Application Note

IP Office 403 and SG VPN Application Note

September 22 2004

Table of Contents

1. Introduction

This document provides the detailed process of configuring an "end to end" solution utilizing the Avaya SG5 VPN product to link remote IP hardphone sets (46xx series) or IP Office softphone clients over Virtual Private Networks to a central site IP Office telephony switch.
Dynamic VPN configurations are utilized, whenever the remote side of the network ISP service cannot provide static IP addresses. In most cases, the ISP provider will provide a "dynamic" IP address through the use of PPPoE hardware or software.
NOTE: The Avaya VSU series of product have been renamed Security Gateway or SG. Although the configuration screens may be different the basic process and principal is the same.

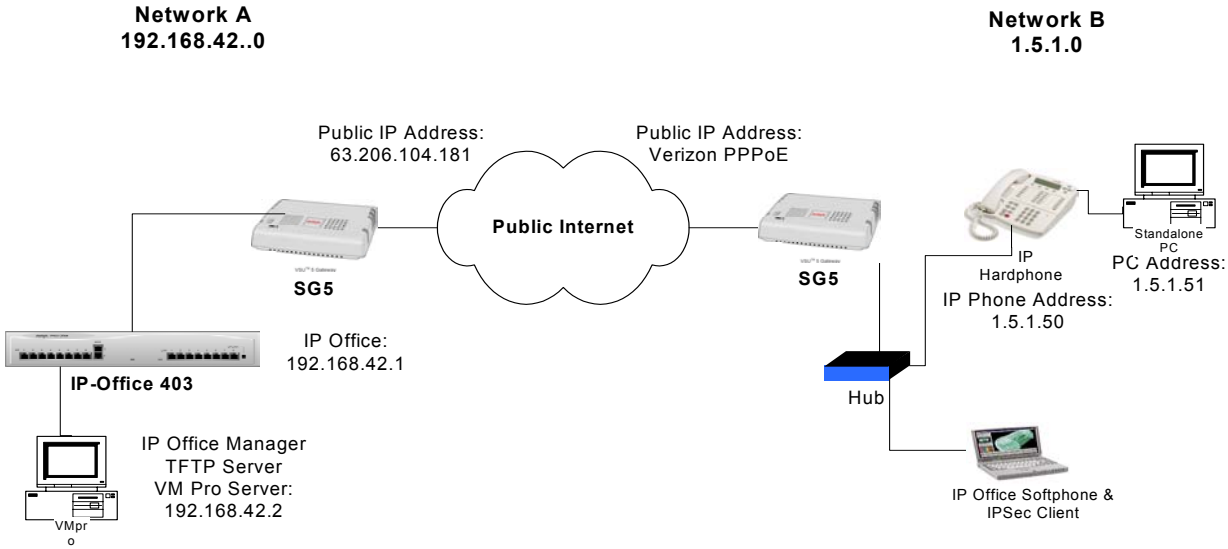
2. Requirements

SG product line
IP office 40x
Avaya phones

3. Network Diagram

The below illustration provides the basic components of the network tested. It is divided into three areas: The main site where the IP Office/VM Pro/SG5 resides, the remote SOHO site where the associated user's IP phone/PC/SG5 resides and the Public ISP services.

Each side of the network is assigned its own network address. On the "Host" side we used 192.168.42.0 as the network address utilizing the default address of the IP Office 192.168.42.1. On the remote side we utilized 1.5.1.0 as the network address and assigning IP addressing accordingly for each associated network device.



It should be noted that for Dynamic mode functionality to operate, the Host side network and VPN policies, MUST be set to Static. The remote side can utilize either static or PPPoE (defined as Dynamic) modes but not DHCP. DHCP mode will not function since the front end device operating as a DHCP server to the SG, would create a NAT issue, on firmware prior to the 4.3 Feature pack. The new firmware will support NAT transversal that will support this functionality.

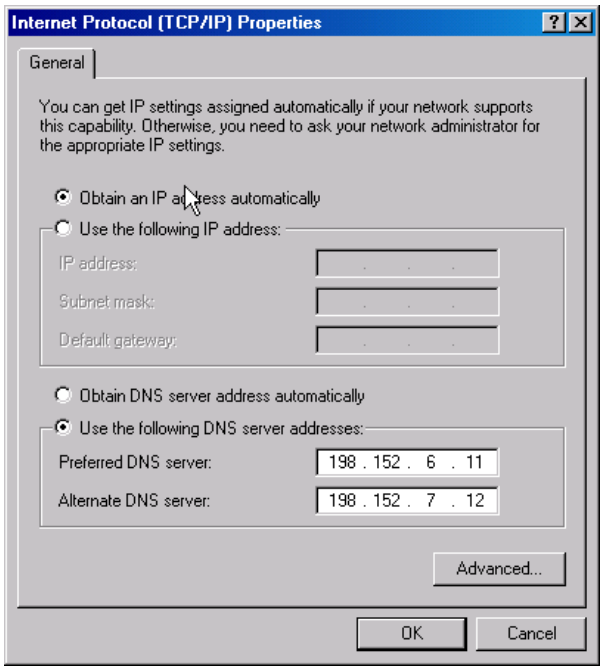
4. SG installation

1. Connect the SG-5's Public port to the Ethernet connector on your DSL or cable modem.

2. Connect the SG-5's Private port to your hub/switch or network port on your workstation.

3. Power on the SG-5. The self-test may take a minute to complete.

4. From your primary workstation: open your control panel, select your TCP/IP network component for your Ethernet controller, then select IP Address. In the IP Address window, Select enable the setting to "obtain an IP address automatically", and close the window. (The obtain DNS server setting is not relative)



Restart your workstation. As your workstation restarts, it will automatically obtain its required IP address/mask, and default router IP address from the SG-5.

5. From your workstation, open your Internet browser and type into the location field **https://192.168.1.1/vsu.html** (this is the default address of the SG-5). The SG-5 Login window then appears.

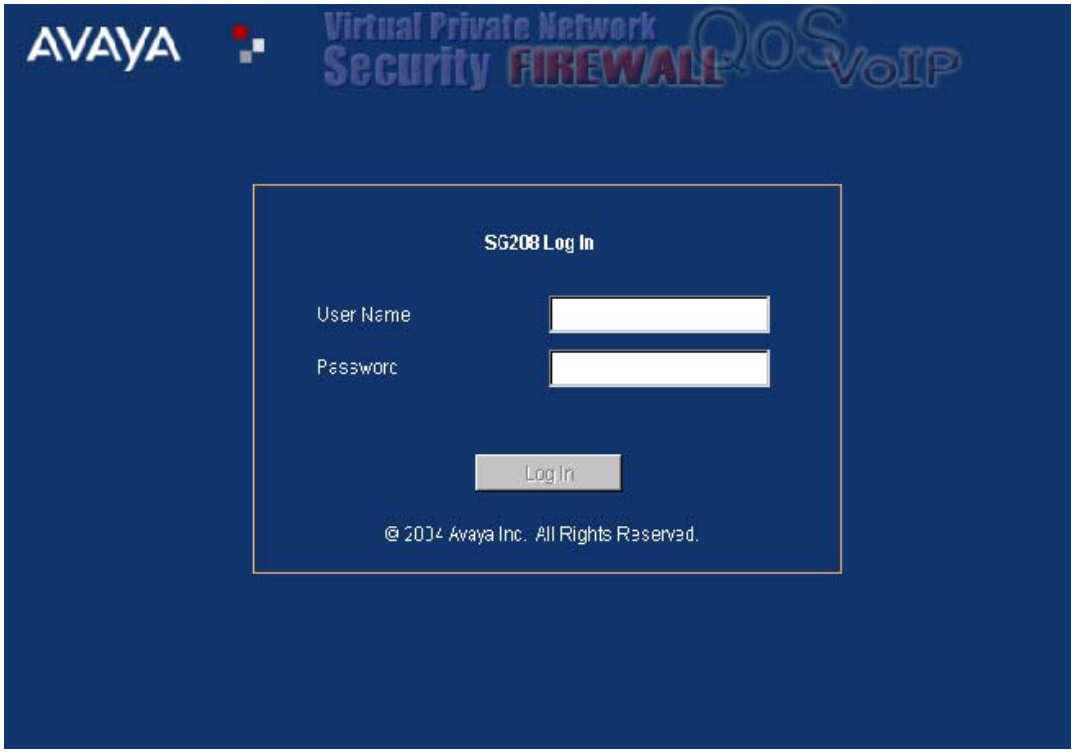
6. On the SG-5 Login window, enter:
User ID: **root**
Password: **password**.

Refer to the Quick Setup or Installation Guides for more detailed information on SG-5 setup and configuration

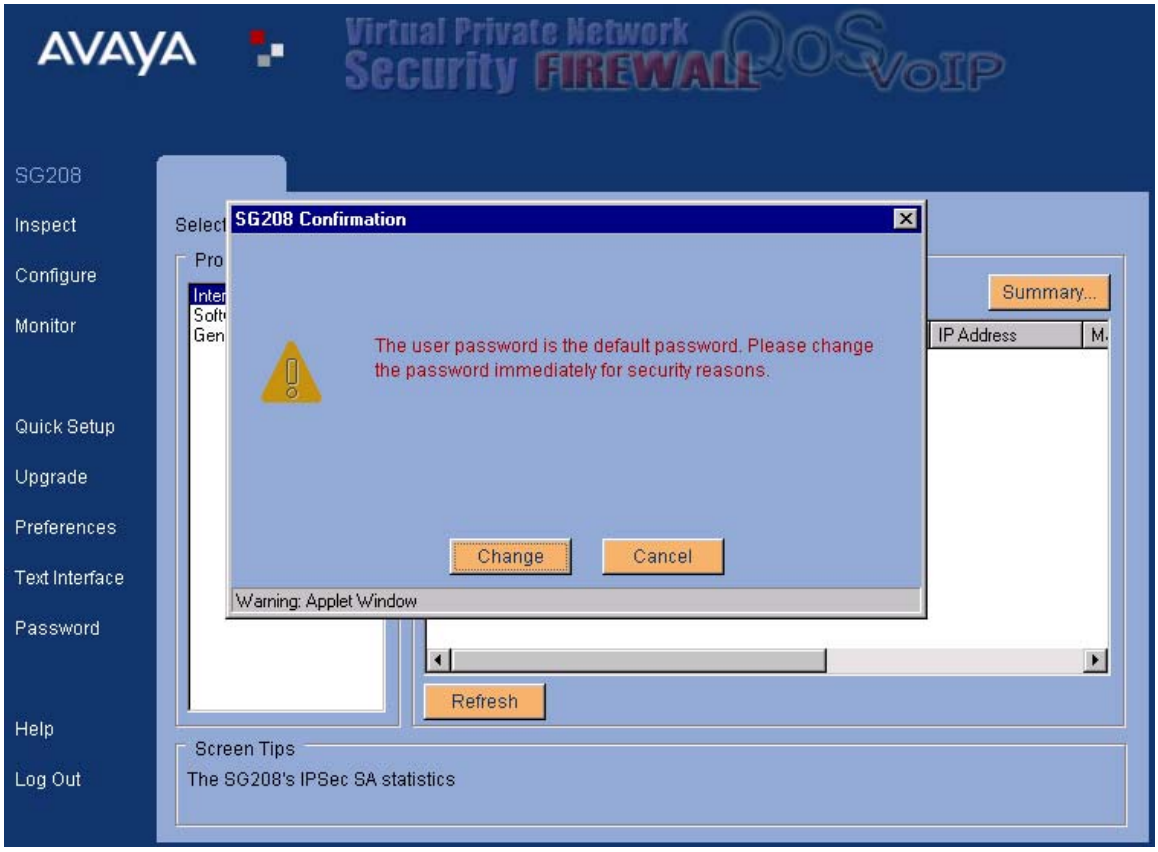
5. Central Site Configuration

Step 1: Login to SG5, 5x, 200, 203 or 208

Default Login: root
Default Password: password



Step 1a: User Password (Click “cancel” for all demos)



It is always recommended to change the “Root” password for security.

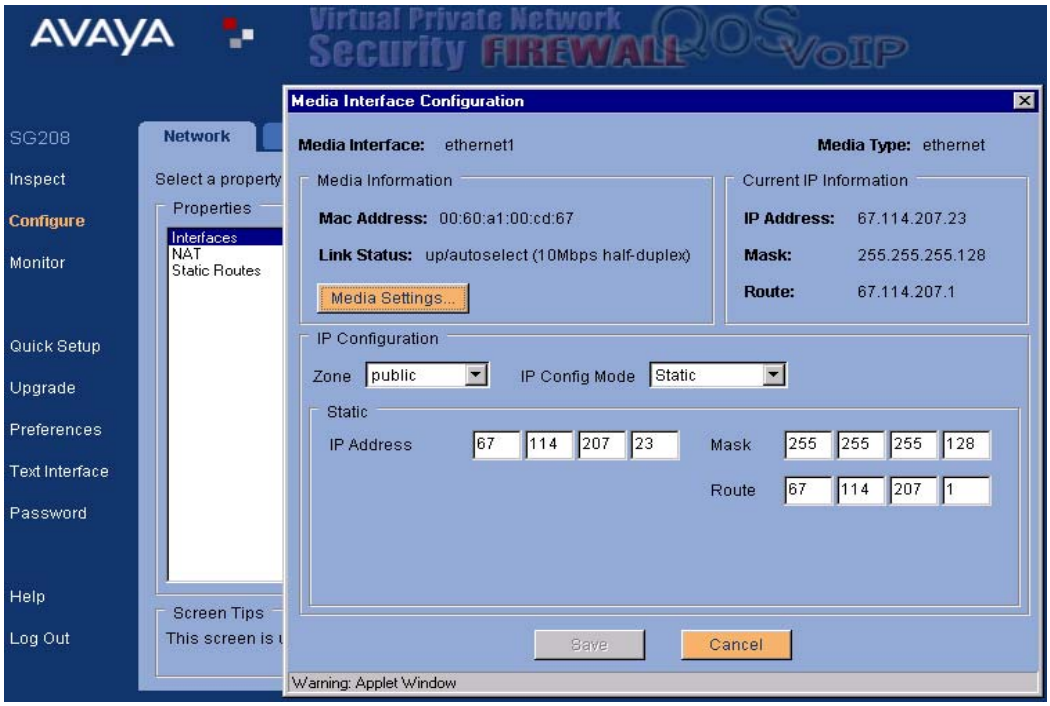
Step 2: Configure Network Interfaces

1. Select option “Configure”
2. Highlight option “Interfaces”

Step 2a: Configure Network Interfaces Ethernet0

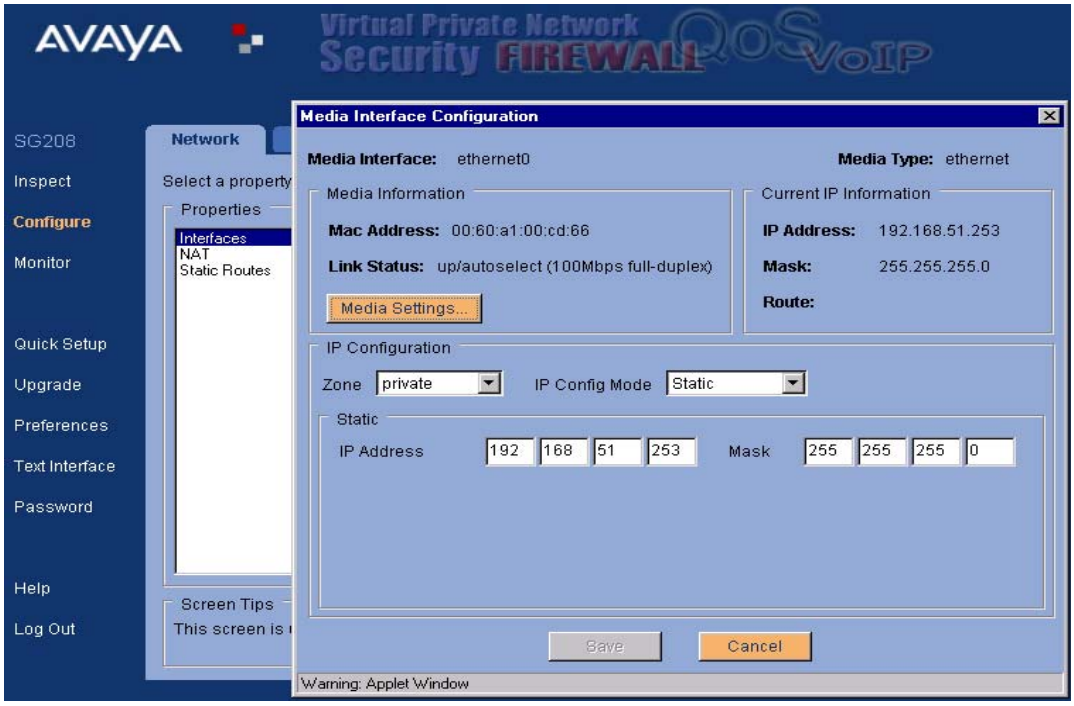
This is the public port address and mask provided by your service provider. The default route provided by your service provider will be the default route for all network traffic. ***NOTE: A static address from your Provider is required***.

1. Select Zone – Public
2. Select IP config Mode – Static
3. Enter the IP address, mask and route(Gateway) provided by the ISP provider.
4. Click Save



Step 2b: Configure Network Interfaces Ethernet1(Private)

1. Select Zone – Private
2. Select IP config Mode – DHCP Server
3. Enter the IP address, mask and route(Gateway) provided by the Network Administrator.
4. Enter the IP range provided by the Network administrator.
5. Enter WINS if required.
6. Click Save



Step 3: Remote Users

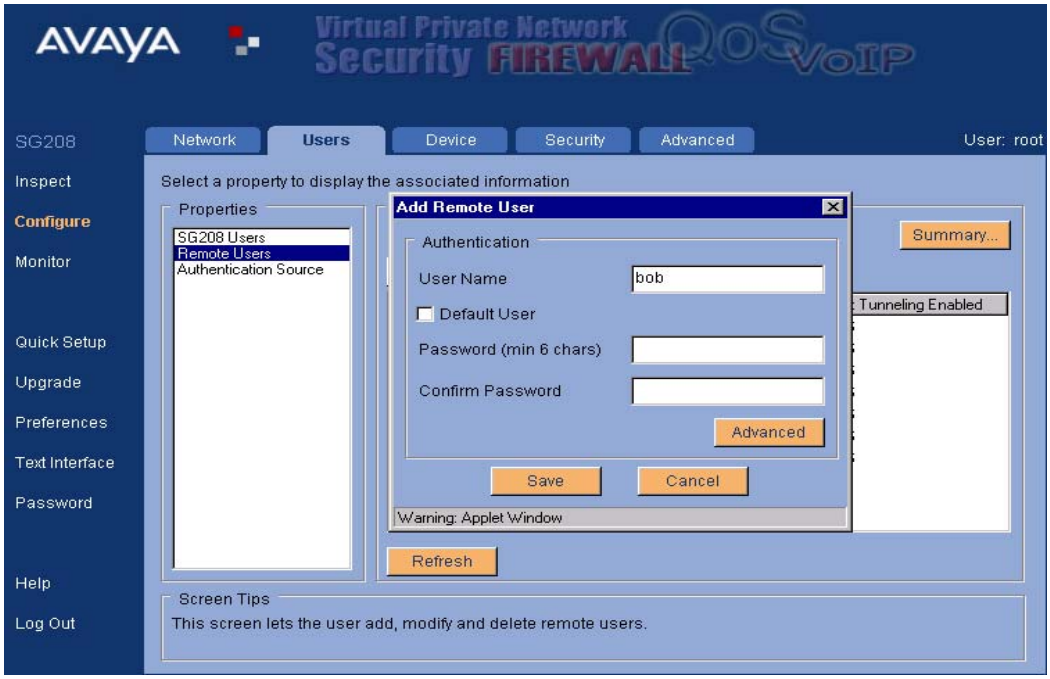
Remote Users are defined as IP devices or as users, which will be authenticated from the remote site. Devices include IP Hardphones and Personal Computers. Softphones will utilize the same tunnel as that of the PC. The PC will be required to enter a separate login and password to gain access to the network based on the user information noted below.

In Dynamic VPN configuration mode noted here, each remote user is assigned a name and associated password. Note: These same *user names and passwords* will be used to configure the SG5 users on the remote end. Passwords for each device can be the same if so desired.

To configure, scroll down and highlight the Remote Users under Properties

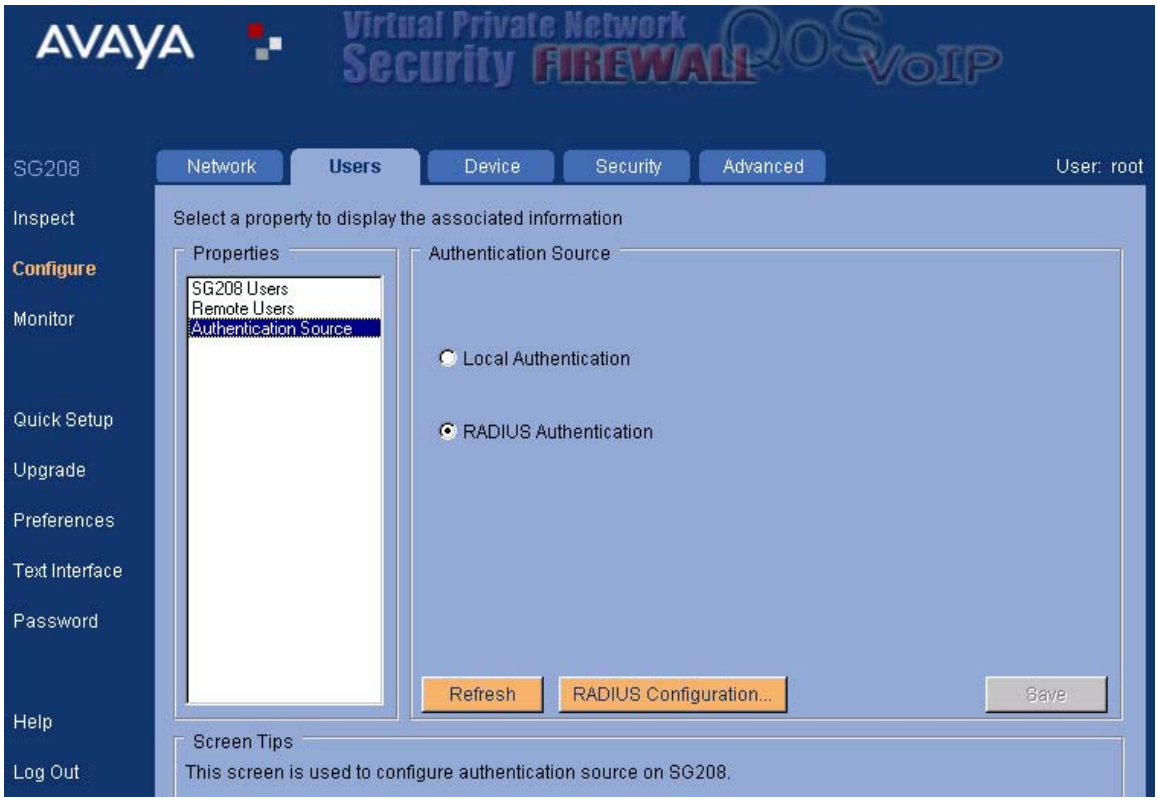
Go to the Remote Users section and click Add

1. Enter the user name and password
2. Click “Save”



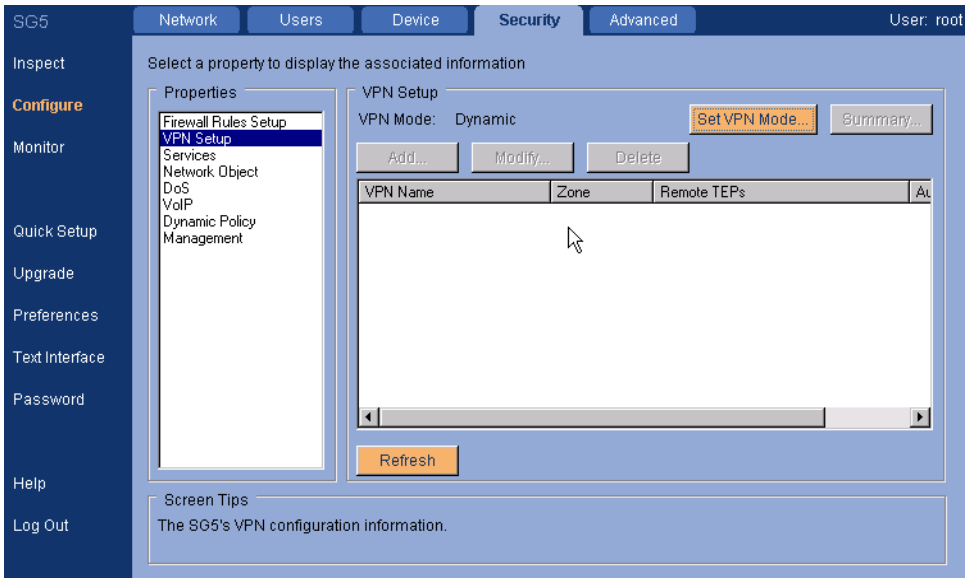
Step 3a: Authentications

Select which form of authentication to be used.
Local means the user will be authenticated from the SG 203 database
Radius means there is a Radius server that has been configured with the user names.

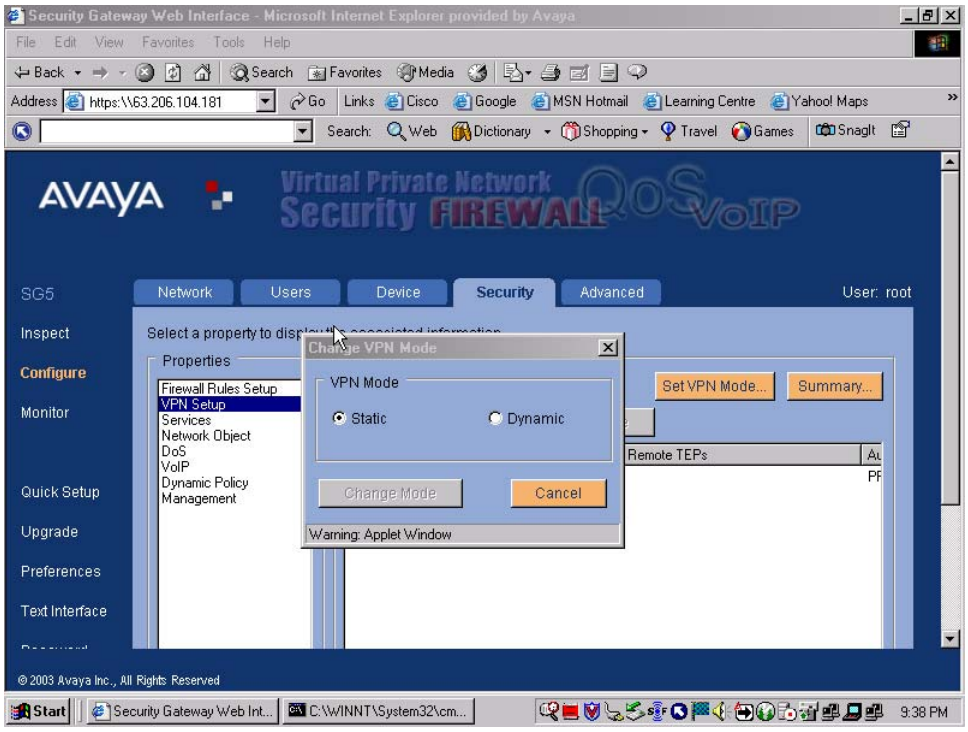


Step 3: Configure Security

In this tab, we will define the mode of VPN connectivity, to the remote location to be Dynamic. Select the SG setup tab under Properties, and then Click on ***"Set VPN Mode***"



Step 3a Once the Set VPN Mode tab is selected, a popup screen appears: *Select Static*



Step 4: Configure Remote Users

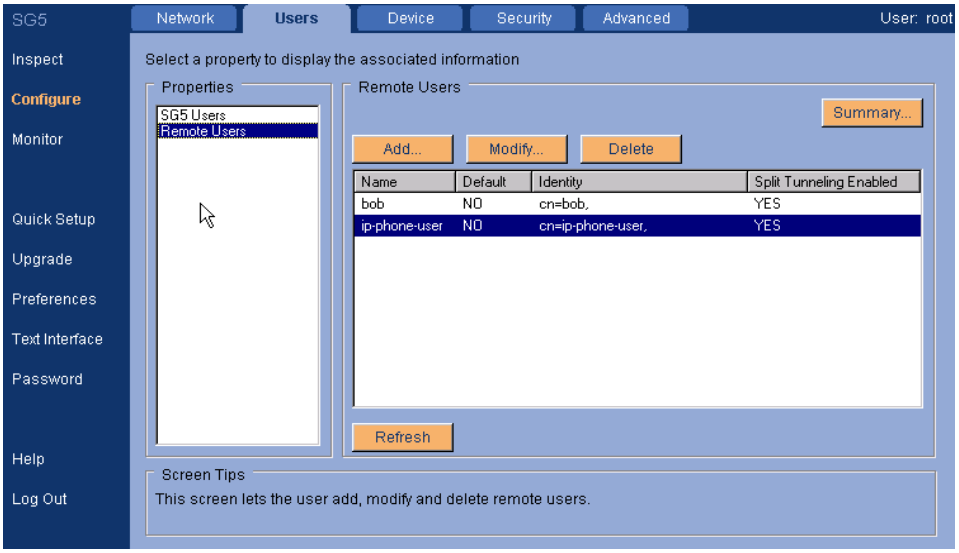
Remote Users are defined as IP devices or as users, which will be authenticated from the remote site. Devices include IP Hardphones and Personal Computers. Softphones will utilize the same tunnel as that of the PC. The PC will be required to enter a separate login and password to gain access to the network based on the user information noted below.

In Dynamic VPN configuration mode noted here, each remote user is assigned a name and associated password. Note: These same *user names and passwords* will be used to configure the SG5 users on the remote end. Passwords for each device can be the same if so desired.

NOTE :IP-Phone-User is a pre-configured default

To configure, scroll down and highlight the Remote Users under Properties

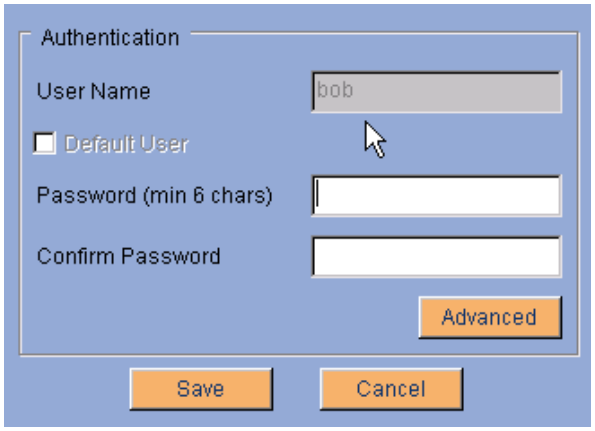
Go to the Remote Users section and click Add



Step 4a: An authentication box appears.

Enter a user name and associated password then click Save

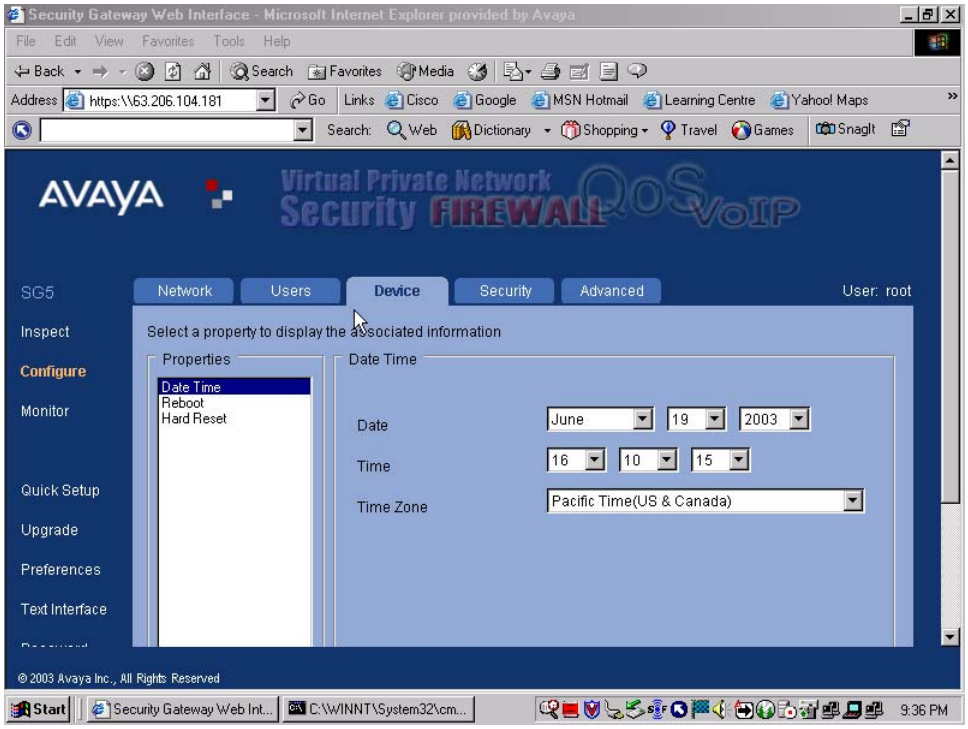
This will be user for a remote PC login.



NOTE: No changes are required in the Advance Tab

Step 5: Device Tab

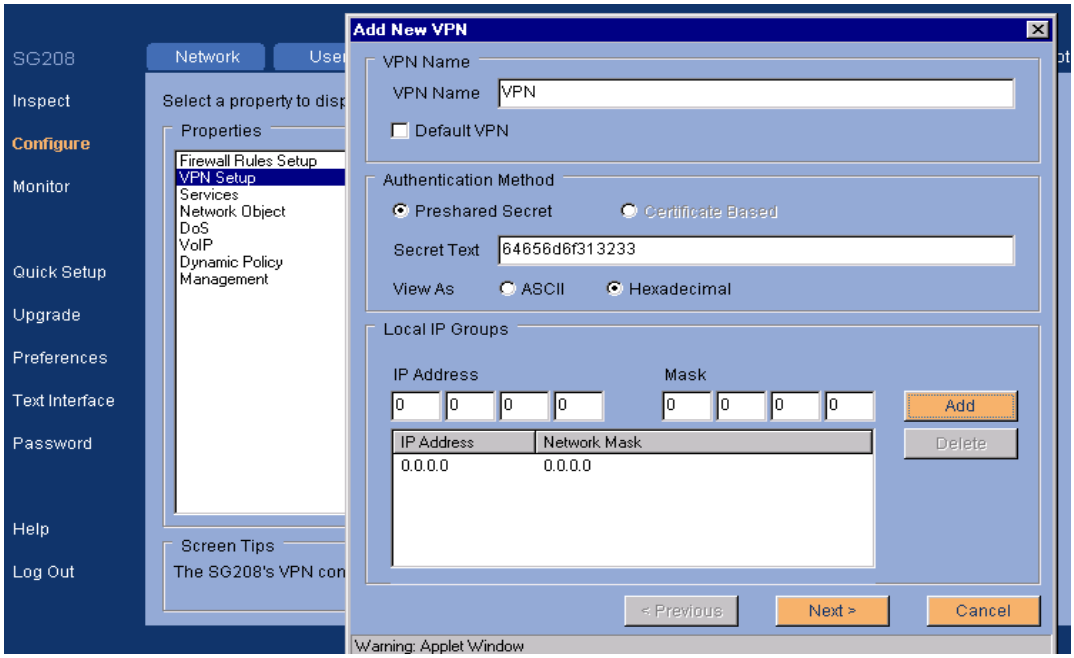
Adjust time accordingly (no other changes required)



Step 6: Security Tab

Click the add tab and Configure a tunnel name, password, and IP Groups for each IP 46xx phone or PC device accordingly.

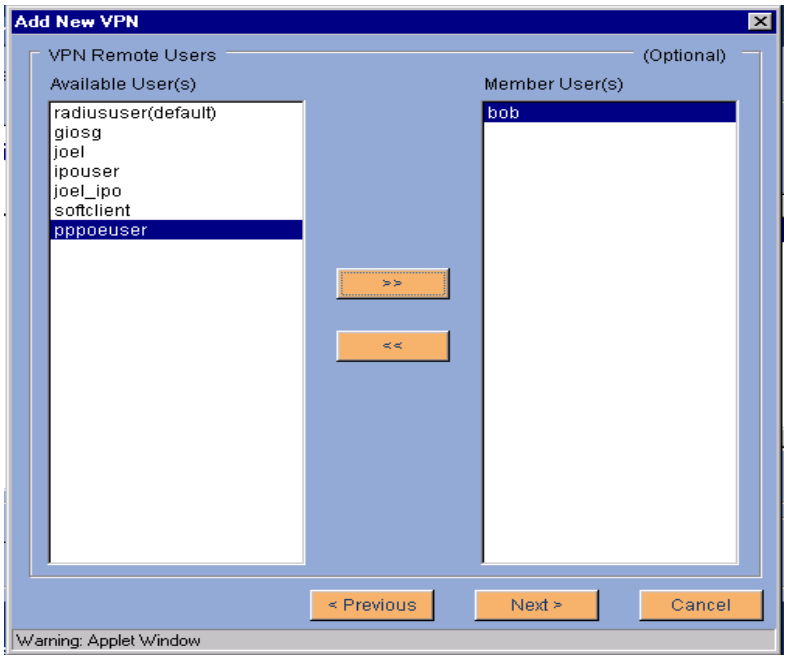
NOTE: All client configurations MUST match those configured on the Central site SG for *remote users.*



Click the Next button.

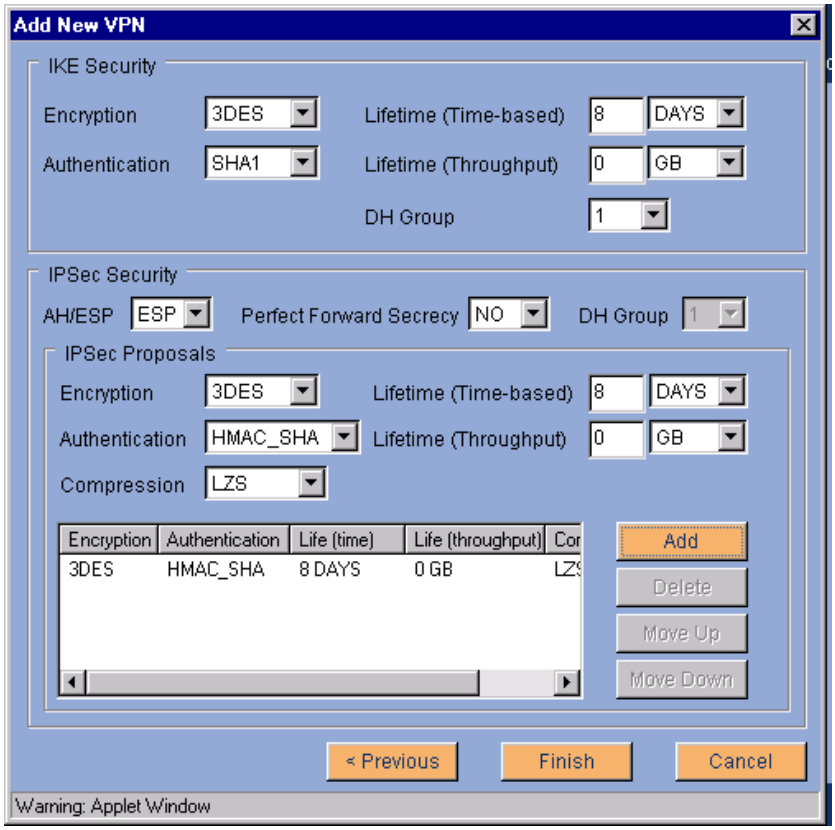
On the next screen click next again.

Select Users that will be part of this VPN and move then to the member pane.



Click Next

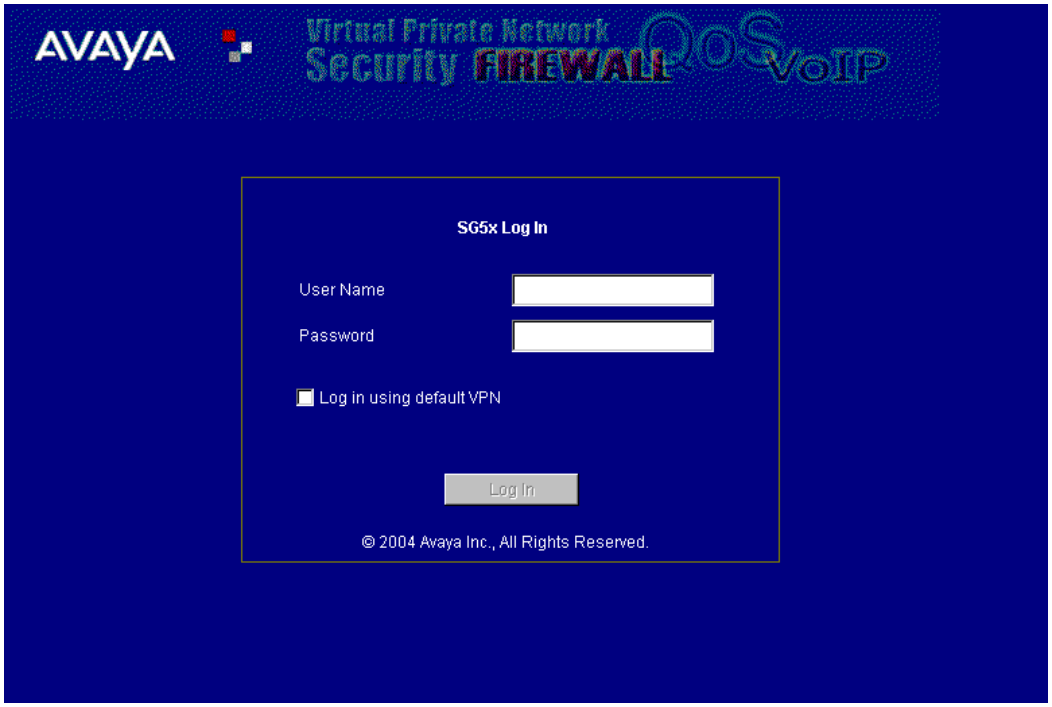
Configure the IKE and IPSec parameters to meet your security needs or click “Add” to accept the default setting which is standard.



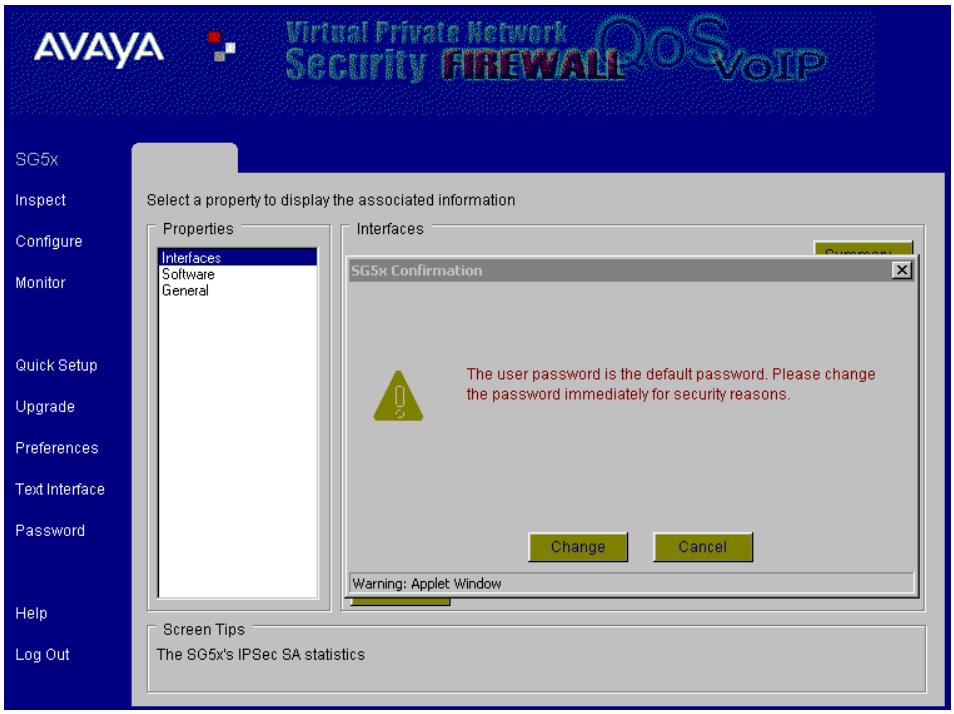
Congratulations: You have now completed the Central SG Configuration

6. Remote Site Configuration

Step 1: Login to SG5, 5X, 200
Default Login: root
Default Password: password



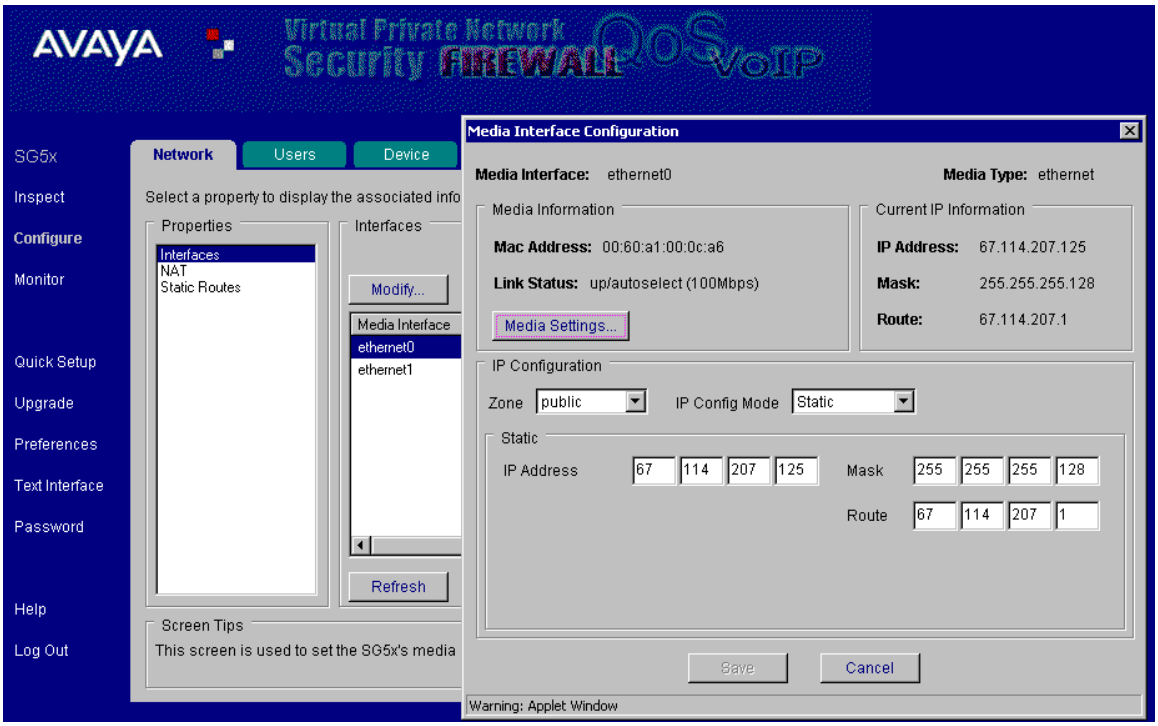
Step 1a: User Password (Click “cancel” for all demos)



Step 2: Configure Network Interfaces (Public & Private)

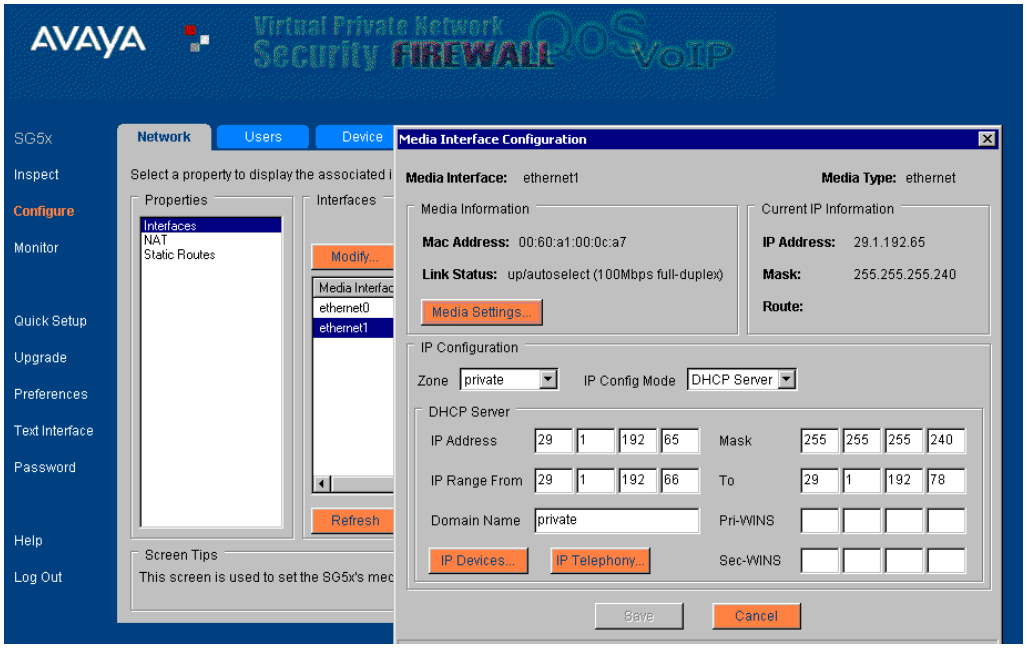
Step 2a: Configure Network Interfaces Public

1. Select Zone – Public
2. Select IP config Mode – Static, DHCP or PPPoE.
3. If static, enter the IP address, mask and route(Gateway) provided by the ISP provider.
4. Click Save



Step 2b: Configure Network Interfaces Private

1. Select Zone – Private
2. Select IP config Mode – DHCP Server
3. Enter the IP address, mask and route(Gateway) provided by the Network Administrator.
4. Enter the IP range provided by the Network administrator.
5. Enter WINS if required.
6. Click Save

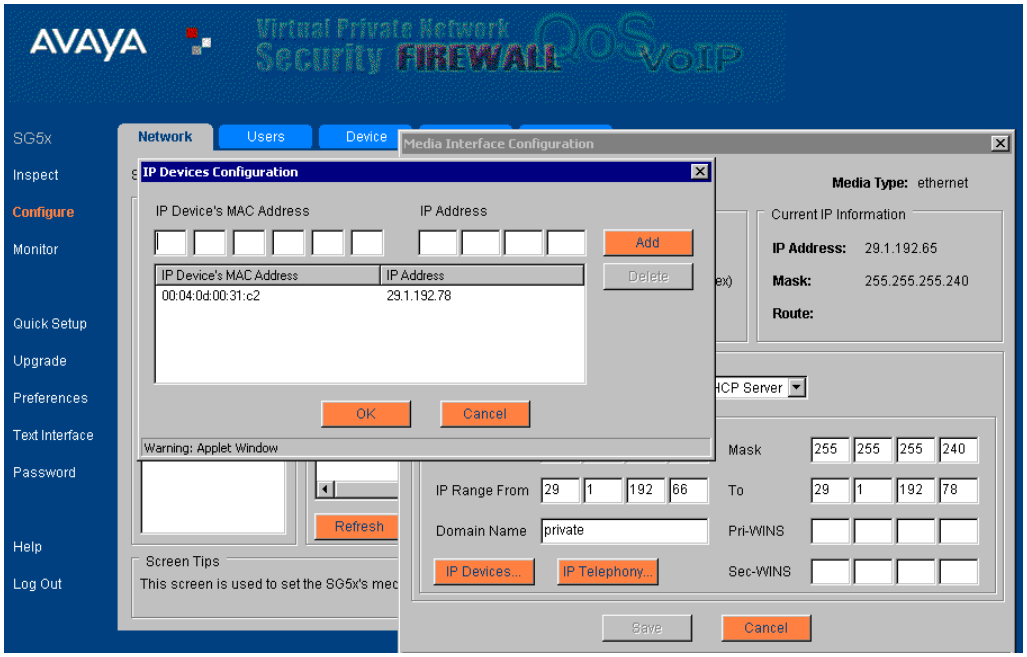


Step 2c: Configure IP Devices

In this screen we will configure the IP 46xx Hardphones connected to the SG5.

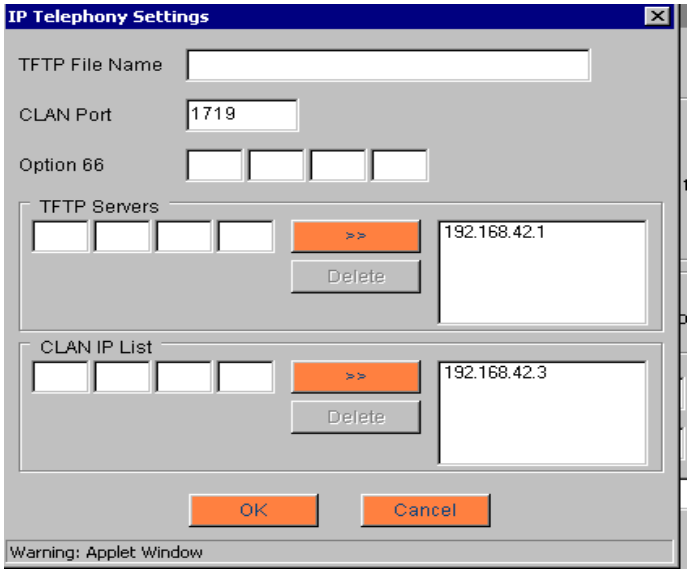
Turn over the phone and review the MAC label. Copy the address into the MAC address field, select an appropriate IP address and then click OK.

1. Select option “IP Devices” from the Private Interface pane.
2. Enter the MAC address of the phone (normally found on the bottom of the phone)
3. Enter an address from the IP range (In this example I choose the last address of the DHCP range)
4. Click “OK”



Step 2d: Configure IP Telephony

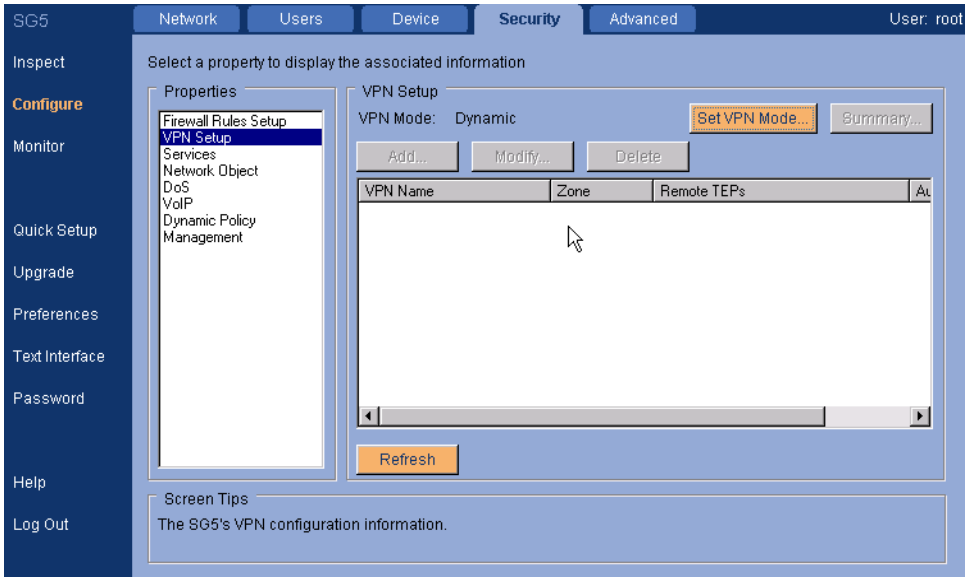
In this screen we associate the 46xx phones with the Host's IP Office and TFTP Server. Configure the IP address of the TFTP Server (default is the IP Office Manager) and then CLAN IP List, which is the address of the IP Office

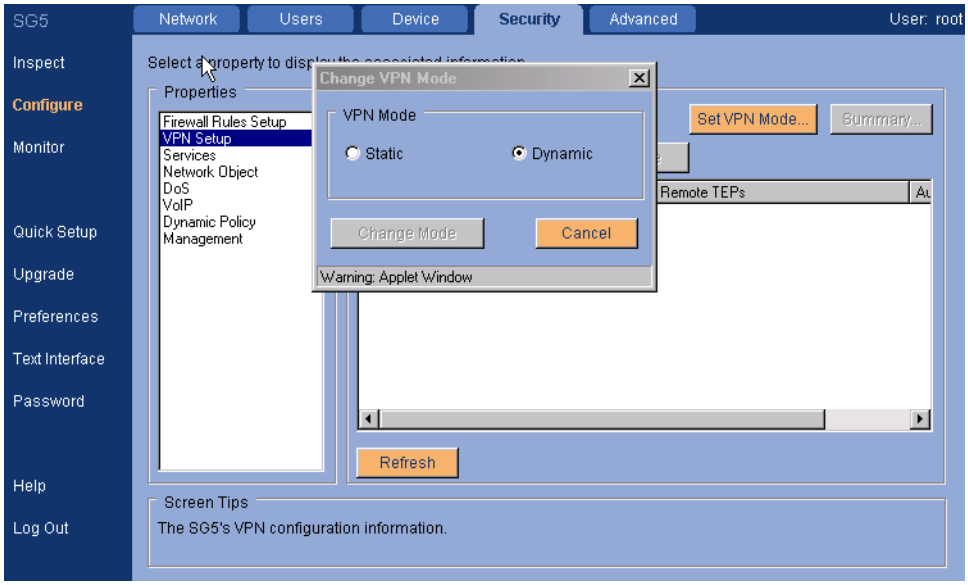


Step 3: Configure Security

In this screen setup, we will define the mode of VPN connectivity, to the remote location to be Dynamic.

Select the SG setup tab under Properties, and then Click on "Set VPN Mode"



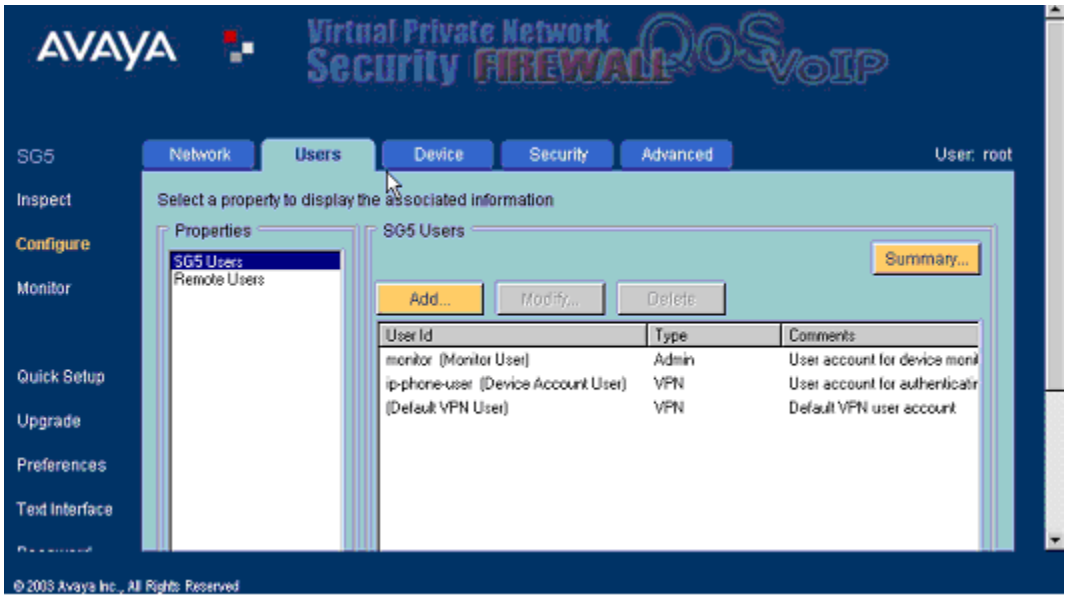


Once the Set VPN Mode tab is selected, a popup screen appears: ***Select Dynamic***
No other changes required

Step 4: Configure Users

SG5 Users are defined as all IP devices or “clients”, which will be authenticated through the VPN tunnel, to the Host site. Devices include IP Hardphones and Personal Computers. Softphones will utilize the same tunnel name and password as that of the PC. The SG5 provides three (3) pre-configured default clients that should not be modified.

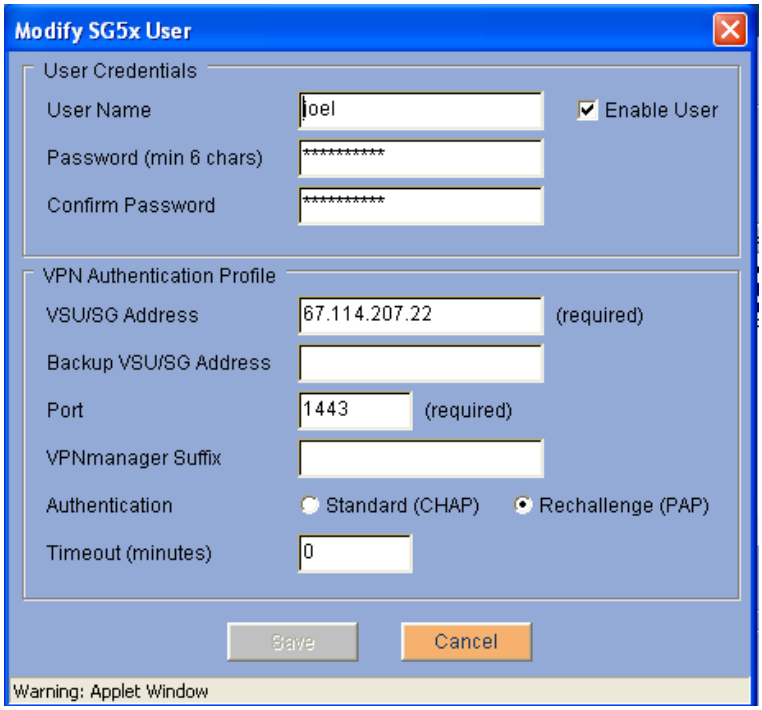
Select the SG Users bar under Properties



Step 4a: Highlight the ip-phone-user and then Click the Modify tab

1. Enter the user name that is configured on the central site Security Gateway
2. Enter the user password
3. Enter the public IP address of the central site Security Gateway
4. Select CHAP or PAP for the authentication method to match the configured method on the central site.
5. Click Save

NOTE: The user password MUST be the same as in the Central site configuration



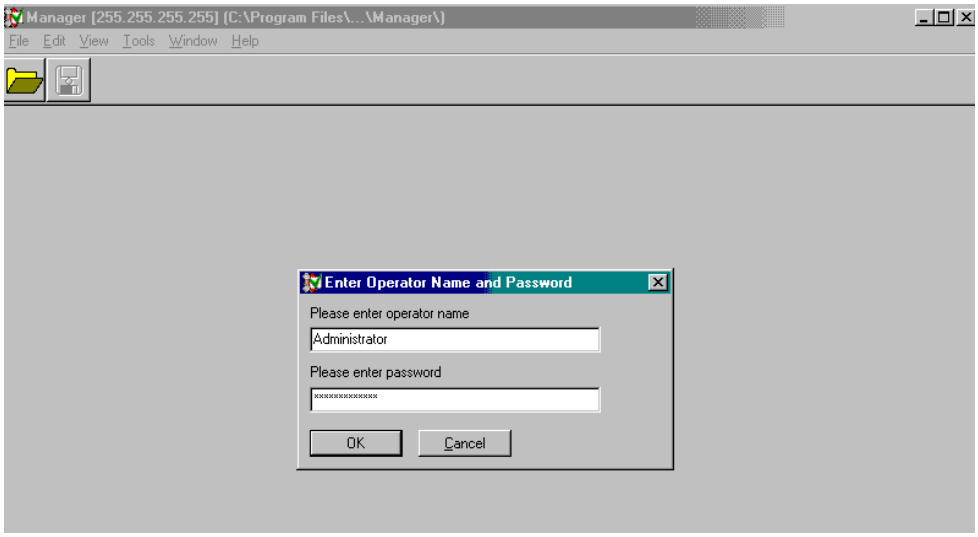
Note: This configuration will be used for authentication when the IP device initiates a dynamic connection.

Congratulations: You have now completed the Remote SG Configuration

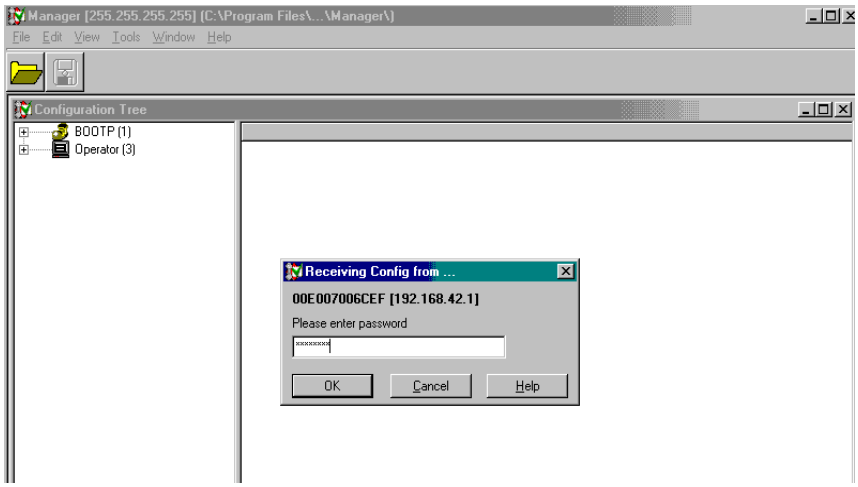
7. IP Office Configuration

The following IP Office configuration will provide the basic configuration to have locally connected phones and remotely connected phone connect.

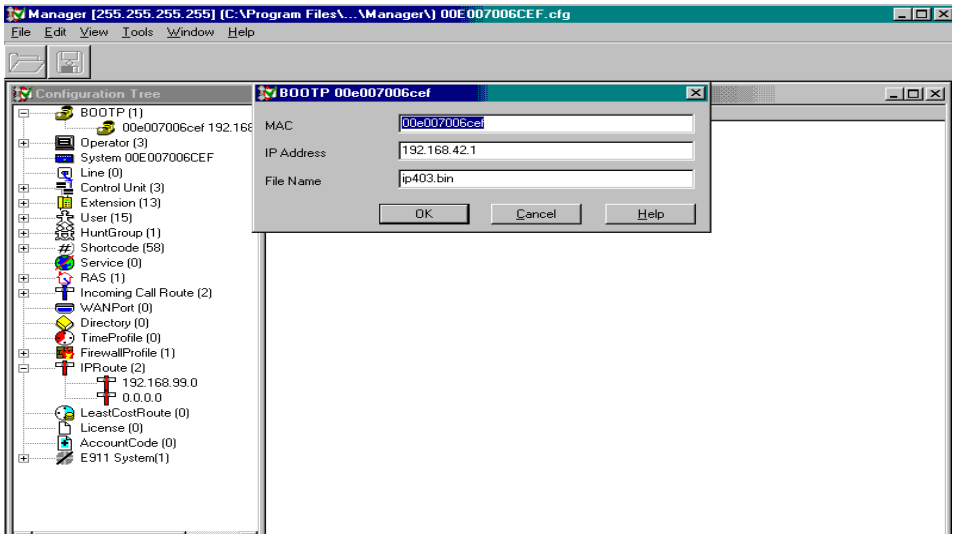
Step 1a: Log into the IP office Manager



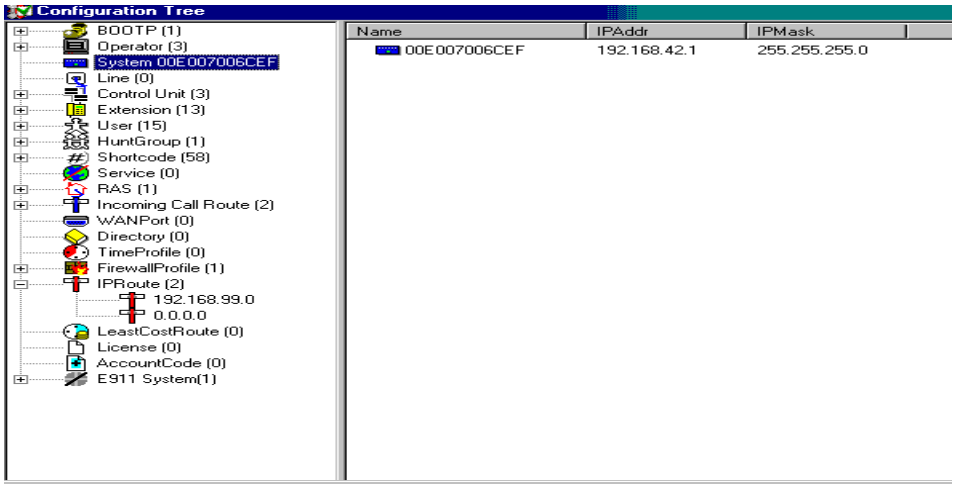
Step 1b: Log into the IP office by clicking on the folder icon.



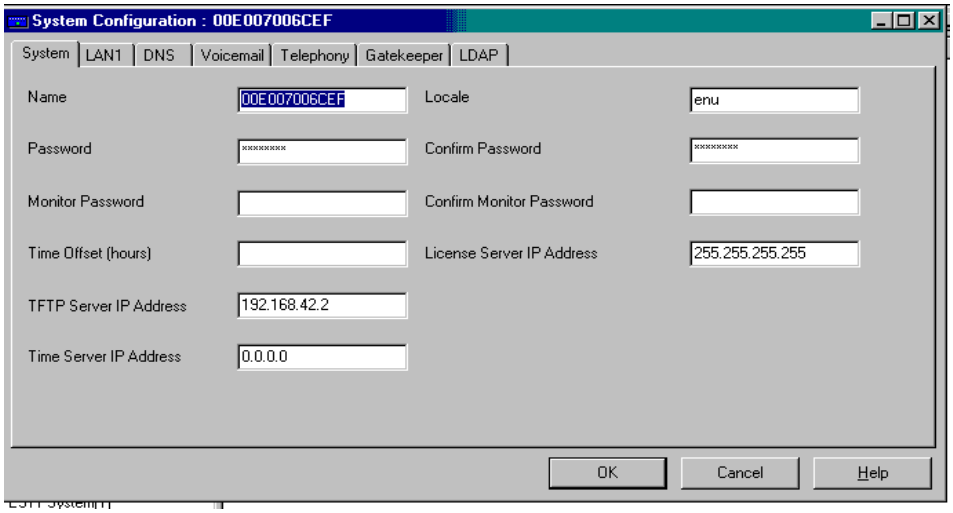
Step 2: Configure the IP address of the IP Office.



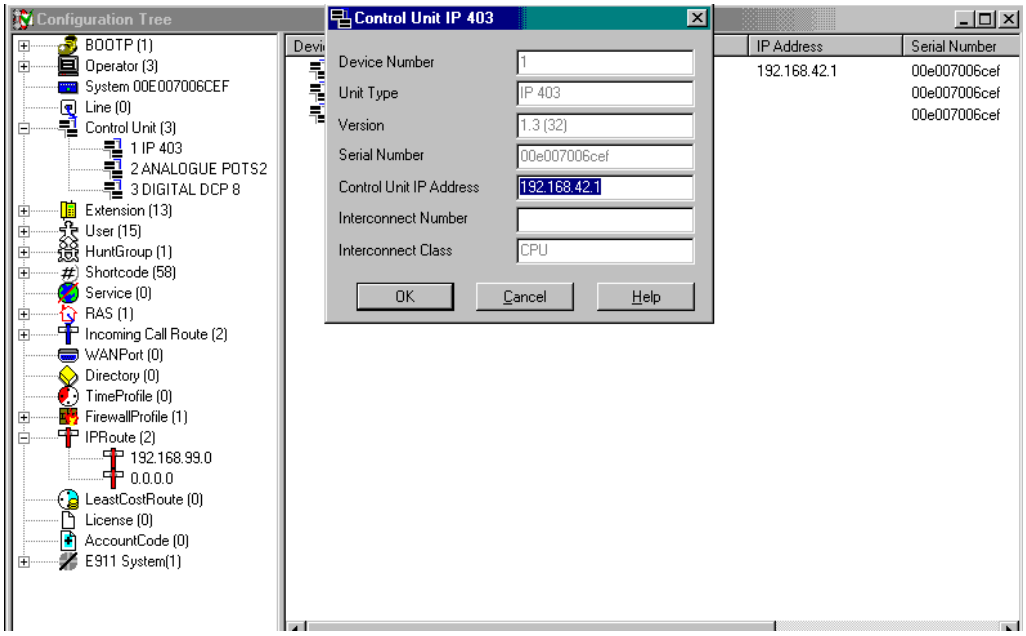
Step 2: Select and Configure the System parameters



Step 2a: Enter the password and TFTP server address.

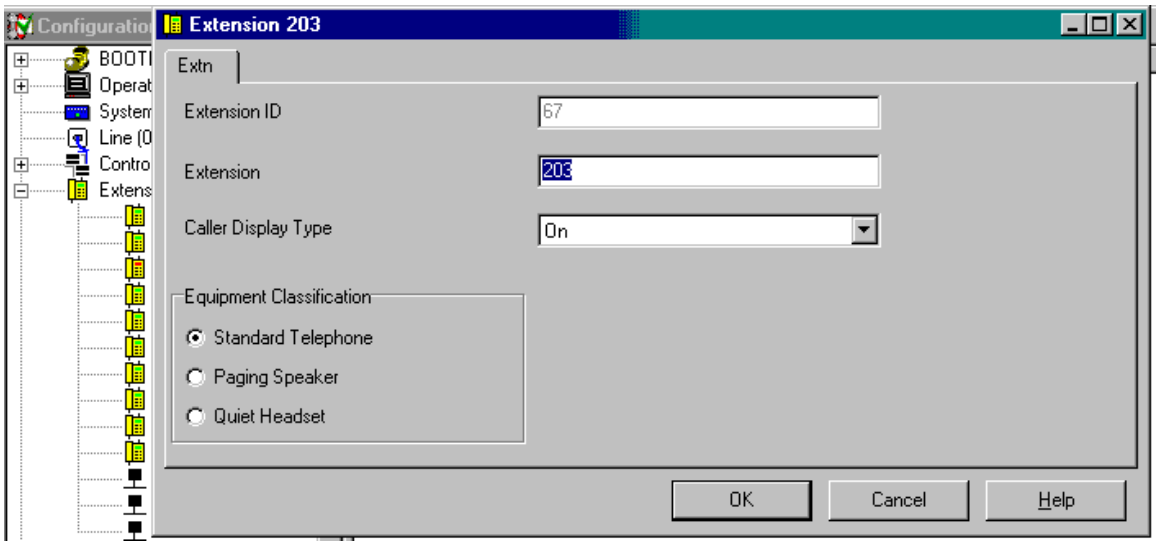


Step 3: Configure the Control unit IP address



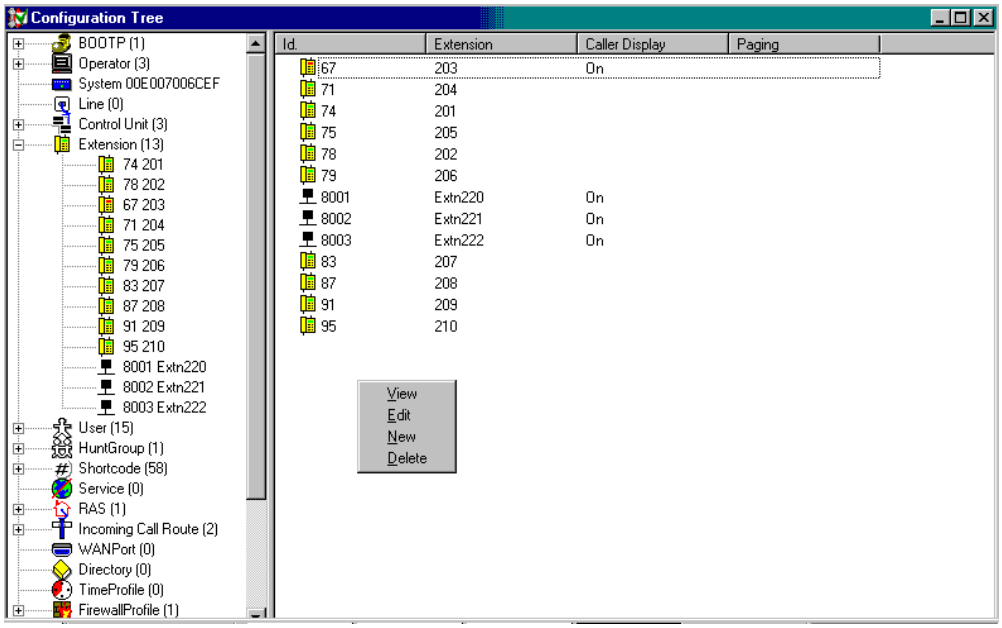
Step 3: Configure extentions locally connected to the IP Office.

Highlight and configure one of the pre-configured extentions

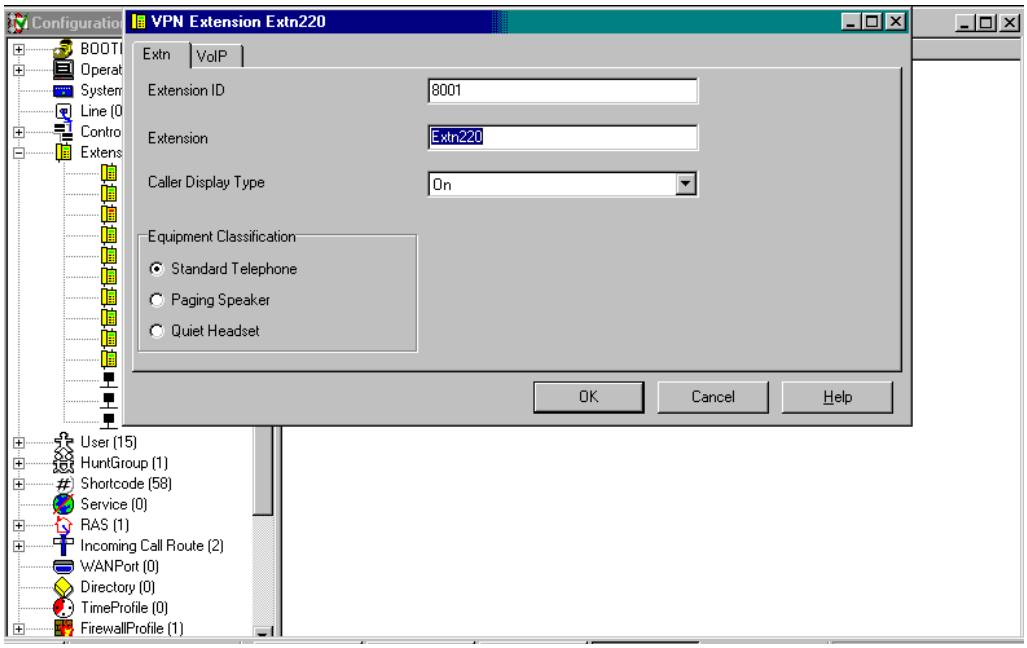


Step 3a: Configure extensions for remotely connected phones to the IP Office.

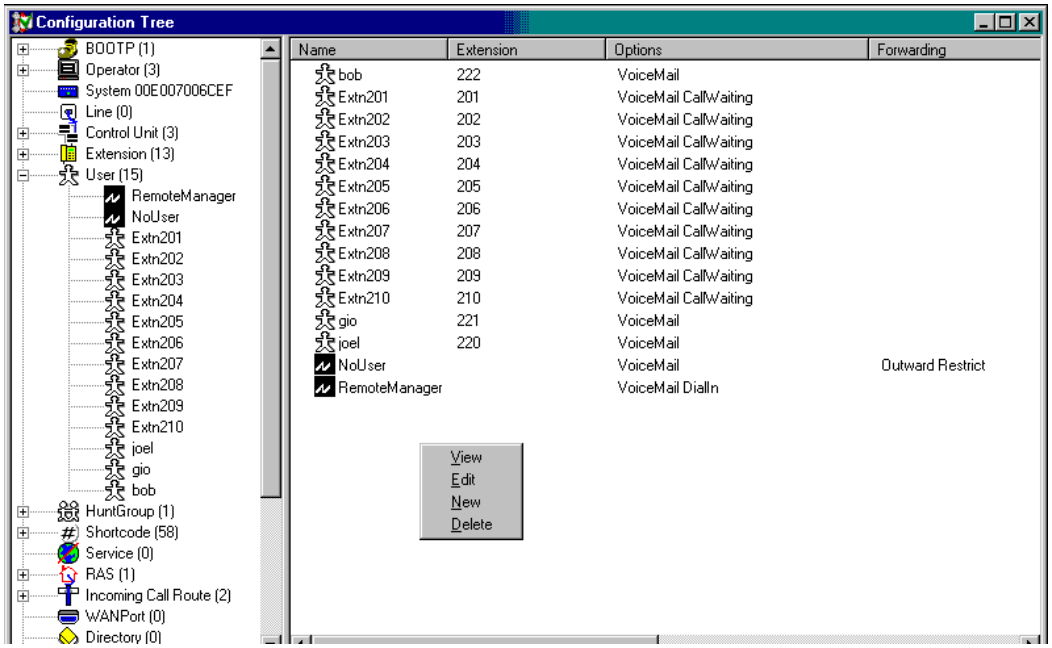
Right mouse click in pane to get option to create a new extension.



Step 3b: Configure extensions for remotely connected phones to the IP Office.

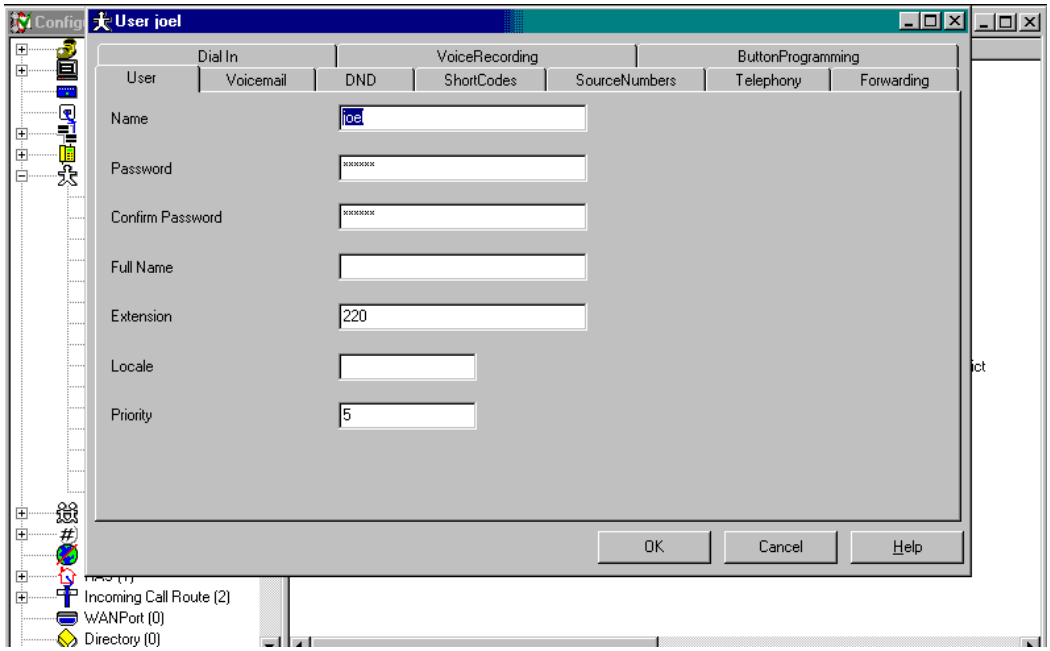


Step 4: Configure Users.



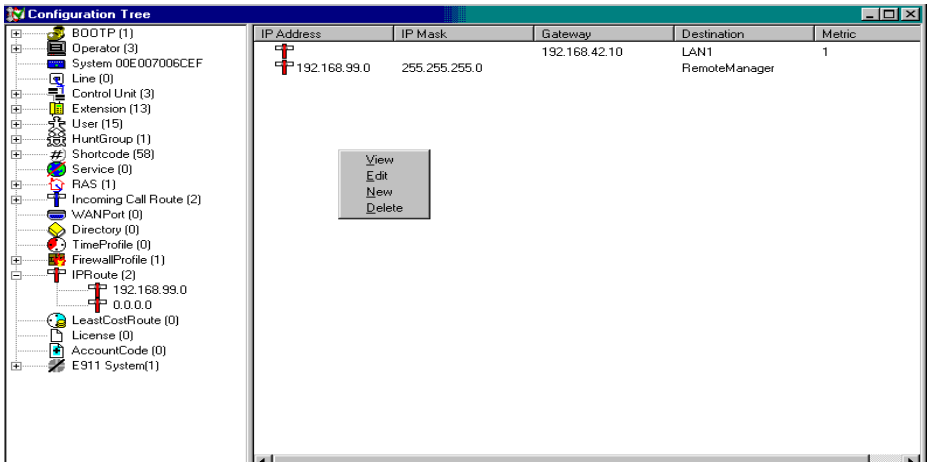
Step 4a: Configure Users.

This will allow configuration of the user name, password and the extension that will be configured on the remotely connected phone.

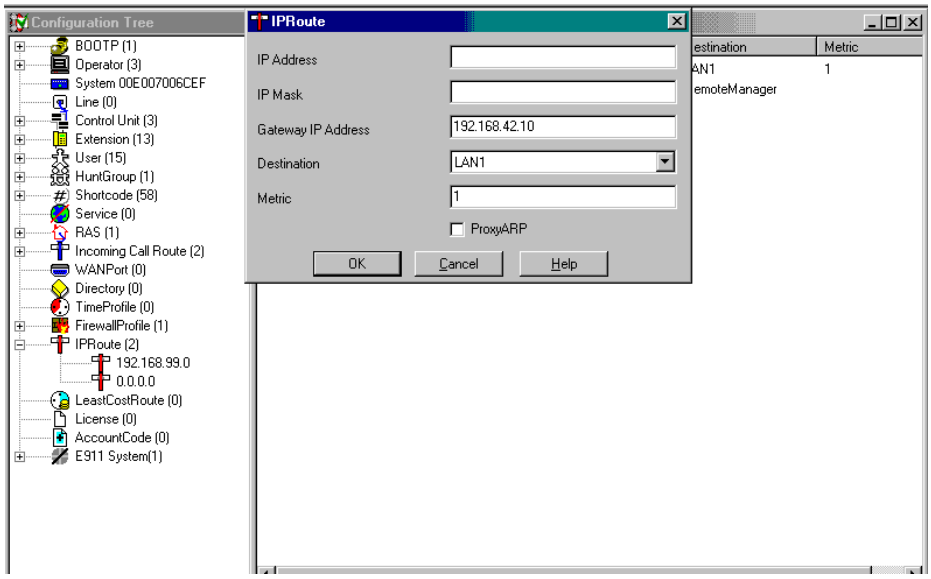


Step 5: Configure required default or static routes.

Right mouse click on right pane to add new



Step 5a: Configure required Default route for the IP Office.



Step 6: Save the configuration and update the IP Office unit.

Congratulations: You have now completed the basic IP Office Configuration.