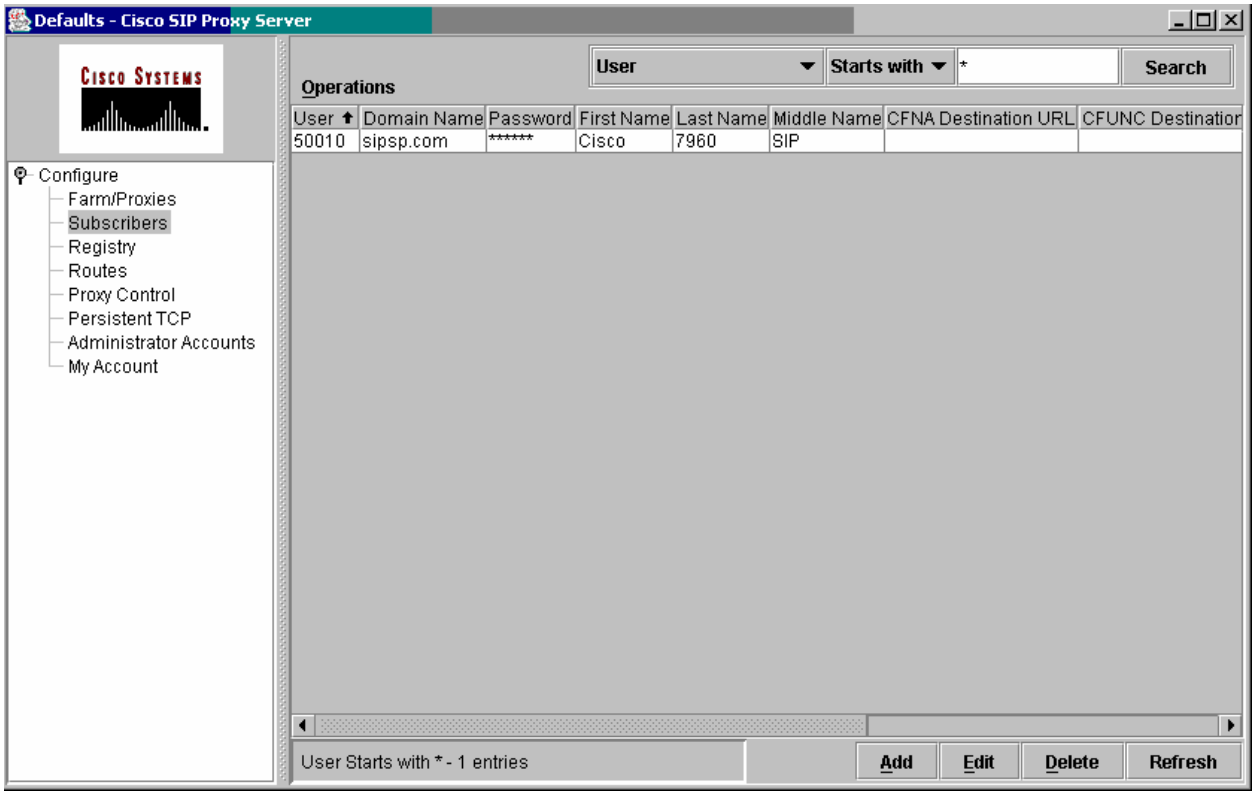
Steps	Description
1.	To add a SIP user (Extension 50010 in the sample configuration), click on **Subscribers** on the main GUI display. The following screen is displayed. Click on **Add**.



©2006 Avaya Inc. All Rights Reserved.

Steps	Description
2.	In the dialog box that is displayed, fill in the **User and Domain** field with the telephone extension, and the **Password** and **Confirm Password** fields. Enter the **First Name**, **Last Name**, and **Middle Name** fields if desired. Click on **Submit**. 

©2006 Avaya Inc. All Rights Reserved.

Steps	Description
3.	To see the current list of subscribers in the system, enter an asterisk in the **Starts with** field, and click on **Search**. 

7.3. Configure Call Routing

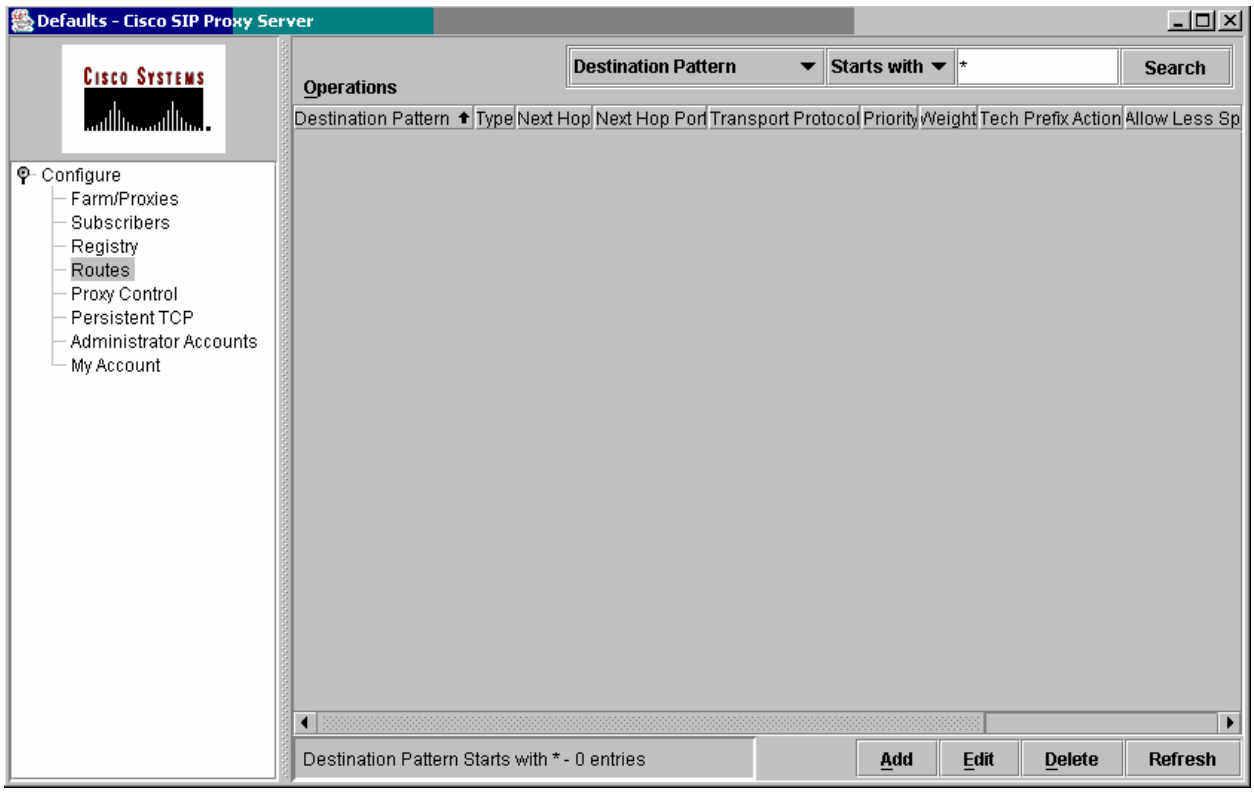
Similarly to Avaya SIP Enablement Services and Avaya Communication Manager, the Cisco SIP Proxy (CSPS) must be configured to route calls based on the dial plan for the sample configuration. From the point of view of the CSPS, the following routing behavior is desired:

Dialed Number format (address map)	Call Type	SIP Network Destination (contact)
3XXXX	Call to *companyx.com* telephone	Avaya SIP Enablement Services edge (120.1.1.4)
733NNNXXXX	PSTN call from *companyx.com*	AS5350 (10.2.2.40)

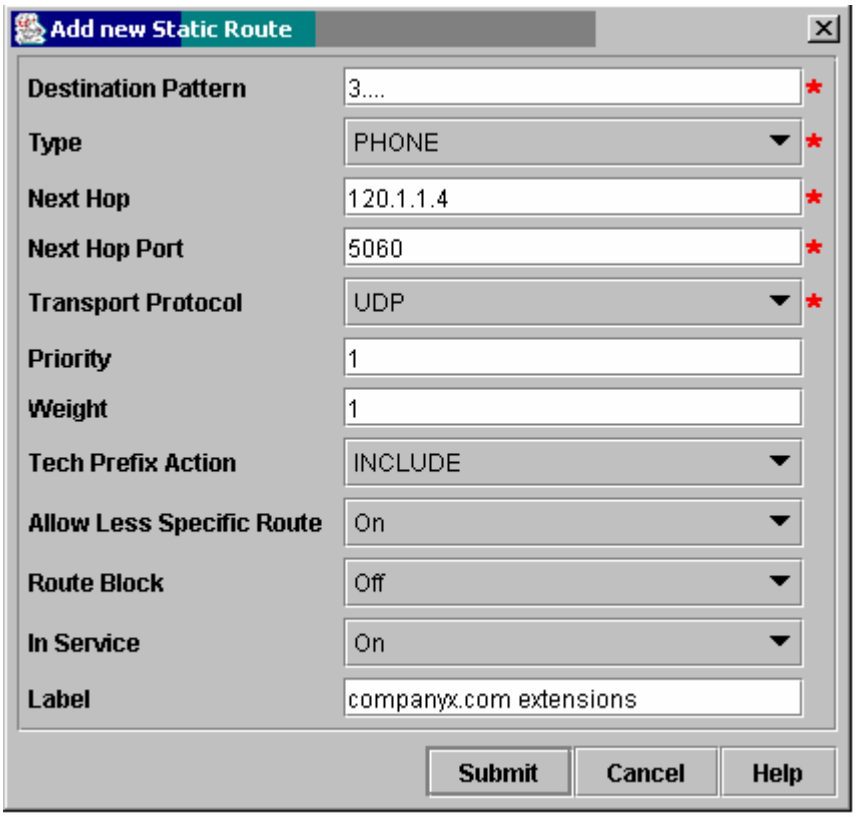
The following steps implement these routing rules.

©2006 Avaya Inc. All Rights Reserved.

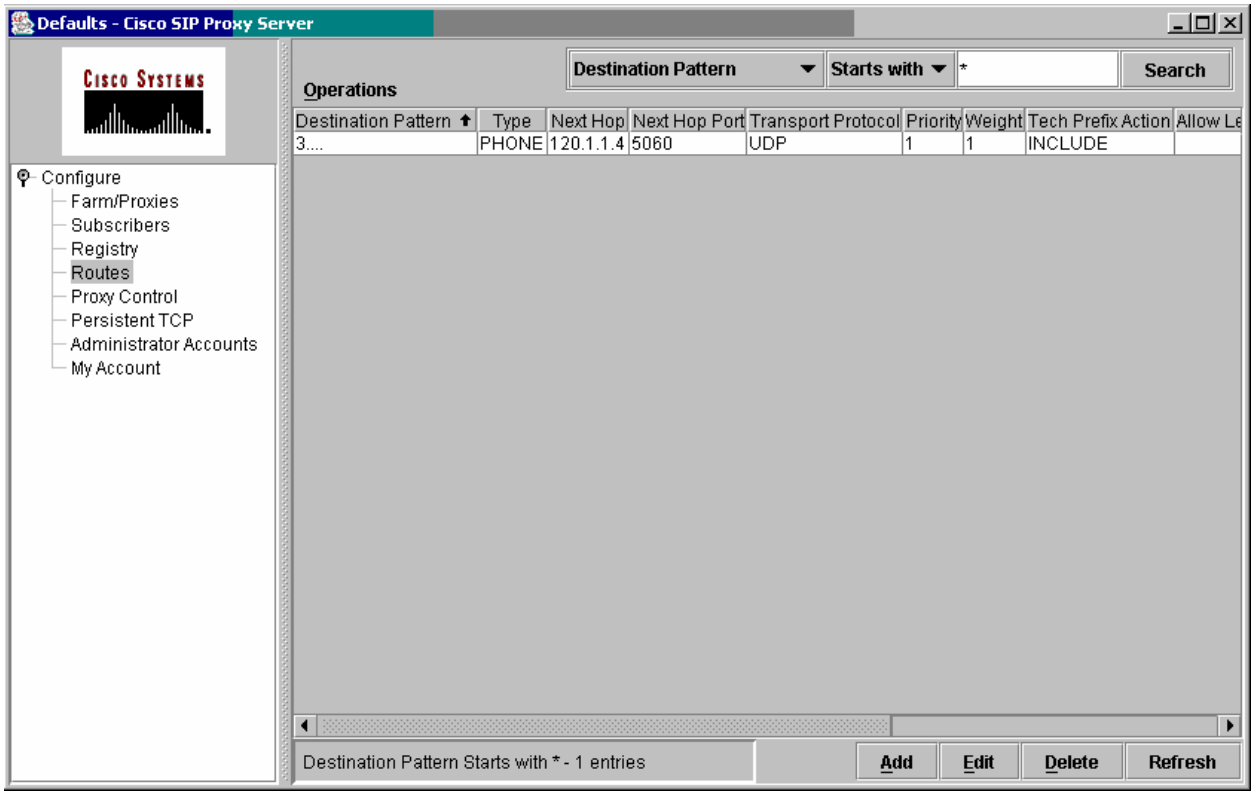
Steps	Description
1.	To add a SIP route, click on **Routes** on the main GUI display. The following screen is displayed. Click on **Add**.



©2006 Avaya Inc. All Rights Reserved.

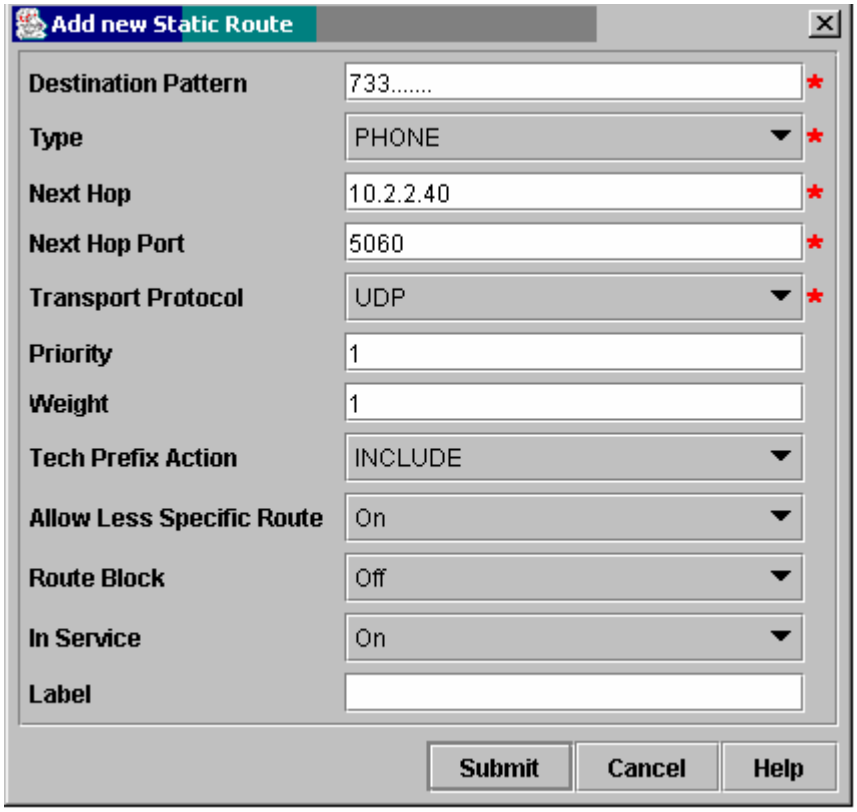
Steps	Description
2.	In the dialog box that is displayed, fill in the **Destination Pattern** field with the pattern match specification. The specification has the same format as that used in the dial-peer configuration in the Cisco AS5350 and 3825 router/gateway. Below is the specification for routing calls to the extensions in *companyx.com*. Fill in the IP address of the next hop, which in this case is the public address for the Avaya SIP Enablement Services edge server. The protocol and port number should match that configured in the edge server (those shown below match the default for Avaya SIP Enablement Services). Enter a **Label** if desired, for later identification. Click on **Submit**, 

©2006 Avaya Inc. All Rights Reserved.

Steps	Description
3.	To see the current list of routes in the system, enter an asterisk in the **Starts with** field, and click on **Search**. 

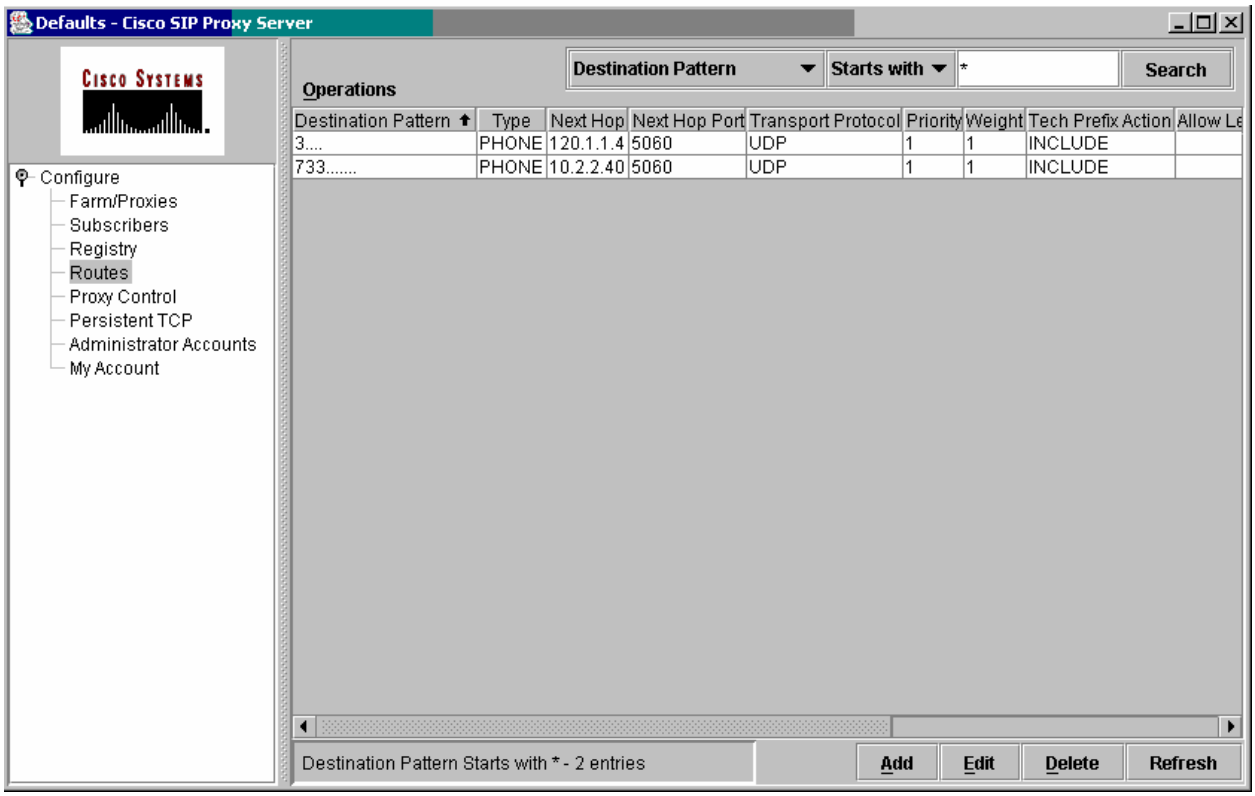
©2006 Avaya Inc. All Rights Reserved.

Steps	Description
4.	Click on **Add** again to add the route for the PSTN call via the Cisco AS5350. Fill in the dialog box as shown. Click on **Submit**.



©2006 Avaya Inc. All Rights Reserved.

Steps	Description
5.	The routes display should now appear as shown below.



8. Configure the Cisco AS5350 Voice Gateway

The following sub-sections show annotated configurations for the AS5350, supporting inbound and outbound dialing between the SIP based VoIP network and the PSTN. The PSTN connectivity uses a T1 PRI link to a DEFINITY® Server R. The configuration screens for the Server R side of the T1 interface are provided in Section 9.

8.1. Configure the T1/PRI Interface.

```
!
isdn switch-type primary-ni
voice call send-alert
!
!
!
!
controller T1 3/0
 framing esf
 linecode b8zs
```

```
Set ISDN PRI switch protocol
Send ALERT message (rather
than PROGRESS) back to
DEFINITY Server R on receipt
of SETUP message.

Configure T1 controller
```


©2006 Avaya Inc. All Rights Reserved.

pri-group timeslots 1-24 ! ! interface Serial0:23 no ip address encapsulation hdlc isdn incoming-voice modem isdn T309-enable isdn T306 30000 isdn T310 40000 no cdp enable ! ! voice-port 3/0:D ! !	Use all 23 bearer channels Define the PRI signaling Channel (last channel) Enable call clearing timer DISCONNECT timer CALL PROCEEDING timer No Cisco Discovery Protocol Switch to voice-port config mode using PRI D channel on T1 controller 0

8.2. Configure Call Routing

The following table shows the configuration steps for call routing between the T1/PRI and SIP interfaces of the Cisco AS5350.

interface FastEthernet0/0 ip address 10.2.2.40 255.255.255.0 duplex auto speed auto ! ! dial-peer voice 20000 voip application session destination-pattern 2.... progress_ind setup enable 1 session protocol sipv2 session target ipv4:10.2.2.50 session transport udp dtmf-relay rtp-nte codec g729br8 ! dial-peer voice 733 pots service session destination-pattern 733....... direct-inward-dial port 3/0:D forward-digits 7 prefix *9732	IP network interface IP address Define dial peer for PSTN- SIP calls Match on 2xxx extensions passed from Avaya DEFINITY Server R Send INVITE to Cisco Proxy RFC 2833 (out-of-band DTMF) Use G.729 Define dial peer for SIP- PSTN calls Match on area code 733 T1/PRI interface to Avaya DEFINITY Server R Translate back to 732 (local area code for sample

©2006 Avaya Inc. All Rights Reserved.

! ! ! ! ! ip route 0.0.0.0 0.0.0.0 10.2.2.1 !	configuration) Avaya DEFINITY Server R uses “*9” feature access code for outbound calls Set default route

9. Configure the Avaya DEFINITY Server R T1 PRI Interface

The following steps detail the administration required on the DEFINITY® Server R for the T1 PRI trunk to the Cisco AS5350 Voice Gateway. The identical administration is used for the PRI trunk to the Cisco 3825 router/gateway, and so is not repeated here. These steps should apply to all Avaya Media Servers and Media Gateways running Avaya Communication Manager. All commands are executed using the System Access Terminal (SAT) interface. Some screens have been truncated for brevity, as indicated by an ellipsis (…) at the bottom. Fields not shown can be assumed to have the default values. Be sure to verify or set the values of fields shown in **bold**.

Use the **`add ds1`** command to configure the DS1 board, and ensure the field values shown in bold text are set. Use the default values for Page 2 of this command.

```
add ds1 01D18                                          Page   1 of   2
                              DS1 CIRCUIT PACK

           Location: 01D18                          Name: PRI
           Bit Rate: 1.544                  Line Coding: b8zs
   Line Compensation: 1                     Framing Mode: esf
      Signaling Mode: isdn-pri
             Connect: line-side
   TN-C7 Long Timers? n                  Country Protocol: 1
Interworking Message: PROGress           Protocol Version: a
Interface Companding: mulaw                         CRC? n
           Idle Code: 11111111
                                DCP/Analog Bearer Capability: 3.1kHz

     Slip Detection? n                 Near-end CSU Type: other
                           Alarm When PRI Endpoint Detached? Y
```

Use the **`add signaling-group`** command to add a signaling group for the T1 PRI trunk. Use the **`display signaling-group`** command to verify the configuration. Note that **`Group Type`** must be configured to *isdn-pri* and **`Primary D-Channel`** must be configured to channel *24*. This signaling group is associated with trunk group *8*.

©2006 Avaya Inc. All Rights Reserved.

```
add signaling-group 8                                        Page   1 of   5
                              SIGNALING GROUP

 Group Number: 8             Group Type: isdn-pri
                   Associated Signaling? y          Max number of NCA TSC: 0
                      Primary D-Channel: 01D1824     Max number of CA TSC: 0
                                                   Trunk Group for NCA TSC:
       Trunk Group for Channel Selection: 8
          Supplementary Service Protocol: a          Network Call Transfer? n
```

Use the **add trunk-group** command to add a trunk group associated with the T1 PRI signaling group. **Group Type** must be configured to *isdn* and **Service Type** to *tie*.

```
add trunk-group 8                                            Page   1 of  22
                              TRUNK GROUP

Group Number: 8                   Group Type: isdn          CDR Reports: y
  Group Name: To Cisco G3725              COR: 1        TN: 1        TAC: 108
   Direction: two-way        Outgoing Display? n      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
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):
 …
```

```
add trunk-group 8                                              Page   2 of  22
TRUNK FEATURES
          ACA Assignment? n            Measured: none     Wideband Support? n
                                 Internal Alert? n       Maintenance Tests? y
                               Data Restriction? n     NCA-TSC Trunk Member:
                                     Send Name: n     Send Calling Number: y
            Used for DCS? n
   Suppress # Outpulsing? n    Numbering Format: public
 Outgoing Channel ID Encoding: preferred   UUI IE Treatment: service-provider
                                            Replace Restricted Numbers? n
                                           Replace Unavailable Numbers? n
                                                 Send Connected Number: y
…
```


©2006 Avaya Inc. All Rights Reserved.

Add the channels associated with trunk group 8.

```
add trunk-group 30                                          Page   6 of  22
                                TRUNK GROUP
                                     Administered Members (min/max):   1/2
GROUP MEMBER ASSIGNMENTS                 Total Administered Members:   2

       Port    Code Sfx Name        Night           Sig Grp
  1: 01D1801  TN464 F                                  8
  2: 01D1802  TN464 F                                  8
…
```

10. Verification Steps

The following steps can be used to troubleshoot network configurations in the field:

Network connectivity:

1. For each proxy server, ping the SIP phones that should be registered to it.
2. For each proxy server, ping the remote proxies to which it should be routing calls. If the pings fail, verify the NAT configuration in network devices such as the edge router and firewalls (Cisco 3825 and PIX 515-E in the sample configuration). Also check any firewall rules that may be in effect to explain the failures, since the security configuration may not allow ping. If security configuration rules prohibit ping, try Step 2 below under "Call Routing."
3. For PSTN gateways, verify that the T1 PRI interface is up (in the sample configuration, via the **`show interface`** command on the Cisco 3825 and AS5350, and the **`status signaling-group`** and **`status trunk-group`** commands on the Avaya DEFINITY® Server R). Refer to References [7-8] for proper T1 interface configuration on the Cisco AS5350 and 3825, respectively.
4. Verify that the Avaya SIP trunks are up between the Avaya S8300 Media Server and the Avaya SIP Enablement Services home servers. Ping the S8300 from the home servers. Use the **`status signaling-group`** command on the S8300.

Call routing:

1. Verify successful calls between SIP phones within each proxy. If calls do not complete, consult the proxy server and phone documentation, including References [1-6], if applicable.
2. Verify on-net (SIP-to-SIP) calls between SIP phones registered to different proxy servers. If the calls are unsuccessful, use a SIP-capable protocol analyzer to view the message exchange between SIP proxies. If a proxy does not route the INVITE message to the proper destination, check the route entries for that proxy to make sure the dial string match specification is correct (e.g., the address map in Avaya SIP Enablement Services, or the static route in Cisco CSPS).
3. Verify off-net (SIP-to-PSTN) calls from SIP phones to the PSTN via the SIP/PSTN gateway. If calls are not routed to the PSTN interface, check the dial string match specification in the gateways (e.g., **`destination-pattern`** in the AS5350 and 3825 dial-peers).

©2006 Avaya Inc. All Rights Reserved.

4. Verify off-net calls from PSTN to SIP phones. If unsuccessful, use the same diagnostic steps as described in 2 and 3 above.
5. In general, if a SIP device in the network does not receive an expected response to a SIP message it has transmitted, the standard procedure is to retransmit that message at an exponentially decreasing interval (½ second, then 1 second, etc.), up to six more times. Look for this behavior at various points in the call routing path if calls are not successful, or if calls only remain established for approximately 32 seconds. Most likely, the expected message has not been routed properly due to NAT, dial-peer, DNS, or firewall configuration errors.

11. Conclusion

These Application Notes have provided the administrative details on configuring:

- SIP call routing among Avaya SIP Enablement Services, Avaya Communication Manager, Cisco 3825 Router/Gateway, Cisco SIP Proxy Server, and Cisco AS5350 Voice Gateway.
- Call routing over a T1 PRI link between the Cisco gateways and Avaya DEFINITY® Server R.
- SIP-aware NAT and PNAT for the Cisco 3825 and the PIX-515E firewall.

This information should be applicable to other Cisco IOS based routers, gateways, and firewalls, as well as Avaya Media Servers and Media Gateways running Avaya Communication Manager.

12. Additional References

[1] *Installing and Administering SIP Enablement Services R3.1*, Issue 1.4, Doc ID 03-600768, February, 2006, available at http://support.avaya.com.

[2] *SIP Support in Release 3.1 of Communication Manager Running on the S8300, S8400, S8500, S8500B, S8700, and S8710 Media Server*, Issue 1.4, Doc ID 555-245-206, February, 2006, available at http://support.avaya.com.

[3] *Administrator Guide for Avaya Communication Manager*, Issue 2, Doc ID 03-300509, February 2006, available at http://support.avaya.com.

[4] *Avaya Extension to Cellular and OPS Installation and Administration Guide*, Version 6.0 Issue 9, DocID 210-100-500, June 2005, available at http://support.avaya.com.

[5] *Configuring SIP IP Telephony Using Avaya SIP Enablement Services, Avaya Communication Manager, and Cisco 7940/7960 SIP Telephones - Issue 1.1*, available at http://support.avaya.com.

[6] *Cisco SIP Proxy Server Administrator Guide*, Version 2.2, available at http://www.cisco.com.

[7] *Cisco AS5350 and Cisco AS5400 Universal Gateway Software Configuration Guide*, available at http://www.cisco.com.

[8] *1/2 Port Channelized T1/E1 PRI Network Module (NM-1CE1T1-PRI and NM-2CE1T1-PRI)*, available at http://www.cisco.com.

©2006 Avaya Inc. All Rights Reserved.

13. Appendix - Address Map Pattern Strings in Avaya SIP Enablement Services

The syntax for the pattern is a Linux regular expression that will match the extension numbers to be mapped. Regular expressions are a way to describe text through pattern matching. The regular expression is a string containing a combination of normal text characters, which match themselves, and special *metacharacters*, which may represent items like quantity, location or types of character(s). For example, **[0-9]** represents any single digit and ***** represents any number of digits or characters. For example, ^**sip:538[0-9]*** would match any SIP INVITE message (^ matches the beginning of a line) for any extension 3 or more digits in length, beginning with the digits **538**, and ending with any other sequence of digits. Square brackets contain a selection of characters to be matched, with a hyphen indicating a range. In the example, **[0-9]** matches any digit, or as another example, **[13579]** matches odd-numbered digits. Curly brackets containing a whole number match that number of instances of the preceding item. For example, **[0-9]{4}** matches any four digits. Note that the braces may require preceding \ escape characters: **\{4\}**. Another helpful *metacharacter* is dot (period), which matches any single character. For example, the regular expression **.*** matches any quantity (including zero) of any character(s).

©2006 Avaya Inc. All Rights Reserved.

1. Introduction 2
2. Equipment and Software Validated 5
3. Configure Avaya SIP Enablement Services 5
3.1. Configure SIP Trunks 5
3.2. Configure Call Routing 10
3.2.1. Outbound Calls 10
3.2.2. Inbound Calls 19
4. Configure Avaya Communication Manager 24
4.1. Configure SIP trunks 24
4.1.1. Verify System Capacity 25
4.1.2. Define Codec Sets 25
4.1.3. Verify Near End IP Network Region 26
4.1.4. Define IP Network Regions 26
4.1.5. Define IP Node Names 28
4.1.6. Define SIP trunks 28
4.1.7. Define Public Numbering Format 33
4.2. Configure Call Routing 34
4.2.1. Outbound Calls 34
4.2.2. Inbound Calls 37
5. Configure Cisco 3825 Router/Gateway 38
5.1. Configure NAT and PNAT 38
5.2. Configure the T1/PRI Interface 40
5.3. Configure Call Routing 41
6. Configure NAT in Cisco PIX 515E Firewall 41
7. Configure the Cisco SIP Proxy Server (CSPS) 41
7.1. Configure Core Proxy Parameters 41
7.2. Configure SIP Users 49
7.3. Configure Call Routing 51
8. Configure the Cisco AS5350 Voice Gateway 56
8.1. Configure the T1/PRI Interface. 56
8.2. Configure Call Routing 56
9. Configure the Avaya DEFINITY Server R T1 PRI Interface 58
Add the channels associated with trunk group 8. 60
10. Verification Steps 60
11. Conclusion 61
12. Additional References 61
13. Appendix - Address Map Pattern Strings in Avaya SIP Enablement Services 62

©2006 Avaya Inc. All Rights Reserved.

©2006 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