ViPNet VPN in Cisco Environment

Supplement to ViPNet Documentation

infotecs

Version: 00121-04 90 02 ENU

Global contacts page http://www.vipnet.com/

Contents

About This Document

This document is intended for the network administrators intending to deploy and configure Cisco IP telephony systems within ViPNet VPN virtual private networks in their organizations.

You don't have to be an IT professional to read and understand this document. However, you should have a general idea of computer networks, IP protocols, firewalls, tunneling, and cryptography.

Advantages of Deploying a ViPNet Network

To protect your corporate Cisco VoIP traffic, you may deploy a ViPNet virtual private network in your organization. The ViPNet technology not only provides traffic protection, but also cuts down the number of settings required to establish connection with remote Cisco users, branch offices and partners, as well as makes the corporate network configuration process easier.

The advantages of deploying and configuring a ViPNet network are as follows:

- When VoIP (Internet telephony) connections' traffic is transferred within an external network, it is encrypted.
- Within a corporate network, VoIP traffic can be either encrypted or unencrypted, up to your choice.
- PSTN (public switched telephone network) users can easily communicate with VoIP users, both with those located in the office and those who work remotely.

Note: Keep in mind that we don't guarantee the privacy of PSTN-to-VoIP and VoIP-to-PSTN connections in case a remote VoIP user works on an unprotected host (without the ViPNet software).

- Remote VoIP users connecting to the Internet from various access points may create several configurations in ViPNet Monitor, one for each connection. Then, they would be able to make calls using Cisco IP Communicator (CIPC) simply by selecting the desired configuration in ViPNet Monitor, without changing settings.
- Due to virtual IP addresses usage, whenever a remote user changes location, his or her visibility address remains the same. That is why changing settings in Cisco CallManager is not required.
- Virtual IP addresses usage prevents conflicts of IP addresses between different local networks where IP telephony is used.
- Encapsulation of any encrypted traffic into a single UDP format makes configuration of firewalls much easier.

This chapter gives an example of network topology for protected Cisco IP telephony.

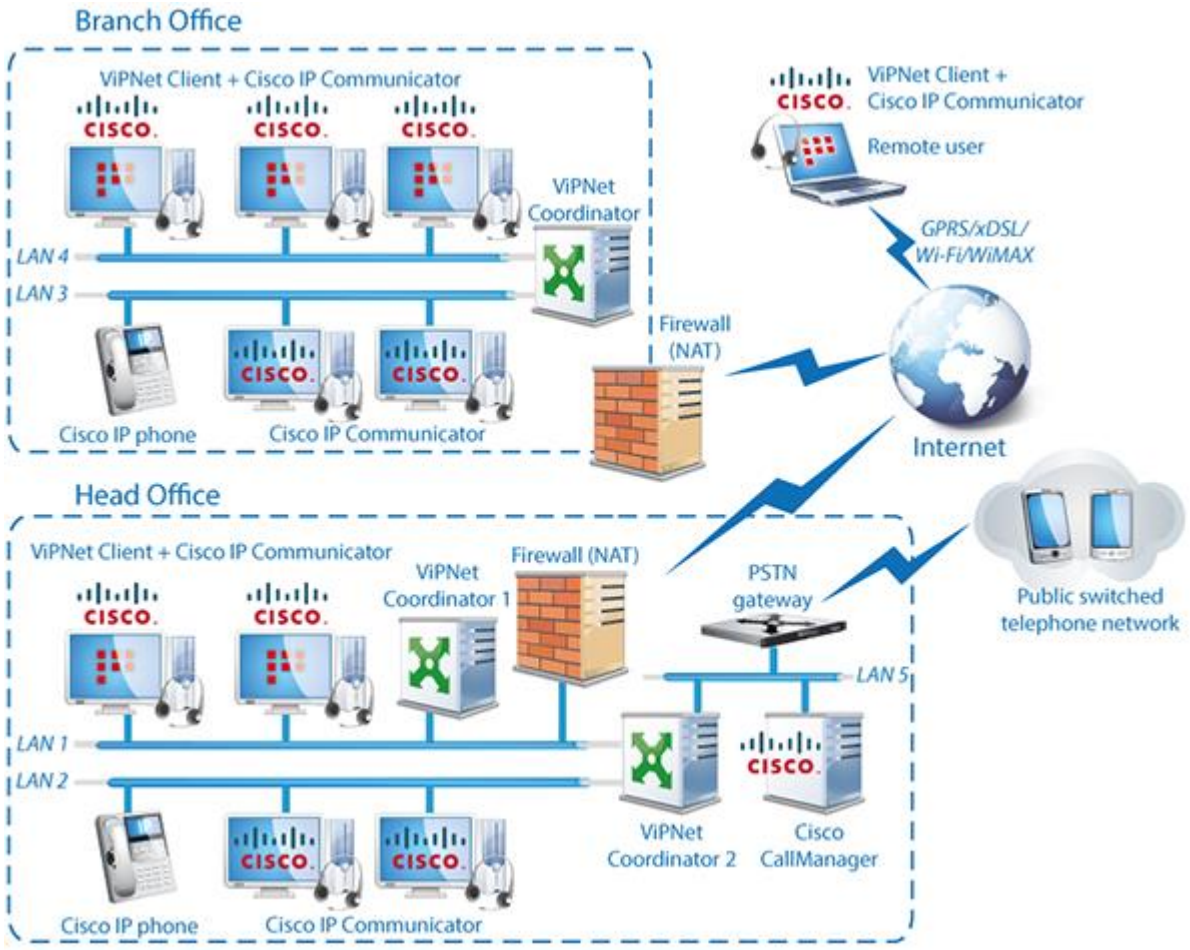

Figure 1. ViPNet software protecting Cisco VoIP traffic

Suppose there are two offices in an organization: head and branch. Let's assume, there are a head and a branch office in your company. Their networks include both:

- ViPNet hosts with Cisco software, which are computers with ViPNet Client and Cisco IP Communicator installed. Hereinafter, we shall call them 'ViPNet hosts'.
- Unprotected hosts, which are computers with Cisco IP Communicator installed, but without ViPNet Client, as well as Cisco IP hardphones, and a server with Cisco CallManager installed. Hereinafter, we shall call them 'tunneled hosts'.

Warning: To enhance network security, we strongly recommend you to place tunneled hosts in a separate network segment from ViPNet hosts.

If you don't have such an opportunity, you should make some additional settings (see If Both ViPNet and Tunneled Hosts Are in the Same Network Segment on page 10) to protect traffic within your LAN.

Remote users (with laptops where ViPNet Client and Cisco IP Communicator are installed) connect to the ViPNet network over the Internet.

The head office LAN is connected to a public switched telephone network (PSTN) via a PSTN gateway.

The PSTN gateway and Cisco CallManager are located in a separate segment of the head office network (LAN_5 on the scheme).

Network Structure Requirements

The following requirements should be met to provide protection of VoIP traffic in a Cisco IP telephony environment:

1 In every office, on the edge of the network, a coordinator should be installed and configured to tunnel the Cisco CallManager server, the PSTN gateway, and all Cisco IP hardphones. Moreover:

- The PSTN gateway, Cisco IP hardphones, and hosts which have Cisco IP Communicator installed but don't have ViPNet Client should be tunneled with the coordinator of their office.
- The Cisco CallManager server should be placed behind another coordinator — Coordinator 2 in the scheme (see. figure 1 on page 5) — and have a unique IP address.

Note: If there are several Cisco CallManager servers in your organization, each serving a separate user group, ask Infotecs technical support for recommendations on configuring the network.

---

2 All hosts with Cisco IP Communicator installed either have the ViPNet Client software installed as well or are tunneled by the coordinator of their office (according to paragraph **1**).

3 All remote hosts with Cisco IP Communicator installed have the ViPNet Client software installed as well.

Guidelines

We recommend you to follow these steps to install and configure the ViPNet software in each office:

1 Install and configure the ViPNet Coordinator software to tunnel unprotected hosts participating in IP telephony (see Configuring Coordinators on page 7).

Note: For the ViPNet Coordinator setup workflow, see “ViPNet VPN. User's Guide,” Chapter 2, “Installing ViPNet Coordinator on ViPNet Network Servers.”

---

2 Install and configure the ViPNet Client software on hosts with installed Cisco IP Communicator (see Configuring Clients on page 9). If installing ViPNet Client on some hosts is undesirable or impossible, these hosts should be tunneled according to paragraph **3** of this section.

Note: For the ViPNet Client setup workflow, see "ViPNet VPN. User's Guide", Chapter 2, "Installing ViPNet Client on ViPNet Users' Computers."

To configure the ViPNet Client software, log on as an administrator.

3 Configure all tunneled hosts participating in IP telephony (see Configuring Tunneled Hosts on page 10). You should not install ViPNet software on tunneled hosts.

4 Install and configure the ViPNet Client software on remote hosts with installed Cisco IP Communicator (see Configuring Remote Clients on page 13).

5 Make test calls from clients in the office, tunneled hosts, and remote hosts (see Making Test Calls on page 14).

Configuring Coordinators

To configure a coordinator:

1 In ViPNet Network Manager, set coordinator access parameters (see the document "ViPNet VPN. User's Guide", Chapter 5, "Configuring Coordinators").

2 In ViPNet Network Manager, specify IP addresses of the unprotected hosts, participating in IP telephony, as tunneled (see the document "ViPNet VPN. User's Guide", Chapter 5, "Tunneling").

3 On the firewall placed on the edge of LAN, configure traffic routing rules.

4 On the coordinator, make the following network settings:

- If the coordinator connects to the Internet via a firewall, set the firewall access parameters (see the document "ViPNet VPN. User's Guide", Chapter 5, "Firewall (for Coordinators)").
- If the coordinator has a network interface directly connected to the Internet, set your Internet service provider's gateway as default for this interface. For other networks the coordinator is connected to, set static routes that forward IP traffic for these networks to corresponding gateways.

5 In ViPNet Coordinator Monitor, on coordinator 2 (see. figure 1 on page 5) of the head office, configure a forward filter for tunneled hosts behind different network interfaces. To do this:

Note: In our example (see. figure 1 on page 5), you should configure a forward filter to connect the LAN_2 subnetwork where unprotected hosts with Cisco IP Communicator and Cisco IP hardphones are placed to the LAN_5 subnetwork where the Cisco CallManager server and PSTN gateway are placed.

- In the main ViPNet Monitor window, in the navigation pane, select **Network Filters** > **Forward Public Network Filters**.
- Click **Create**.

- In the displayed forward filter's properties window, in the **General Options** section, specify the filter name and the action it implies: allow traffic.
- In the **Sources** section, click **Add** and select **IP address or IP addresses range**.

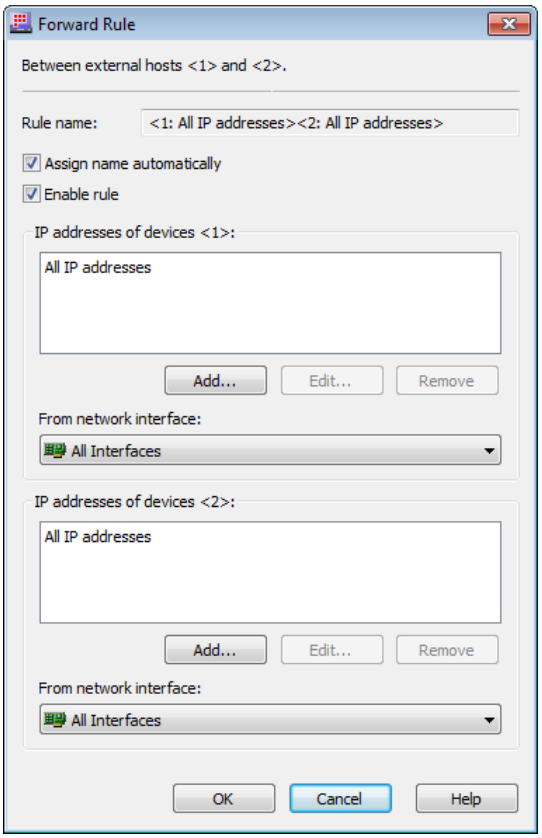

Figure 2. Configuring a forward filter

- In the **IP Address** window, choose **IP addresses range** and specify the starting and the ending addresses from the range of IP addresses belonging to tunneled hosts of the LAN 2 subnetwork. Click **OK**.
- In the **Destination** section, specify the IP addresses belonging to tunneled hosts of the LAN 5 subnetwork (the Cisco CallManager server and the PSTN gateway).

6 If IP addresses of the same subnetwork are used in the network segments of both head and branch offices, to avoid a conflict of IP addresses, for each coordinator in the hosts list, in ViPNet Coordinator Monitor, do the following:

- In the **Private Network** section, double-click one of the coordinators. The **ViPNet Host Properties** dialog box will be displayed.
- Click the **Tunnel** tab and select the **Use virtual IP addresses** check box (cleared by default).

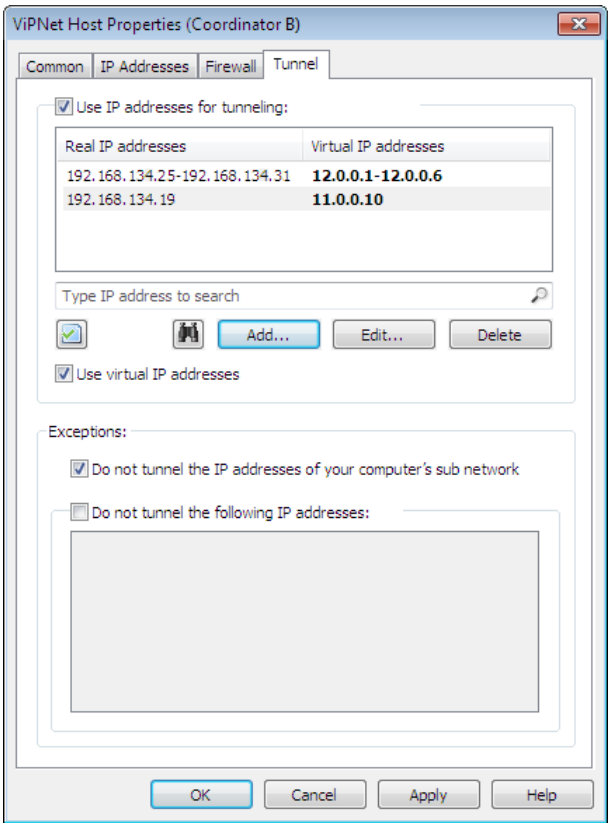

Figure 3. Using virtual IP addresses

Configuring Clients

On each client located in the head or branch office:

1. Log on to ViPNet Client Monitor as an administrator.
2. To avoid a conflict of IP addresses, for each coordinator, in the **Private Network** section, make the following settings:
   - In the **Private Network** section, double-click one of the coordinators. The **ViPNet Host Properties** dialog box will be displayed.
   - Click the **Tunnel** (see. figure 3 on page 9) tab and select the **Use virtual IP addresses** check box (cleared by default).

Configuring Tunneled Hosts

Warning: To enhance network security, we strongly recommend you to place tunneled hosts in a separate network segment from ViPNet hosts.

If you don't have such an opportunity, you should make some additional settings (see If Both ViPNet and Tunneled Hosts Are in the Same Network Segment on page 10) to protect traffic within your LAN.

To configure tunneled hosts:

1. In both offices' networks, on each tunneled host (except for the Cisco CallManager server and the PSTN gateway), specify the default gateway address. It must be an IP address of a coordinator located in the same network segment. If you can't use this coordinator as the default gateway, see step **2**.

   Note: Tunneled hosts within the same subnetwork exchange traffic directly, without using a coordinator.

2. In the head office, configure the subnetwork with the Cisco CallManager server and the PSTN gateway.

   You can't set a coordinator as the default gateway for the Cisco CallManager server, as the PSTN gateway should be its default gateway for access to a public switched telephone network.

   To solve this problem, on the Cisco CallManager server, set a static route to have all traffic exchange between Cisco CallManager and the head office network directed through the coordinator.

If Both ViPNet and Tunneled Hosts Are in the Same Network Segment

By default, clients connect to tunneled hosts located in the same network segment directly. To ensure control over access to tunneled hosts, you can configure clients to connect to tunneled hosts through a coordinator. To do this:

1. On each client in the same network segment, in ViPNet Monitor:
   - In the navigation pane, click **Private Network**.
   - In the **Private Network** section, double-click the tunneling coordinator of this subnetwork. The **ViPNet Host Properties** dialog box will be displayed.
   - On the **Tunnel** tab, under **Exceptions**, clear the **Do not tunnel the IP addresses of your computer's sub network** check box (selected by default).

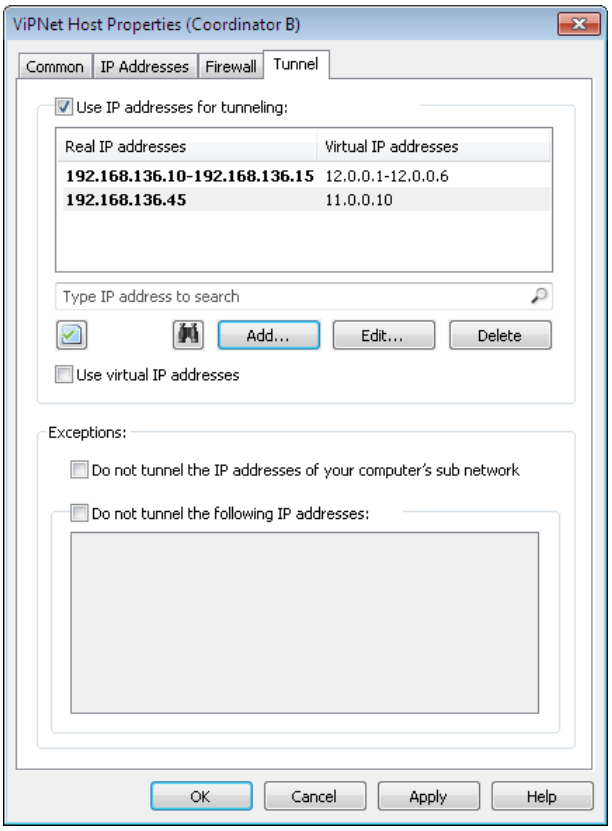

Figure 4. Configuring a network segment with ViPNet hosts and tunneled hosts

- If you need the traffic pass directly between a client and a tunneled host:
  - Under **Exceptions**, select the **Do not tunnel the following IP addresses** check box.

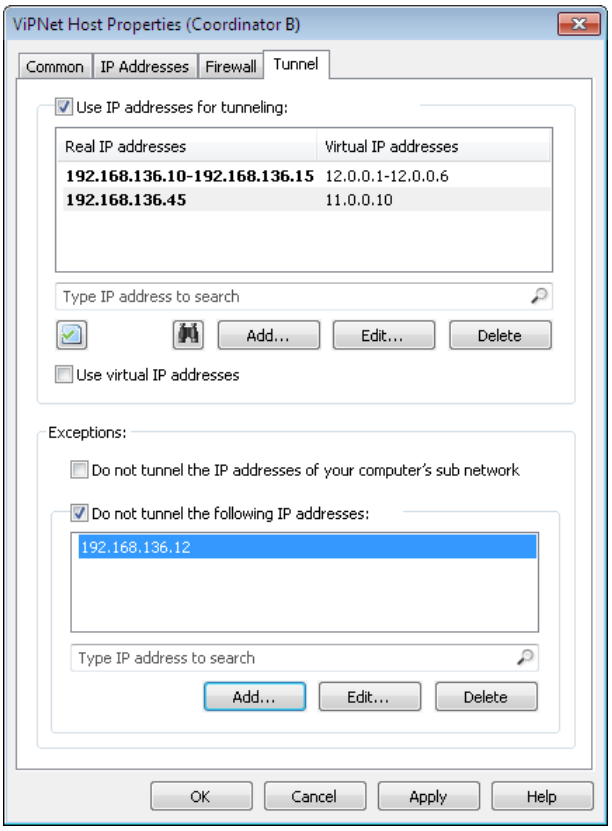

Figure 5. Specifying addresses that should not be tunneled

- Click **Add**. The **Add IP address or range** window will be displayed.

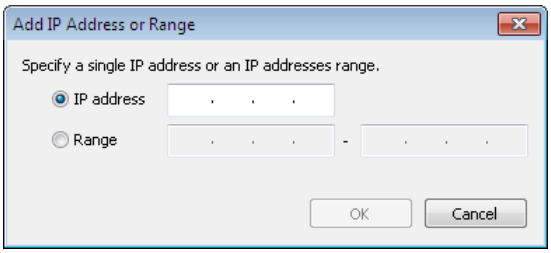

Figure 6. Specifying an IP address

- In the **Add IP address or range** window, select **Range** and specify the starting and ending IP addresses from the range of addresses that should not be tunneled. Click **OK**.

o Click **OK**.

2 On each tunneled host, set a static route to have all traffic exchange between this host and clients directed through the coordinator.

3 On each client, configure a static route to have all traffic exchange between this client and tunneled hosts directed through the coordinator.

Configuring Remote Clients

In this scenario, remote users may work on a desktop computer or a laptop.

Configuring a Remote User's Laptop

Suppose that a remote user with a laptop connects to the Internet from different locations, using different connection types. To avoid reconfiguring of the ViPNet software every time the user connects to the ViPNet network, we recommend you to create several configurations in ViPNet Monitor for different connection types. Then, to access the ViPNet network, it will take only choosing one of the configurations.

To create a new configuration:

1 Log on to ViPNet Client Monitor as an administrator.

2 In the main ViPNet Monitor window, in the navigation pane, right-click **Configurations** and, on the context menu, click **Create a New Configuration**.

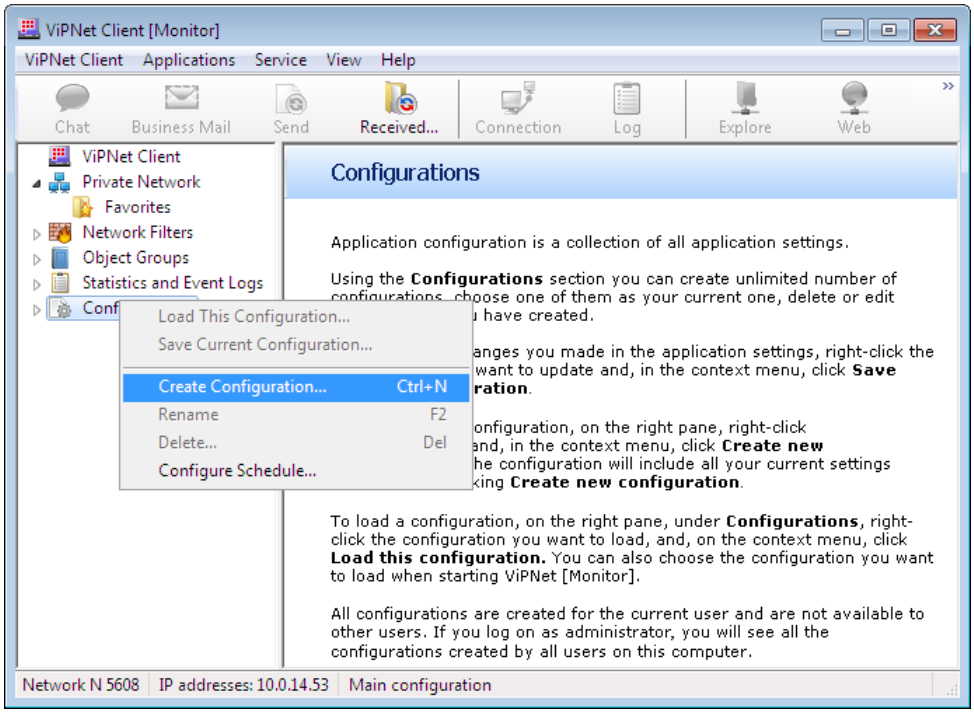

Figure 7. Creating a new configuration

A "New configuration" element will be displayed in the configurations list. The current program settings will be automatically saved to the new configuration.

3 We recommend you to rename the configuration for easier search. To do this, select the configuration and press **F2** or right-click it and, on the context menu, click **Rename**.

4 To save the configuration, in the navigation pane, right-click **Configurations** and, on the context menu, click **Save Current Configuration**.

We recommend you to create and save the following configurations (to do this, log on as an administrator):

- In one of the configurations, save the settings to work in the office local network. These settings should be the same as the settings on clients on that network (see Configuring Clients on page 9).
- In another configuration, save the settings to connect to your ViPNet network over the Internet when you work out of the office.

To avoid a conflict of IP addresses, in any configuration:

1 In the navigation pane of the main ViPNet Client Monitor window, select **Private Network**.

2 In the **Private Network** section, double-click your coordinator. The **ViPNet Host Properties** dialog box will be displayed.

3 In the **ViPNet Host Properties** dialog box, on the **Tunnel** (see. figure 3 on page 9) tab, select the **Use virtual IP addresses** check box (cleared by default).

Configuring a Remote User's Desktop Computer

Suppose that a remote user with a stationary desktop computer connects to the ViPNet network over the Internet and does not change his or her location. To configure a desktop computer (in other words, a stationary ViPNet host):

1 Log on to ViPNet Client Monitor as an administrator.

2 To avoid a conflict of IP addresses:

   - In the navigation pane of the main ViPNet Client Monitor window, select **Private Network**.
   - In the **Private Network** section, double-click your coordinator. The **ViPNet Host Properties** dialog box will be displayed.
   - In the **ViPNet Host Properties** dialog box, on the **Tunnel** (see. figure 3 on page 9) tab, select the **Use virtual IP addresses** check box (cleared by default).

Making Test Calls

After deploying a corporate ViPNet network and configuring all coordinators, clients and tunneled hosts, make sure that Cisco IP telephony is operable. To do this:

1 Make sure that Cisco hardware and software is set up properly.

2. Check connection between clients and their coordinators, as well as connection between different coordinators.
3. If connection is not established, make sure that access IP addresses of all ViPNet hosts are specified correctly and all hosts have correct connection type settings.
4. Use the ping command to make sure that tunneled hosts are accessible from clients and tunneled hosts located in the other office.

   If you can't connect to tunneled hosts, make sure that tunneling has been configured correctly on coordinators and that tunneled hosts have proper gateways and static routes set.
5. Make test calls from clients in the office, tunneled hosts and remote hosts.

   If all the settings have been made correctly, your corporate Cisco IP telephony system is ready to use.