Avaya Solution & Interoperability Test Lab

Application Notes for the Kagoor VoiceFlow 200 with Avaya Converged Communication Server (CCS) - Issue 1.0

Abstract

These Application Notes describe the configuration steps required for interoperability of the Kagoor VoiceFlow 200 Application Level Gateway (ALG) with the Avaya CCS in an enterprise Session Initiation Protocol (SIP) telephony configuration. The VoiceFlow 200 performs SIP-aware Network Address Translation (NAT) as well as firewall functions. Basic and supplementary telephony services were tested. Emphasis was placed on NAT as opposed to firewall functionality. All tests were successful.

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

1. Introduction

Customers implementing multi-location communication networks often use Network Address Translation (NAT) to conserve public IP addresses as well as hide the internals of the enterprise network configuration. SIP communication networks additionally require NAT be performed on IP addresses embedded in protocol layers above the IP layer (e.g., Session Description Protocol (SDP)). The Kagoor VoiceFlow 200 permits customers to add this capability without impacting existing router/firewall configurations. The VoiceFlow is offered in several model sizes (200, 1000, 3000) to support small, medium, and large enterprises, as well as service providers. See Reference [5] for application of the VoiceFlow 3000 in a hosted telephony environment.

The configuration tested consisted of an Avaya CCS within an enterprise SIP network, as shown in **Figure 1**. Several SIP telephones are registered to the CCS. The enterprise edge router performs IP-level Port NAT (PNAT) for non-SIP network devices within the enterprise. The VoiceFlow performs SIP-level PNAT on behalf of the CCS and SIP phones. For simplicity, NAT was not performed for devices within or beyond the simulated SIP Service Provider (SSP) network.

The Avaya CCS proxy is configured to route all off-enterprise calls to the VoiceFlow, which is configured to route them to the simulated SSP network that supports SIP-to-SIP and SIP-to-PSTN service. The VoiceFlow is configured to route inbound calls to the CCS.

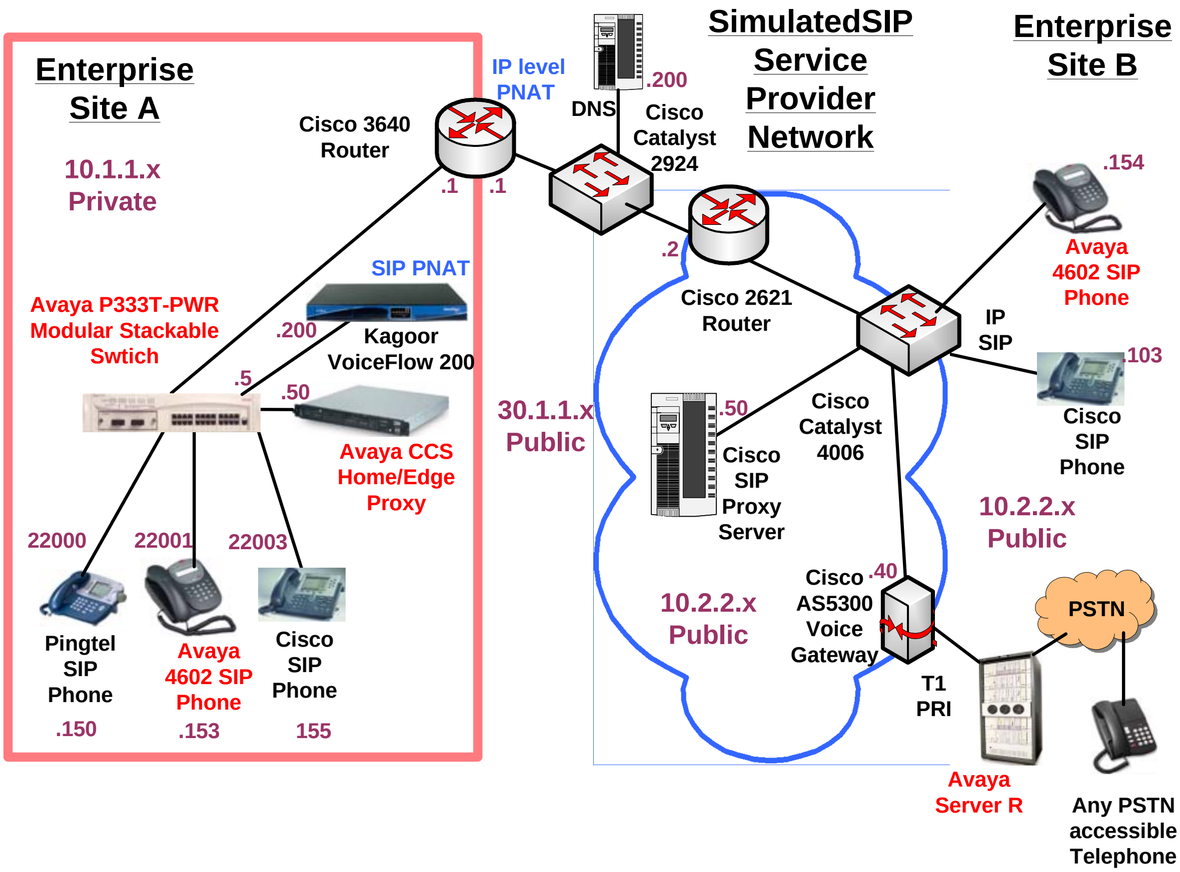


Figure 1: Kagoor VoiceFlow 200/Avaya CCS Test Configuration

2. Equipment and Software Validated

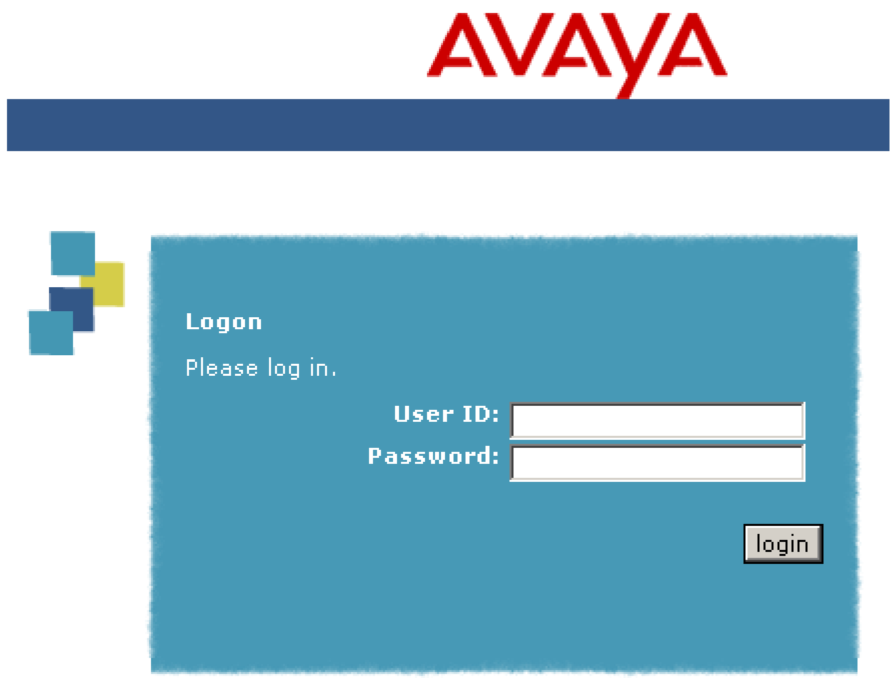
The following equipment and software were used for the configuration in **Figure 1**:

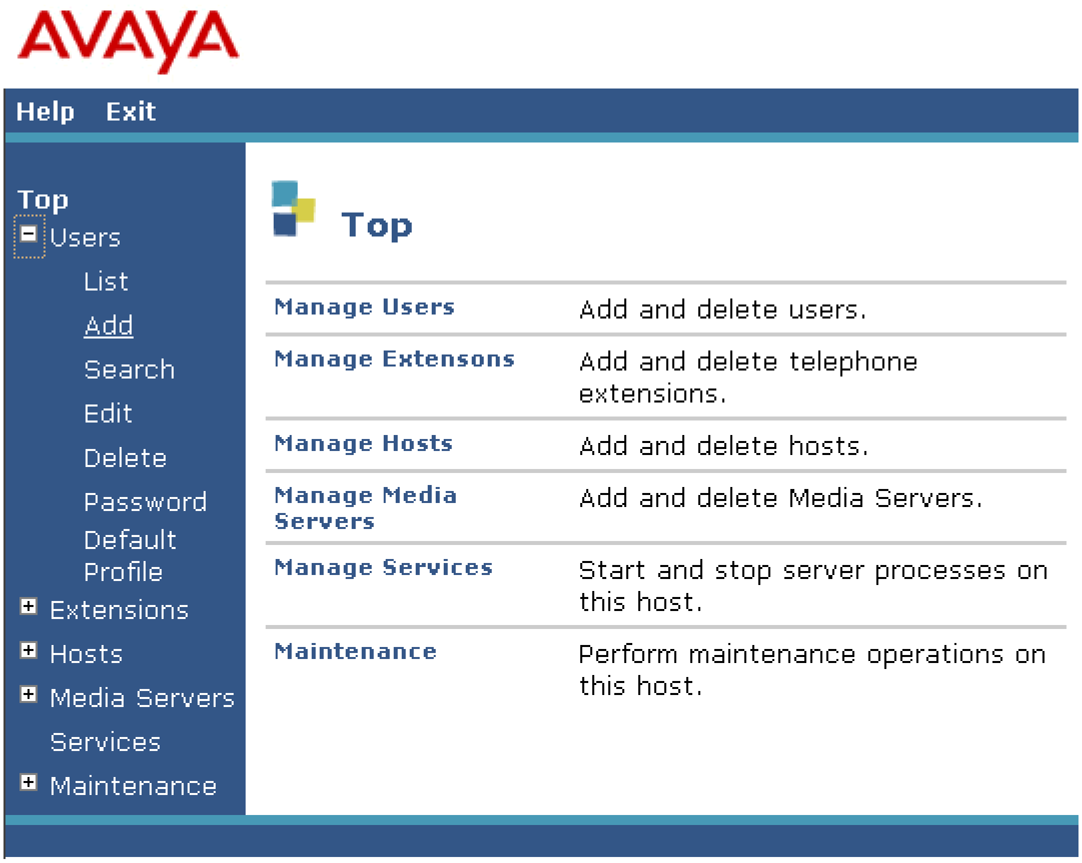
Equipment	Software
Avaya Converged Communication Server (CCS)	15.2
Avaya P333T-PWR Modular Stackable Switch	3.12.1
Avaya 4602 SIP Telephone	0.79
VoiceFlow 200	5.3.1.212
Cisco 7940 SIP Telephone	POS3-04-1-00
Cisco SIP Proxy Server	2.0
Cisco 3640 Router/ NAT	IOS 12.2(4)T
Cisco 2621 Router	IOS 12.2(4)T1
Cisco AS5300 Voice Gateway	12.3(1)
Pingtel SIP Telephone	2.1.7.5

3. Configure the Avaya CCS

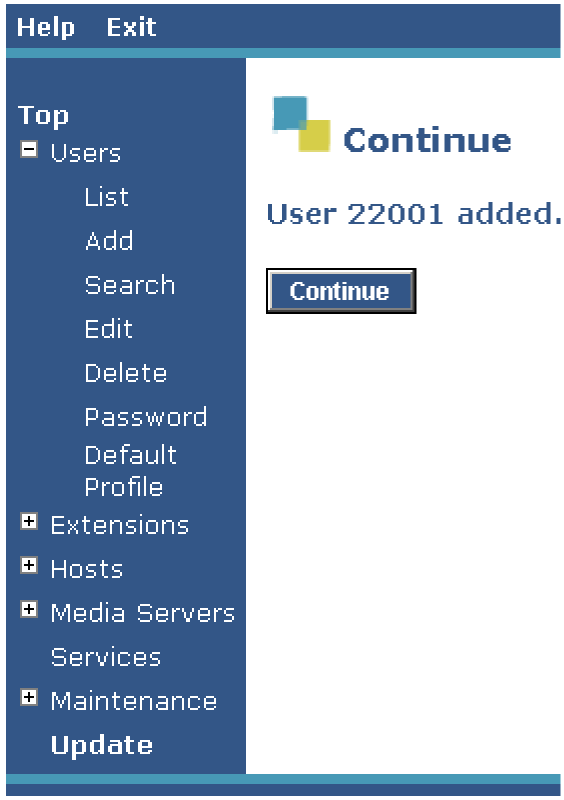
The following steps describe configuration of the Avaya CCS to support a telephony user, and to route calls to the VoiceFlow. Other standard installation and administration functions are covered in Reference [1].

3.1. Adding a SIP Telephone User

Steps	Description
1.	The Avaya CCS is configured using a web browser. Set the URL of the browser to the IP address of the CCS, and log in as *admin* using the appropriate administrator password. 

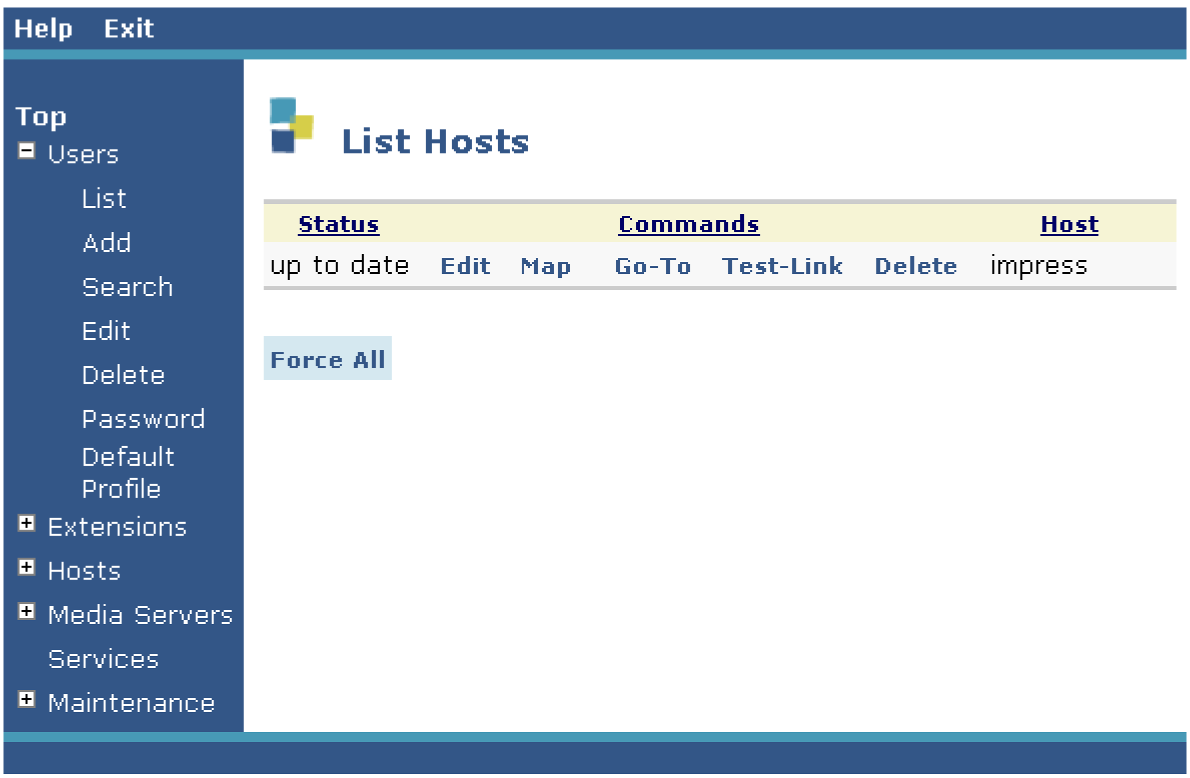
Steps	Description
2.	The CCS administration web interface will be displayed. Expand the **Users** link on the left side of the page and click on **Add**. 

Steps	Description
3.	The *Add User* page will be displayed. Fill in the appropriate fields. In the screen below, the user corresponding to the Avaya 4602 SIP telephone is being added. Enter the extension number in the **Handle** and **User ID** fields.  Click on **Add**.

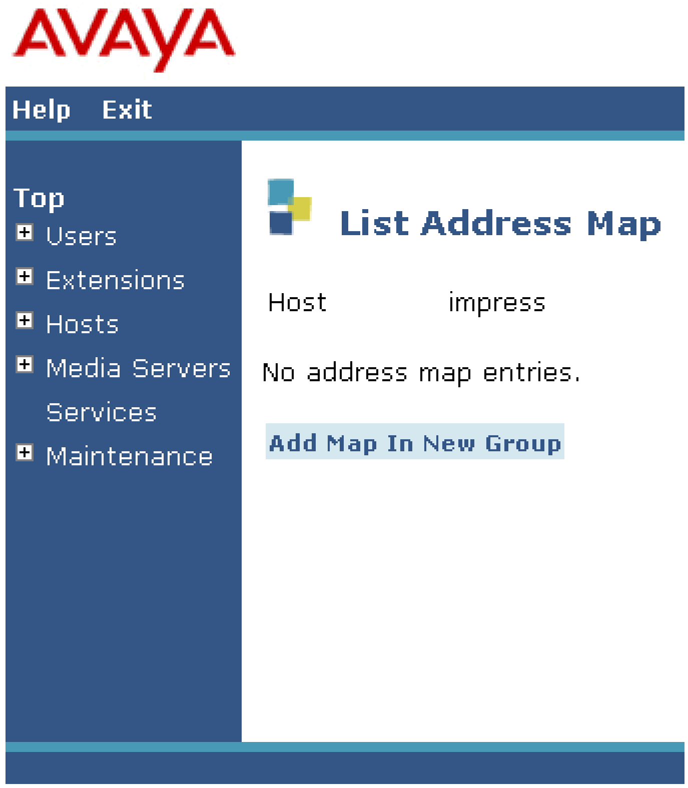
Steps	Description
4.	The confirmation page will be displayed. Click **Continue**.  Repeat Steps 1-4 for each user to be supported.

3.2. Adding an Address Map

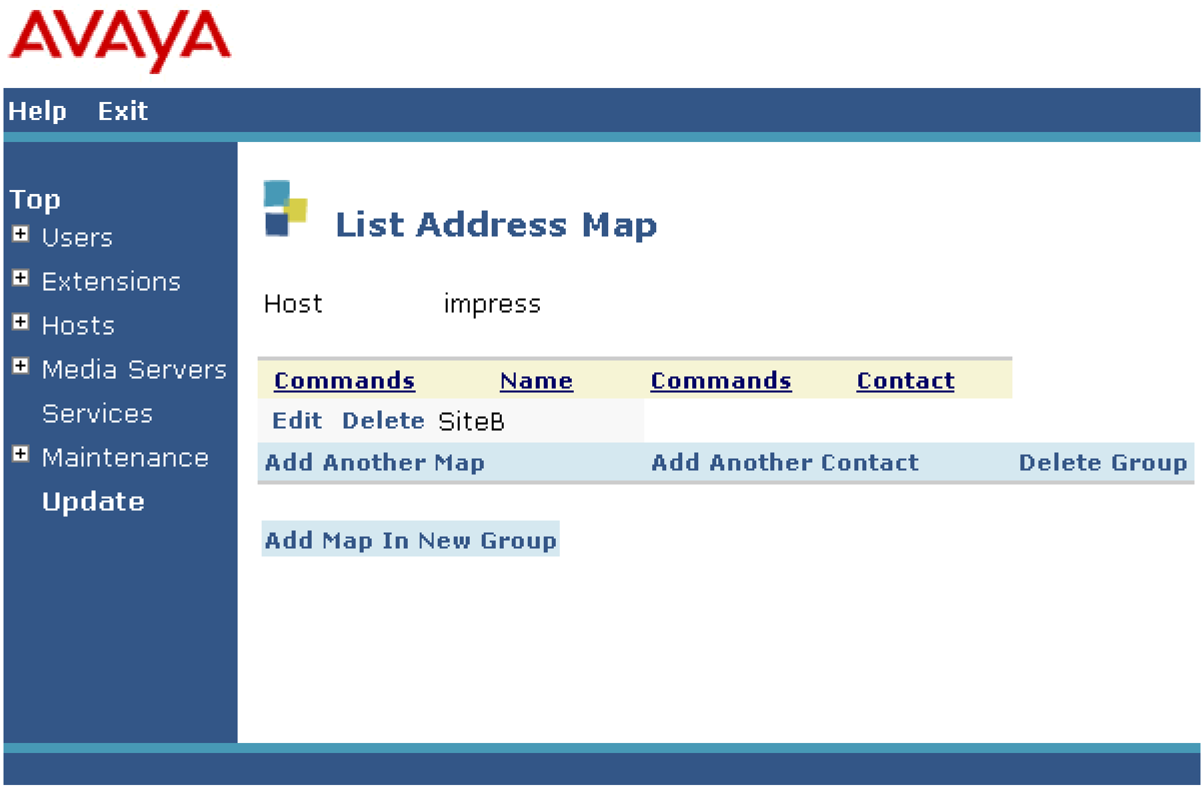
Address maps are used in the CCS to specify how incoming SIP calls are to be routed, based on the dialed number. They are grouped by the SIP contact to which they will be routed. In this configuration, calls to phones at Site B and the PSTN need to be routed to the simulated SSP. The following steps describe how to administer this. See Reference [1] for more information on the syntax used to specify address maps.

<table>
<tr><th>Steps</th><th>Description</th></tr>
<tr><td>1.</td><td>Click on the Hosts link on the left side of the main CCS web page. The List Hosts page is displayed.


Click on Map.</td></tr>
</table>

Steps	Description
2.	The *List Address Map* page is displayed.  Select **Add Map in New Group**.

Steps	Description
3.	The *Add Address Map* page will be displayed. Specify a **Name** for the first address map, and the **Pattern** match specification. In this example, all telephone extensions beginning with 5 are to be routed to Site B. 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 this example, the user is actually the telephone number of the phone. An example of a URI would be sip:50001@pop.ssp.com or sip:50001@10.2.2.50. The specification means "match on the characters 'sip:5' if they occur at the beginning of the URI, followed by any number of digits." Check **Replace URI**. When routing the incoming INVITE, the CCS 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.

Steps	Description
4.	The *List Address Map* page will be displayed again, this time with the updated map information.  Click on **Add Another Map**, so that the next address map will also be associated with the contact to be defined in Step 6.

<table>
<tr><th>Steps</th><th>Description</th></tr>
<tr><td>5.</td><td>

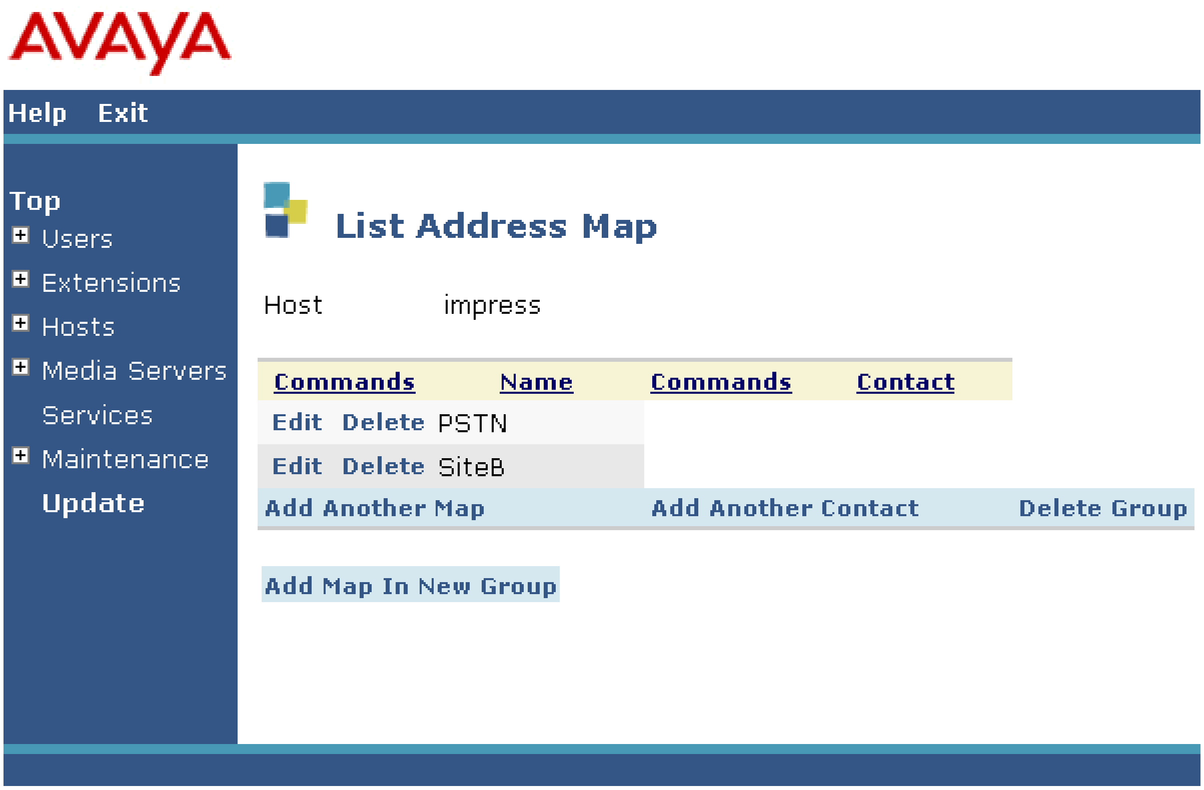
The *Add Address Map* page will be displayed. Again, enter a **Name** and a **Pattern** corresponding to a PSTN number plan (the example specification is very general – much more specific dial plans can be used). This pattern specification matches on a “1” at the beginning of the URI, followed by any number of digits, and will therefore support 11 digit dialing (1 + area code + number).

Click on **Add**; then click on **Continue** on the confirmation page.

</td></tr>
</table>

<table>
<tr><th>Steps</th><th>Description</th></tr>
<tr><td>6.</td><td>

The *List Address Map* page will be displayed again, this time with the updated map information.



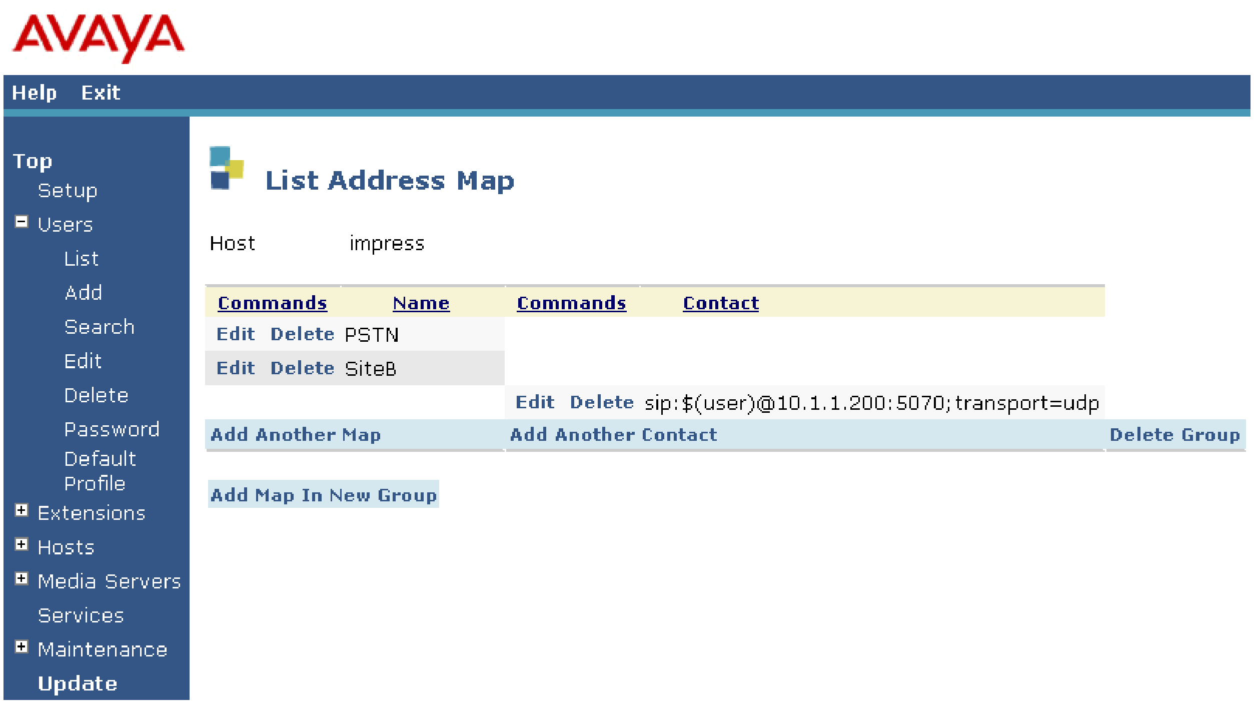
Click on **Add Another Contact**.

</td></tr>
</table>

Steps	Description
7.	The *Add Contact* page will be displayed. In **Contact**, enter the SIP URI corresponding to the inside interface of the VoiceFlow. "$(user)" instructs the CCS to substitute the *user* portion of the URI of the incoming INVITE message at this point in the contact. Port 5070 will be used by the VoiceFlow to associate incoming INVITE messages for routing to the Cisco Proxy (10.2.2.50) (See Section 5.2 Step 5). "transport=UDP" specifies the transport protocol used by the proxy server to receive requests.

Click on **Add**; then click on **Continue** on the confirmation page.

Steps	Description
8.	The *List Address Map* page will be displayed again with the updated map information. The address map administration is now complete. Incoming INVITE messages whose URI matches either the *PSTN* or *SiteB* map specification will be routed to the contact shown.

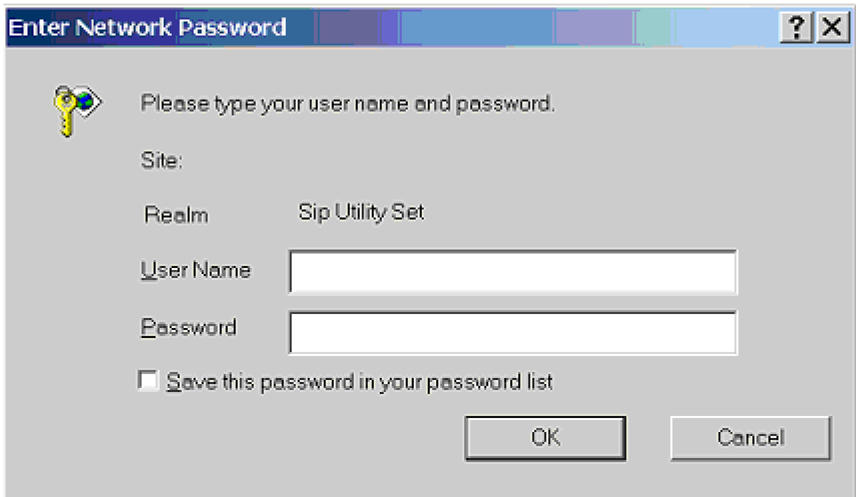


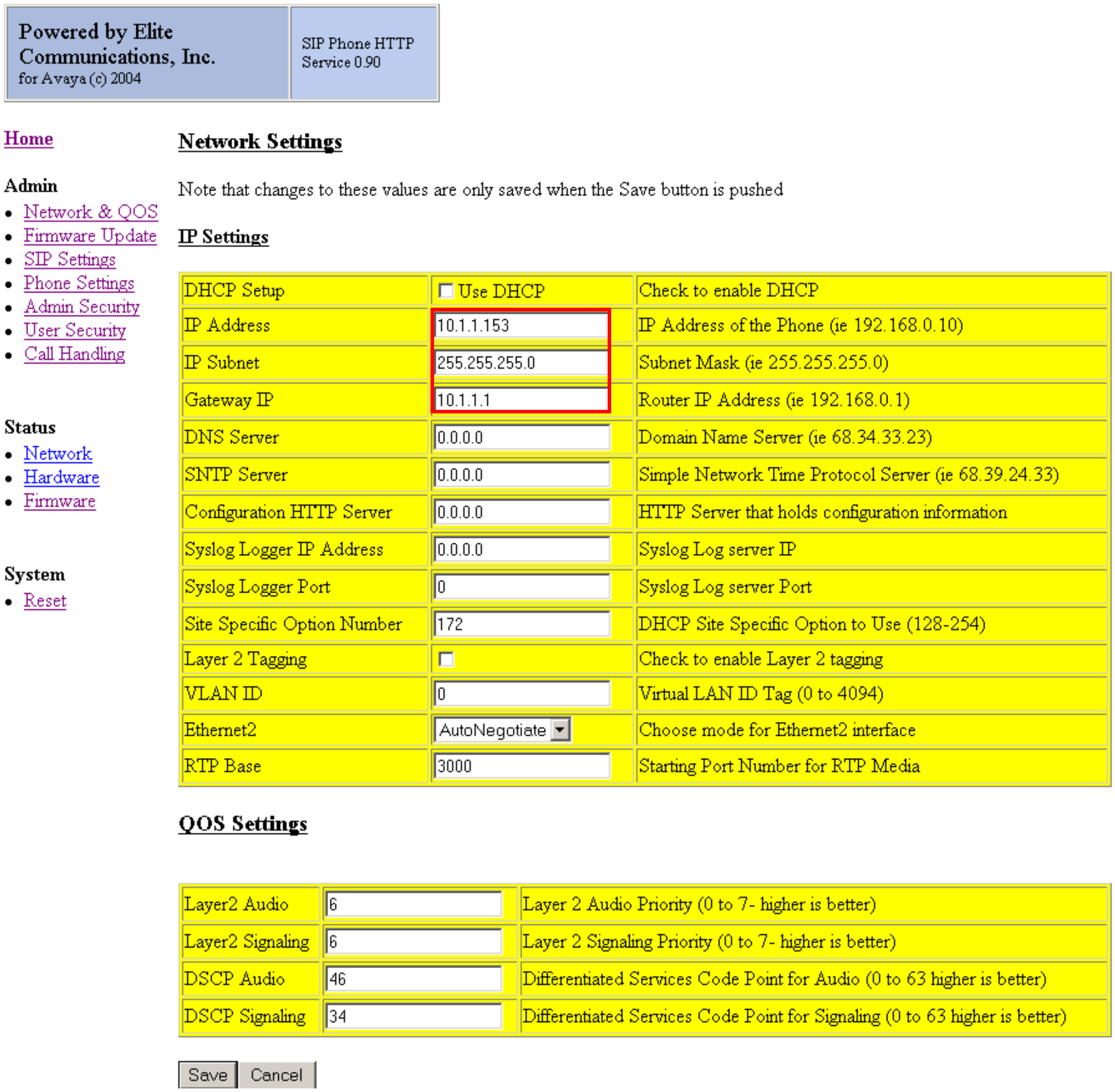
Steps	Description
9.	To apply the administration in Steps 1-8 above, click on **Update** on the left side of the page. This link appears on the current page whenever updates are outstanding, and can be used at any time to save the administration performed to that point.

4. Configure the Avaya 4602 SIP Telephone

The following steps describe how to configure the 4602 SIP telephone to register with the CCS in enterprise Site A. In this configuration, the phone is configured with static settings. Configuration using DHCP and HTTP servers can be found in Reference [2].

Steps	Description
1.	• Apply power to the telephone. During the boot sequence, the message "Press * to Setup" will be displayed. Press ***** on the keypad at this time. • The current IP address will be displayed. Enter the appropriate value and press **#.** • The current IP address mask will be displayed. Enter the appropriate value and press **#.** • Press ***** to end the configuration process at the phone. The remaining configuration can be performed using the web interface in the following steps.

Steps	Description
2.	Set the URL of a browser to the IP address entered in Step 1, and log in as *admin* using the appropriate administrator password.  The 4602 SIP Phone administration web interface will be displayed.

Steps	Description
3.	To assign static network parameters, select the **Network & QOS** link under *Admin* and enter the information outlined below in red. All other parameters can be left as default. Make sure **Use DHCP** is unchecked.  Select **Save**.

Powered by Elite Communications, Inc.
for Avaya (c) 2004

SIP Phone HTTP Service 0.90

Home

Admin
- Network & QOS
- Firmware Update
- SIP Settings
- Phone Settings
- Admin Security
- User Security
- Call Handling

Status
- Network
- Hardware
- Firmware

System
- Reset

Network Settings

Note that changes to these values are only saved when the Save button is pushed

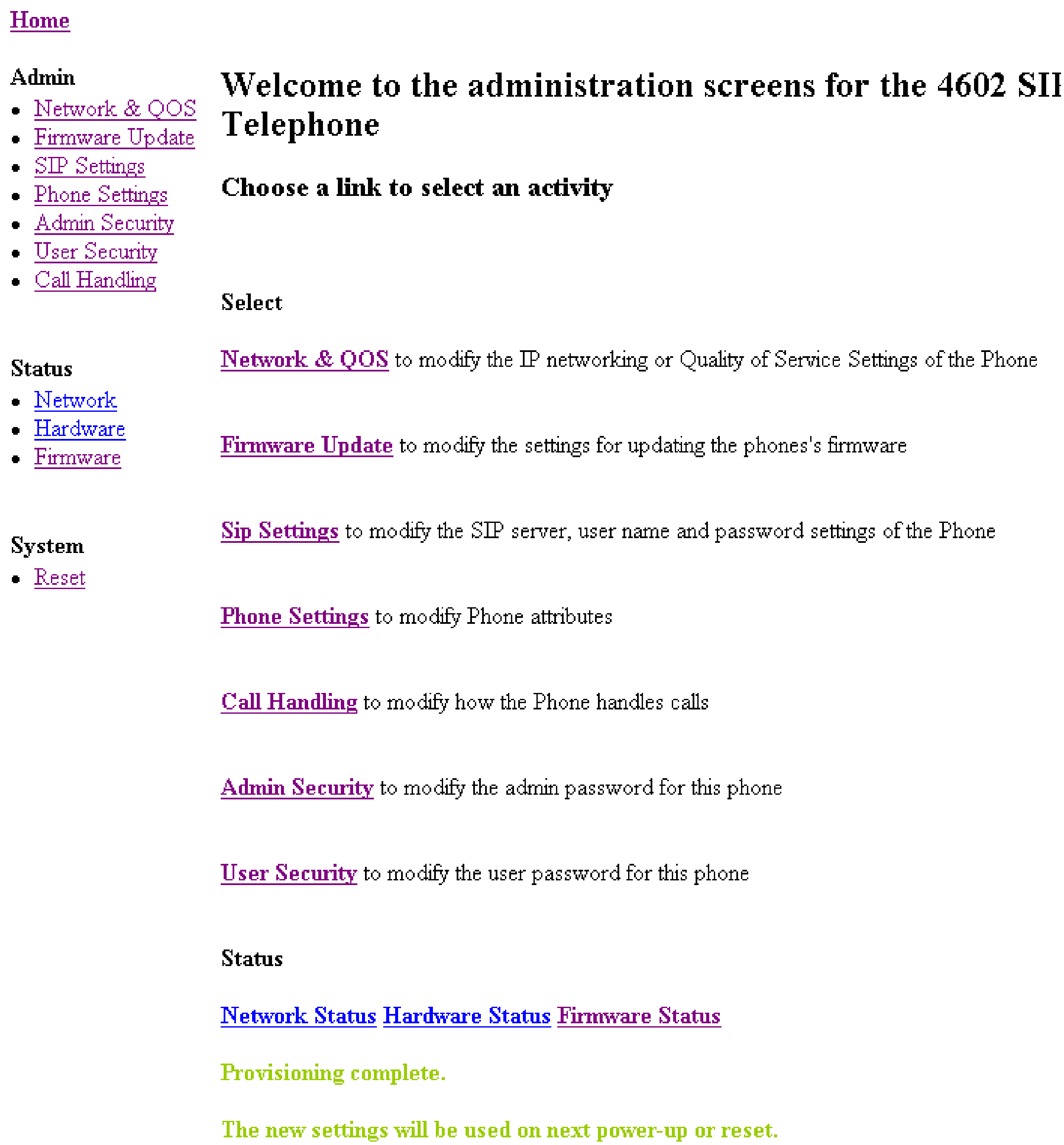
IP Settings

DHCP Setup	☐ Use DHCP	Check to enable DHCP
IP Address	10.1.1.153	IP Address of the Phone (ie 192.168.0.10)
IP Subnet	255.255.255.0	Subnet Mask (ie 255.255.255.0)
Gateway IP	10.1.1.1	Router IP Address (ie 192.168.0.1)
DNS Server	0.0.0.0	Domain Name Server (ie 68.34.33.23)
SNTP Server	0.0.0.0	Simple Network Time Protocol Server (ie 68.39.24.33)
Configuration HTTP Server	0.0.0.0	HTTP Server that holds configuration information
Syslog Logger IP Address	0.0.0.0	Syslog Log server IP
Syslog Logger Port	0	Syslog Log server Port
Site Specific Option Number	172	DHCP Site Specific Option to Use (128-254)
Layer 2 Tagging	☐	Check to enable Layer 2 tagging
VLAN ID	0	Virtual LAN ID Tag (0 to 4094)
Ethernet2	AutoNegotiate	Choose mode for Ethernet2 interface
RTP Base	3000	Starting Port Number for RTP Media

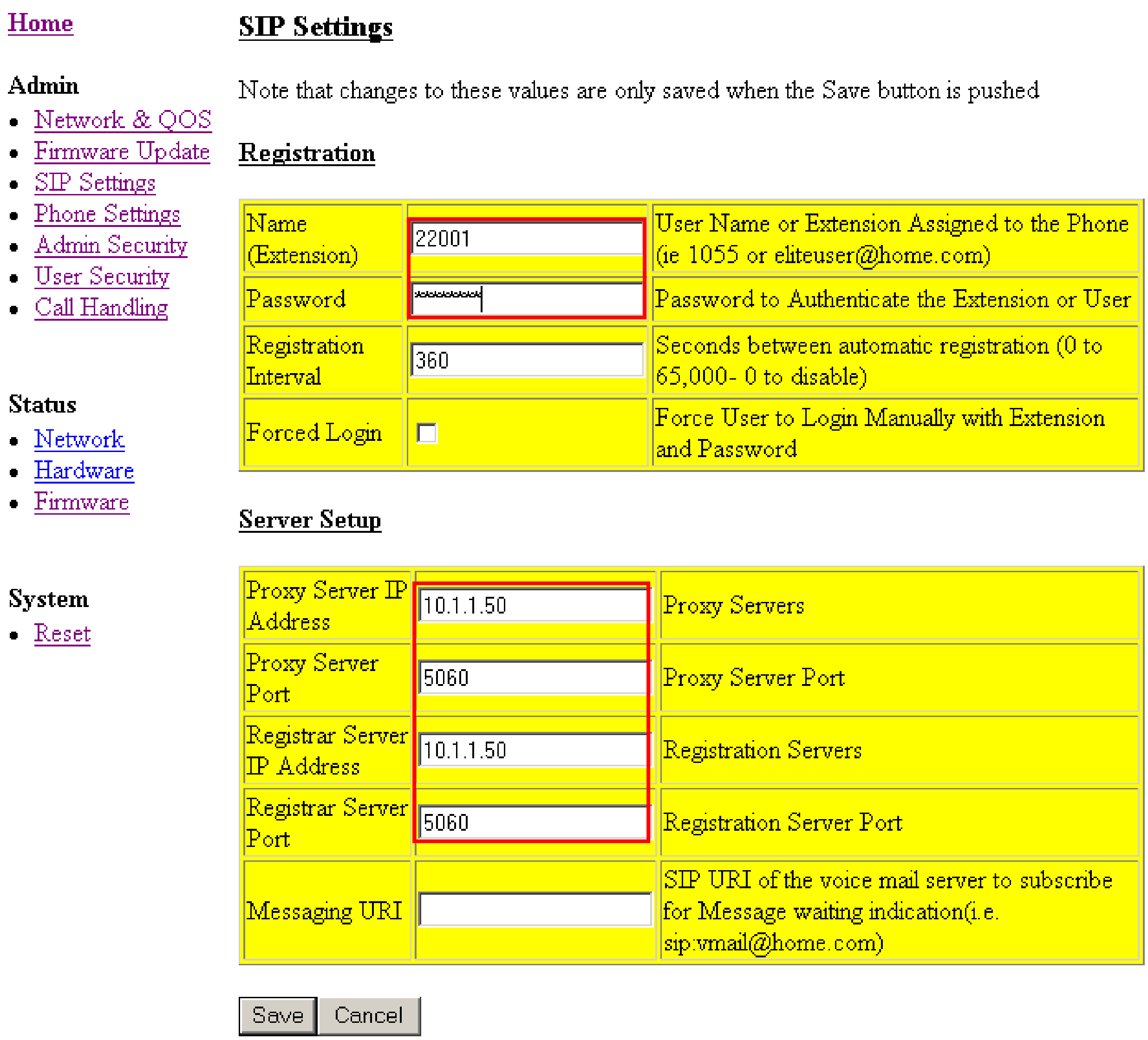
QOS Settings

Layer2 Audio	6	Layer 2 Audio Priority (0 to 7- higher is better)
Layer2 Signaling	6	Layer 2 Signaling Priority (0 to 7- higher is better)
DSCP Audio	46	Differentiated Services Code Point for Audio (0 to 63 higher is better)
DSCP Signaling	34	Differentiated Services Code Point for Signaling (0 to 63 higher is better)

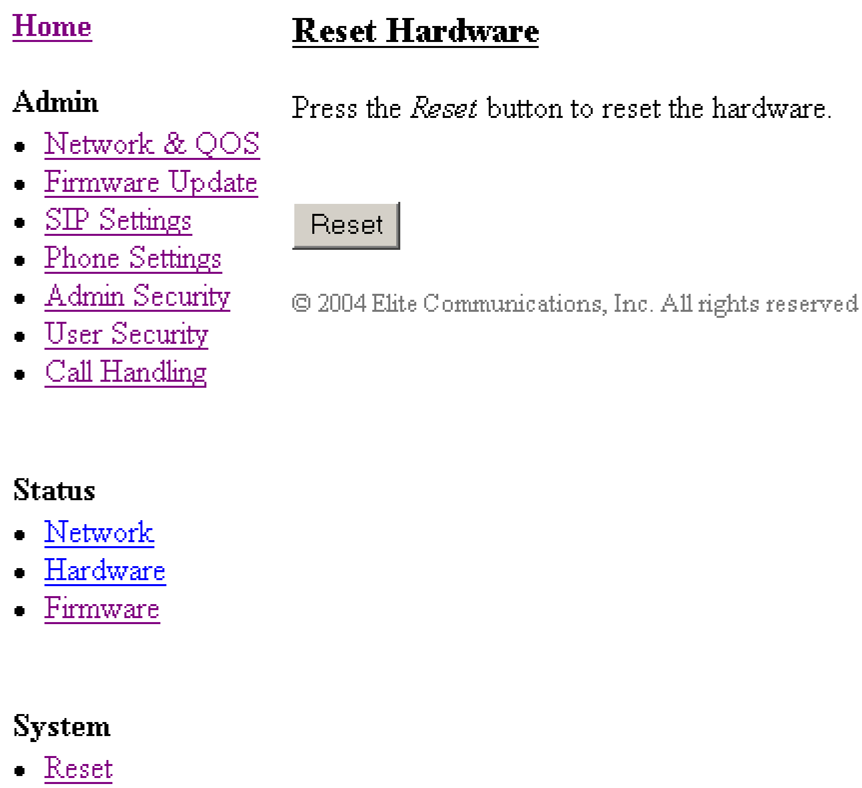
Save Cancel

Steps	Description
4.	The main administration web page will be displayed as shown below. Check the bottom of the page for the green confirmation message. 

<table>
<tr><th>Steps</th><th>Description</th></tr>
<tr><td>5.</td><td>To set the SIP parameters, select the SIP Settings link under Admin and enter the information outlined below in red. In this configuration, the phone will be registering to the CCS (10.1.1.50).



Select Save, and check the main administration page displayed next for the green confirmation message.</td></tr>
</table>

Steps	Description
6.	Select the **Reset** link under *System*. The Reset Hardware page will be displayed.  Click the **Reset** button to confirm. This will reset the phone and put the saved settings into effect. The phone will then attempt to register with the CCS. The following display will appear on the phone, indicating successful registration. 

5. Configure the VoiceFlow 200

The following steps describe administration of the VoiceFlow, configured as shown in **Figure 1**. The VoiceFlow is administered using a command line interface (CLI). First, the Ethernet interface must be configured. This can be accomplished using the COM 1 serial port, as described in the next section.

5.1. Configure the Ethernet Interface

Attach a serial cable to the COM 1 serial port. Using a terminal emulator program, access the port using the following parameters:

Speed	9600
Parity	None
Number of Data Bits	8
Number of Stop Bits	1
Flow Control	None

Note – Use *tab* to complete a partial command string.

1. Press Enter to get the prompt.

```
Welcome to VoiceFlow
ALG-V/OS [ip missing]>
```

2. Type *enable* and press Enter.

```
ALG-V/OS [ip missing]>enable
```

3. Enter the appropriate password when prompted to enter enabled mode.

   The prompt will change to:

```
ALG-V/OS [ip missing]#
```

4. Enter maintenance mode by entering *mode maintenance.*

```
ALG-V/OS [ip missing]>mode maintenance
```

IMPORTANT – While in maintenance mode, the VoiceFlow will NOT process traffic.

5. Set the IP address of the VoiceFlow.

ALG-V/OS [ip missing]# **ip 10.1.1.200/24**

The prompt will change to:

ALG-V/OS 10.1.1.200#

6. Set the default gateway.

ALG-V/OS 10.1.1.200# **default-gateway 10.1.1.1**

7. Exit maintenance mode by entering *mode normal.*

ALG-V/OS 10.1.1.200# **mode normal**

8. Verify that the VoiceFlow is in normal mode by entering *show mode.*

ALG-V/OS 10.1.1.200# **show mode**

The VoiceFlow will return the following message:

ALG-V/OS 10.1.1.200#	
mode:	normal

9. Verify the changes by entering *show ip.*

ALG-V/OS 10.1.1.200# **show ip**

The VoiceFlow will return the following message:

IP Address:	10.1.1.200
Default Gateway:	100.1.1.1

5.2. Configure NAT

The following steps illustrate administration of NAT for the sample configuration in **Figure 1**. In general, Kagoor performs NAT on the SIP headers by dynamically assigning different port numbers to the single public address (port NAT). In the case of SIP proxy servers however, it is necessary to identify the servers by statically assigning a port number to each (see *nat-static* command below). The Kagoor identifies "server" SIP devices as residing on its public side or *outside*, and "endpoint" devices as residing on the private side or *inside*.

Architecturally, the VoiceFlow supports NAT with an application module, or "SoftBlade." This NAT blade is configured in the following steps. If continuing from the previous section, remain in the enabled and maintenance modes (i.e., skip Step 1).

1. Enter maintenance mode by entering *mode maintenance* (To check the current mode, enter *show mode*).

ALG-V/OS 10.1.1.200# **mode maintenance**

IMPORTANT – While in maintenance mode the VoiceFlow will NOT process traffic.

2. Enter *blade nat.*

ALG-V/OS 10.1.1.200# **blade nat**

The prompt will change to:

ALG-V/OS 10.1.1.200 (nat)#

3. Set the NAT mode to correspond to the Application Level Gateway mode.

ALG-V/OS 10.1.1.200# **nat-mode alg**

4. Identify the address space of the private side, and the public IP address.

ALG-V/OS 10.1.1.200# **inside 10.1.0.0/16** ALG-V/OS 10.1.1.200# **outside 30.1.1.4**

5. Enter the following commands to set up static NAT assignments for the two proxy servers in the sample configuration. The Cisco proxy server is at 10.2.2.50 port 5060 on the public side, so the *server* designation should be used. The CCS is 10.1.1.50 port 5060 on the private side, and should be designated as *endpoint*. In order for the Kagoor to map requests to the appropriate server, a unique port number must be associated with each, in this case 5060 for CCS and 5070 for Cisco proxy. When a phone at Site B calls Site A, the INVITE message received by the Kagoor at 30.1.1.4 on port 5060 will be routed to the CCS (10.1.1.50:5060). When a phone at Site A calls Site B or the PSTN, the INVITE received at 10.1.1.200 on port 5070 will be routed to the Cisco proxy (10.2.2.50:5060).[1]

[1] See Section 3.2 Step 7 on how the CCS is administered to route calls to the public side through the Kagoor.

```
ALG-V/OS 100.2.2.80(nat)# nat-static sip 10.2.2.50:5060 5070 server
ALG-V/OS 100.2.2.80(nat)# nat-static sip 10.1.1.50:5060 5060 endpoint
```

6. Exit NAT mode by entering *exit.*

```
ALG-V/OS 100.2.2.80(nat)#exit
```

7. Exit maintenance mode by entering *mode normal.*

```
ALG-V/OS 100.2.2.80#mode normal
```

6. Interoperability Compliance Testing

The test plan used for compliance testing was Reference [4]. The test configuration was identical to that of **Figure 1**, and focused on SIP telephony interoperability, as opposed to instant messaging and presence features. The results from an existing test plan executed against the test bed without the VoiceFlow were compared to those with the VoiceFlow installed.

6.1. General Test Approach

Feature and functional testing was performed manually. Testing verified the ability of the VoiceFlow to:

- Route SIP call requests inbound to and outbound from the enterprise.
- Perform NAT at both the IP and SIP/SDP layers on SIP signaling and media traffic.

6.2. Test Results

All test cases passed. In all cases, the VoiceFlow performed the tested features as expected. No VoiceFlow-specific issues were observed.

7. Verification Steps

The following verification steps can be used when troubleshooting configurations in the field:

- Verify that the Avaya 4602 SIP telephone has registered to the CCS by looking at the display (see Section 4, Step 6). If the following display appears, registration has failed:

  No Service

  Verify that the 4602 was administered with the correct IP address for the CCS in the Proxy Server IP Address *and* Registrar Server IP Address fields.

- Make a call from a 4602 in Site A to a SIP phone in Site B. Verify good quality audio in both directions. If the call fails, use a SIP-capable network analyzer to verify that the INVITE message is being routed from the CCS to the VoiceFlow. If it is not, check the address map(s) administered in the CCS (Section 3.2). Also, check that the transport protocol supported by the remote SIP proxy server is correctly specified. If these are correct, use the analyzer to verify that the VoiceFlow routes the INVITE to the remote site. If it is not, check the *nat-static* administration in the VoiceFlow (Section 5.2, Step 5).

- Make a call from a SIP phone at the remote site to the 4602 at Site A. Verify good quality audio in both directions. If the call fails, use the techniques described in the previous step to verify proper routing of the INVITE message from the SSP to the VoiceFlow, and then on to the CCS.

8. Support

Sales information is available from Kagoor on 1-650-572-7200 or by emailing info@kagoor.com. Technical support is available on 1-866-5-KAGOOR or by emailing to support@kagoor.com.

9. Conclusion

The Kagoor VoiceFlow 200 has been successfully compliance tested in the configuration outlined in these Application Notes. The administration steps provided here can be used to implement SIP-aware NAT in the enterprise without changing the existing router and firewall configurations.

10. Additional References

[1] *Converged Communications Server Installation and Administration,* Doc # 555-245-705, February, 2004.

[2] *4602 SIP Telephone – Release 1.0 Administrator's Guide,* Doc # 16-300037, Issue 1.0, May 2004.

[3] *The VoiceFlow series v/OS Release 5.3 CPE Border Controller Installation & User Manual, Part No. DO-0024-01*.

[4] *Interoperability Test Plan and Results for Avaya R2.0 CCS and CM SIP offers with Kagoor SIP-Aware NAT Products,* April 26, 2003, Issue 1.0, Fred Schmidt and James Feeney.

[5] *Configuring Kagoor VoiceFlow 3000 Network NAT Traversal (NTRV) in a Hosted Telephony SIP Environment - Issue 1.0*

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 Developer*Connection* Program at devconnect@avaya.com.