



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

---

# **Application Notes for Avaya IP Office and Avaya VPNremote Phone – Issue 1.0**

### **Abstract**

These Application Notes describe a sample configuration of the Avaya IP Office 412 with an Avaya VPNremote Phone. This solution can be used for a remote worker who wants to use a multi-button telephone and have the same functionality (for example, Message Waiting Indication) as a telephone co-located with the IP Office. The Virtual Private Network (VPN) spans from the Avaya VPNremote Phone at the remote location to an Avaya Security Gateway 203 that connects to the Avaya IP Office 412 at the main site. Testing was conducted at the Avaya Solution and Interoperability Test Lab.

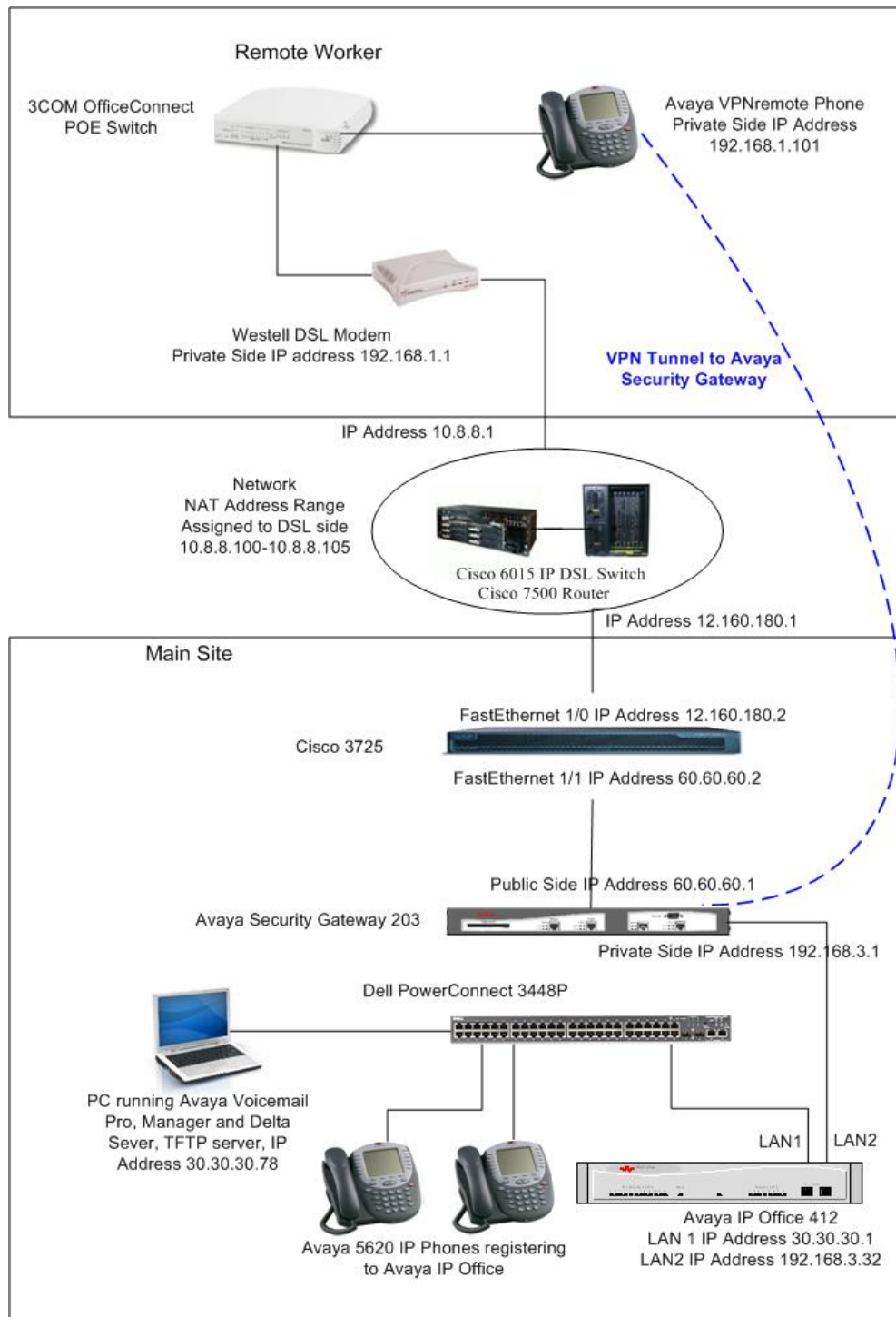
# 1. Introduction

As illustrated in **Figure 1**, the Avaya VPNremote Phone registers to an Avaya IP Office 412 via an Avaya Security Gateway 203. A VPN tunnel spans between the Avaya Security Gateway and the VPNremote Phone. The VPNremote Phone has the same IP Office feature operation as any other Avaya IP telephone.

The VPNremote Phone firmware is available with the 4610SW, 4620SW or 4621SW<sup>1</sup> model telephones.

---

<sup>1</sup> These are the only VPNremote Phones supported on IP Office.



**Figure 1: Avaya VPNremote Phone registered to Avaya IP Office 412**

This document does not describe the configuration of the Cisco 6015 IP DSL switch and the Cisco 7500 Router. For an example of a similar configuration, see item [4] of the Additional References section.

Quality of Service configuration is not described in this document.

The configuration of the Avaya Security Gateway 203 firewall, other than what is needed for the VPN, is not described in this document.

## **1.1. IP Office Features**

The configuration presented in this document uses the IP Office Hot Desking feature. This allows a user to easily switch from an office phone to the VPNremote Phone with the ability to have one telephone number by logging into the telephone of choice. A user can go to either the office phone or the VPNremote Phone and log in (via a short code). Once the user has successfully logged in, the functionality that is available is provided (for example message waiting, programmed buttons and feature access). Once the user is done working, the user can log out. Calls to the logged out user receive coverage or busy treatment.

The following features were successfully tested in this configuration:

1. Message Waiting Indication for the Hot Desk Extension at the VPNremote Phone.
2. Call Recording at the VPNremote Phone. See Step 2 in Section 3 for details.
3. Call Intrude capability from a user at Main Site to the VPNremote Phone.
4. Delta Server information for the VPNremote Phone user. The Compact Business Center (CBC), Compact Contact Center (CCC) and SMDR applications use this information.
5. User and Hunt Group button operation at the Avaya VPNremote Phone.
6. Bridged and Line Appearance buttons at the Avaya VPNremote Phone.

Note: The Call Listen capability on IP Office is not available on the Avaya VPNremote Phone. This is the same restriction as other IP telephones registered to an IP Office.

## 2. Equipment and Software Validated

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

Quantity	Device Description	Versions Tested
1	Avaya IP Office 412	3.1.56
1	Avaya Delta Server	3.1.5
1	Avaya IP Office Voicemail Pro	3.1.16
2	Avaya 5610 IP Telephones	2.3
1	Avaya VPNremote Phone (4620SW)	2.3
1	Avaya Security Gateway 203	4.6
1	Dell PowerConnect™ 3448P switch	1.0.0.112
1	Westell 2200 DSL Modem	01.06.53
1	Cisco 3725	OS version 12.2(8r)T2 Software (fc1)
1	3COM OfficeConnect Managed Switch 9	Software: 1.01 Hardware: R01B
1	Cisco 6015 IP DSL Switch	12.2(12)DA
1	Cisco 7500 Router	12.2(32)

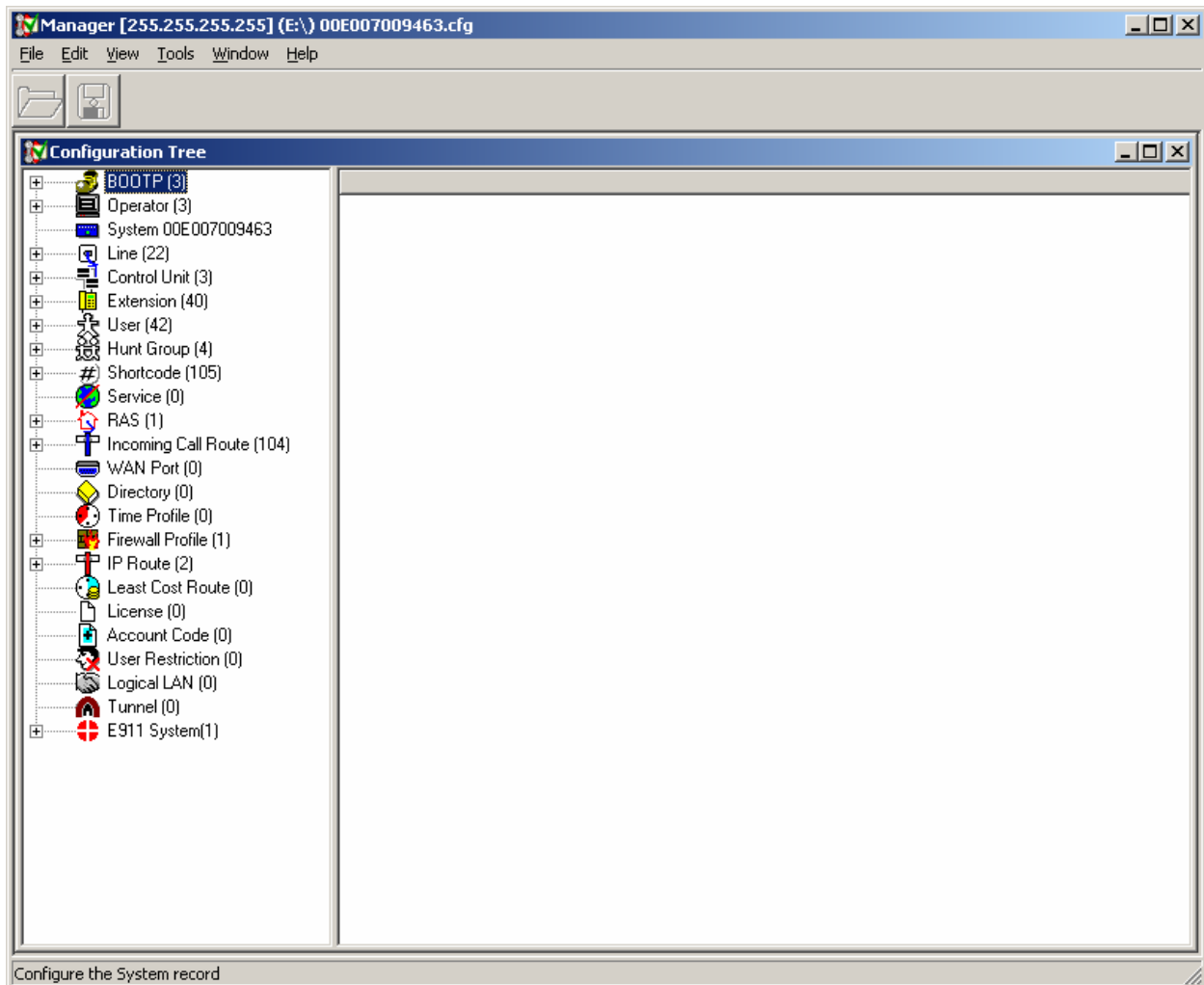
## 3. Configure IP Office at Main Site

This section describes the IP Office configuration at Main Site. This includes configuring:

1. An IP Extension,
2. A Hot Desk User,
3. A default IP Route to the Avaya Security Gateway,
4. Short Codes for the ExtnLogin and ExtnLogout features

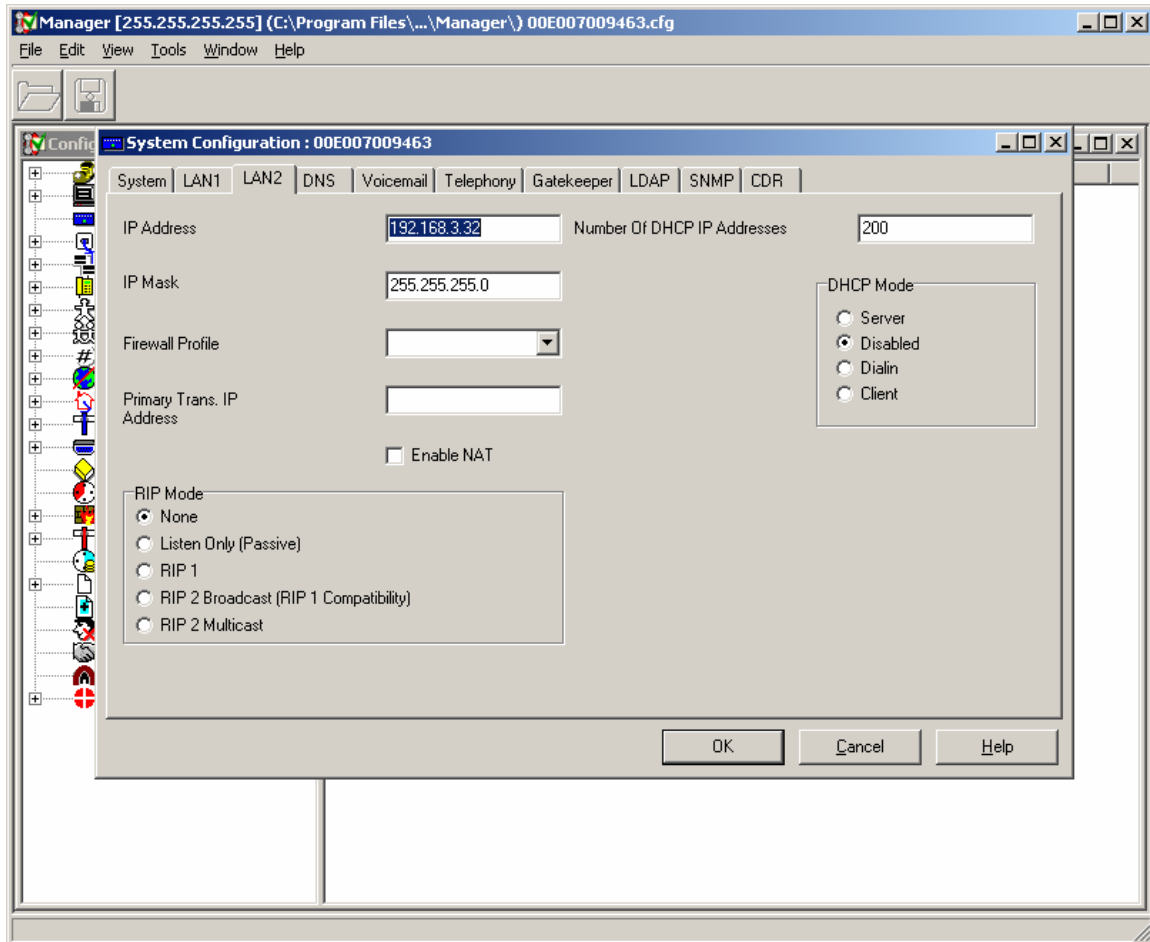
IP Office is configured via the IP Office Manager program. Log into the IP Office Manager PC and select **Start** → **Programs** → **IP Office** → **Manager** to launch the Manager application. Log into the Manager application using the appropriate credentials.

There are two panels in IP Office Manager. The left panel contains the configuration tree. Select from the Configuration tree, as described in the following steps, to configure the system.



1. *Configure the LAN2 IP Address.* In IP Office Manager, select **System** in the left panel. Double-click on the entry in the right panel.

Select the **LAN2** Tab. Enter an **IP Address** and **Mask** and set the **DHCP Mode** to **Disabled**. Press the **OK** button.



2. *Configure a user for the VPN remote Phone.* In IP Office Manager, select **User** in the left panel. In the right panel, right click and select the **New** option. Enter a unique **Name** and **Extension** number. Press the **OK** button.

Manager [255.255.255.255] (E:\) 00E007009463.cfg

File Edit View Tools Window Help

**User VPNremote Phone**

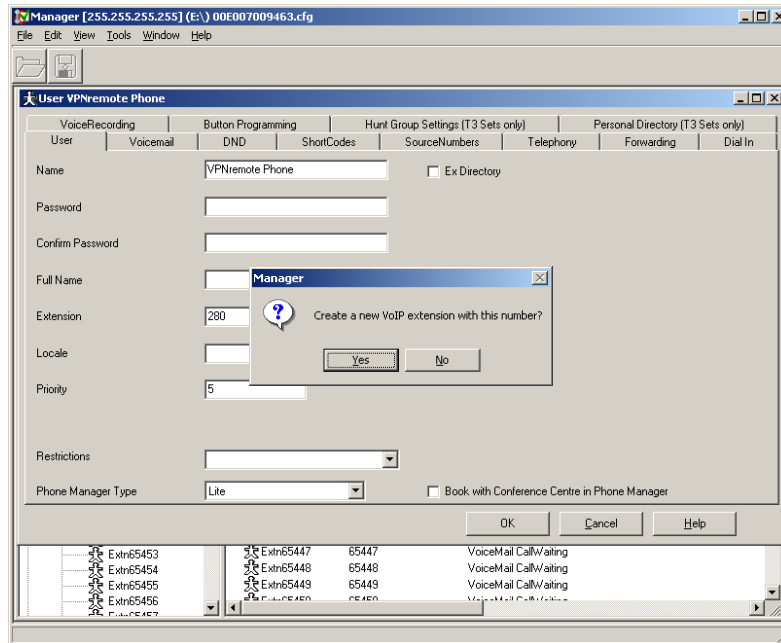
VoiceRecording		Button Programming		Hunt Group Settings (T3 Sets only)		Personal Directory (T3 Sets only)	
User	VoiceMail	DND	ShortCodes	SourceNumbers	Telephony	Forwarding	Dial In
Name	VPNremote Phone			<input type="checkbox"/> Ex Directory			
Password							
Confirm Password							
Full Name							
Extension	280						
Locale							
Priority	5						
Restrictions							
Phone Manager Type	Lite			<input type="checkbox"/> Book with Conference Centre in Phone Manager			

OK Cancel Help

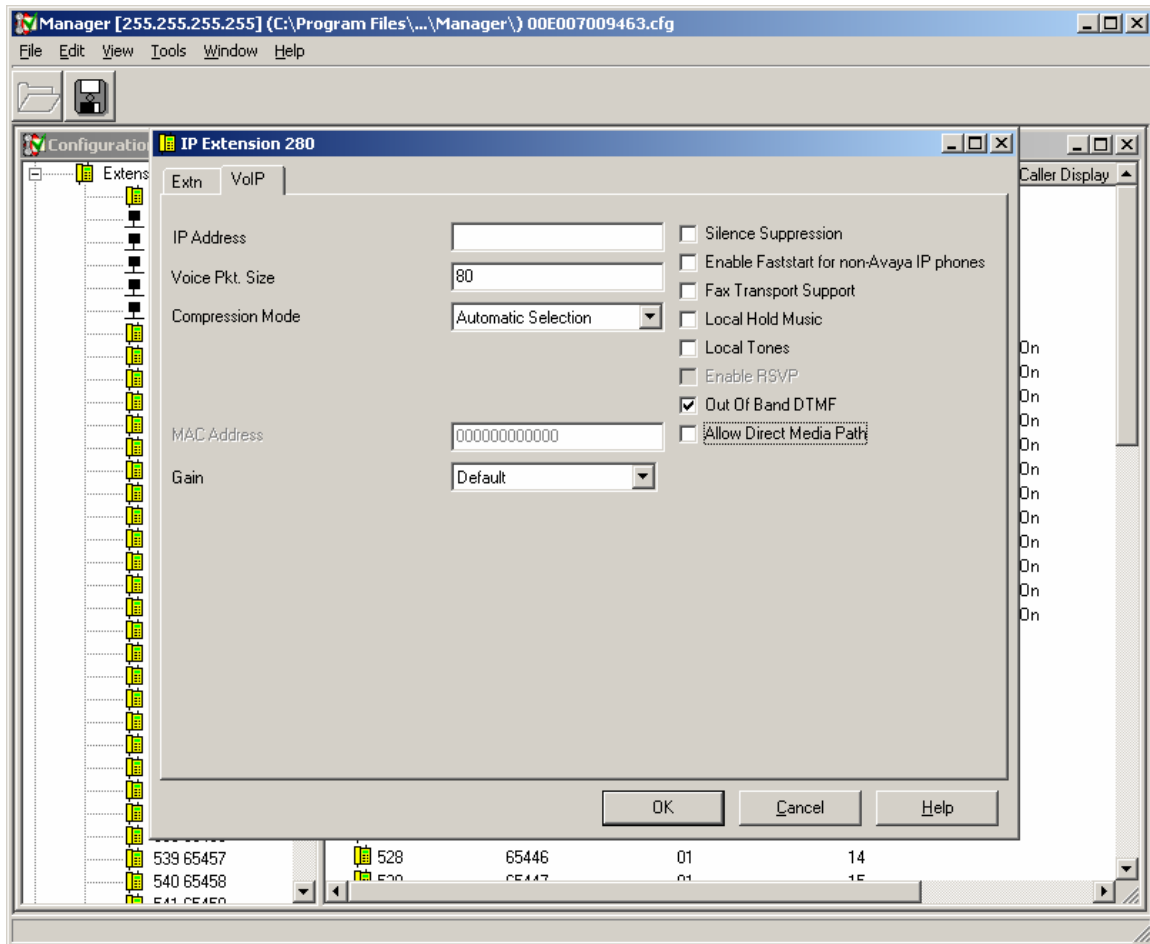
Extn65453	Extn65447	65447	VoiceMail CallWaiting
Extn65454	Extn65448	65448	VoiceMail CallWaiting
Extn65455	Extn65449	65449	VoiceMail CallWaiting
Extn65456	Extn65450	65450	VoiceMail CallWaiting



3. *Complete the user.* Choose the **Yes** option for creating a new VoIP extension. This will create a default IP Extension for the user.



4. *Configure the Direct Media options for the VPNremote Phone extension.* Follow this step when the Call Recording feature is going to be used at the VPNremote Phone. In IP Office Manager, select Extensions in the left panel. Select the extension created in the previous step in the right panel and double click on it. Select the **VoIP** Tab. Un-check the **Allow Direct Media Path** option. Press the **OK** button. With this setting, a Voice Compression Module (VCM) channel will be used for all calls involving this extension. VCM channels are hardware resources configured at installation. If Call Recording is being used on the system and there will be users with VPNremote Phone, it should be taken into account when planning the system.



- 
- Manager [255.255.255.255] (C:\Program Files\...\Manager\)\\_00E007009463.cfg
- File Edit View Tools Window Help
- User Hot Desk 277
- VoiceRecording Button Programming Hunt Group Settings (T3 Sets only) Personal Directory (T3 Sets only)
- User Voicemail DND ShortCodes SourceNumbers Telephony Forwarding Dial In
- Name Hot Desk 277 ☐ Ex Directory
- Password
- Confirm Password
- Full Name
- Extension 277
- Locale
- Priority 5
- Restrictions
- Phone Manager Type Lite ☐ Book with Conference Centre in Phone Manager
- OK Cancel Help
- Extn65453 Extn65443 65443 VoiceMail CallWaiting
- Extn65454 Extn65444 65444 VoiceMail CallWaiting
- Extn65455 Extn65445 65445 VoiceMail CallWaiting
- Extn65456 Extn65446 65446 VoiceMail CallWaiting
- Extn65457 Extn65447 65447 VoiceMail CallWaiting
- Extn65458 Extn65448 65448 VoiceMail CallWaiting
- Extn65459 Extn65449 65449 VoiceMail CallWaiting
- Extn65460 Extn65450 65450 VoiceMail CallWaiting
- Extn65461 Extn65451 65451 VoiceMail CallWaiting
- Extn65462 Extn65452 65452 VoiceMail CallWaiting
- Extn65463 Extn65453 65453 VoiceMail CallWaiting
- Extn65464 Extn65454 65454 VoiceMail CallWaiting
- Extn65465 Extn65455 65455 VoiceMail CallWaiting
- Extn65466 Extn65456 65456 VoiceMail CallWaiting
- Extn65467 Extn65457 65457 VoiceMail CallWaiting
- Extn65468 Extn65458 65458 VoiceMail CallWaiting
- Extn65469 Extn65459 65459 VoiceMail CallWaiting
- Extn65470 Extn65460 65460 VoiceMail CallWaiting
- Extn65471 Extn65461 65461 VoiceMail CallWaiting
- Extn65472 Extn65462 65462 VoiceMail CallWaiting
- Extn65473 Extn65463 65463 VoiceMail CallWaiting
- Extn65474 Extn65464 65464 VoiceMail CallWaiting
- Extn65475 Extn65465 65465 VoiceMail CallWaiting
- Extn65476 Extn65466 65466 VoiceMail CallWaiting
- Extn65477 Extn65467 65467 VoiceMail CallWaiting
- Extn65478 Extn65468 65468 VoiceMail CallWaiting
- Extn65479 Extn65469 65469 VoiceMail CallWaiting
- Extn65480 Extn65470 65470 VoiceMail CallWaiting
- Extn65481 Extn65471 65471 VoiceMail CallWaiting
- Extn65482 Extn65472 65472 VoiceMail CallWaiting
- Extn65483 Extn65473 65473 VoiceMail CallWaiting
- Extn65484 Extn65474 65474 VoiceMail CallWaiting
- Extn65485 Extn65475 65475 VoiceMail CallWaiting
- Extn65486 Extn65476 65476 VoiceMail CallWaiting
- Extn65487 Extn65477 65477 VoiceMail CallWaiting
- Extn65488 Extn65478 65478 VoiceMail CallWaiting
- Extn65489 Extn65479 65479 VoiceMail CallWaiting
- Extn65490 Extn65480 65480 VoiceMail CallWaiting
- Extn65491 Extn65481 65481 VoiceMail CallWaiting
- Extn65492 Extn65482 65482 VoiceMail CallWaiting
- Extn65493 Extn65483 65483 VoiceMail CallWaiting
- Extn65494 Extn65484 65484 VoiceMail CallWaiting
- Extn65495 Extn65485 65485 VoiceMail CallWaiting
- Extn65496 Extn65486 65486 VoiceMail CallWaiting
- Extn65497 Extn65487 65487 VoiceMail CallWaiting
- Extn65498 Extn65488 65488 VoiceMail CallWaiting
- Extn65499 Extn65489 65489 VoiceMail CallWaiting
- Extn65500 Extn65490 65490 VoiceMail CallWaiting

6. *Configure the Hot Desking options.* Select the **Telephony** tab. Check the **Force Login** box and enter a **Login Code**. The Login Code text box displays a “\*” for each number in the code. Press the **OK** button.

Manager [255.255.255.255] (C:\Program Files\... \Manager\ 00E007009463.cfg)

File Edit View Tools Window Help

User Hot Desk 277

VoiceRecording		Button Programming		Hunt Group Settings (T3 Sets only)		Personal Directory (T3 Sets only)	
User	Voicemail	DND	ShortCodes	SourceNumbers	Telephony	Forwarding	Dial In
Outside Call Sequence		DefaultRing			<input checked="" type="checkbox"/> Call Waiting On		
Inside Call Sequence		DefaultRing			<input checked="" type="checkbox"/> Answer Call Waiting on Hold (Analogue)		
Ring Back Sequence		DefaultRing			<input type="checkbox"/> Busy On Held		
Allocated Answer Interval (secs)					<input type="checkbox"/> Outgoing Call Bar		
Wrap-up Time (secs)		2			<input type="checkbox"/> Offhook Station		
Transfer return Time (secs)					<input type="checkbox"/> Can Intrude		
Individual Coverage Time (secs)		10			<input checked="" type="checkbox"/> Cannot be Intruded		
Login Code		****			<input checked="" type="checkbox"/> Force Login		
Login Idle Period (secs)					<input type="checkbox"/> Force Account Code		
Monitor Group					<input type="checkbox"/> System Phone		

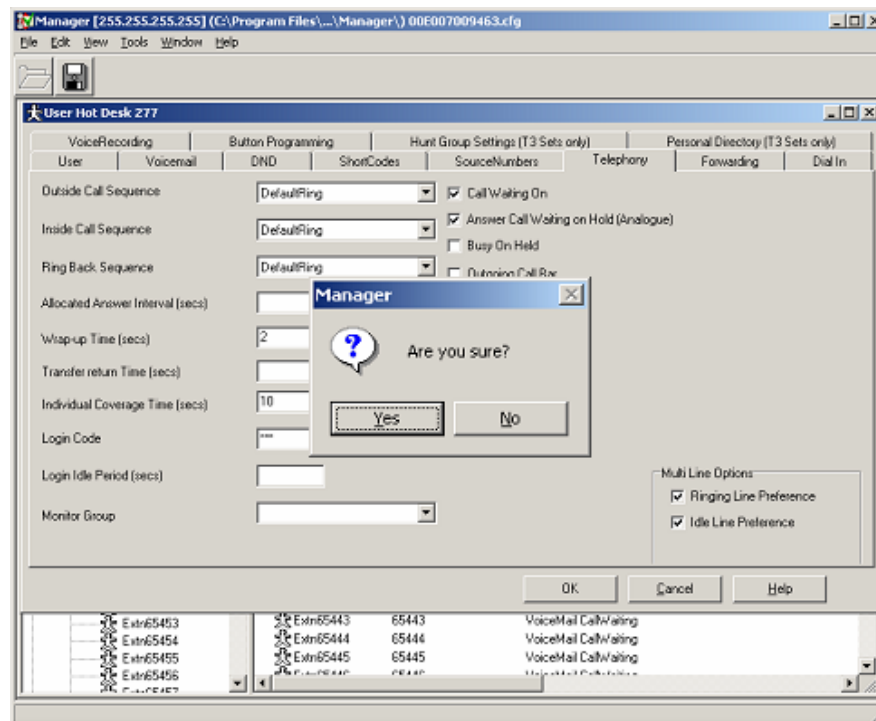
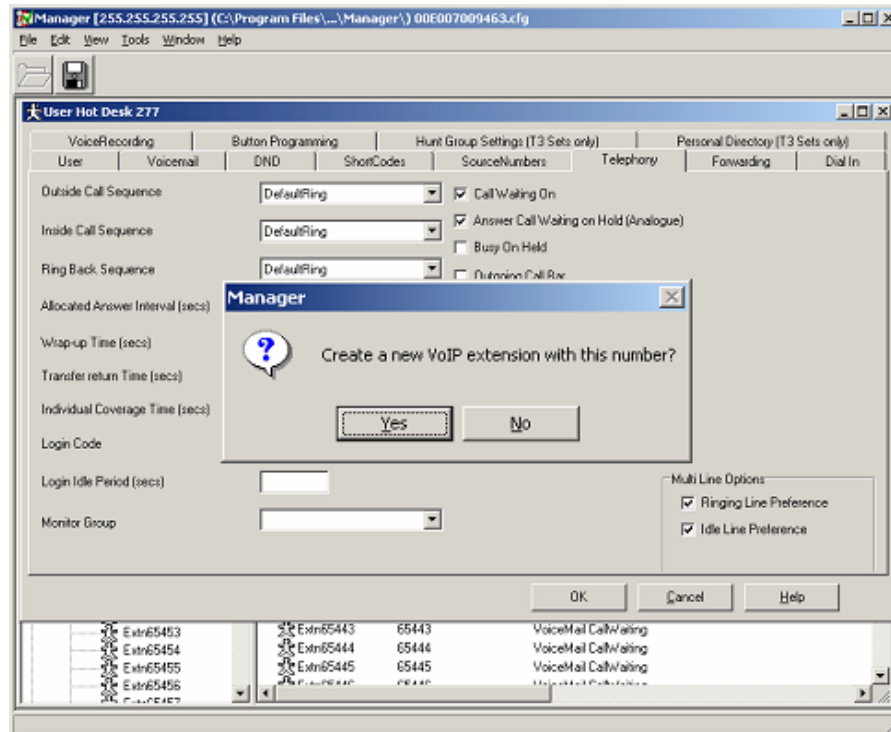
Multi Line Options:

- ☒ Ringing Line Preference
- ☒ Idle Line Preference

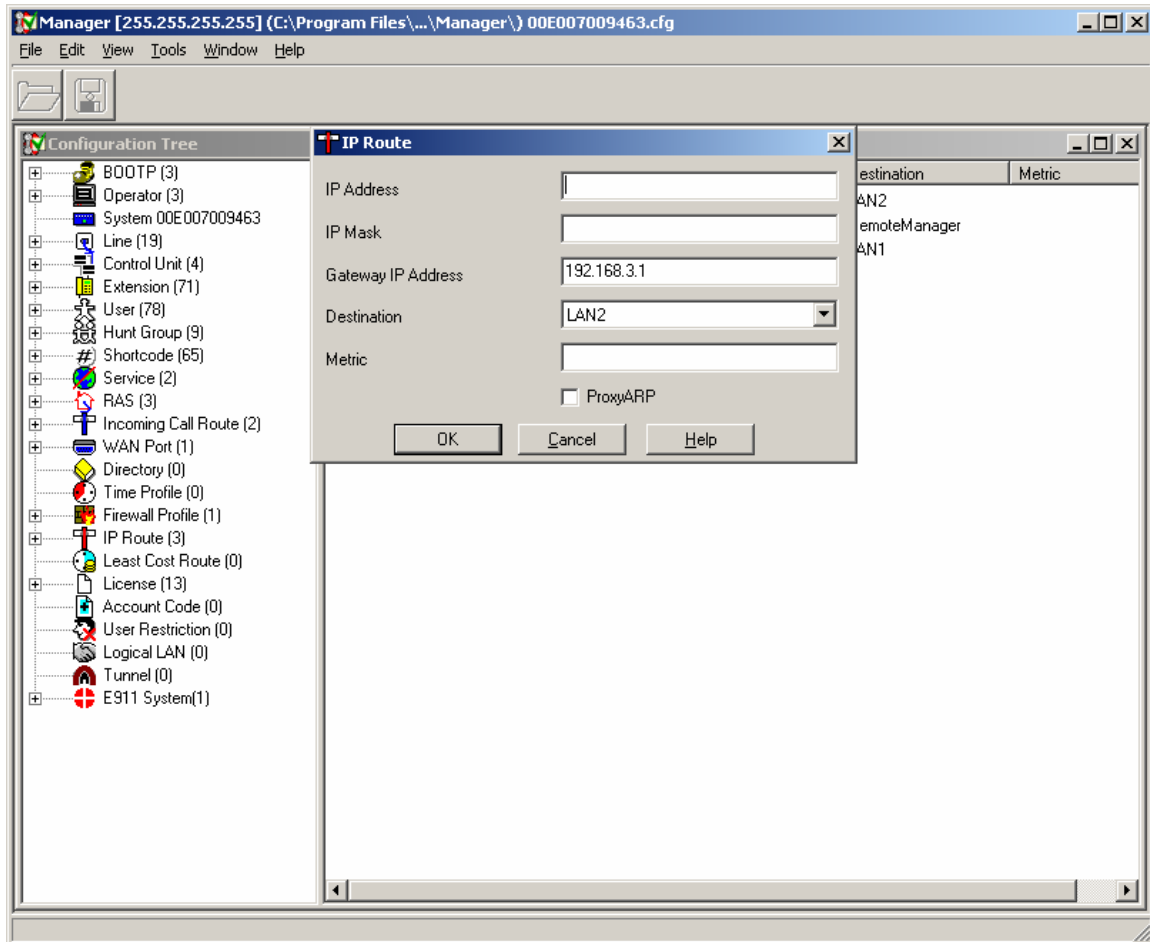
OK Cancel Help

Extn65453	Extn65443	65443	VoiceMail CallWaiting
Extn65454	Extn65444	65444	VoiceMail CallWaiting
Extn65455	Extn65445	65445	VoiceMail CallWaiting
Extn65456	Extn65446	65446	VoiceMail CallWaiting
Extn65457	Extn65447	65447	VoiceMail CallWaiting

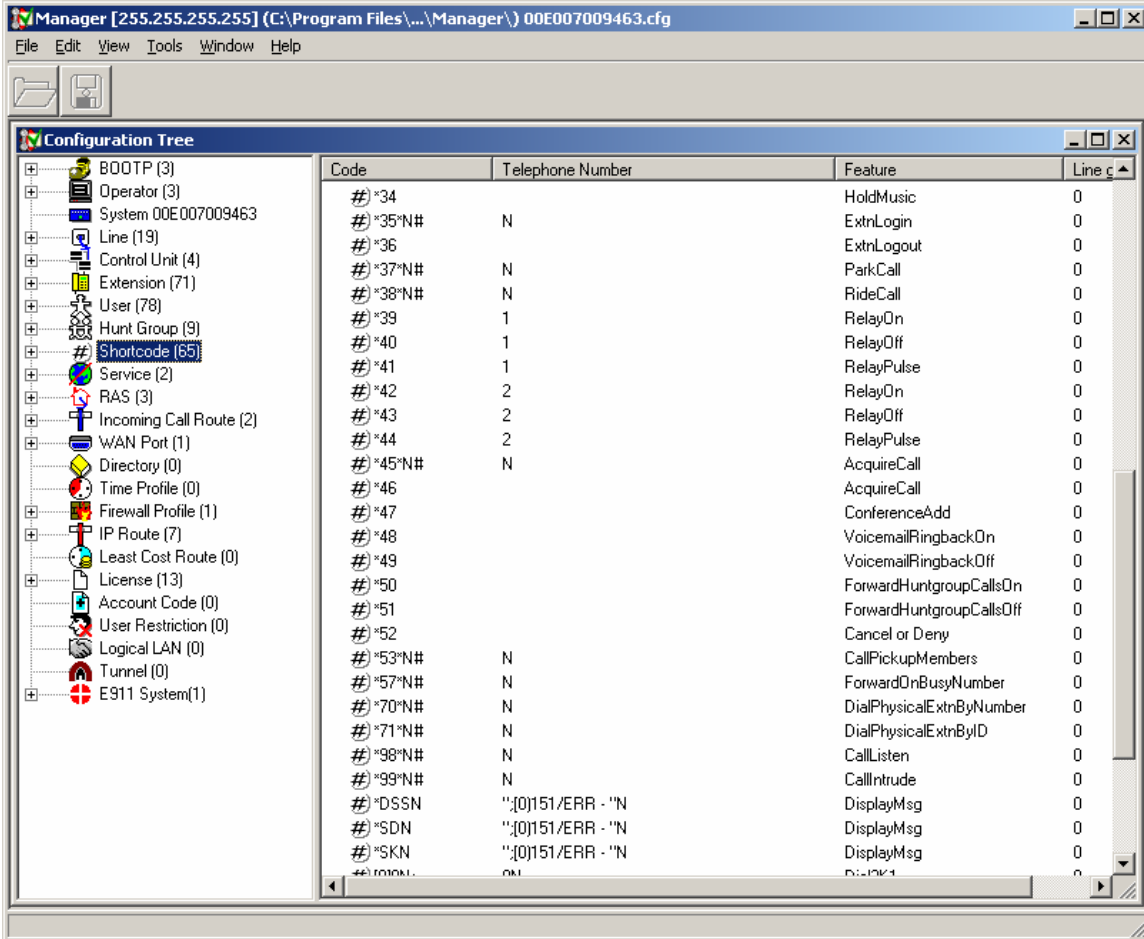
7. *Complete the user.* Choose the **No** option for creating a new VoIP extension. This allows the user to be used easily at any telephone. Choose the **Yes** option when asked **Are you Sure?**



8. *Make the Avaya Security Gateway 203 the default IP Route.* In IP Office Manager, select **IP Route** in the left panel. In the right panel, right click and select the **New** option. Enter the Avaya Security Gateway's private side IP Address in the **Gateway IP Address** field and select LAN2 as the **Destination**. Retain all other default values. Press the **OK** button.



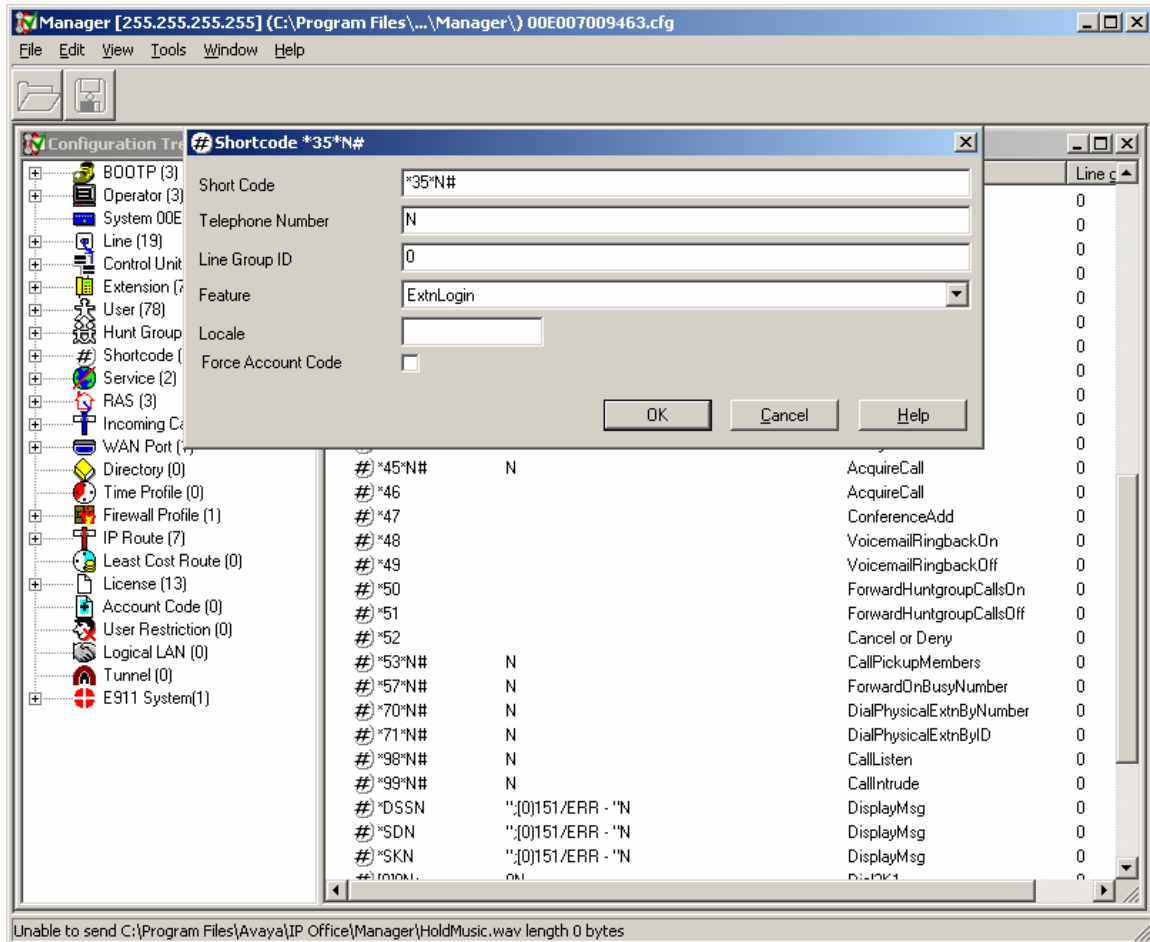
9. Check to see if there are ExtnLogin and ExtnLogout shortcodes. In the IP Office Manager Configuration Tree, click on **Shortcode** in the left panel. In the right panel, check to see if the ExtnLogin and ExtnLogout shortcodes exist. The defaults are shown below.



The screenshot shows the IP Office Manager Configuration Tree with the 'Shortcode' node selected. The right pane displays a table of shortcodes with their corresponding telephone numbers and features.

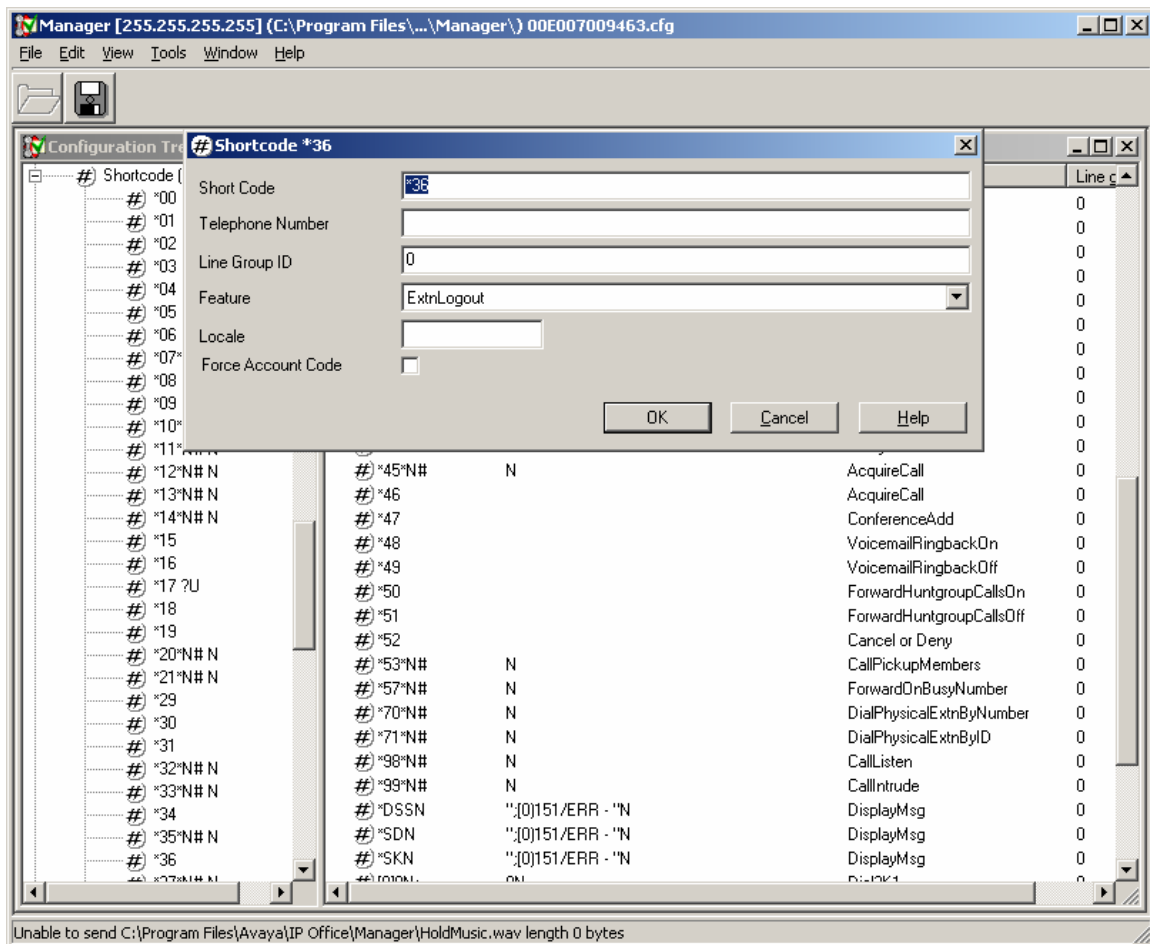
Code	Telephone Number	Feature	Line
#*34		HoldMusic	0
#*35*N#	N	ExtnLogin	0
#*36		ExtnLogout	0
#*37*N#	N	ParkCall	0
#*38*N#	N	RideCall	0
#*39	1	RelayOn	0
#*40	1	RelayOff	0
#*41	1	RelayPulse	0
#*42	2	RelayOn	0
#*43	2	RelayOff	0
#*44	2	RelayPulse	0
#*45*N#	N	AcquireCall	0
#*46		AcquireCall	0
#*47		ConferenceAdd	0
#*48		VoicemailRingbackOn	0
#*49		VoicemailRingbackOff	0
#*50		ForwardHuntgroupCallsOn	0
#*51		ForwardHuntgroupCallsOff	0
#*52		Cancel or Deny	0
#*53*N#	N	CallPickupMembers	0
#*57*N#	N	ForwardOnBusyNumber	0
#*70*N#	N	DialPhysicalExtnByNumber	0
#*71*N#	N	DialPhysicalExtnByID	0
#*98*N#	N	CallListen	0
#*99*N#	N	CallIntrude	0
#*DSSN	":[0]151/ERR - "N	DisplayMsg	0
#*SDN	":[0]151/ERR - "N	DisplayMsg	0
#*SKN	":[0]151/ERR - "N	DisplayMsg	0

10. If the shortcode is not present, add an *ExtnLogin* shortcode. In the right panel right-click and select **New**. Set the **Feature** and **Telephone Number**, as shown below. Select a unique code for the **Short Code** field. The code must end with a “\*N#”. Press the **OK** button. In this case, the “N” represent a string of dialed digits; the extension number, a “\*” and the login code entered in Step 6 of this section. The user logs in by dialing **\*35\*extension number\*login code\*#**.





11. If the shortcode is not present, add an *ExtnLogout* shortcode. In the right panel right click and select **New**. Set the **Feature** and **Telephone Number**, as shown below. Select a unique code for the **Short Code** field. Press the **OK** button.



## 4. Configure the Main Site Avaya Security Gateway 203

This section describes the Avaya Security Gateway 203 configuration at Main Site. The configuration includes:

- Configuring IP addresses for the public and private side
- Creating a remote user for the Avaya VPNremote Phone
- Configuring a VPN
- Configuring IP Routes

To configure the Avaya Security Gateway 203, open a web browser and enter the IP Address of the Avaya Security Gateway 203 in the Address field. The following is presented:

Security Gateway Web Interface - Microsoft Internet Explorer

Address: https://3.0.0.1

AVAYA Virtual Private Network Security FIREWALL QoS VoIP

SG203 User: root

Inspect

Select a property to display the associated information

Properties

Interfaces

Summary...

Media Interface	Zone	IP Config Mode	Status	IP Address	M.
ethernet0	private	Static	In Use	192.168.3.1	25
ethernet1	public	Static	In Use	60.60.60.2	25
ethernet2	management	Static	In Use	3.0.0.1	25
ethernet3	unused	None	Link Down		

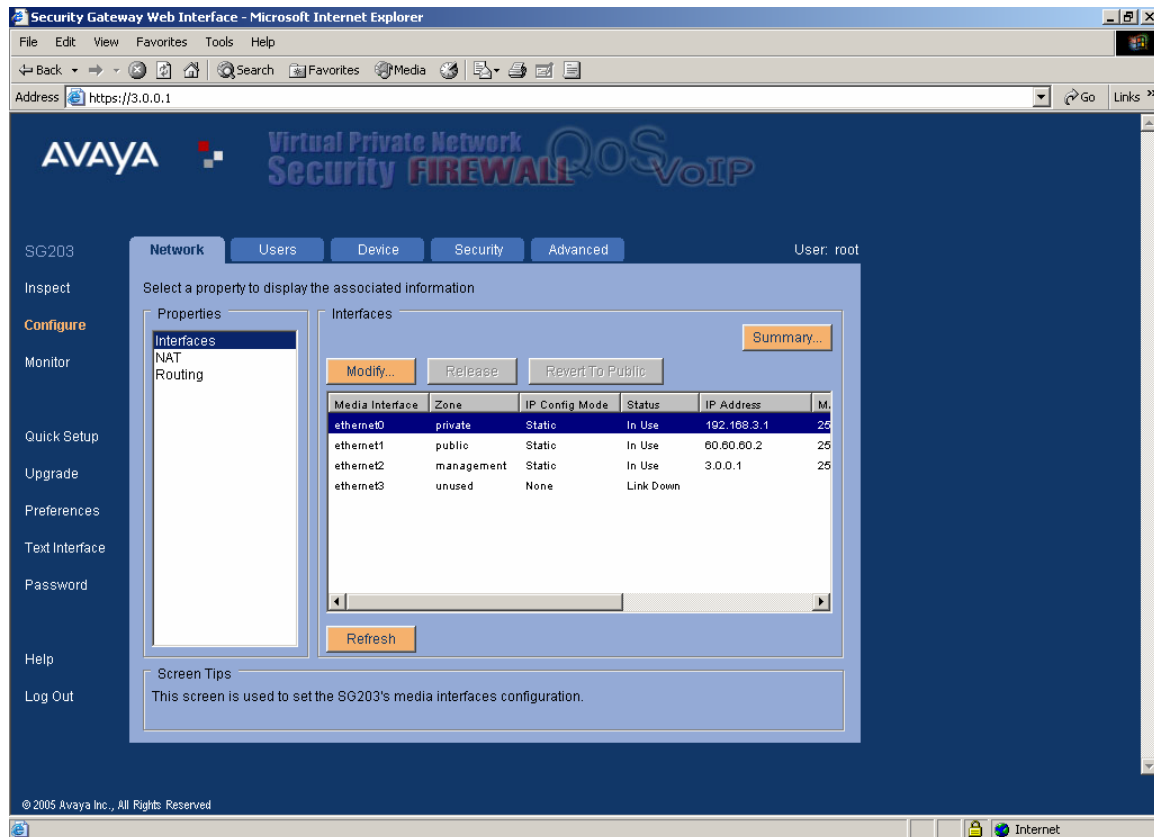
Refresh

Screen Tips

This screen shows the SG203's media interfaces configuration details.

© 2005 Avaya Inc., All Rights Reserved.

1. *Configure the Private Side IP Address.* In the left column, select **Configure**. Select the **Network** tab and **Interfaces** in the **Properties** area. Select the **Media Interface** labeled **private** in the **Zone** column and press **Modify**.



2. *Change the IP Address for the Private Side.* Set the **Zone** to **private**. Set the **IP Config Mode** to **Static** and set the **IP Address** and **Mask** to the values for the private side. Press the **Save** button.

The image shows a 'Media Interface Configuration' window. At the top, it displays 'Media Interface: ethernet0' and 'Media Type: ethernet'. Below this, there are two panels: 'Media Information' and 'Current IP Information'. The 'Media Information' panel shows 'Mac Address: 00:60:a1:00:cd:96' and 'Link Status: up/autoselect (100Mbps)', with a 'Media Settings...' button below. The 'Current IP Information' panel shows 'IP Address: 192.168.3.1', 'Mask: 255.255.255.0', and 'Route:'. Below these panels is the 'IP Configuration' section, which includes a 'Zone' dropdown set to 'private' and an 'IP Config Mode' dropdown set to 'Static'. Under the 'Static' mode, the 'IP Address' is configured as 192.168.3.1 and the 'Mask' as 255.255.255.0. At the bottom of the window are 'Save' and 'Cancel' buttons. The window title bar says 'Media Interface Configuration' and the bottom status bar says 'Java Applet Window'.

<b>Media Interface:</b> ethernet0		<b>Media Type:</b> ethernet	
<b>Media Information</b>		<b>Current IP Information</b>	
<b>Mac Address:</b> 00:60:a1:00:cd:96		<b>IP Address:</b> 192.168.3.1	
<b>Link Status:</b> up/autoselect (100Mbps)		<b>Mask:</b> 255.255.255.0	
<a href="#">Media Settings...</a>		<b>Route:</b>	
<b>IP Configuration</b>			
Zone: private		IP Config Mode: Static	
<b>Static</b>			
IP Address		Mask	
192	168	255	255
3	1	255	0
<div>Save Cancel</div>			

Java Applet Window

3. *Configure the Public Side interface IP Address.* From the screen shown in Step 1, select the **Module Interface** labeled **public** in the **Zone** column and press **Modify**.

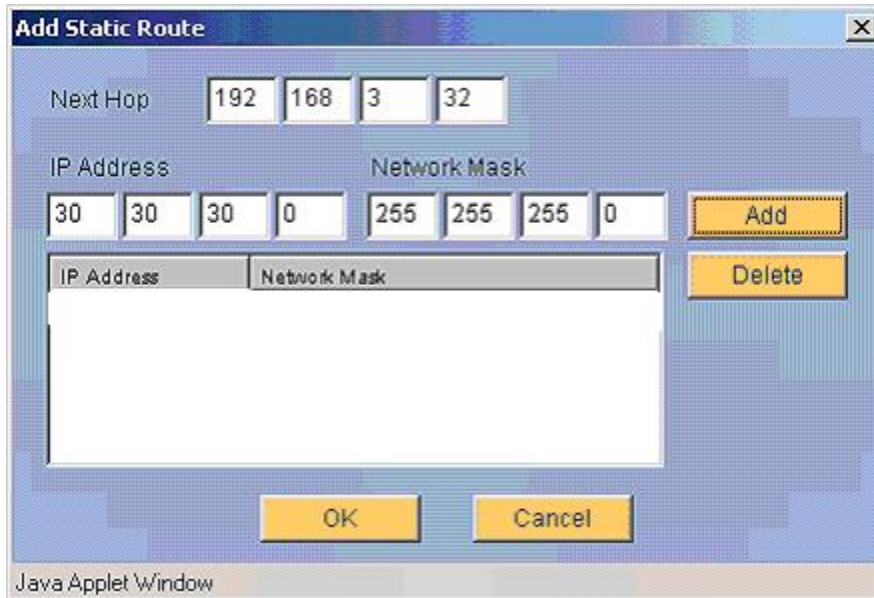
Set the **Zone** to **public**. Set the **IP Config Mode** to **Static** and set the **IP Address** and **Mask** to the values for the public side. Enter the IP Address of the Cisco 3725 interface to the Avaya Security Gateway (see Step 3 in Section 5) in the **Route** field. Press the **Save** button.

The screenshot shows a 'Media Interface Configuration' window. At the top, it displays 'Media Interface: ethernet1' and 'Media Type: ethernet'. Below this, there are two main sections: 'Media Information' and 'Current IP Information'. The 'Media Information' section includes 'Mac Address: 00:60:a1:00:cd:97' and 'Link Status: up/autoselect (100Mbps full-duplex)', with a 'Media Settings...' button. The 'Current IP Information' section shows 'IP Address: 60.60.60.2', 'Mask: 255.255.255.0', and 'Route: 60.60.60.1'. Below these is the 'IP Configuration' section, which has a 'Zone' dropdown set to 'public' and an 'IP Config Mode' dropdown set to 'Static'. Under the 'Static' mode, there are input fields for 'IP Address' (60, 60, 60, 2), 'Mask' (255, 255, 255, 0), and 'Route' (60, 60, 60, 1). At the bottom of the window are 'Save' and 'Cancel' buttons. The footer of the window reads 'Java Applet Window'.

Media Interface Configuration	
<b>Media Interface:</b> ethernet1	<b>Media Type:</b> ethernet
<b>Media Information</b>	<b>Current IP Information</b>
<b>Mac Address:</b> 00:60:a1:00:cd:97	<b>IP Address:</b> 60.60.60.2
<b>Link Status:</b> up/autoselect (100Mbps full-duplex)	<b>Mask:</b> 255.255.255.0
<a href="#">Media Settings...</a>	<b>Route:</b> 60.60.60.1
<b>IP Configuration</b>	
Zone: public	IP Config Mode: Static
<b>Static</b>	
IP Address: 60 60 60 2	Mask: 255 255 255 0
	Route: 60 60 60 1
<a href="#">Save</a> <a href="#">Cancel</a>	
Java Applet Window	

4. *Configure a static IP Route to IP Office LAN1 Subnet.* From the screen shown in Step 1, select **Routing** in the Properties box and press the Add button.

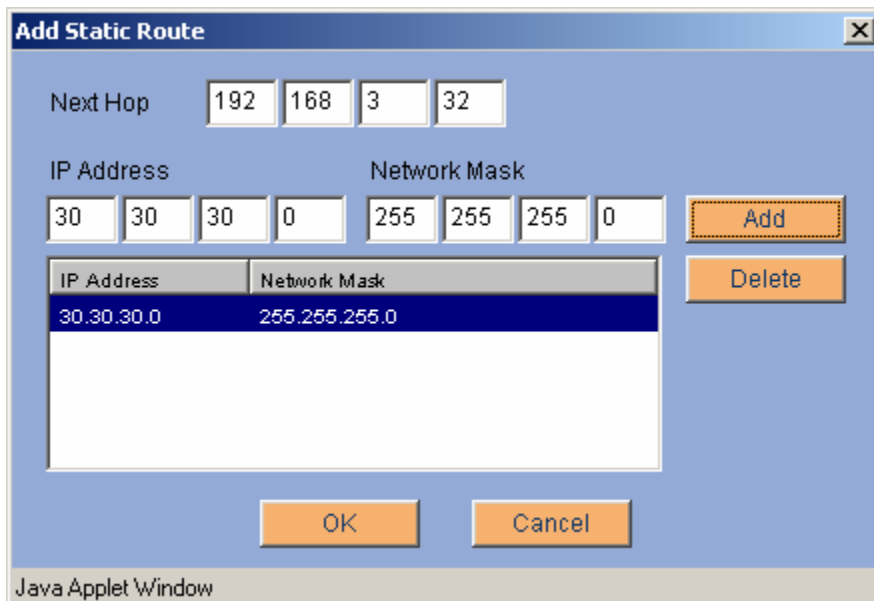
Enter the LAN2 IP Address in the **Next Hop** field. Enter the LAN1 Subnet in the **IP Address** and enter the appropriate Subnet Mask in the **Network Mask** field. Press the **Add** button.



The 'Add Static Route' dialog box is shown. It has a title bar with a close button. The 'Next Hop' field contains the IP address 192.168.3.32. The 'IP Address' field contains 30.30.30.0 and the 'Network Mask' field contains 255.255.255.0. There are 'Add' and 'Delete' buttons to the right of the IP and mask fields. Below these fields is a table with two columns: 'IP Address' and 'Network Mask'. The table is currently empty. At the bottom are 'OK' and 'Cancel' buttons. The status bar at the bottom says 'Java Applet Window'.

IP Address	Network Mask
------------	--------------

5. *Complete the static IP Route.* Press the **OK** button



The 'Add Static Route' dialog box is shown again. The 'Next Hop' field still contains 192.168.3.32. The 'IP Address' field still contains 30.30.30.0 and the 'Network Mask' field still contains 255.255.255.0. The 'Add' button is now disabled (greyed out). The table below the fields now contains one row: 30.30.30.0 under 'IP Address' and 255.255.255.0 under 'Network Mask'. The 'Delete' button is still present. At the bottom are 'OK' and 'Cancel' buttons. The status bar at the bottom says 'Java Applet Window'.

IP Address	Network Mask
30.30.30.0	255.255.255.0

6. *Add a Remote User.* From the **Configure** screen shown in Step 1, select the **Users Tab** and **Remote Users** in the **Properties** box. Press the **Add** button.

Enter a unique name in the **User Name** field and a password in the **Password** and **Confirm Password** fields. These fields must match what is configured on the VPNremote Phone (see Section 6 for details). Press the **Save** button. This will automatically create a user on the SG203.

The screenshot shows a Java Applet Window titled "Add Remote User". The window contains an "Authentication" section with the following fields and controls:

- User Name:** A text field containing the value "db".
- Default User:** A checkbox that is currently unchecked.
- Password (min 6 chars):** A text field containing six asterisks "\*\*\*\*\*".
- Confirm Password:** A text field containing six asterisks "\*\*\*\*\*".

At the bottom of the "Authentication" section is an orange button labeled "Advanced". Below this section are two orange buttons: "Save" and "Cancel". The bottom of the window displays the text "Java Applet Window".

7. *Verify the Authentication Method for the Remote User.* From the **Configure** screen shown in Step 1, select the **Users Tab** and **SG203 Users** in the **Properties** box. Select the user labeled **ip-phone-user** and press the **Modify** button.

The **VPN Authentication Profile** section shows whether the Authentication is **Standard (CHAP)** or **Rechallenge (PAP)**. Note this value as it will be needed when configuring the VPNremote phone. See Section 6 for details. Press the **Cancel** button.

**Modify SG203 User**

User Credentials

User Name: ip-phone-user ☒ Enable User

Password (min 6 chars):

Confirm Password:

VPN Authentication Profile

VSU/SG Address: (required)

Backup VSU/SG Address:

Port: 1443 (required)

VPNmanager Suffix:

Authentication: ☒ Standard (CHAP) ☐ Rechallenge (PAP)

Timeout (minutes): 0

Save Cancel

Java Applet Window



8. *Create a VPN for the VPNremote Phone.* From the **Configure** screen shown in Step 1, select the **Security Tab** and **VPN Setup** in the **Properties** area. Press the **Add** button.

Enter a unique name in the **VPN Name** textbox. Select **Preshared Secret** for the **Authentication Method**.

Enter the IP Office LAN1 and LAN2 subnet by entering each subnet and mask in the **IP Address** and **Mask** fields in the **Local IP Groups** section and pressing the **Add** button. Press the **Next** button.

**Add New VPN**

VPN Name  
VPN Name: tovpnphone  
☐ Default VPN

Authentication Method  
☒ Preshared Secret ☐ Certificate Based  
Secret Text: abcdef  
View As: ☒ ASCII ☐ Hexadecimal

Local IP Groups

IP Address: 192 168 3 0 Mask: 255 255 255 0 **Add**

IP Address	Network Mask
30.30.30.0	255.255.255.0
192.168.3.0	255.255.255.0

**Delete**

< Previous Next > Cancel

Java Applet Window

9. *Configure the Remote End of the VPN.* No changes are required on this screen. Press the **Next** button.

**Add New VPN**

Zone:  **Media Interface:** ethernet1  
( NOTE: Zone will be ignored for 'User VPNs' )

Remote Tunnel End Points (TEP) (Optional)

Remote TEP IP:     **Add** **Delete**

Member Remote TEPs:

IP Group(s) For:

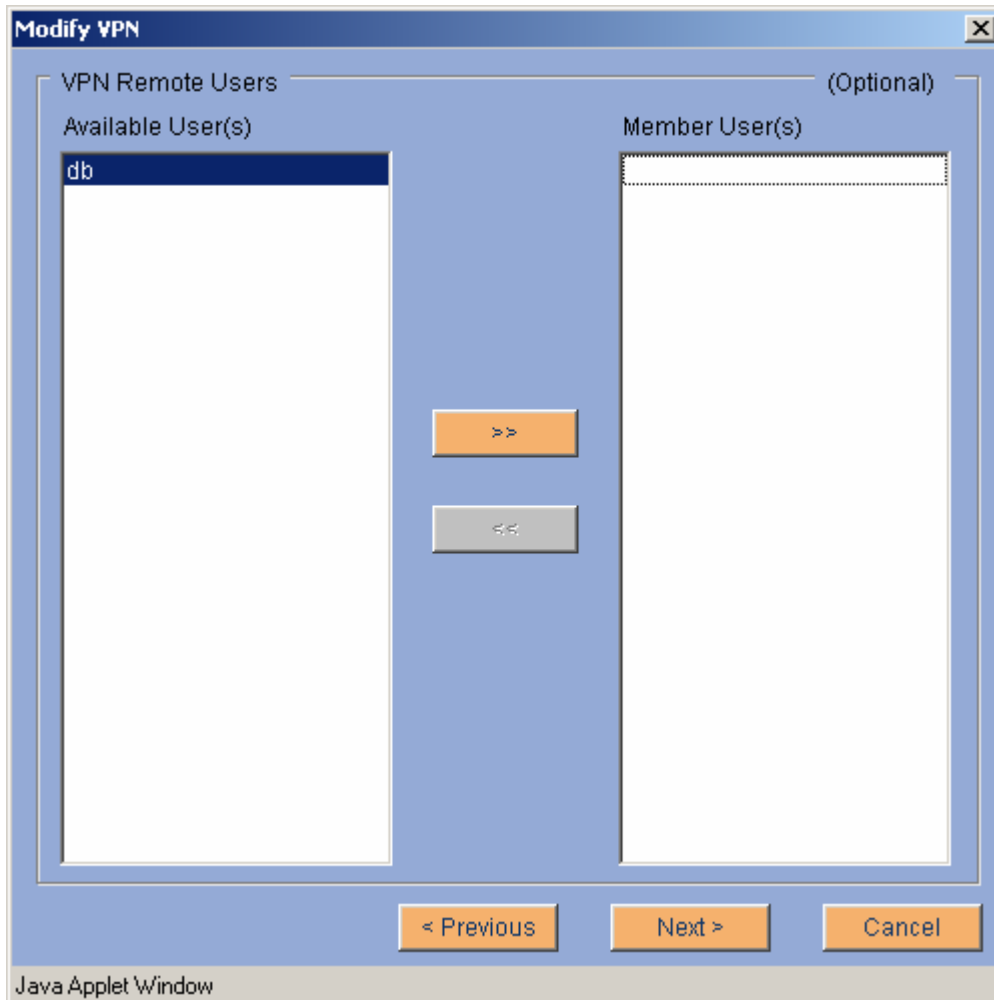
IP Address:     Mask:     **Add** **Delete**

IP Address	Network Mask
------------	--------------

< Previous **Next >** Cancel

Java Applet Window

10. *Configure the Remote User of the VPN.* Select the User created in Step 8 of this section from the **Available User(s)** box. Press the >> button and then the **Next** button.



11. *Configure the VPN Security.* Set the security levels as shown below. Press the **Add** button. Press the **Finish** button.

The screenshot shows a 'Modify VPN' window with the following settings:

- IKE Security:**
  - Encryption: 3DES
  - Authentication: SHA1
  - Lifetime (Time-based): 8 DAYS
  - Lifetime (Throughput): 0 GB
  - DH Group: 1
- IPsec Security:**
  - AH/ESP: ESP
  - Perfect Forward Secrecy: NO
  - DH Group: 1
- IPsec Proposals:**
  - Encryption: 3DES
  - Authentication: HMAC\_SHA
  - Lifetime (Time-based): 8 DAYS
  - Lifetime (Throughput): 0 GB
  - Compression: LZS

Below the IPsec Proposals section is a table with columns: Encryption, Authentication, Life (time), Life (throughput), and Cor. The table is currently empty. To the right of the table are buttons: Add, Delete, Move Up, and Move Down.

At the bottom of the window are buttons: < Previous, Finish, and Cancel.

Java Applet Window

## 5. Configure the Cisco 3725 Router at the Main Site

This section describes the configuration for the Cisco 3725 router, which resides at Main Site and connects to the network and the Avaya Security Gateway 203.

The following steps were followed to configure the Cisco 3725 Router:

1. Configuring the Ethernet interface connected to the Avaya Security Gateway.
  2. Configuring the Ethernet interface connected to the Network.
  3. Configuring IP Routes for:
    - o IP Office LAN2 Subnet.
    - o Default static IP route.
1. *Connect to the Cisco 3725 Router with its serial cable.* Run a terminal emulator, such as HyperTerminal with settings of 9600Kb/s, 8 data bits, 1 stop bit and no parity. Set the flow control to none and change the emulation mode to VT100.
  2. *Configure one Ethernet connection for the Network.*

```
DGK-3725>enable
DGK-3725#configure
Configuring from terminal, memory, or network? [terminal] terminal
DGK-3725(config)#interface FastEthernet 0/1
DGK-3725(config-if)#ip address 60.60.60.2 255.255.255.0
```

3. *Configure one Ethernet connection for the Avaya Security Gateway.*

```
DGK-3725(config)#interface FastEthernet 0/0
DGK-3725(config-if)#ip address 12.160.180.2 255.255.255.0
```

4. *Configure an ip route for the IP Office 412 LAN2 Subnet*

```
DGK-3725(config)#ip route 192.168.3.0 255.255.255.0 60.60.60.2
```

5. *Configure a default ip route to the Network.*

```
DGK-3725(config)#ip route 0.0.0.0 0.0.0.0 12.160.180.1
```

## 6. Configure the Avaya VPNremote Phone at the Remote Worker Site

This section describes the key items in the configuration of the VPNremote Phone at the Remote Worker Site.

As the IP telephone powers up, press \* to enter program mode. As prompted, enter the associated data and # to complete each entry.

Prompt	Type of Entry	Configured Data
Phone	IP Telephone IP Address	<b>192.168.1.101</b>
CallSrv	IP Telephony Server (IP Office LAN2) IP Address	<b>192.168.3.32</b>
CallSvPort	IP Telephony Server Registration Port	<b>1719</b>
Router	Default Router for off-subnet traffic – this is the DSL modem	<b>192.168.1.1</b>
Mask	Subnet Mask	<b>255.255.255.0</b>
FileSv	File Server to download firmware and settings file from. – This is the IP Address of the PC with the VPNremote Phone firmware.	<b>30.30.30.78</b>
802.1Q	Use VLAN tagging for IP Telephony Traffic	<b>Off</b>
Save New Values?		<b>Yes</b>

The following are the VPN settings. In addition to the original programming, this can be modified by pressing the **Mute** button followed by **VPNMOD#**.

Prompt	Type of Entry	Configured Data	Notes
Server	IP Telephone IP Address	<b>60.60.60.2</b>	This is the <b>IP Address</b> of the Cisco 3725 Avaya Security Gateway from Step 2 of Section 5.
User Name	Remote User configured on the Avaya Security Gateway.	<b>db</b>	<b>Remote User</b> from Step 6 in Section 4.
Password	Password configured on the Avaya Security Gateway	<b>abcdef</b>	<b>Password</b> from Step 6 in Section 4.
Authentication Mode	Type of authentication used (PAP, CHAP)	<b>CHAP</b>	Authentication from Step 7 in Section 4.
Password Type	How the password needs to be entered and where the information is stored.	<b>Save in Flash</b>	Saving it in flash means that the user does not need to re-enter the password every time the VPNremote Phone is rebooted.
VPN Start Mode	When the VPN is established (on Booting, on demand, not at all)	<b>Boot</b>	
Encapsulation	Type of encapsulation	<b>Disable</b>	
Done	Save changed values	<b>Yes</b>	

## 7. Testing

The interoperability testing focused on verifying interoperability between the Avaya VPNremote Phone and the Avaya IP Office using the configuration shown in **Figure 1**.

### 7.1. General Test Approach

The general test approach was to connect the VPNremote Phone in **Figure 1**. Calls were placed from the VPNremote Phone to IP Office and talkpath was verified. The features listed in Section 1.1 were tested using the VPNremote Phone.

## **7.2. Test Results**

All tests passed successfully. All products operated as expected. There are two items to note. In order to use the IP Office Call Recording feature at the VPNremote Phone, the “Allow Direct Media” option must be turned off for the extension. This means that a VCM channel will always be used for a call involving the Avaya VPNremote Phone. Call Listen is not supported on the Avaya VPNremote Phone.

## **8. Verification and Troubleshooting**

First check to see that all of the cables are connected to the appropriate ports. From the Avaya Security Gateway, ping the IP Office on the private side and the VPNremote Phone on the public side.



## 8.1. Avaya Security Gateway 203 Troubleshooting

Check to see if the private and public side interfaces are up. In the left column, select **Configure**. Select the **Network Tab** and **Interface** in the **Properties** area. Check that the **Zones** labeled **public** and **private** show **In Use**.

The screenshot shows the Avaya Security Gateway 203 web interface in a Microsoft Internet Explorer browser window. The address bar shows <https://3.0.0.1/>. The interface has a dark blue header with the Avaya logo and text: "Virtual Private Network Security FIREWALL QoS VoIP". Below the header, there are tabs for "Network", "Users", "Device", "Security", and "Advanced". The "Network" tab is selected. On the left side, there is a vertical menu with options: "Inspect", "Configure" (highlighted in orange), "Monitor", "Quick Setup", "Upgrade", "Preferences", "Text Interface", "Password", "Help", and "Log Out". The main content area is titled "Select a property to display the associated information". It has a "Properties" section on the left with a list: "Interfaces" (selected), "NAT", and "Routing". To the right of this list is a table titled "Interfaces". Above the table are buttons: "Modify..." (highlighted in orange), "Release", and "Revert To Public". To the right of the table is a "Summary..." button. The table has columns: "Media Interface", "Zone", "IP Config Mode", "Status", "IP Address", and "M.". The table contains four rows of data:

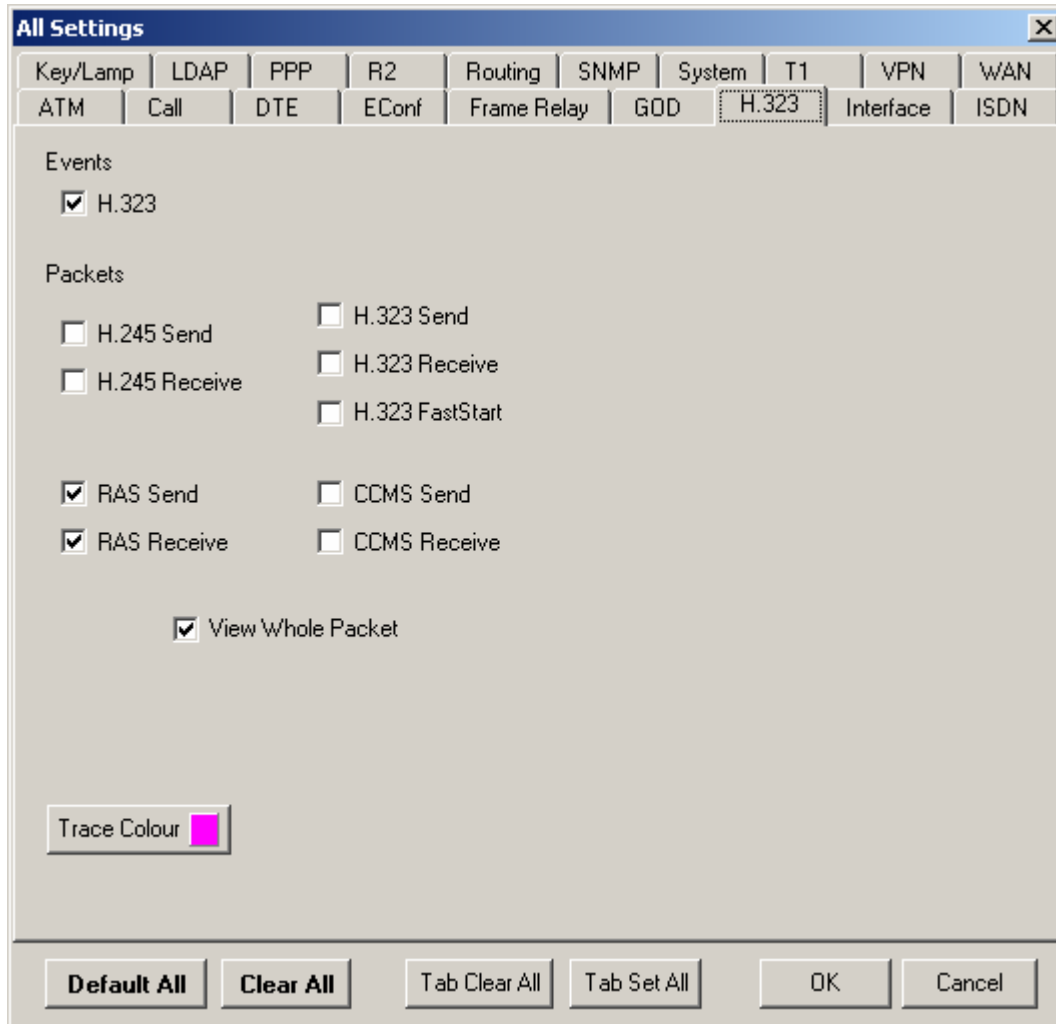
Media Interface	Zone	IP Config Mode	Status	IP Address	M.
ethernet0	private	Static	In Use	192.168.3.1	25
ethernet1	public	Static	In Use	60.60.60.2	25
ethernet2	management	Static	In Use	3.0.0.1	25
ethernet3	unused	None	Link Down		

Below the table is a "Refresh" button. At the bottom of the main content area, there is a "Screen Tips" section with the text: "Modify the configuration of the selected media interface." The footer of the page shows "© 2005 Avaya Inc., All Rights Reserved" and an "Internet" icon.

## 8.2. Avaya IP Office Troubleshooting

Troubleshooting can be done for the IP Office via the IP Office System Monitor application. Log into the IP Office Monitor PC and select **Start** → **Programs** → **IP Office** → **Monitor** to launch the IP Office System Monitor application. Log into the application using the appropriate credentials.

Select **Trace Options** under the **Filters** Menu. Select the **H.323** tab and configure as illustrated below.



When the system is configured correctly, the following Registration messages are displayed for the VPNremote Phone.

```
163667mS RasRx: v=IFace=LAN1, Src=192.168.1.101:49301, Dst=30.30.30.1.1:1719 tos=88
peb=0
RasMessage = registrationRequest = {
```

```

requestSeqNum = 0x6
protocolIdentifier = 0.0.8.2250.0.2
discoveryComplete = true
callSignalAddress = { 1 item(s)
  [0] = ipAddress = {
    ip =
      28 28 28 15
    port = 0xcf8
  }
}
rasAddress = { 1 item(s)
  [0] = ipAddress = {
    ip =
      28 28 28 15
    port = 0xc095
  }
}
terminalType = {
  terminal = {
  }
  mc = false
  undefinedNode = false
}
endpointVendor = {
  vendor = {
    t35CountryCode = 0xb5
    t35Extension = 0x0
    manufacturerCode = 0x4156
  }
  productId =
    49 50 5f 50 68 6f 6e 65
  versionId =
    32 2e 31 33 30
}
keepAlive = true
endpointIdentifier =
  0030 0030 0045 0030 0030 0037 0030 0031 00E00700
  0041 0036 0031 0041 005f 0034 0034 0031 9463_441
  0066 0063 0034 0037 0036 0032 0039 0062 fc47629b
  0066 0037 0034 0062 0064 f74bd
}

```

163668mS PRN: Recv: RegistrationRequest 28282815; Endpoints registered: 2; Endpoints in registration: 0

163669mS RasTx: v=Src=30.30.30.1.1:1719, Dst=192.168.1.101tos=88 peb=0

```

RasMessage = registrationConfirm = {
  requestSeqNum = 0x6
  protocolIdentifier = 0.0.8.2250.0.2
  callSignalAddress = { 1 item(s)
    [0] = ipAddress = {
      ip =
        1E 1E 1E 01
      port = 0x6b8
    }
  }
  gatekeeperIdentifier =
    0053 004d 0042 0053
  endpointIdentifier =
    0030 0030 0045 0030 0030 0037 0030 0031 00E00700
    0041 0036 0031 0041 005f 0034 0034 0031 9463_441
    0066 0063 0034 0037 0036 0032 0039 0062 fc47629b
    0066 0037 0034 0062 0064 f74bd
  timeToLive = 0x3c
}

```

```

willRespondToIRR = false
preGrantedARQ = {
    makeCall = true
    useGKCallSignalAddressToMakeCall = true
    answerCall = true
    useGKCallSignalAddressToAnswer = true
}
}
175718mS RasRx: v=IFace=LAN1, Src=192.1681.101:11143, Dst=30.30.30.188 peb=0
RasMessage = registrationRequest = {
    requestSeqNum = 0x26
    protocolIdentifier = 0.0.8.2250.0.2
    discoveryComplete = true
    callSignalAddress = { 1 item(s)
        [0] = ipAddress = {
            ip =
                28 28 28 a8                (((.
            port = 0x2b88
        }
    }
    rasAddress = { 1 item(s)
        [0] = ipAddress = {
            ip =
                28 28 28 a8                (((.
            port = 0x2b87
        }
    }
    terminalType = {
        mc = false
        undefinedNode = false
    }
    terminalAlias = { 1 item(s)
        [0] = e164 =
            32 38 30                        280
    }
    endpointVendor = {
        vendor = {
            t35CountryCode = 0xb5
            t35Extension = 0x0
            manufacturerCode = 0x4c54
        }
        productId =
            49 50 5f 50 68 6f 6e 65        IP_Phone
        versionId =
            31 2e 35 00 00                1.5..
    }
    keepAlive = true
    endpointIdentifier =
        0030 0030 0045 0030 0030 0037 0030 0031 00E00700
        0041 0036 0031 0041 005f 0034 0034 0031 9463_441
        0066 0061 0034 0037 0065 0032 0039 0062 fa47e29b
        0066 0037 0034 0062 0063          f74bc
    }
}

```

### 8.3. Avaya VPNremote Phone Troubleshooting

If the VPNremote Phone displays:	Explanation	Actions
Bad Router	The VPNremote Phone cannot “ping” the router.	Verify that the cables are connected and that the IP Routes are properly administered.
Discover aaa.bbb.ccc.ddd	This means that the VPNremote Phone is not receiving a Registration request response from the aaa.bbb.ccc.ddd IP Address, which should be the IP Office 412 LAN2 IP Address.	Check that the appropriate IP routes are administered for the Avaya IP Office, the Avaya Security Gateway 203 and the Cisco 3725

## 9. Conclusion

These Application Notes describe the steps for configuring the Avaya VPNremote Phone with the Avaya IP Office 412. The VPNremote Phone can be successfully used with IP Office.

## 10. Additional References

1. Product documentation for Avaya IP Office may be found at:  
<http://marketingtools.avaya.com/knowledgebase/>.
2. Product documentation for the Avaya Security Gateway and the VPNremote Phone can be found at:  
<http://www.avaya.com>.
3. *VPNremote Phone for the 4600 Series IP Telephone Administrators Guide* can be found at:  
<http://support.avaya.com>
4. *Application Notes for the Configuring an Avaya G250 Media Gateway as a VPN IKE Responder for a Cisco 877 Access Router and an Avaya G350 Media Gateway*  
<http://devconnect.avaya.com>.
5. Product documentation for Cisco products may be found at:  
<http://www.cisco.com>.

---

**©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.