



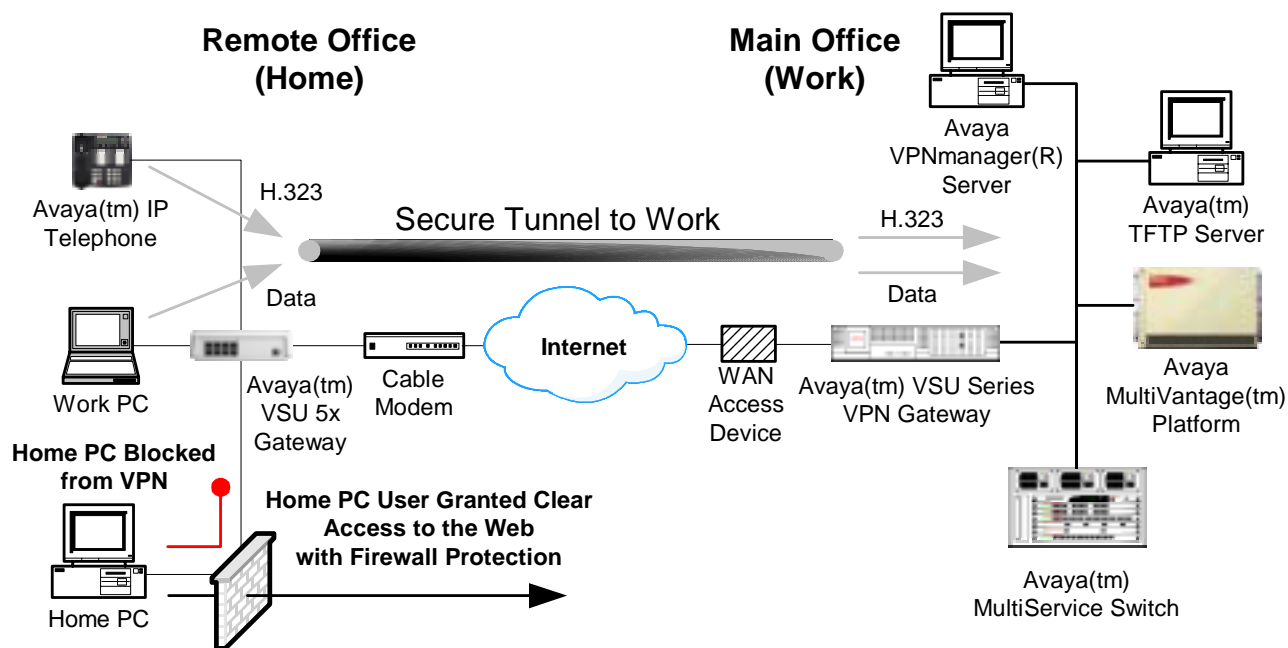
Configuring an Avaya™ VSU 5X Gateway in User Authentication mode with Avaya™ IP Telephones or Avaya™ IP Softphones – Issue 1.0

Abstract

These Application Notes describe a sample Avaya™ VSU 5X Gateway configuration for providing IP telephony and data VPN tunneling using a broadband connection. This document focuses specifically on the use of a Cable Modem; however, these steps can be applied to other broadband connections such as DSL. Support for Avaya™ 4600 Series IP Telephone DHCP option 176 is demonstrated. This document was written to aid customers planning on deploying Avaya VSU 5X Gateways with Avaya™ IP Telephones and/or Avaya™ IP Softphones over broadband connections.

1. Introduction

The diagram in **Figure 1** depicts how the Avaya VSU 5X Gateway gives users the ability to securely access the functionality of their Avaya 4600 Series IP Telephone or Avaya IP Softphone remotely via a broadband connection. The gateway has a built-in Dynamic Host Configuration Protocol (DHCP) server that can provide IP addressing to all local PC's attached to its private ports. Additionally when VPNs 4.2 becomes available the Avaya VSU 5X Gateway will support the option to use DHCP relay as opposed to its onboard DHCP server. The gateway allows local PCs to access the Internet via a single public port by using Network Address Translation (NAT) and an integrated firewall for security. Additionally, the onboard DHCP server supports option 176 which can push IP address, TFTP Server and Gatekeeper parameters down to Avaya IP Telephones for registration purposes. A special VPN Proxy User profile on the gateway provides automatic VPN authentication and establishment for any attached Avaya IP Telephones. When the VPN Proxy User is created, a VPN Policy is applied to all IP (Telephony)



Devices automatically and the tunnel will always be up on reboot. Each secure user PC must authenticate separately via a web browser login/password challenge. Optionally, SecureID can be used to provide an additional level of security for each user.

Figure 1: Securing IP Telephony and Data from Home

2. Equipment and Software Validated

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

Equipment	Software
Avaya™ S8100 Media Server and an Avaya™ G600 Media Gateway	Avaya MultiVantage™ software 1.1
Avaya™ 4624 Series IP Telephone	Release 1.6
Avaya™ IP Softphone	v3.2.3
Work PC - Dell Latitude C800	Windows 2000 Professional
Home PC – Dell Latitude C600	Windows XP Professional
Cubix Density Blade Server 1	WinNT 4.0 Server SP5, Avaya™ TFTP Server 3.6.1
Cubix Density Blade Server 2	Win2K Server SP1, Avaya VPNmanager™ 3.2.12
Avaya™ VSU 5X VPN Gateway	Avaya VPNos® 4.1.25
Avaya™ VSU 5000 VPN Gateway	Avaya VPNos® 3.2
LinkSys BEFSR41 V.2	Firmware Version 1.42.7
RCA Cable Modem	Unknown

3. Network Considerations

The following should be considered when deploying Avaya VSU 5X Gateways:

1. Direct IP-IP Audio Connections otherwise referred to as Shuffling is not supported with the sample configuration provided in these Application Notes.
2. In order for the Avaya VSU 5X gateway to operate behind an existing third-party broadband router the router must support IPSec Pass-Through and be capable of forwarding UDP port 500 for IKE. This scenario has been validated using a LinkSys BEFSR41 V.2 with firmware version 1.42.7.
3. For a VoIP connection through a VSU 5X, a DSL or a cable modem connection is required in order to achieve acceptable voice quality. As the voice traffic is highly sensitive to delay, the quality of the connection depends on the available bandwidth at the time when the call is made. The actual available bandwidth may vary significantly depending on the time of day, the number of simultaneous users and differs from ISP to ISP. If the VSU 5X deployment is in the business environment as a small office, a Service Level Agreement (SLA) with the service provider can help to ensure a business quality VoIP connection. Please reference **Section 4.2.1** for guidelines on audio codec selection in order to ensure adequate per call bandwidth.

4. Configuration

The sample configuration provided in Figure 2 assumes that the Avaya VSU 5X gateway is using its onboard DHCP server to assign IP addresses to remote office devices. As a reminder the VSU 5X gateway will optionally support DHCP relay when VPNos 4.2 becomes available. There is no public address depicted in Figure 2 for the Avaya VSU 5X gateway because this configuration assumes that it will be obtained automatically from the service provider via DHCP. Please refer to the DEFINITY® Administration and Administration for Network Connectivity Guides for additional details beyond the scope of this paper. All administration steps described in section 3.2 were done using terminal emulation through Avaya Site Administration software.

4.1. Detailed IP Addressing Scheme

The diagram in Figure 2 represents the IP addressing scheme used throughout these Application Notes. This has been included as a reference.

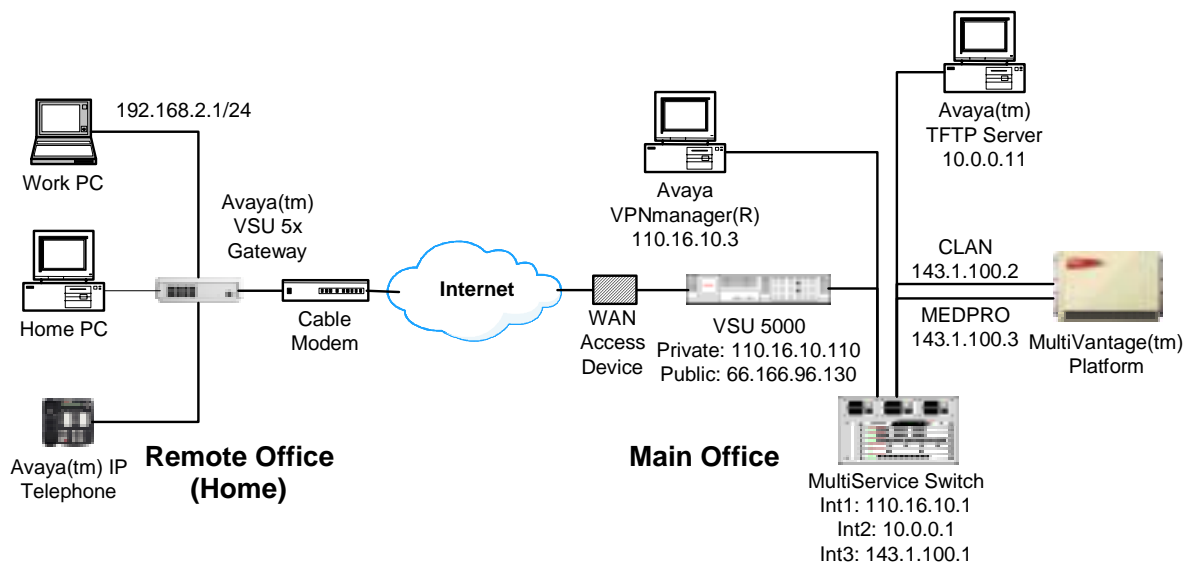


Figure 2: Detailed IP Addressing Scheme

4.2. Avaya MultiVantage Configuration

4.2.1. Determining Audio Codec Selection

Avaya recommends 30ms (3 Frames Per Pkt), G.729 packets for WAN connections. If WAN bandwidth utilization is of concern the administrator may enable Silence Suppression, which can further reduce the bandwidth per call by approximately 30-50%. The trade-off is that Silence Suppression can also significantly reduce the perceived voice quality of the call. The choice to implement silence suppression depends on the end user expectations and needs. Do not enable

suppression unless the bandwidth constraints are severe and the users are aware of the quality impairments.¹

If the broadband connection being used provides uplink or downlink line rates that are at or below the average per call throughput for the chosen codec, voice quality will be adversely affected. The Audio Codec and Frames Packet Size for users should be carefully chosen in order to ensure adequate bandwidth per call with acceptable delay. The following measurements have been included as a guide for administrators to use for estimating remote site bandwidth requirements. **Table 1** is based on G.729 and **Table 2** is based on G.711MU with typical Frames Per Packet settings:

Frames Per Pkt	Packet Size (ms)	Average L2 Frame Size in Bytes	Average Per Call Throughput with No Silence Suppression	Average Bytes Per Second Per Call
2	20	130	104.98 Kbps	13,121.99
3	30	138	74.31 Kbps	9289.24
4	40	154	62.16 Kbps	7769.97

Table 1: G.729 RTP with ESP Overhead

Frames Per Pkt	Packet Size (ms)	Average L2 Frame Size in Bytes	Average Per Call Throughput with No Silence Suppression	Average Bytes Per Second Per Call
2	20	274	220.52 Kbps	27,564.66
3	30	353	189.82 Kbps	23,727.68
4	40	433	175.84 Kbps	21,979.98

Table 2: G.711MU RTP with ESP Overhead

The International Telecommunications Union (ITU) recommends a maximum delay of 150 (milliseconds) for one-way voice traffic. Anything above this value theoretically degrades the perception of voice quality. Tests conducted in Avaya Labs, however, show that delay can vary over a range before users notice it. Different individuals, and people from different cultures, have a varying tolerance for communication delay. Many users do not seem to notice a problem with one-way delay of 200ms. Therefore, the ITU's 150ms standard for one-way delay should not be taken literally, but as a boundary at which communication degradation becomes observable.

¹ Paragraph quotes from (S8700/G600) Network Requirements & Configuration Guidelines Issue 1.1

4.2.2. Avaya MultiVantage Basic H.323 Administration Tasks

1. Specify the type of codec used for voice encoding and companding.

At the Avaya MultiVantage™ terminal prompt, enter **change ip-codec-set 3** and match the parameters shown in **Figure 3**. Then apply the changes. The parameters (reference **Figure 3**) that need to be changed are:

- Audio Codec
- Frames Per Pkt
- Packet Size (ms)

```
change ip-codec-set 3

                               IP Codec Set

Codec Set: 3

Audio      Silence      Frames      Packet
Codec      Suppression  Per Pkt    Size(ms)
1: G.729      n              3          30
2:
```

Figure 3: Configuring the IP Codec Set

2. Define IP Network Region for optimal audio packet performance.

At the Avaya MultiVantage terminal prompt, enter **change ip-network-region 3** and match the parameters shown in **Figure 4**. Then apply the changes.

Note: A different ip-network-region number may be chosen depending on your setup. The parameters (reference **Figure 4**) that need to be changed are:

- Codec Set
- Direct IP-IP Audio Connections
- IP Audio Hairpinning

```

change ip-network-region 3                                     Page 1 of 2

                                IP Network Region

                                Region: 3
                                Name: VSU 5X Remote Region
Audio Parameters
                                Codec Set: 3

                                UDP Port Range
                                Min: 2048
                                Max: 65535

DiffServ PHB Value: 0                                         Direct IP-IP Audio Connections? n
                                                                IP Audio Hairpinning? y

802.1p/Q Enabled? N

```

Figure 4: Configuring the IP Network Region

3. Assign node names and IP addresses to each node in the network.

At the Avaya MultiVantage terminal prompt, enter **change node-names ip** and match the parameters shown in **Figure 5**. Then apply the changes.

Note: The C-LAN and MEDPRO cards must have unique names and IP addresses assigned in the node-names list. These values will eventually be matched to the physical card interfaces in **step 4**. The parameters (reference **Figure 5**) that need to be changed are:

- Name
- IP Address

```

change node-names ip                                         Page 1 of 1

                                IP NODE NAMES
                                Name                IP Address
RemoteClanG3r1        143.1 .100.2
RemoteMediaG3r1       143.1 .100.3

```

Figure 5: Configuring IP Node Names

- Define the IP interface for the C-LAN and MEDPRO cards being used for the trunk.

At the Avaya MultiVantage terminal prompt, enter **change ip-interfaces** and match the parameters shown in **Figure 6**. Then apply the changes.

Note: Different Slot values may be needed depending on the specific configuration. The Node Names used for each card interface must match those previously specified in the Node Names table for **step 3** in order to correctly correlate each IP address to its respective card. The parameters (reference **Figure 6**) that need to be changed are:

- Enable Eth Pt
- Type
- Slot
- Node Name
- Subnet Mask
- Gateway Address
- Net Rgn

Change ip-interfaces										Page	1 of	6
IP INTERFACES												
Enable	Eth Pt	Type	Slot	Code	Sfx	Node Name	Subnet Mask	Gateway	Address	Net	Rgn	
y		C-LAN	01A05	TN799	C	RemoteClan	255.255.255.0	143.1	.100.1	3		
y		MEDPRO	01A07	TN2302		RemoteMedia	255.255.255.0	143.1	.100.1	3		

Figure 6: Configuring IP Interfaces

- Assign Link via Ethernet Data Module to the C-LAN.

At the Avaya MultiVantage terminal prompt, enter **add data-module next** and match the parameters shown in **Figure 7**. Then apply the changes.

Note: Different data-module extension and C-LAN slot may be needed depending on the specific configuration. If multiple C-LAN cards are in use a different link number may be necessary. However, port 17 must be used on the C-LAN card regardless. The parameters (reference **Figure 7**) that need to be changed are:

- Type
- Port
- Link

```
add data-module next                                     Page 1 of 1
                                                         DATA MODULE
Data Extension: 20003                                  Name: Remote VPN C-LAN Interface
Type: ethernet
Port: 01A0517
Link: 3
```

Figure 7: Configuring the Date Module

4.3. Quick Setup of the Main Office VSU 5000 Gateway

These notes assume that no previous configuration exists on the VSU 5000 gateway prior to provisioning the unit. In addition, these Application Notes modify the minimum number of parameters necessary to recreate the sample configuration. Different applications may require that some default parameters be changed especially when it comes to default username and password settings. Information on flushing existing configurations and modifying default parameters is available in the VPNmanager help system.

1. Connect to the VSU.

Using a null modem cable, connect the VSU 5000 to a PC serial port. Start a HyperTerminal session to the VSU 5000 using the following parameters:

```
Bits per second    9600
Data bits          8
Parity             None
Stop bits          1
Flow control       None
```

2. Run Quick Setup.

On the main console menu enter the required VSU console password. Then press 5 to select **(5) – Quick Setup** and enter the following information:

```
Enter IP Address: 66.166.96.130
Enter IP Mask: 255.255.255.248
Do you want a secondary IP address on this unit? [yn] y
Secondary IP address:  Mask:
Enter IP Address: 110.16.10.110
Enter IP Mask: 255.255.255.0
Enter Default Route: 66.166.96.129
Change VSU console password? [yn] n
Change superuser name? [yn] n
Change superuser password? [yn] n
Non-VPN Config Menu choice 3
Do you really want to deny all non-VPN traffic? [yn] y
Do you want this unit to run in FIPS-Compliant mode? n
Enter date [MM-DD-YYYY]: [press enter]
Enter time [HH:MM:SS]: [press enter]
Reboot Now? [yn] y
```

4.4. Configure the VPNmanager

1. Start the VPNmanager console.

For VPNmanager 3.2:

On the desktop, select **Start → Programs → VPNmanager → VPNmanager Console**

2. Login to the VPNmanager console.

On the VPNmanager Login window, enter the **User Name** and **Password** (defined during VPNmanager installation) under Identity. Click the **Add** button under VPNmanager Servers list. In the Configure Server popup window, enter the **IP Address** or **DNS Name** of the VPNmanager server and click the **OK** button. Select the server from the VPNmanager Servers list and click the **Connect** button.

3. Create a new VPN domain.

From the VPNmanager, select **VPN Domain → New** from the pull-down menu. Match the parameters shown in **Figure 8**. Click the **Apply** button.

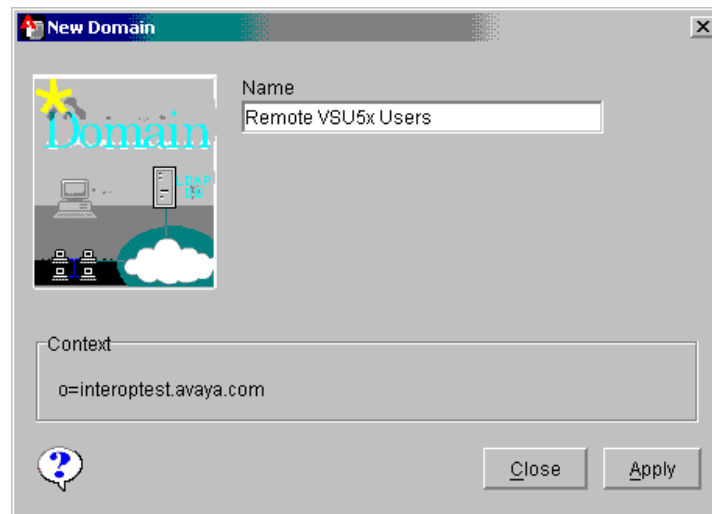


Figure 8: Add a new VPN Domain

4. Enter the configuration console.

From the **VPNmanager** window click on the **Config** button depicted in **Figure 9**.



Figure 9: Enter the Configuration Console

5. Add the VSU 5000 to the VPN domain.

From the **Configuration Console** window, select **Edit** → **New Object** → **VSU** from the pull-down menu. From the **VSU Setup Wizard** popup depicted in **Figure 10**

- ❑ Enter the new VSU name **vsu5000gateway**
- ❑ Click the **Next >>** button

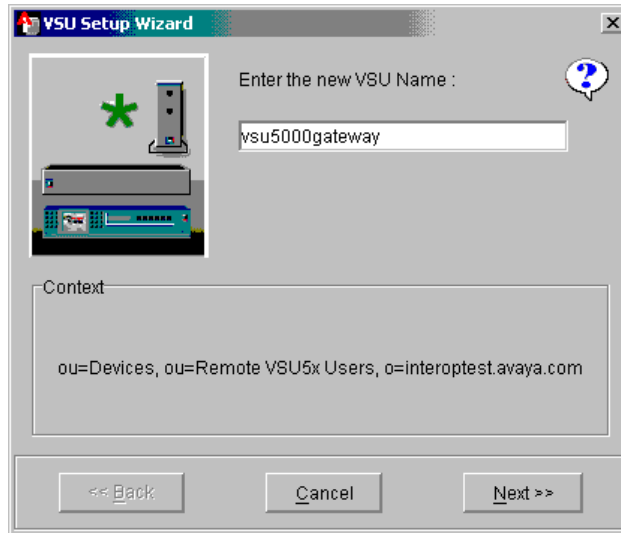


Figure 10: Add the VSU 5000 to the Manager

From the **VSU Setup Wizard** popup depicted in **Figure 11**

- ❑ Select **New VSU Setup**
- ❑ Click the **Next >>** button

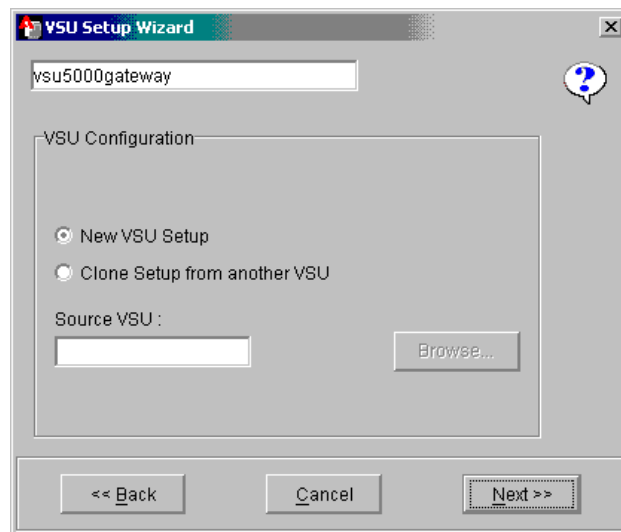
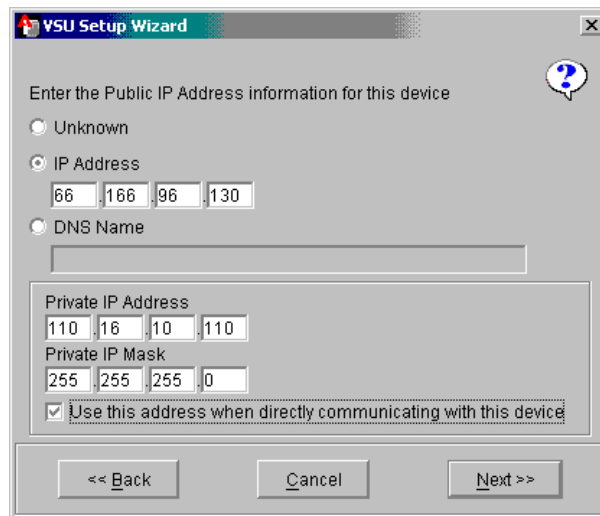


Figure 11: VSU Setup Wizard – New VSU Setup

From the **VSU Setup Wizard** popup depicted in **Figure 12**

- ❑ Select **IP Address**
- ❑ Enter IP Address **66.166.96.130** (Public Address)
- ❑ Enter Private IP Address **110.16.10.110** (Private Address)
- ❑ Enter Private IP Mask **255.255.255.0**
- ❑ Select **Use this address when directly communicating with this device**
- ❑ Click the **OK** button in the **Warning** popup
- ❑ Click the **Next >>** button

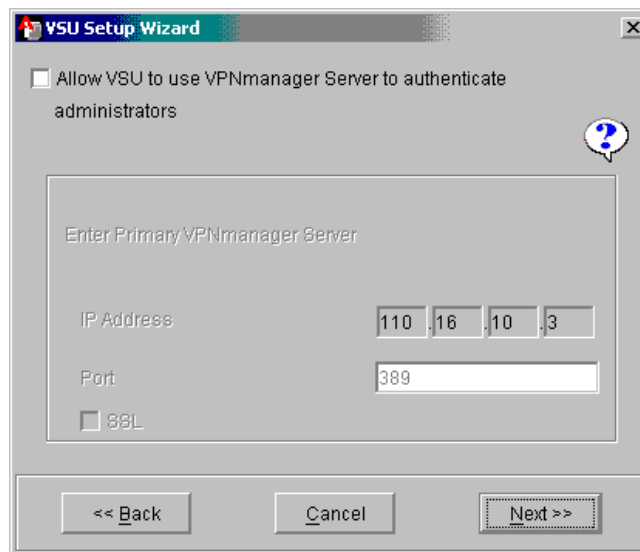


The screenshot shows the 'VSU Setup Wizard' dialog box. The title bar reads 'VSU Setup Wizard'. The main text says 'Enter the Public IP Address information for this device'. There are three radio buttons: 'Unknown', 'IP Address' (which is selected), and 'DNS Name'. Below 'IP Address', there are four input fields for the IP address: '66', '.166', '96', and '.130'. Below 'DNS Name' is an empty text box. In the lower section, there are two groups of input fields: 'Private IP Address' with fields '110', '.16', '10', and '.110'; and 'Private IP Mask' with fields '255', '.255', '255', and '0'. A checkbox labeled 'Use this address when directly communicating with this device' is checked. At the bottom, there are three buttons: '<< Back', 'Cancel', and 'Next >>'. A help icon (question mark in a circle) is in the top right corner.

Figure 12: VSU Setup Wizard – Address Information

From the **VSU Setup Wizard** popup depicted in **Figure 13**

- ❑ Click the **Next >>** button



The screenshot shows the 'VSU Setup Wizard' dialog box. The title bar reads 'VSU Setup Wizard'. The main text says 'Allow VSU to use VPNmanager Server to authenticate administrators'. There is an unchecked checkbox next to this text. Below this is a large empty text box labeled 'Enter Primary VPNmanager Server'. Underneath, there are two groups of input fields: 'IP Address' with fields '110', '.16', '10', and '.3'; and 'Port' with a text box containing '389'. There is also an unchecked checkbox labeled 'SSL'. At the bottom, there are three buttons: '<< Back', 'Cancel', and 'Next >>'. A help icon (question mark in a circle) is in the top right corner.

Figure 13: VSU Setup Wizard - Authentication

From the **VSU Setup Wizard** popup depicted in **Figure 14**

- Click the **Next >>** button

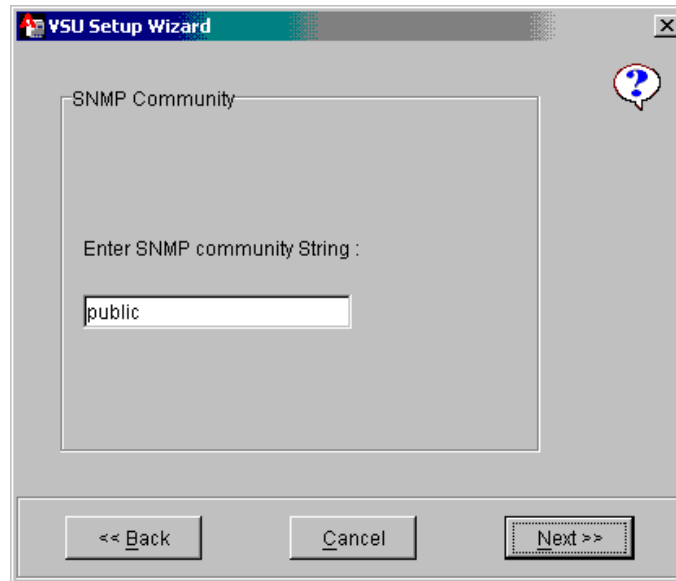


Figure 14: VSU Setup Wizard – SNMP Community

From the **VSU Setup Wizard** popup depicted in **Figure 15**

- Select **On** under **Listen/Learn Routes** in order to learn private RIPv2 routes
- Click the **Next >>** button

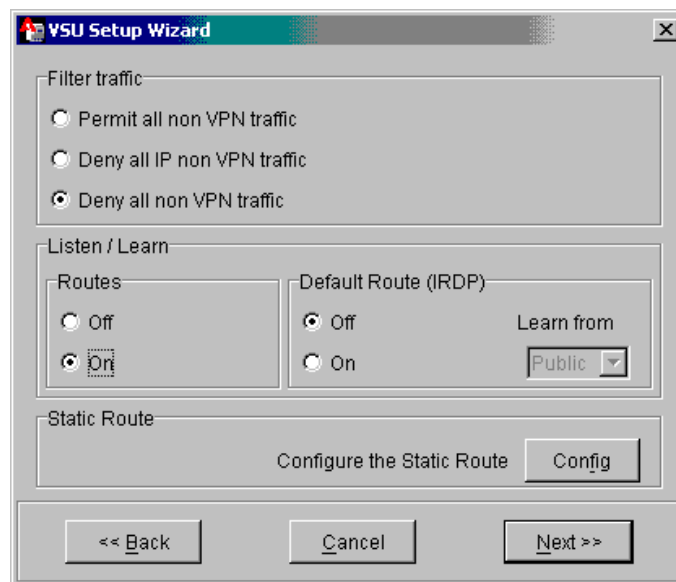


Figure 15: Modifying Filtering and Routing

From the **VSU Setup Wizard** popup depicted in **Figure 16**

- ❑ Select **Setup Now**
- ❑ Click the **Finished** button

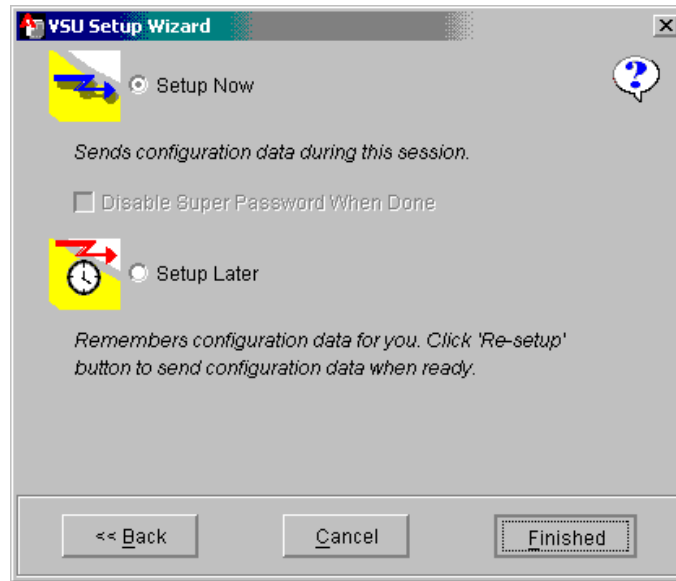


Figure 16: Setup Now

From the **VSU Setup Wizard** popup depicted in **Figure 17**

- ❑ Click the **Done** button

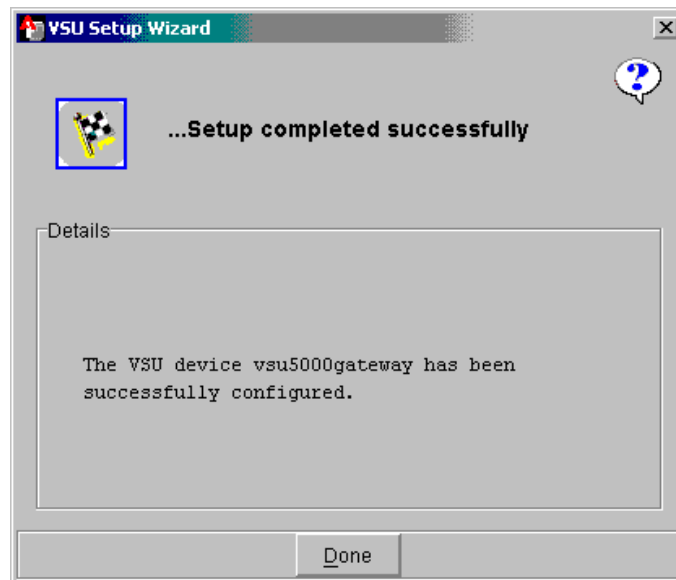


Figure 17: Setup Complete

6. Add an IP Group for the VSU 5000 (private networks to be protected)

From the **Configuration Console** window

- ❑ Select **Edit** → **New Object** → **IPGroup** from the pull-down menu
- ❑ In the **New IP Group** popup **Figure 18** enter Name **protectednetworks**
- ❑ Click the **A**pply button
- ❑ Click the **C**lose button

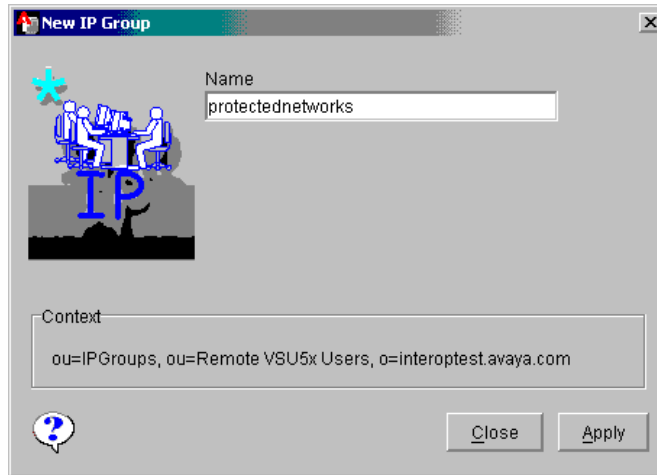


Figure 18: Add New IP Group

From the **Configuration Console** window under **Details - protectednetworks**

- ❑ Click the **A**dd... button under the **General** tab
- ❑ From the **Add IPGroup Members** popup depicted in **Figure 19**, enter
New IP Address 10.0.0.0
New IP Mask 255.255.255.0
- ❑ Click the **A**pply button

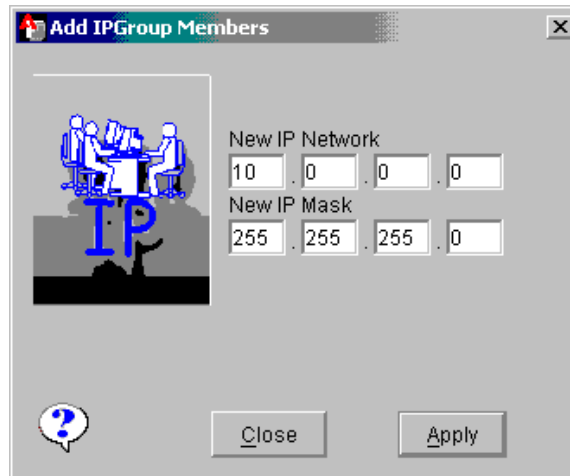


Figure 19: Add 10.0.0.0 Network

- ❑ From the **Add IPGroup Members** popup depicted in **Figure 20**, enter
 New IP Address **143.1.100.0**
 New IP Mask **255.255.255.0**
- ❑ Click the **A**pply button
- ❑ Click the **C**lose button

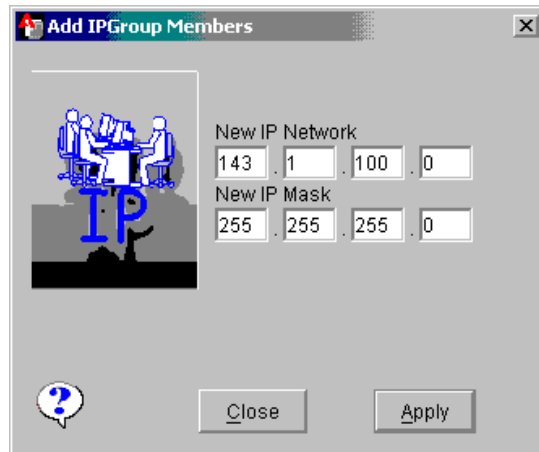


Figure 20: Add IP Group Members

In the **Details - protectednetworks** IP Group screen depicted in **Figure 21**

- ❑ Click on the **Associate this group with VSU** pull-down menu
- ❑ Select **vsu5000gateway** in place of *Extranet device*

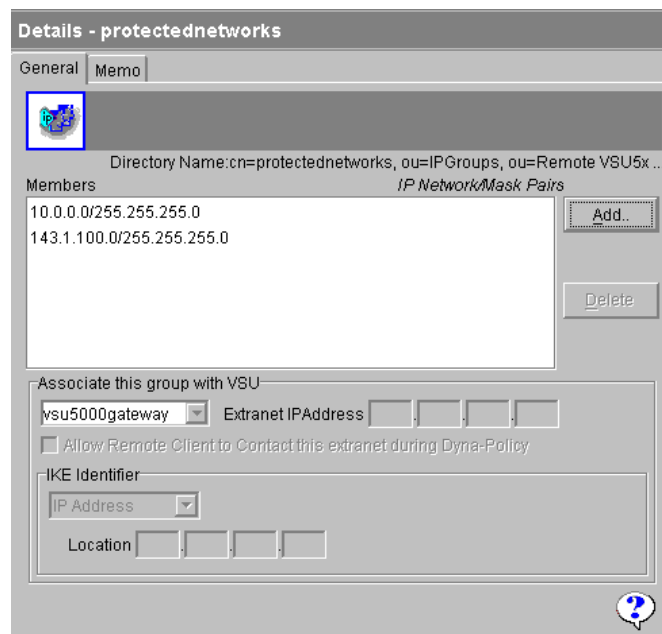


Figure 21: Details – protectednetworks

7. Add all required remote Users.

From the **Configuration Console** window

- ❑ Select **Edit → New Object → User** from the pull-down menu
- ❑ From the New User popup shown in **Figure 22** enter Name **ipphoneuser**
- ❑ Enter Password **password**, or other depending on security requirements
- ❑ Click the **Apply** button

Note: This user profile will be used to authenticate all IP Telephony devices specified in the VSU 5X gateways IP Device list. Remember this password because it must match the password that will be entered in the VSU 5X **VPN Proxy User** profile later on.

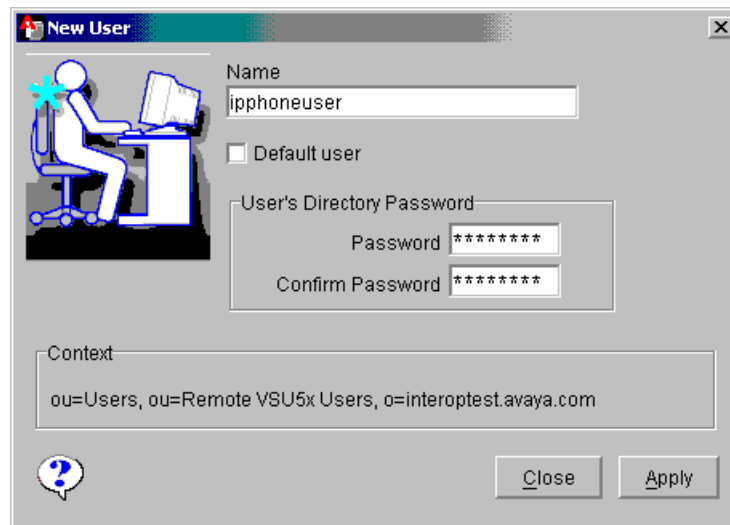


Figure 22: VPN Proxy User Profile

From the **New User** popup depicted in **Figure 23**

- ❑ Enter Name **workpc**
- ❑ Enter Password **password**, or other depending on security requirements
- ❑ Click the **Apply** button
- ❑ Click the **Close** button

Note: This user profile will be used to authenticate the secure Work PC attached behind the Avaya™ VSU 5X Gateway. The user must browse to the VSU 5x private IP address (<https://192.168.1.1> assigned by default) and login using this username and password. Remember this username because it must be added to the VSU 5X user profiles later on.

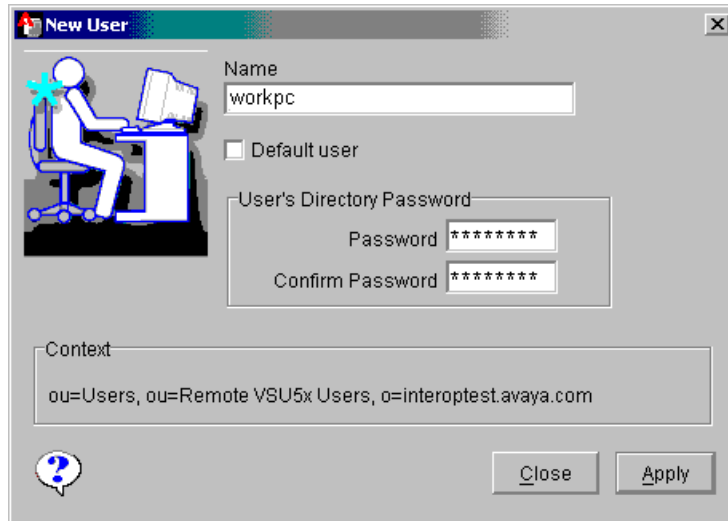


Figure 23: Work PC User Profile

8. Add a new User Group to the VSU 5000.

From the **Configuration Console** window

- ❑ Select **Edit** → **New Object** → **User Group** from the pull-down menu
- ❑ Enter the name **remoteSOHOvsu5X** in the New User Group popup **Figure 24**
- ❑ Click the **Apply** button
- ❑ Click the **Close** button
- ❑ From the **SOHOvsu5X** User Group select the **General** tab
- ❑ Select the **iphoneuser** and **workpc** Users from the *Available Users* column and click the **Move Left** button to move the selections to the *Current Users* column.

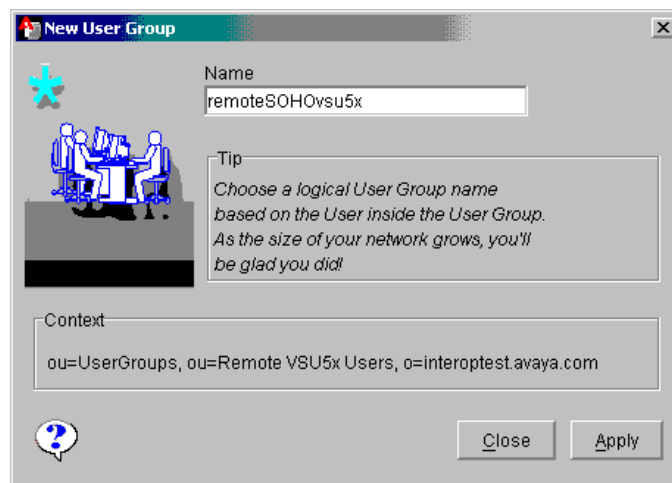


Figure 24: New User Group Popup

9. Add a new VPN to the VSU 5000.

From the **Configuration Console** window

- ❑ Select **Edit → New Object → VPN** from the pull-down menu
- ❑ From the **New VPN** popup **Figure 25**, enter
 - New VPN Name **remoteSOHOvsu5X**
 - VPN Type **IKE**
- ❑ Click the **Apply** button
- ❑ Click the **Close** button

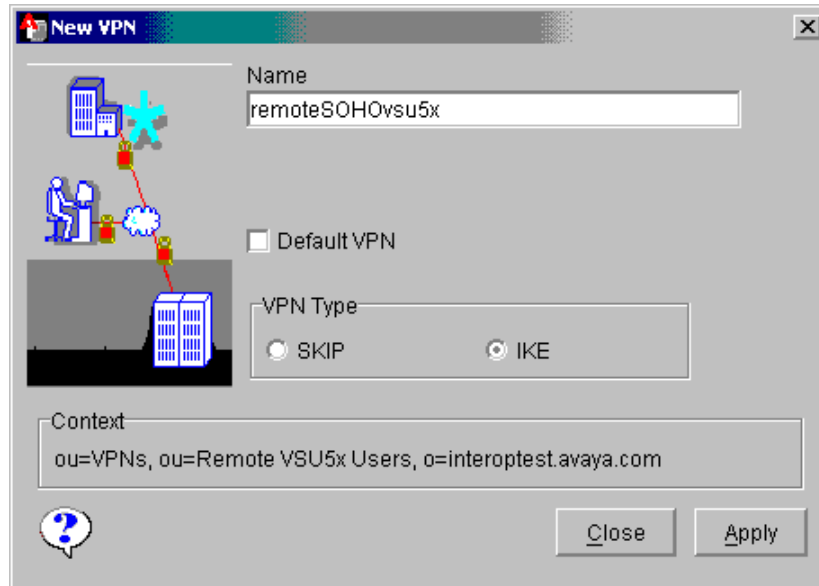


Figure 25: Adding a New VPN

From the **Configuration Console** window

- ❑ Click on the **General** tab under the **SOHOvsu5X** User Group
- ❑ Select **Preshared Secret**
- ❑ Select **Enable VPN**
- ❑ Click on the **Security (IPSec)** tab
- ❑ Select **No** from the **LZS** pull-down menu
- ❑ Click on the **Members – Users** tab
- ❑ Select the **remoteSOHOvsu5X** User Group from *Available* column and click on the **Move Left** button to move the selection to the *Current VPN Members* column
- ❑ Click on the **Members – IP Groups** tab
- ❑ Select the **protectednetworks** IP Group from *Available* column and click on the **Move Left** button to move the selection to the *Members* column

10. Save and Apply the changes to the VSU 5000 gateway.

From the Configuration Console window

- ❑ Click the **S**ave button (highlighted in yellow in the GUI not shown)
- ❑ Click the **U**ppdate VSUs (highlighted in yellow in the GUI not shown)
- ❑ Select the **vsu5000gateway** VSU and click the **O**k button
- ❑ Click the **C**lose button

11. Reboot to enable RIPv2 listening.

From the Configuration Console window

- ❑ Click the **VSU** object under the Objects list then click on the **vsu5000gateway** under the **C**ontents list.
- ❑ Click on the **A**ctions tab
- ❑ Click the **R**eboot Device button
- ❑ Select the **vsu5000gateway** VSU and click the **O**k button
- ❑ Click the **C**lose button

4.5. Configure a VSU 5X Gateway for use with a Cable Modem

These procedures assume that the Avaya™ VSU 5X Gateway has no pre-existing configuration.

1. Preparing to log into the VSU 5X gateway for the first time.

Using an available PC.

- ❑ Enable DHCP addressing under TCP/IP properties and attach the PC to an available private port on the VSU 5X gateway (ports 1-7)
- ❑ Open a web browser and enter the default URL **https://192.168.1.1**

Note: If the browser is currently configured to use a Proxy Server, disable this capability. Alternatively, add the VSU 5X gateways default IP address to the bypass local proxy address list.

2. Log into the VSU 5X for the first time.

From the **Welcome** screen depicted in **Figure 26**

- ❑ Enter the default **User Name**
- ❑ Enter the default **Password**
- ❑ Click the **Log In** button

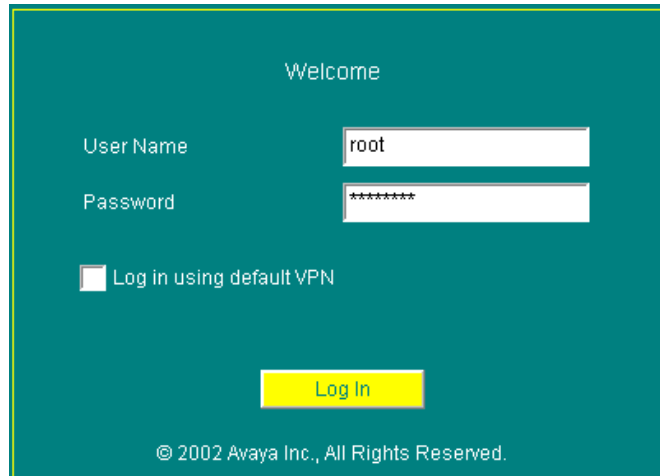


Figure 26: Welcome Login Screen

3. Confirm password change notification.

From the **VSU 5X Confirmation** popup depicted in **Figure 27**

- ❑ Click on the **Cancel** button.

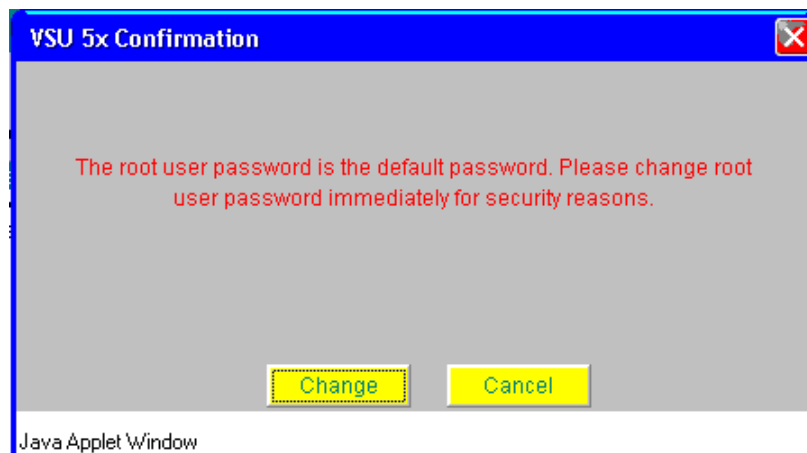


Figure 27: Password Change Confirmation

4. Use the quick setup wizard to setup VSU 5X.

From the **VSU Web Interface** page depicted in **Figure 28**

- ❑ Select **Quick Setup** link
- ❑ Click the **Next >** button

Note: If the cable modem being used requires a static address select Static Addressing and modify the IP address, subnet mask and gateway then click Next.

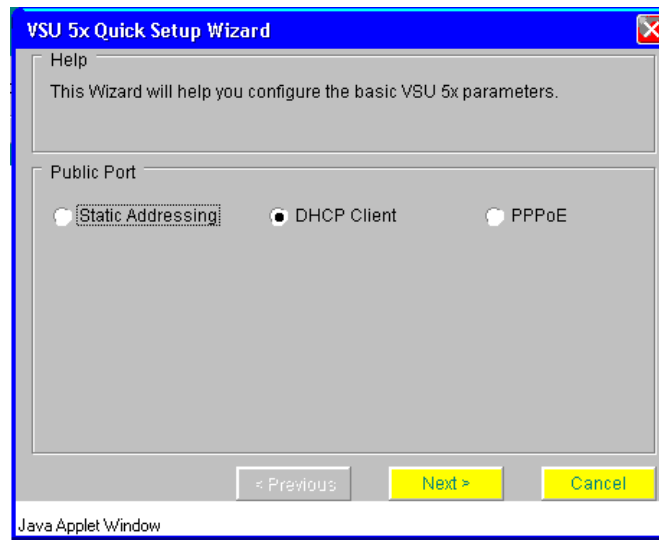


Figure 28: Quick Setup Wizard Popup

5. Setup the date and time information.

From the **VSU Quick Setup Wizard** popup depicted in **Figure 29**

- ❑ Modify VPNmanager User Name, Password and Confirm Password if necessary for centralized management.
- ❑ Modify the Date, Time and Time Zone if necessary.
- ❑ Click the **Finish** button

Note: The default Username and Password for VPNmanager centralized management may be changed for security purposes. These notes do not address this scheme.

VSU 5x Quick Setup Wizard

VPNmanager (for centralized management only)

User Name: superuser

Password: *****

Confirm Password: *****

Date & Time

Date: July 11 2002

Time: 11 10 55

Time Zone: Eastern Time(US & Canada)

< Previous Finish Cancel

Java Applet Window

Figure 29: Configuring Date and Time Information

6. Change the DHCP server IP address space.

From the **DHCP Server** page depicted in **Figure 30**

- ❑ Click on the **Configure** link
- ❑ Click on the **Network** tab
- ❑ Select **DHCP Server** properties
- ❑ Change the default IP Address to **192.168.2.1**
- ❑ Change the IP Address Range to **192.168.2.32** to **192.168.2.127**
- ❑ Click the **Save** button

The screenshot shows a web-based configuration interface for a DHCP server. It includes fields for IP Address (192.168.2.1), Network Mask (255.255.255.0), Domain Name (private), and IP Address Range (192.168.2.32 to 192.168.2.127). There are also buttons for Refresh, IP Devices, and Save.

Figure 30: DHCP Server Settings

7. Confirm changes to the DHCP server.

From the **VSU 5X Confirmation** popup depicted in **Figure 31**

- ❑ Click the **OK** button

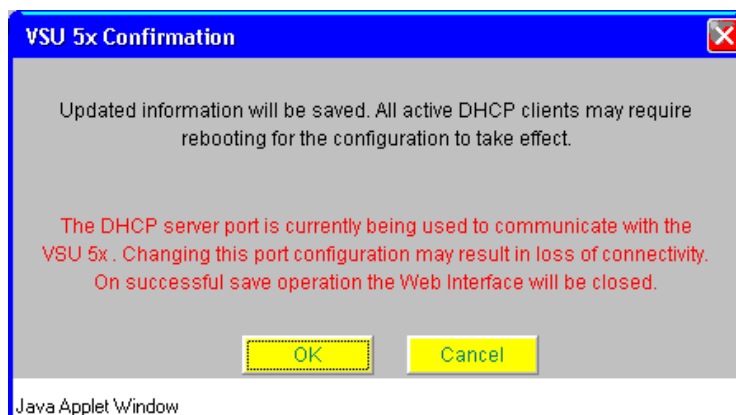


Figure 31: Confirming DHCP Modification

8. Get new IP address assignment from the VSU 5X.

From the **VSU 5X Web Interface** page depicted in **Figure 32**

- A message indicating that the DHCP server port has been changed appears

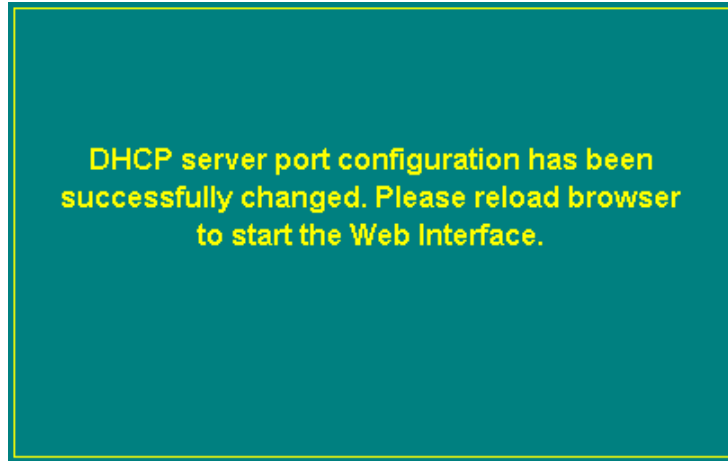


Figure 32: DHCP Server Port Change Notification

Note: The user must obtain a new IP address. Either issue an ipconfig/release then ipconfig/renew from the PC command or simply reboot the PC. For example:

```
C:\DOCUME~1\GKAMIN>ipconfig
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : private
    IP Address. . . . . : 192.168.1.34
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

C:\DOCUME~1\GKAMIN>ipconfig/release

C:\DOCUME~1\GKAMIN>ipconfig/renew
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : private
    IP Address. . . . . : 192.168.2.32
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.2.1
```

9. Log in using the new DHCP IP address.

Enter the URL **https://192.168.2.1** from a web browser to log into the VSU 5X using the newly updated DHCP server address. This may require proxy server disable or bypass.

- ❑ From the **Welcome** window enter the User Name **root**
- ❑ Enter the required Password for the root user
- ❑ Click the **Log In** button
- ❑ Click the **Cancel** button on the change default password notification popup.

10. Provision the VPN Proxy User for tunneling Avaya IP Telephone traffic.

From the **VSU Web Interface** page depicted in **Figure 33**

- ❑ Click on the **Configure** link
- ❑ Click on the **Users** tab
- ❑ Click the **VPN Proxy User** button

Note: The VPN Proxy User profile is used to authenticate any IP Telephony devices including Avaya™ IP Telephones, which have been added to the IP Devices list.

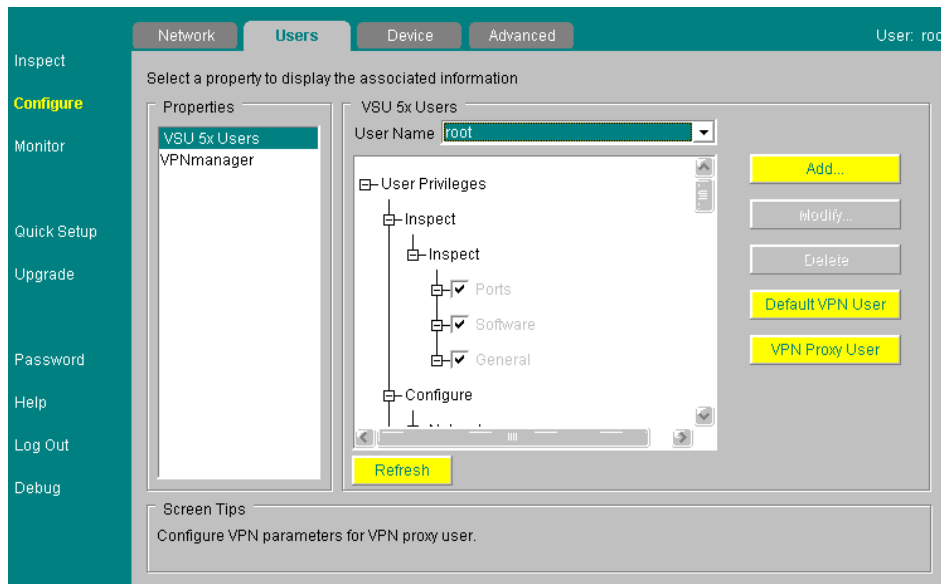


Figure 33: Configure the VPN Proxy User

11. Configure VPN Proxy User for VPN authentication.

From the **VPN Proxy User** popup depicted in **Figure 34**

- ❑ Select **Enable** under Enable/Disable VPN User
- ❑ Select **Change Password**
- ❑ Change the password and confirm fields to **password**
- ❑ Click **Next** button

Note: The password entered here must match the password chosen for the **ipphoneuser** user object provisioned on the VPNmanager® for the Avaya™ VSU 5000 gateway.

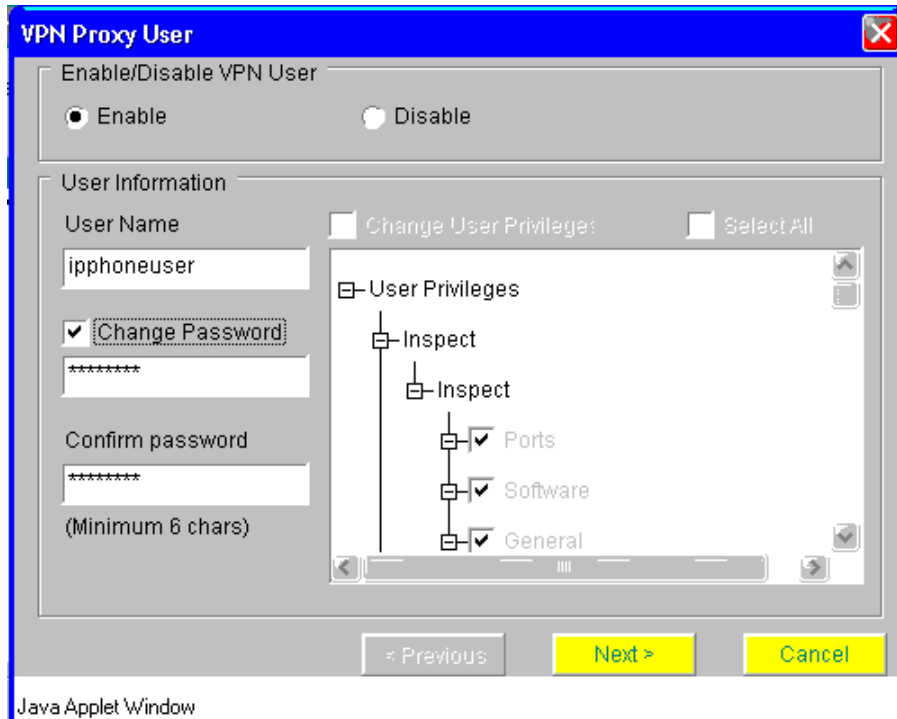


Figure 34: Enable the VPN Proxy User

12. Change the VSU Address for VPN Proxy User.

From the **VPN Proxy User** popup depicted in **Figure 35**

- Enter the VSU Address **66.166.96.130**
- Click **Finish** button

Note: The VSU Address must be the public IP address of the Avaya VSU 5000 Gateway at the main office. The Avaya VSU 5X Gateway will attempt to establish an IPsec tunnel with this address for all IP Telephony devices listed in the IP Devices list including Avaya IP Telephones.

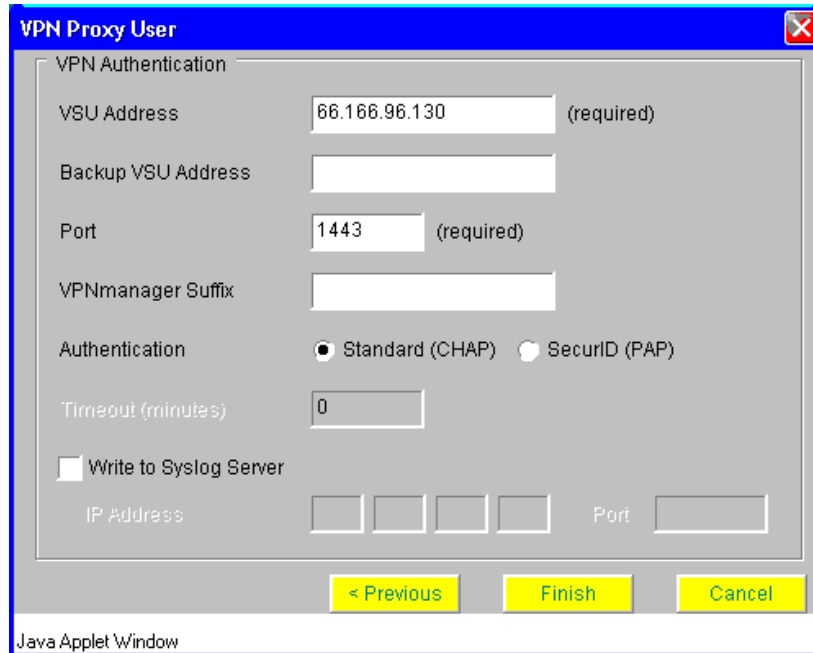


Figure 35: VPN Proxy User Authentication

13. Add a new VPN User for tunneling PC data traffic.

From the **VSU Web Interface** page depicted in **Figure 36**

- ❑ Click on the **Configure** link
- ❑ Click on the **Users** tab
- ❑ Click the **Add...** button

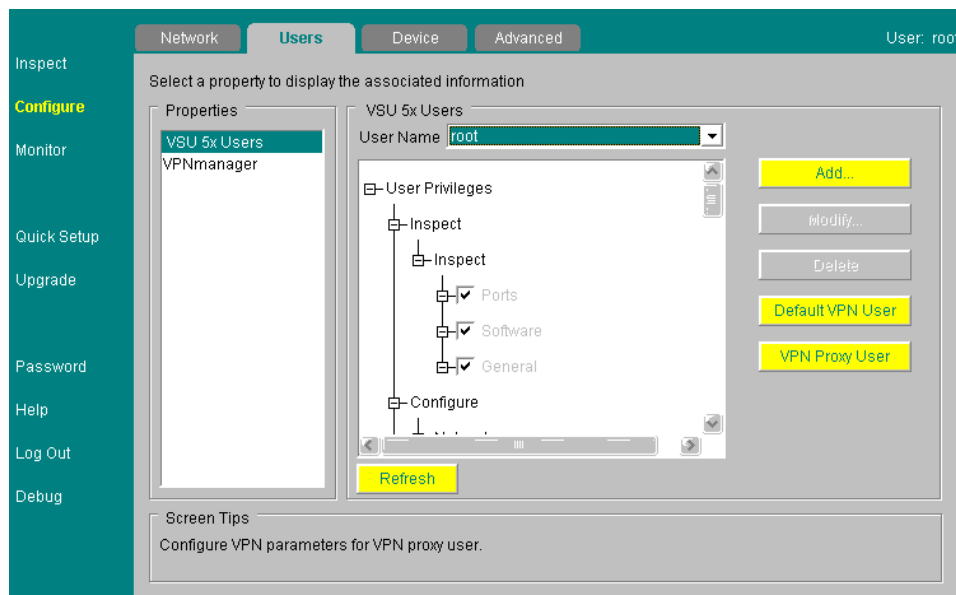


Figure 36: Add a New VPN User

14. Configure the new User for VPN authentication.

From the **Add VSU 5X User** popup as depicted in **Figure 37**

- ❑ Select **VPN Authentication** under Authentication Source
- ❑ Enter the User Name **workpc**
- ❑ Modify the **User Privileges Tree** for user **workpc** accordingly (See note)
- ❑ Click the **Next** button

Note: In this example, the User Name **workpc** was previously added to the VPN in the VPNmanager console. Since CCD will be used for registration, the VSU 5X does not need to supply a password because the user will be challenged for it at the time of tunnel registration by the VSU 5000 gateway. For security purposes it may be necessary to modify the User Privileges Tree for user **workpc** so that this user only has access to the monitoring features of the VSU 5X as opposed to complete administration control. For the purposes of these Application Notes, all privileges except Monitoring were disabled for this user.

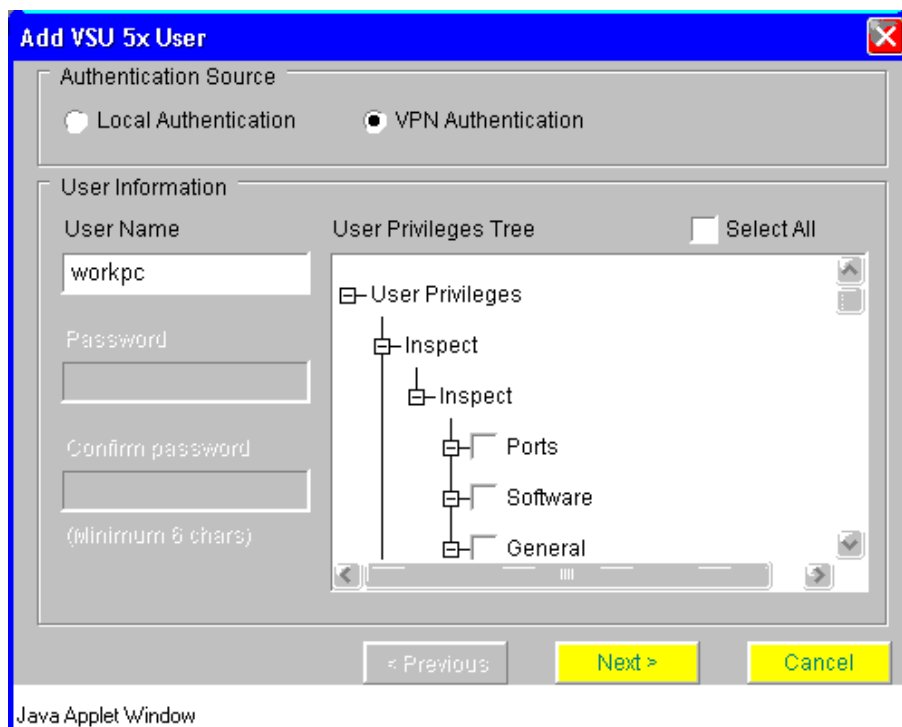


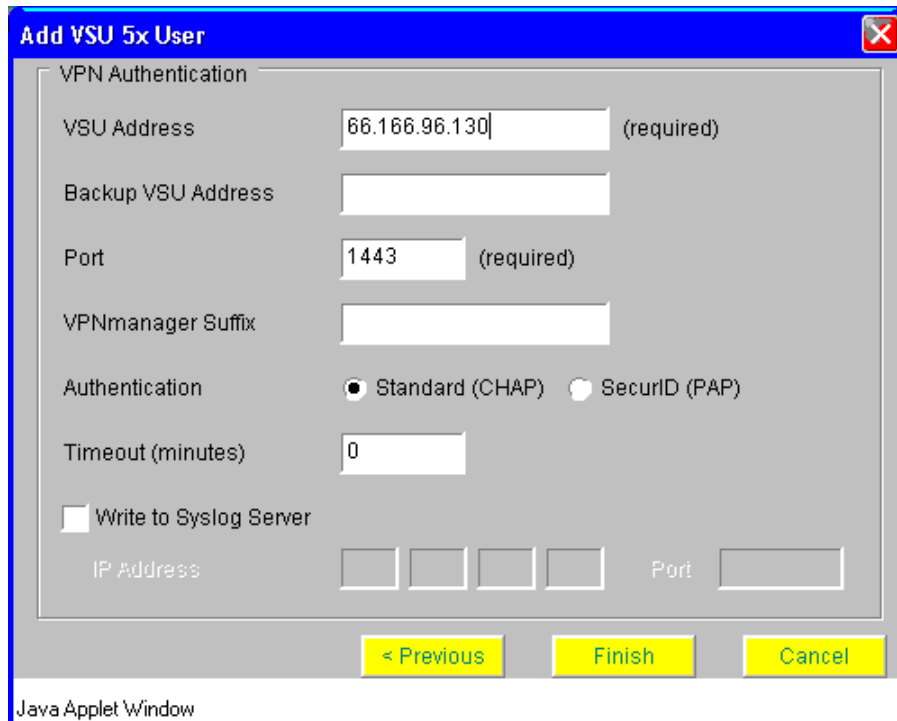
Figure 37: Adding a VSU 5X User

15. Change the VSU Address for authenticating the new User.

From the **Add VSU 5X User** popup depicted in **Figure 38**

- ❑ Enter the VSU Address **66.166.96.130**
- ❑ Click the **Finish** button

Note: The VSU Address is the public IP address of the Avaya™ VSU 5000 located at the main office. The user will login using a web browser to authenticate and establish a VPN tunnel for secure data traffic to this address.



The screenshot shows a Java Applet Window titled "Add VSU 5x User". The window contains a "VPN Authentication" section with the following fields and options:

- VSU Address: 66.166.96.130 (required)
- Backup VSU Address: (empty)
- Port: 1443 (required)
- VPNmanager Suffix: (empty)
- Authentication: Standard (CHAP) SecurID (PAP)
- Timeout (minutes): 0
- Write to Syslog Server
- IP Address: (four empty boxes) Port: (empty)

At the bottom of the window, there are three buttons: "< Previous", "Finish", and "Cancel". The window title bar includes a close button (X).

Figure 38: Adding a User – VPN Authentication

16. Add an Avaya 4624 IP Telephone to the IP Devices list.

From the **VSU Web Interface** page

- ❑ Click on the **Configure** link
- ❑ Click on the **Network** tab
- ❑ Select **DHCP Server** properties
- ❑ Click the **IP Devices** button
- ❑ Click the **Add** button and enter the information for the Avaya IP Telephone as depicted in **Figure 39**
- ❑ Click the **OK** button

Note: The Avaya™ VSU 5X gateway will allow for the administration of up to eight IP Devices (IP Telephones). The Avaya™ IP Telephone MAC address is located on a sticker on the underside of the device. The IP Device IP address must be within the usable DHCP server subnetwork of the VSU 5X; however, it is recommended that available addresses outside of the range to be assigned be used. In this example, the DHCP server assigns addresses from the range 192.168.2.32 through 192.168.2.127; therefore, the address 192.168.2.128 was chosen for this particular Avaya™ IP Telephone. When using Avaya™ IP Telephones, the TFTP Server IP and TFTP File Path are optional; however, the Definity Clan IP and Definity Clan Port fields are required. If the TFTP File Path is left blank, the root directory of the TFTP Server is assumed for IP Telephone firmware updates.

IP Device Configuration

IP Device MAC Address: 00 60 1d 24 6f 85

IP Device IP Address: 192 168 2 128

IP Telephony Configuration (optional)

TFTP Server IP: 10 0 0 11

TFTP File Path:

Definity Clan IP: 143 1 100 2

Definity Clan Port (0 - 65535): 1719

OK Cancel

Java Applet Window

Figure 39: Add an IP Telephone to the IP Devices List

17. Confirm the changes to the DHCP server.

From the **VSU 5X Confirmation** popup depicted in **Figure 40**

- ❑ Click the **OK** button

Note: At this point, the administrator should reboot all attached IP Telephones to ensure that the changes take effect.

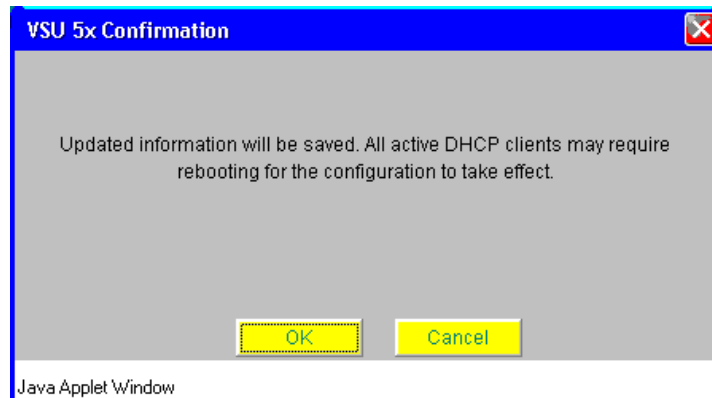


Figure 40: Confirming the DHCP IP Device Changes

5. Logging In Secure User PC's

Browse the DHCP server IP address of the Avaya™ VSU 5X gateway and log in using the credentials of the **workpc** user. In this case, the Work PC user would first browse to <https://192.168.2.1> (see **Figure 41**), then enter the User Name **workpc** and the Password **password**. Click the **Log In** button. See Section 7.1 for validation steps to ensure authentication and encryption.

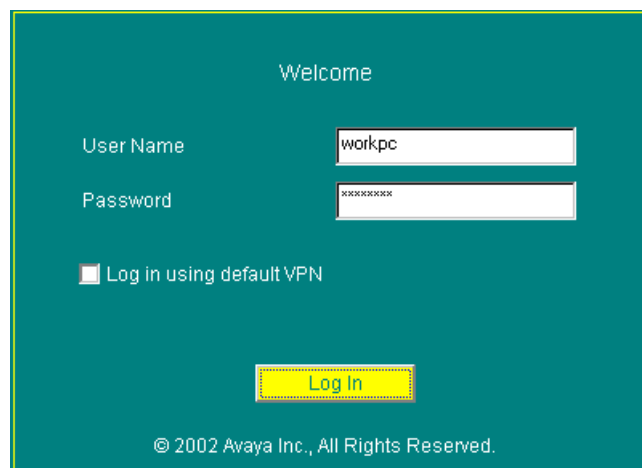


Figure 41: PC User Tunnel Authentication

6. Configuring IP Softphone

In order to ensure audio quality when using Avaya IP Softphone, the Avaya iClarity IP Audio Driver bandwidth setting must be configured correctly. In order to configure this parameter, navigate to **Audio** → **Options** from the main Avaya IP Softphone window. See **Figure 42** & **Figure 43**.

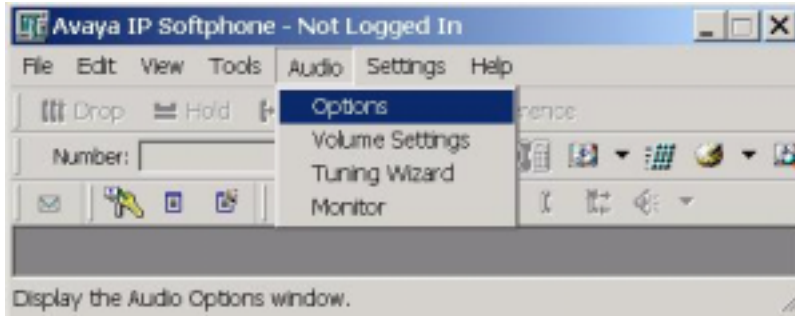


Figure 42: Configuring iClarity Audio



Figure 43: Audio Options Screen with Bandwidth Setting Pull-Down Menu

The bandwidth setting specifies how the PC connects to the server. The Avaya iClarity IP Audio uses the connection bandwidth setting to determine which codec to use. Avaya iClarity IP Audio has the following bandwidth settings²:

- **Cable connection**

For a cable connection, the following codecs may be used:

- G.729a (This codec is used for mid-speed connections.)
- G.723 (This codec is used for low-speed connections.)

- **xDSL connection**

For an xDSL connection, the following codecs may be used:

- G.729a (This codec is used for mid-speed connections.)
- G.723 (This codec is used for low-speed connections.)

- **ISDN connection**

For an ISDN connection, the following codecs may be used:

- G.729a (This codec is used for mid-speed connections.)
- G.723 (This codec is used for low-speed connections.)

- **Local Area Network (LAN) connection**

For a LAN connection, the following codecs may be used:

- G.711 u-law (CCITT u-law) (This codec is used for high-speed connections.)
- G.711 A-law (CCITT A-law) (This codec is used for high-speed connections.)
- G.729a (This codec is used for mid-speed connections.)
- G.723 (This codec is used for low-speed connections.)

- **28800 bps or better mode connection**

For a 28800 bps or better mode connection, the G.723 codec may be used. (This codec is used for low-speed connections.)

When SoftPhone connects to the Media Server running MultiVantage™ Software, Avaya™ iClarity IP Audio uses the bandwidth setting specified to select the appropriate codec that is compatible with the server configuration. For example, if the Cable, xDSL, or ISDN option is enabled for IP Softphone, then the corresponding ip-codec-set on the server must be administered to use G.729a, G.723 or either. The Avaya™ IP Softphone allows the end-user to choose between available codecs on a per call basis, so at a minimum one of these two codecs must be provisioned to successfully establish a call. Administrators should provision the MultiVantage Software to allow any of the available codecs permitted by the Avaya iClarity IP Audio connection bandwidth setting so that the user has the most flexibility for controlling call quality.

² Bullet lists taken from Avaya™ IP Softphone v3.2.3 help system.

7. Verification

7.1. Verifying That an Avaya™ IP Telephone is Authenticated

1. Plug in an Avaya™ IP Telephone that has been administered with the MultiVantage™ Software and has been administered as an IP Device for the Avaya VSU 5X Gateway.
2. Power up the Avaya IP Telephone.
3. Enter the extension number and security pass code.
4. Verify that the phone receives the current date and call appearance indication lamp. Check for dial tone. This may take a few moments.

7.2. Verifying That a PC (with Softphone) Has Been Authenticated

1. Establish a constant Ping to a protected network residing behind the VSU 5000 gateway at the main office. The ping should fail assuming that the main office IP addressing scheme is private.
2. Using a web browser and attached PC, log in a provisioned user such as the **workpc** profile created for the purposes of these notes.
3. Verify that Ping replies are received after successful log in. Also check encryption and SA statistics to verify that each echo request and echo reply is being encrypted.

8. Troubleshooting Tips

8.1. Typical Problems Encountered

A few common problems that have been encountered during validation of these notes have been included as a reference. This list does not encompass all possible problems, scenarios, causes or solutions.

Problem #1:	When the Avaya IP Telephone goes off hook there is no dial tone, but if it is hung up right away and taken back off hook dial tone occurs. The problem seems to be cyclical.
Likely Cause:	The Avaya Media Server platform is using two gateways, which are sharing the same ip-network-region, but only one of these gateways has connectivity to the VPN tunnel.
Solution:	Put the gateway for VPN users on its own ip-network-region.

Problem #2:	During login as a VPN user via the web browser a message occurs that the VSU 5x cannot connect to the VSU.
Likely Cause:	The Avaya VSU 5X Gateway cannot reach the main office VSU 5000 Gateways public IP address because of a problem with the WAN. This can be attributed to several factors including: <ul style="list-style-type: none"> • Physical connectivity problem • Service provider outage • Incorrect gateway address administered on the VSU 5X or VSU 5000
Solution:	Use the VSU 5X proxy ping utility to verify connectivity with the service provider. Attempt to ping the VSU series gateway at the main office location. If the ping to the main office VSU fails verify that the default gateway address is correct and use a tracing utility to troubleshoot where the connection fails. Troubleshoot the network.

Problem #3:	The Avaya IP Telephone is getting an IP address from the VSU 5X Gateway DHCP server but it doesn't seem to be getting the correct TFTP server address.
Likely Cause:	The IP Devices form on the VSU 5X was incorrectly administered and the phone is getting an address from the regular address pool. Use the key sequence Mute A-D-D-R # to determine what IP address the phone is using. If all of the information is correct go to Problem #5 solutions.
Solution:	Check that the correct MAC address for the phone is provisioned in the IP Devices form and that the correct TFTP server address is set.

Problem #4:	When the remote Avaya IP Telephone goes off hook heavily distorted dial tone is experienced. When a call is placed the voice path is also heavily distorted.
Likely Cause:	Check the broadband connection uplink and downlink speeds. The codec that was administered for the network-region may be using a packet size that is exceeding the broadband connections bandwidth capacity.
Solution:	There are two possible solutions: Solution 1 – Have the administrator change the codec type or modify the current codec setting via frames per packet and/or silence suppression settings to try and reduce the per call bandwidth utilization. Solution 2 – Request a faster or dedicated uplink or downlink connection from the service provider.

Problem #5:	The remote office Avaya IP Telephone is getting the correct option 176 information but it is not registering with the MultiVantage server.
Likely Cause:	This can be attributable to several factors including: <ul style="list-style-type: none"> • The station was not administered • The VPN is not active because authentication is failing
Solution:	Check that the station was administered in the server. Check that the VPN is active either from the VSU 5X monitoring utilities or from the VSU 5000 at the main office. If the VPN is down check that the VPN Proxy User name and password are identical on both the VSU 5X and with the VPNmanager®. Also check that the user object has been associated with the VPN properly and that the VPN was associated with the VSU 5000 gateway properly.

Problem #6:	The remote office Avaya IP Telephone is getting the correct custom option 176 parameters and the VPN tunnel seems to be established but the phone fails to connect with the TFTP server.
Likely Cause:	This is most likely a routing problem behind the VSU 5000 gateway or the TFTP service is not up.
Solution:	Add a route for the protected network behind the VSU 5X and make the private port of the VSU 5000 gateway the next hop address if necessary. Check that the TFTP service is running.

8.2. VSU 5000 console menu options for troubleshooting

The following console navigations are good tools for verifying and troubleshooting some configurations. These are not the only utilities available, but are frequently used.

Navigate: (3) Utilities → (1) Ping

Usage: Use the Ping utility to verify connectivity with the VPNmanager, protected private network interfaces and the WAN connection.

Troubleshooting Tip: If any of the Ping tests specified in the usage fail, check your cabling, IP addressing, subnet masks, gateways addresses and dynamic routing.

Navigate: (3) Utilities → (9) Network Tables → (2) Routing Table → (1) Show Routing Table

Usage: Verify that RIPv2 updates from protected routers are propagating to the VSU gateway.

Troubleshooting Tip: If internal routes are not being learned from Third Party Routing devices or Avaya™ MultiService switches be sure that the internal routing devices of choice are provisioned to send and receive RIPv2 routes.

Navigate: (3) Utilities → (19) IPSEC Utilities → (1) Display ISAKMP Security Associations

Usage: Verify phase 1 security associations.

Troubleshooting Tip: If phase 1 is failing, check end-to-end connectivity and Tunnel Endpoint addressing.

8.3. Flushing the VSU 5X Configuration

These following steps have been included for restoring the VSU 5X back to factory defaults. They can be used for scenarios where a previous configuration exists on the VSU 5X and the user would like to begin the configuration from the default state.

1. Click on the **Debug** link
2. From the VSU 5X Debug Operations pull-down menu select **Flush Configuration**
3. Click on the **Go** button
4. Confirm the Flush and click the **OK** button **Figure 44**
5. Once confirmed click the **Close** button **Figure 45**
6. Click on the **Configure** link
7. Click on the **Device** tab
8. Select the **Reboot** option
9. Click the **Reboot** button

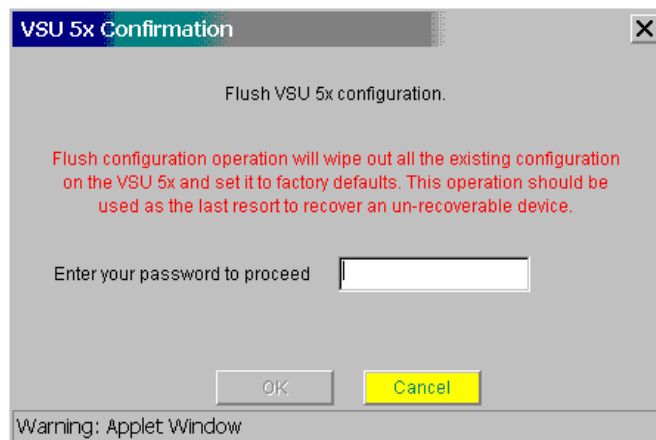


Figure 44: Confirm Configuration Flush

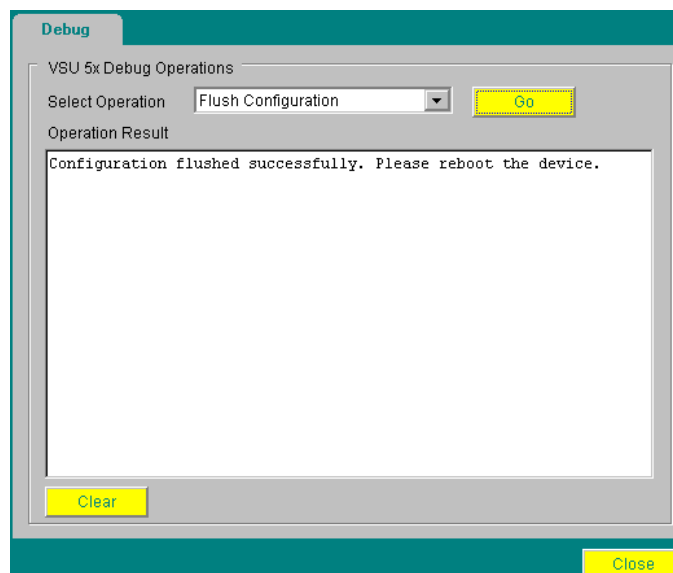


Figure 45: Flush Confirmed

9. Conclusion

These Application Notes provide the basic steps necessary to establish secure H.323 connectivity between an Avaya IP Telephone or IP Softphone and a main office Avaya MultiVantage™ Software platform using an Avaya VSU 5X gateway and cable modem. These Application Notes were validated both in a lab environment and at an actual residential cable modem connection. These notes serve to aid administrators wishing to equip remote office users with an Avaya VSU 5X gateway and Avaya IP Telephone or Softphone for work from home scenarios.

10. Additional References

1. VSU User's Guide: Covering the VSU 5 and 5X, July 2002
2. Administration for Network Connectivity for Avaya MultiVantage™ Software 1.1

The Avaya MultiVantage™ Administration Guide referenced can be downloaded from:
<http://support.avaya.com>

3. A Guide for Ensuring Service Quality In IP Voice Networks White Paper, June 2002
4. Avaya IP Voice Quality Network Requirements White Paper, Issue 2.0, August 2002
5. Voice Over IP Via Virtual Private Networks: An Overview White Paper, February 2001
6. Delivering High Performance VoIP Over A VPN White Paper, 2001
7. Quality of Service (QoS) considerations with 4600 Series IP Telephones White Paper, December 2000

The White Papers referenced throughout this document can be downloaded from:
<http://www.avaya.com/eclips>

© 2002 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