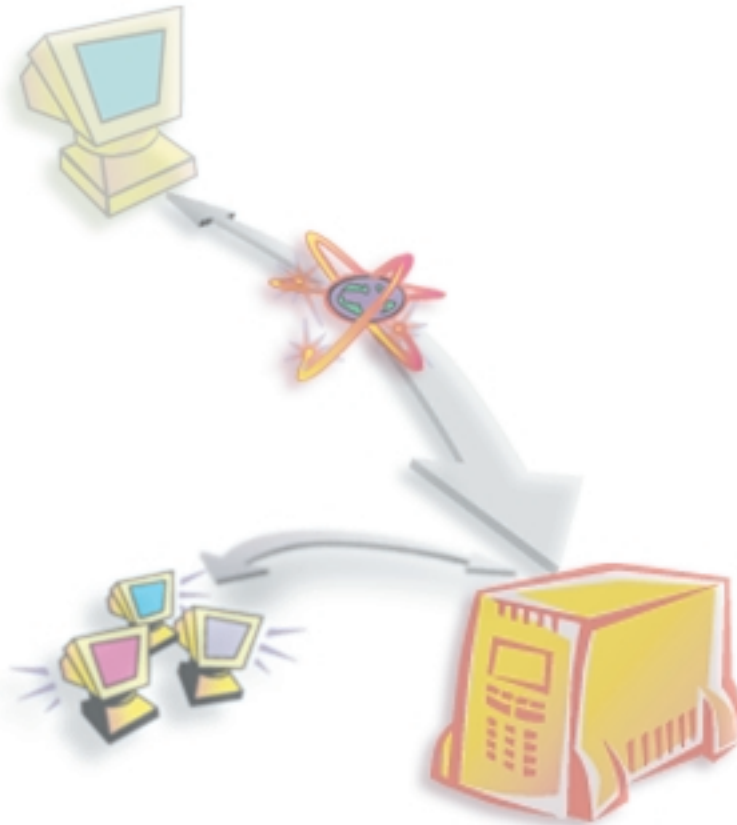


Secure Remote Access

Configuration and User's Guide



Requires a service contract that includes the Secure Remote Access feature

Secure Remote Access

Configuration and User's Guide

Requires a service contract that includes the Secure Remote Access feature



110 Marsh Drive
Foster City, CA 94404
U.S.A.

First Edition (July 2000)

Copyright ©2000 Whistle Communications, an IBM Company. All rights reserved.

Under the copyright laws, neither the documentation nor the software may be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form, in whole or in part, except in the manner described in the documentation.

Note to U.S. Government Users Restricted Rights—Use, duplication, or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Table of Contents

Important Notices v

About This Guide

What This Guide Contains vii

Typographical Conventions Used in This Guideviii

Icons Used in This Guide ix

Obtaining Assistance ix

How To Send Comments About This Guide x

Chapter 1. Introducing Secure Remote Access

How Secure Remote Access Works 1-1

Encryption 1-2

Requirements 1-3

Tunneling Protocol Support 1-3

Network Protocol Support 1-3

Network Server Support 1-4

Chapter 2. Configuring the InterJet for Secure Remote Access

Configure the Secure Remote Access feature. 2-1

Specify who can use Secure Remote Access. 2-4

Specify when Secure Remote Access is available. 2-6

Option: Turn on remote dial-back. 2-7

Determine the InterJet VPN server name. 2-9

For networks running Windows NT Server:

Ensure that the InterJet configuration includes NT Server settings. 2-11

Next steps 2-12

Chapter 3. Setting Up Your Remote Computer for Secure Remote Access

Before you begin 3-1

Windows 95, 98, 2000, or NT users only: Ensure that you can access network resources. 3-3

Preventing computer name conflicts. 3-4

Using Network Neighborhood/My Network Places. 3-4

Changing your computer's name or workgroup. 3-4

Windows 95 or 98. 3-4

Windows 2000. 3-6

Windows NT 3-7

Configure a PPTP client program on your remote computer. 3-8

Configuring the Microsoft VPN Adapter for Windows 95 or 98 3-10

Verifying that the Microsoft VPN Adapter is installed on your computer. 3-10

Creating a new VPN connection 3-11

Verifying that network components are installed on your computer.. . . . 3-14

Configuring the Microsoft PPTP client for Windows 2000 3-17

Configuring the Microsoft PPTP client for Windows NT 3-21

Installing the Microsoft PPTP client 3-21

Creating a new phonebook entry for your VPN connection 3-24

Configuring TunnelBuilder for Mac OS 3-29

Remote TunnelBuilder 3-29

LAN TunnelBuilder 3-30

Option: Set up a mail program on your remote computer. 3-31

Creating a new mail account in your mail program 3-31

Creating a new mail account using Netscape Messenger (Communicator 4.0 or later) for Windows . . . 3-31

Creating a new mail account using Netscape Messenger (Communicator 4.0 or later) for Mac OS . . . 3-32

Creating a new mail account using Microsoft Outlook Express 5.0 or later for Windows and Mac OS . . 3-32

Creating a new mail account using Qualcomm Eudora 4.3 or later for Windows. 3-32

Creating a new mail account using Qualcomm Eudora 4.3 or later for Mac OS 3-33

Guidelines for setting up your new mail account 3-33

Chapter 4. Accessing Your Network Using Secure Remote Access

Before you begin	4-1
Using the Microsoft PPTP Clients for Windows 95, 98, 2000, and NT	4-2
Using TunnelBuilder for Mac OS	4-6
Using remote dial-back	4-7

Chapter 5. Managing Secure Remote Access

Viewing information about a remote connection	5-2
Disconnecting a remote computer from your Office network	5-3
Viewing the Remote Users report	5-4

Appendix A. Troubleshooting Secure Remote Access

Important Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to: IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785, U.S.A. IBM is a registered trademark and the e-business logo and IBM Small Business WebConnections are trademarks of International Business Machines Corporation.

Trademarks

IBM is a registered trademark and the e-business logo and IBM Small Business WebConnections are trademarks of International Business Machines Corporation.

InterJet, Whistle Communications, and WhistleWare are either trademarks or registered trademarks of Whistle Communications, an IBM Company.

Apple, Macintosh, Mac, AppleShare, and AppleTalk are registered trademarks of Apple Computer, Inc., registered in the U.S. and other countries.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names mentioned herein may be the trademarks or service names of others.

Legal Statements

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This publication includes information that supports multiple models; therefore, not all text may apply to your model. This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new

editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Year 2000 Compliance Information

This is a Year 2000 Readiness Disclosure.

A product is Year 2000 Ready if the product, when used in accordance with its associated documentation, is capable of correctly processing, providing and/or receiving date data within and between the 20th and 21st centuries, provided all other products (for example, software, hardware, and firmware) used with the product properly exchange date data with it.

This InterJet hardware product has been designed use 32 bits to process 4-digit date information correctly within and between the 20th and 21st centuries, starting at January 1, 1970. This approach allows the correct representation of dates up to 03:14:07, January 19, 2038 (GMT).

This InterJet product cannot prevent errors that might occur if software you use or exchange data with is not ready for the Year 2000. IBM software that comes with this product is Year 2000 Ready.

About This Guide

This guide, the *Secure Remote Access Configuration and User's Guide*, explains how to configure and use the Secure Remote Access feature, which allows users to access your private Office network from remote locations. This guide explains how to configure the Secure Remote Access feature on the InterJet, set up remote computers for Secure Remote Access, and access your network remotely using a remote computer.

This guide assumes that you are familiar with at least *one* of the following operating systems: Microsoft® Windows® 95 or 98, Windows 2000, Windows NT® Workstation 4.0 or a later version, , or Macintosh® System 7.5 or a later version of the Mac® OS.

What This Guide Contains

This guide contains the following information:

- Chapter 1, “Introducing Secure Remote Access,” describes the Secure Remote Access feature, how the feature works, the requirements for using the feature, and the feature’s limitations.
- Chapter 2, “Configuring the InterJet for Secure Remote Access,” explains how to
 - configure the Secure Remote Access feature on the InterJet
 - specify which users can use Secure Remote Access
 - specify when Secure Remote Access is available to remote users
 - determine the InterJet VPN (virtual private network) server name, which users need when setting up their remote computers
- Chapter 3, “Setting Up Your Remote Computer for Secure Remote Access,” explains how to
 - set up a remote Windows 95, 98, 2000, or NT Workstation computer for Secure Remote Access

- obtain instructions for setting up a remote Mac OS computer for Secure Remote Access
- set up a remote mail program to retrieve e-mail messages remotely



Tip: You can provide a photocopy of Chapter 3 to each remote user.

- Chapter 4, “Accessing Your Network Using Secure Remote Access,” explains how to use your remote computer to log in to the InterJet and access network resources.



Tip: You can provide a photocopy of Chapter 4 to each remote user.

- Chapter 5, “Managing Secure Remote Access,” explains how to view information about a remote connection to your network, disconnect a remote computer from your network, and view the Remote Users report.

Typographical Conventions Used in This Guide

This guide uses the following typographical conventions.

Type or Style	Indicates	Example
Bold	An object, command, button, option, or label that appears on a WhistleWare page, a command or option in another program, or the name of a key on the front panel of the InterJet or on your computer's keyboard.	edit
Monospaced font	A file or folder name, URL, screen message, or text that you must type precisely as indicated.	<code>setup.exe</code>
Monospaced italic font	A description of information, or a variable, that you must replace with specific information.	<i>domain_name</i>
Italics	A document name, emphasis, or a new term being defined.	<i>Customer Care Guide</i>

Icons Used in This Guide

The following icons highlight important information:



Note: Calls attention to supplementary or noteworthy information.



Important: Calls attention to important information that helps you to use the InterJet effectively.



Caution: Calls attention to instructions that you must follow to avoid loss of data, damage to the InterJet, or a security risk to your network.



Tip: Provides helpful techniques for using your InterJet and information that enhances your knowledge of the InterJet.

Obtaining Assistance

If, after using this guide, you need further assistance when configuring your InterJet for Secure Remote Access or setting up remote computers, refer to your *Customer Care Guide*. This guide provides information about how to obtain technical assistance using online support resources or by contacting a customer support specialist.

How To Send Comments About This Guide

Your opinion is important to us. If you have comments about this guide, please send e-mail to the following address:

whistledocs@whistle.com.

In your e-mail message, please include this guide's title and either the page number or topic to which your comment applies. Your comments should pertain to the information in this guide or the way in which the information is presented. If you have a technical question, please refer to your *Customer Care Guide* for information about contacting a support specialist.

If you would like a response to your comments, please include your name and contact information in your e-mail message.



Introducing Secure Remote Access

The Secure Remote Access feature is an optional feature for the Whistle InterJet. If you are not sure whether your InterJet has the Secure Remote Access feature, please refer to your service contract.

The Secure Remote Access feature allows up to ten users to simultaneously log in to the InterJet® and access your private Office network from remote locations—such as their homes or remote offices—using computers running Microsoft® Windows® 95 or 98, Windows 2000, Windows NT®, or Mac® OS. Thus, telecommuters and mobile users can access resources on your Office network—for example, Web pages, e-mail messages, and files on the InterJet and other computers—just as they would in your office. The InterJet firewall protects remote computers as though they were clients on your Office network.

The InterJet provides you with much flexibility in managing remote access. You can allow all users or only specific users to access your Office network remotely. You can also specify the times at which remote access is available to remote users. To help you to optimize use of Secure Remote Access, the InterJet provides a Remote Users report showing which users use the feature the most and the durations of their remote connections.

How Secure Remote Access Works

The Secure Remote Access feature uses *virtual private networking* technology, which allows you to create a completely private, secure connection between a remote computer and the InterJet using the communications infrastructure of the public Internet.

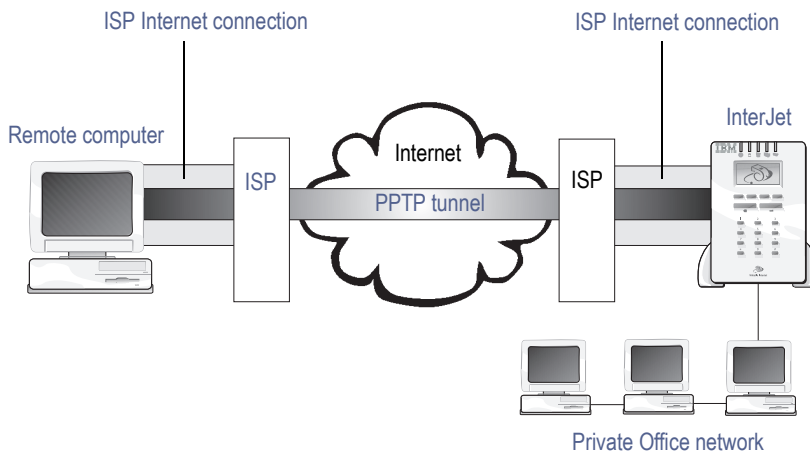
To establish a remote connection, a remote computer and the InterJet use the Point-to-Point Tunneling Protocol (PPTP) to create a private “tunnel” that transports encrypted data across the public Internet. Through this tunnel, users can access your private Office network to view Web pages on your intranet,

retrieve e-mail messages from their InterJet mailboxes, and access files on the InterJet and other computers.

To access your Office network, remote users must first connect to the Internet in either of the following ways:

- through their own Internet service provider (ISP) accounts—such as AT&T WorldNet Service, MCI WorldCom Internet, Earthlink, and so on—which they use for Internet access at home or other locations
- through an ISP Internet connection provided by a remote local area network (LAN), such as a branch office

Once a remote user connects to the Internet, the user then uses a PPTP client program to contact the InterJet virtual private network (VPN) server. The VPN server authenticates the remote user and establishes a secure PPTP tunnel, thereby allowing the remote user to access your private Office network, as shown in the following figure.



Encryption

The InterJet uses the strongest encryption available for remote PPTP connections. In the United States, the InterJet uses either 128-bit encryption or 40-bit encryption, depending on the level of encryption that the remote user's PPTP client program supports. In other countries, the InterJet uses 40-bit encryption.

Requirements

To provide remote access to your private Office network, your service contract must include the Secure Remote Access feature.

Remote computers must be running one of the following operating systems:

- Microsoft Windows 95 or 98
- Microsoft Windows 2000
- Microsoft Windows NT 4.0 or a later version
- Macintosh® System 7.5 or a later version of the Mac OS.

Remote computers must have a PPTP client program installed on them. For details about PPTP clients, see Chapter 3, “Setting Up Your Remote Computer for Secure Remote Access.”

If you want to establish a Secure Remote Access connection between a client computer on a remote LAN—such as a branch office—and the InterJet, the remote network’s firewall must allow PPTP connections to pass through it. Specifically, the firewall must be configured to allow IP protocol number 47 packets to pass through it. If the firewall on the remote network restricts PPTP traffic, you cannot access the InterJet and your Office network from the remote network.

Tunneling Protocol Support

Secure Remote Access supports PPTP (Point-to-Point Tunneling Protocol). It does not currently support L2TP (Layer 2 Tunneling Protocol).

Network Protocol Support

Secure Remote Access supports the following protocols over a PPTP connection:

- TCP/IP (Transmission Control Protocol/Internet Protocol)
- NetBIOS (Network Basic Input/Output System) over TCP/IP and SMB (Server Message Block) over TCP/IP, which provide remote file-sharing services with computers on your network that are running Windows 95 or 98, Windows 2000, or Windows NT

- AFP (Apple Filing Protocol) over TCP/IP, which provides remote file-sharing services with computers on your network that are running either Mac OS 9.0 or later or AppleShare® IP server

Secure Remote Access does *not* currently support other network protocols over a PPTP connection, including:

- Microsoft NetBEUI
- AppleTalk®
- Novell IPX/SPX

Network Operating System Support

If your network is running a network operating system, remote clients must be running the appropriate network client software to access resources on your network. Whistle Communications has verified that the Secure Remote Access feature functions with the following network operating systems running on a TCP/IP LAN:

- Windows NT Server 4.0, with remote clients running Client for Microsoft Networks. This client is included with Windows 95, 98, 2000, and NT.
- AppleShare IP Server 6.3, with remote clients running AppleShare Client 3.7.4 or a later version. This client is included with Mac OS 8.1 and later versions.
- Novell Netware 5.0 or 5.1, with remote clients running Novell Client for Windows 95/98.

For more information about using Secure Remote Access with Novell Netware, please contact your customer support specialist.

Configuring the InterJet for Secure Remote Access

This chapter explains how to configure the InterJet so remote users can log in to the InterJet remotely and access resources on your private Office network.

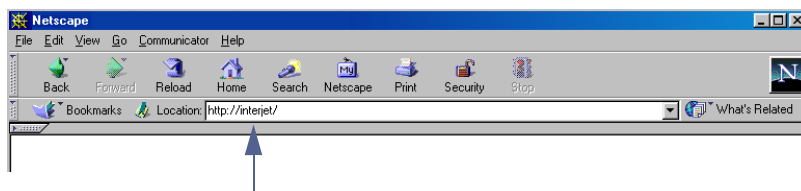


Important: To complete the steps in this chapter, you must log in to the InterJet using an account that has both the System Administrator and Personnel Administrator privileges. If your personal InterJet account does not have these privileges, you can log in to the InterJet using the Administrator, or admin, account.

1 Configure the Secure Remote Access feature.

To configure the Secure Remote Access feature on the InterJet, follow these steps:

- 1 Start your Web browser, then type `interjet` in the **Location** or **Address** box.



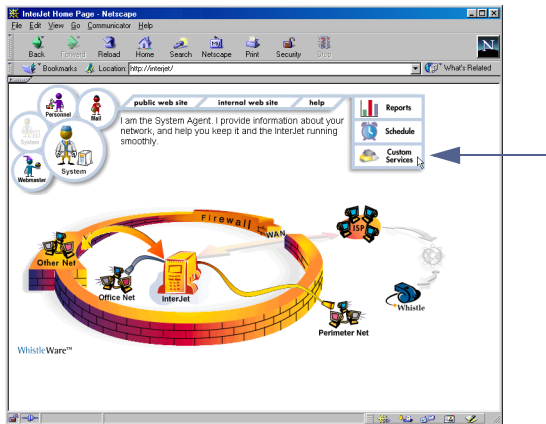
A login dialog box appears.

- 2 Type your InterJet login name and password to log in to the InterJet.



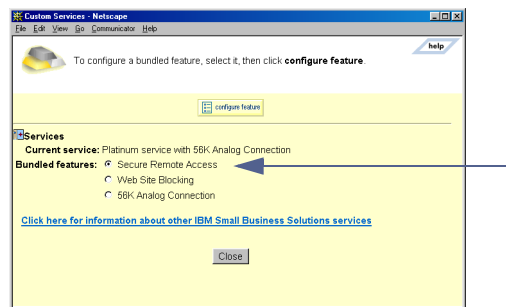
WhistleWare™ starts, and the InterJet home page appears.

- 3 On the InterJet home page, click **Custom Services**.



The Custom Services page appears.

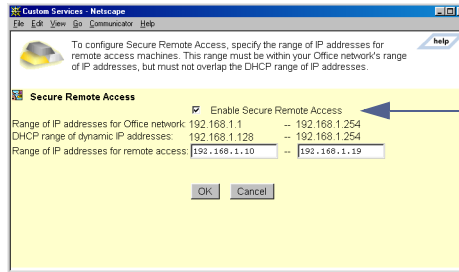
- 4 Under **Bundled features**, click the **Secure Remote Access** option button.



- 5 Click **configure feature** at the top of the page.

The Configure Secure Remote Access page appears.

- 6 To turn on Secure Remote Access, select the **Enable Secure Remote Access** check box.

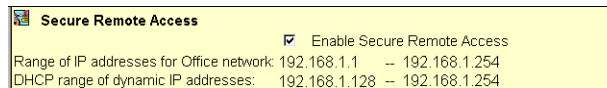


- 7 In the **Range of IP addresses for remote access** boxes, specify the first and last IP addresses in a range of up to ten addresses that you want to reserve for use by remote computers.

Choose any range of up to ten IP addresses, ensuring that the range

- is within the range of IP addresses assigned to your Office network, which appears under **Range of IP addresses for Office network**
- does not overlap with your Office network's DHCP range of dynamic IP addresses

For example, if the range of IP addresses for your Office network and the DHCP range appear as follows:



then you could choose a range of ten addresses *outside* the DHCP range, such as

192.168.1.2 to 192.168.1.11.

In this example, the first three numbers in the IP address are common to all IP addresses on the network, as follows:

192.168.1

The fourth number in the IP address—2 for the first address and 11 for the last address—are the numbers that uniquely identify the first and last computers in the range for remote access.

The IP address 192.168.1.1 is usually reserved for the InterJet itself, so you generally do not include that address in the range.

- 8 Click **OK**.
- 9 Click **Close** to close the Custom Services page.

2 Specify who can use Secure Remote Access.

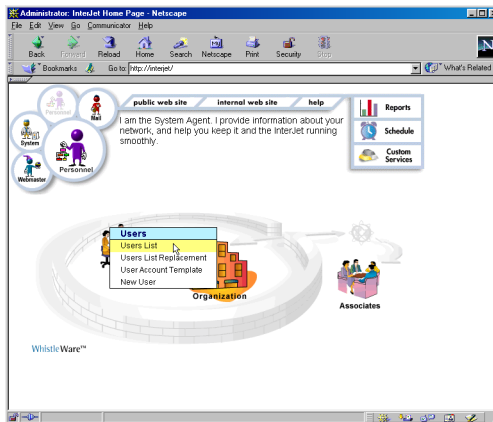
To use Secure Remote Access, users must have the Secure Remote Access privilege enabled for their InterJet accounts. To enable Secure Remote Access for a user's account, follow these steps:

- 1 In the Agent Selector, click **Personnel**.

The Personnel Agent View appears.

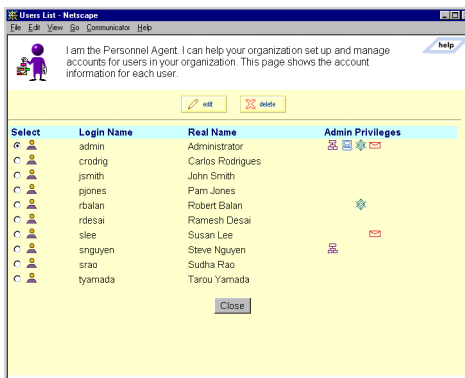
- 2 Point to the **Users** object.

The Users menu appears.

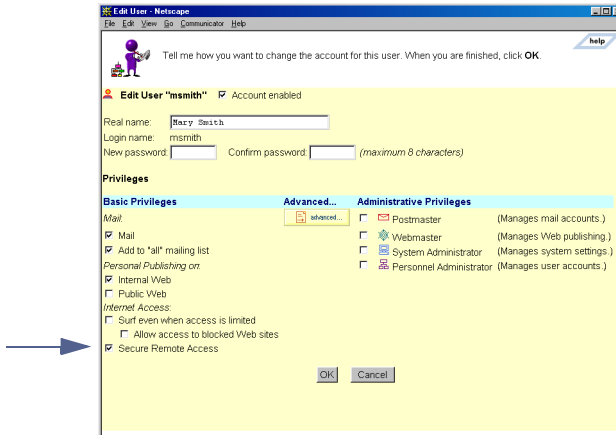


- 3 On the menu, click **Users List**.

The Users List page appears.



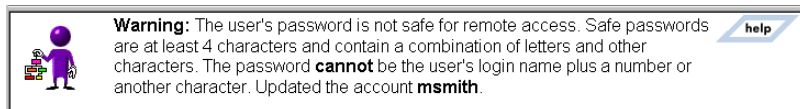
- 4 Under **Select**, click the option button for a user account for which you want to provide the Secure Remote Access privilege.
- 5 Click **edit** at the top of the page.
The Edit User page appears.
- 6 Under **Basic Privileges**, select the **Secure Remote Access** check box.



- 7 Click **OK**.



Caution: If the user's existing InterJet password is not safe for remote access, the following warning message appears in the message area at the top of the Users List page.



If such a message appears, instruct the user to change his or her password so that it is at least four characters and contains at least one character other than a letter, such as a number or symbol. Note that the password *cannot* be the user's login name followed by a number or another character—for example, `msmith1`.

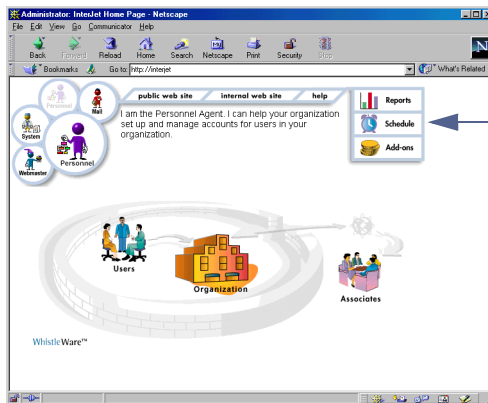
- 8 Repeat steps 3 through 7 for each user account for which you want to assign the Secure Remote Access privilege.
- 9 Once you are finished assigning the Secure Remote Access privilege to user accounts, click **Close** to close the Users List page.

3 Specify when Secure Remote Access is available.

You can use the InterJet Activity Schedule to specify the work periods during which users can access the InterJet and your Office network remotely.

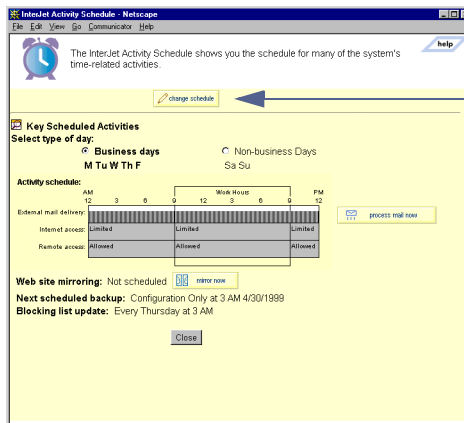
To schedule remote access, follow these steps:

- 1 On the InterJet Home page, click **Schedule**.



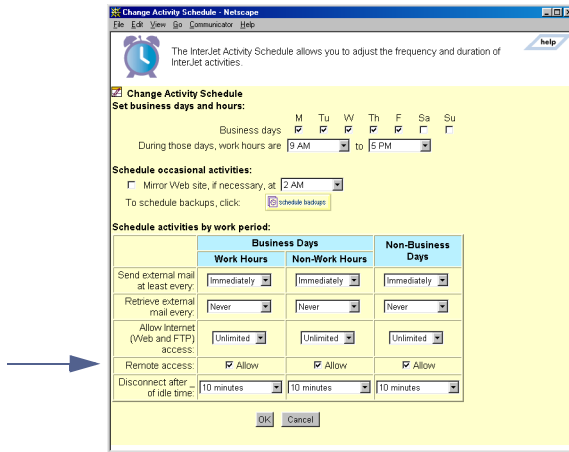
The InterJet Activity Schedule page appears.

- 2 Click **change schedule** at the top of the page.



The Change Activity Schedule page appears.

- Under **Schedule activities by work period**, change the schedule for **Remote access** by selecting or clearing the **Allow** check box for each work period.



Tip: You can change your organization's work periods by selecting new options under **Set business days and hours** at the top of the Change Schedule page.

- Click **OK** to close the Change Activity Schedule page.
- Click **Close** to close the InterJet Activity Schedule page.

4 Option: Turn on remote dial-back.

Remote dial-back allows users who are out of the office to access your network at any time using the Secure Remote Access feature, regardless of whether the InterJet is currently connected to your ISP.

If your InterJet uses a *dial-on-demand* connection to IBM or another ISP—such as a 56K modem or ISDN connection—you can turn on the remote dial-back feature on the InterJet to allow a remote user to establish a connection between the InterJet and your ISP.

If your InterJet uses a *full-time* connection to IBM or another ISP—such as a DSL, cable modem, or leased-line connection—the remote dial-back feature is unnecessary and therefore unavailable. Skip to the next step, “Determine the InterJet VPN server name.” on page 2-9.

Once you turn on remote dial-back, remote users can simply call the telephone number for the telephone line that InterJet uses for your ISP connection, which causes the InterJet to dial your ISP to establish a connection to the Internet. For complete information about using remote dial-back, see “Using remote dial-back” on page 4-7.

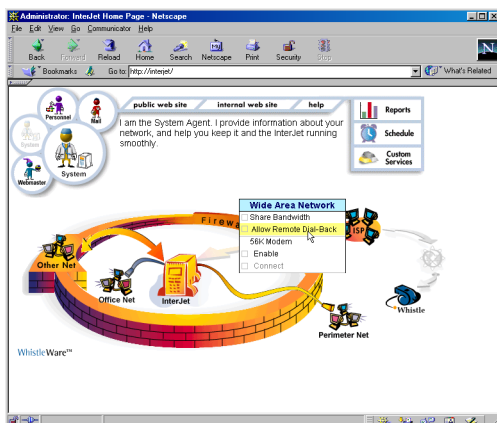
To turn on remote dial-back on the InterJet, follow these steps:

- 1 In the Agent Selector, click **System**.

The System Agent View appears.

- 2 Point to the **WAN** object.

The Wide Area Network menu appears.



- 3 On the menu, click the **Allow Remote Dial-Back** check box.



Tip: Make sure that you provide remote users with the telephone number for the line that the InterJet uses to connect to your ISP—that is, the number for the telephone line to which the InterJet is connected. If you do not know this number, ask your telephone company.

5 Determine the InterJet VPN server name.

To use Secure Remote Access, users must set up their remote computers to establish a remote connection. When setting up their remote computers, users must know the fully qualified domain name (FQDN) for the InterJet virtual private network (VPN) server.

The FQDN for the InterJet VPN server consists of the *primary public name* for the InterJet, followed by your organization's domain name—for example, `interjet.whistle.com`, where

- `interjet` is the primary public name
- `whistle.com` is the organization's domain name

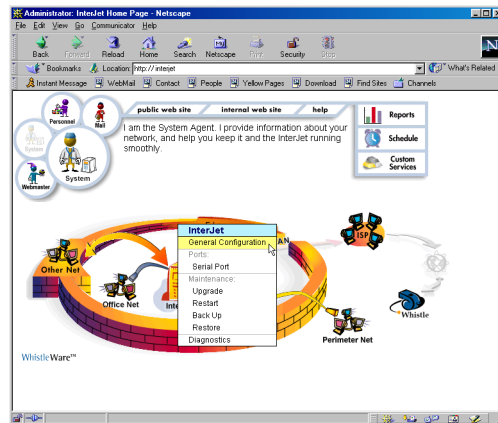
To determine the InterJet primary public name so you can provide remote users with the FQDN for the InterJet VPN server, follow these steps:

- 1 In the Agent Selector, click **System**.

The System Agent View appears.

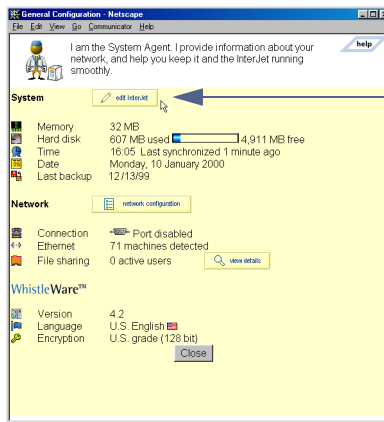
- 2 Point to the **InterJet** object.

The InterJet menu appears.



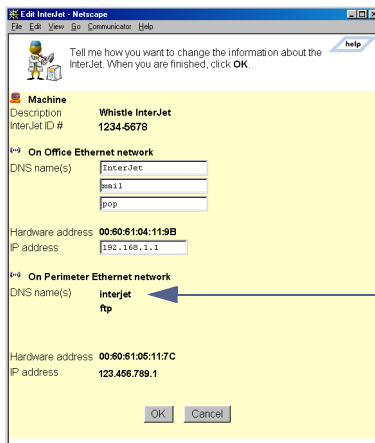
- 3 On the menu, click **General Configuration**.

The General Configuration page appears.

4 Click **edit InterJet**.

The Edit InterJet page appears.

Under **On Perimeter Ethernet network**, the primary public name for the InterJet appears as the *first name* under **DNS name(s)**. IBM or another ISP assigns this name to your InterJet. You cannot change this name.



The primary public name constitutes the first part of the InterJet FQDN, which has the following form:

primary_public_name.your_domain_name

For example, if the primary public name for your InterJet is `public` and your organization's domain name is `whistle.com`, then the FQDN for the InterJet VPN server is `interjet.whistle.com`.

- 5 Write the FQDN for the InterJet VPN server in the box below so you can provide it to users who are setting up their remote computers for Secure Remote Access.

My InterJet VPN server name is:

- 6 Click **OK** to close the Edit InterJet page.
- 7 Click **Close** to close the General Configuration page.

6 For networks running Windows NT Server: Ensure that the InterJet configuration includes NT Server settings.

If your network is running a Windows NT Server, the server may include a Windows Internet Naming Service (WINS) server for name resolution on your network. Because each Windows computer on your network registers its name—called a NetBIOS name—with the WINS server, this server can provide Windows computers with name-to-IP address mappings. These mappings allow Windows computers to display the names of other computers in Network Neighborhood (for Windows 95, 98, and NT) and My Network Places (for Windows 2000), and use other Windows Networking services.

For a Windows computer to discover name-to-IP address mappings, it must send a request over your network. The type of request that your computer sends depends on your WINS server's configuration—called a NetBIOS name server (NBNS) type.

A remote Windows computer must receive the WINS server address and NBNS type from the InterJet; otherwise, a remote user cannot use Network Neighborhood/My Network Places to access computers on your network or use other Windows Networking services. If your InterJet is running a Dynamic Host Configuration Protocol (DHCP) server for your network, the InterJet is usually configured with this information manually during its installation. However, if your NT Server or another machine is running your network's DHCP server, you must ensure that the InterJet is configured with the WINS server's IP address and the NBNS type. For instructions on setting a WINS server IP address and an NBNS type on the InterJet, refer to *Installing the InterJet II*.

For more information about WINS servers and NBNS types, please refer to your Microsoft Windows NT Server documentation.

Next steps . . .

Your InterJet is now ready to provide remote access. To access your private Office network from remote locations, users must first set up their remote computers. See Chapter 3, “Setting Up Your Remote Computer for Secure Remote Access.”



Setting Up Your Remote Computer for Secure Remote Access

This chapter explains how to set up your remote computer so you can log in to the InterJet and access private network resources, such as Web pages, files, and e-mail messages.

Before you begin . . .

Before you begin setting up your remote computer for Secure Remote Access, ensure that you have the following:

- **Internet access:** You must have access to the Internet at your remote location. For example, if you are at home, you must have an individual ISP account for Internet access, such as AT&T WorldNet Service, EarthLink, and so on. If you are at a remote office, and your computer is connected to a network that has access to the Internet, you can use that network's Internet connection when using Secure Remote Access.
- **A PPTP client program:** Your remote computer must have PPTP (Point-to-Point Tunneling Protocol) client program installed on it. This program allows you to create a secure, private connection to your Office network across the Internet. The InterJet works with the following PPTP client programs:
 - **Microsoft VPN Adapter for Windows 95 or 98:** Included with Windows 98. For Windows 95, you may need to obtain the Dial-Up Networking Upgrade, version 1.3 or greater, from the Microsoft Web site:
<http://www.microsoft.com>
 - **Microsoft PPTP client for Windows 2000:** Included with Windows 2000.
 - **Microsoft PPTP client for Windows NT:** Included with Windows NT 4.0 or a later version.

- **NTS TunnelBuilder for Mac OS:** Available from Network Telesystems: <http://www.nts.com>. When setting up TunnelBuilder for Mac OS, please refer to the instructions that Network Telesystems provides. For guidelines to follow when setting up TunnelBuilder, see “Configuring TunnelBuilder for Mac OS” on page 3-29.
- **The InterJet VPN server name:** Your InterJet administrator must provide you with the fully qualified domain name (FQDN) for the InterJet virtual private network (VPN) server. This server name allows your remote computer to identify the InterJet when establishing a Secure Remote Access connection across the Internet. You specify this server name when configuring a PPTP client program on your computer.

My InterJet VPN server name is:

- **Public IP address for the InterJet (for Remote Macintosh computers only):** If your remote Macintosh computer uses a dial-up connection to your ISP, you must obtain the public IP address for the InterJet. TunnelBuilder requires you to specify the IP address for the InterJet VPN server—that is, you cannot specify a FQDN.
 - If your InterJet has a static, or fixed, public IP address, your InterJet administrator can provide you with the address.
 - If your InterJet uses a dynamic IP address, the address may change frequently, so you must determine the IP address each time you want to use Secure Remote Access. To determine this address, you can use a domain name lookup utility, several of which are available on the Internet. Whistle Communications provides a custom domain name lookup utility for Secure Remote Access users, called LookupName. This utility is available at the following URL:

<ftp://ftp.whistle.com/pub/mac>

If you unsure whether your InterJet uses a dynamic IP address, ask your InterJet system administrator.

- **(Optional) The InterJet telephone number:** If your InterJet uses a dial-on-demand connection to your organization's ISP—for example a 56K modem or ISDN connection—you may need the telephone number for the telephone line that the InterJet uses to connect to your ISP. If your InterJet administrator has turned on the remote dial-back feature on the InterJet, you can dial this number to connect the InterJet to the Internet so you can access your network. Ask your InterJet administrator whether you need this number.

My InterJet telephone number is:

1 Windows 95, 98, 2000, or NT users only: Ensure that you can access network resources.

To use Secure Remote Access to access shared resources on your network using a computer running Windows 95, 98, 2000, or NT, you must ensure that your remote computer's name and workgroup or domain settings are compatible with your Office network. If your computer is running Windows 95 or 98, you must also ensure that your Windows login name matches your InterJet login name.

- If you are accessing your network remotely on the *same* portable Windows computer that you also use in the office, you do *not* need to change your computer's name, workgroup, or Windows login settings. Skip to the next step, "Configure a PPTP client program on your remote computer." on page 3-8.
- If you are accessing your network remotely on a *different* Windows computer than the one you use at the office, you may need to change your remote computer's name, workgroup or domain, and Windows login settings to prevent computer name conflicts and to use Network Neighborhood (for Windows 95, 98, and NT) or My Network Places (for Windows 2000).

Preventing computer name conflicts

To prevent name conflicts with Windows computers on your network, you must ensure that your office and remote computers have different names. Windows computers register their names—called NetBIOS names—on a network to identify each other. If both your office and remote computers have the same name, your remote computer cannot register its name on the network, thereby preventing you from accessing network resources.

Using Network Neighborhood/My Network Places

On your remote computer, you can use Network Neighborhood/My Network Places to access shared or private files on the InterJet file server and shared files on other Windows computers on your network. To use Network Neighborhood/My Network Places, you must ensure that your remote computer and the InterJet reside in the same workgroup or NT domain. If you do not know the workgroup for the InterJet, either check the workgroup setting on the computer that you use at the office, or ask your InterJet administrator.



Important: If your remote computer is running Windows 95 or 98, you must log in to Windows or Microsoft Networking using your InterJet login name to access shared or private storage space on the InterJet file server. If your Windows or Microsoft Networking password and your InterJet password are not the same, the InterJet asks you to provide your password whenever you attempt to access the file server using Network Neighborhood/My Network Places.

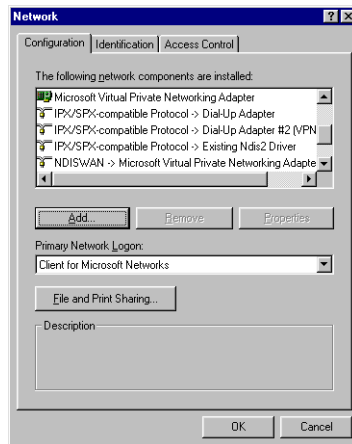
Changing your computer's name or workgroup

To change the name or workgroup for your remote computer, follow these steps, as appropriate for your computer's operating system:

Windows 95 or 98

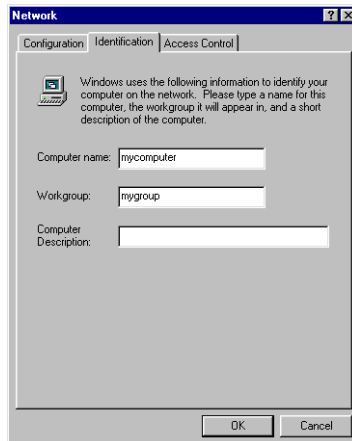
- 1 On your computer's desktop, double-click **My Computer**.
- 2 Double-click **Control Panel**.
- 3 Double-click **Network**.

The Network dialog box appears.



- 4 Click the **Identification** tab.

The Identification dialog box appears.



- 5 Option: In the **Computer name** box, type a new name for your computer.
- 6 In the **Workgroup** box, type the workgroup for your Office network.
- 7 Click **OK**.

Windows 2000

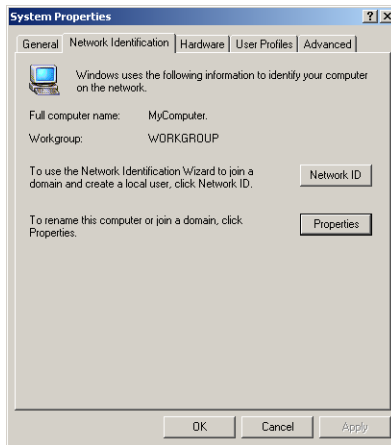
- 1 On your computer's desktop, double-click **My Computer**.

- 2 Click **Network and Dial-up Connections** on the left.

The Network and Dial-up Connections window appears.

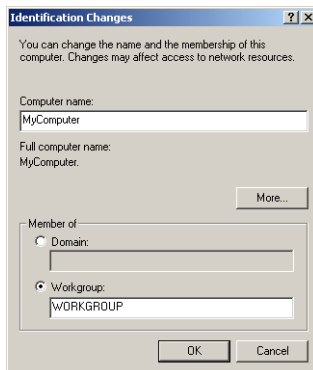
- 3 Click **Network Identification** on the left.

The System Properties dialog box appears.



- 4 Click **Properties**.

The Identification Changes dialog box appears.



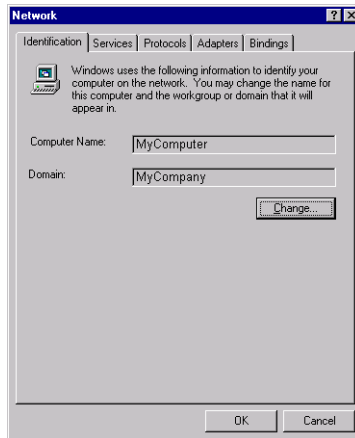
- 5 Option: In the **Computer Name** box, type a new name for your computer.

- 6 Under **Member of**, select either **Workgroup** or **Domain name**, as appropriate for your Office network, then type the domain or workgroup name in the box.
- 7 Click **OK**.

Windows NT

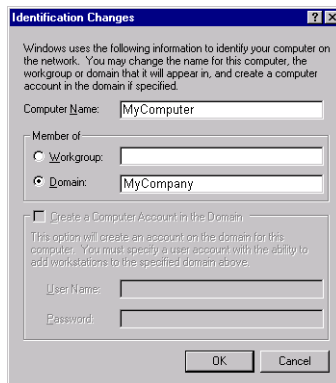
- 1 On your computer's desktop, double-click **My Computer**.
- 2 Double-click **Control Panel**.
- 3 Double-click **Network**.

The Network dialog box appears.



- 4 Click **Change**.

The Identification Changes dialog box appears.



- 5 Option: In the **Computer Name** box, type a new name for your computer.
- 6 Under **Member of**, select either **Workgroup** or **Domain name**, as appropriate for your Office network, then type the NT domain or workgroup name in the box.
- 7 Click **OK**.

2 Configure a PPTP client program on your remote computer.

Your remote computer must have one of the following PPTP (Point-to-Point Tunneling Protocol) clients installed on it:

- Microsoft VPN Adapter for Windows 95 or 98
- Microsoft PPTP client for Windows 2000
- Microsoft PPTP client for Windows NT
- NTS TunnelBuilder for Mac OS

For information about obtaining these clients, see “Before you begin . . .” on page 3-1.

A PPTP client on your remote computer allows you to access all InterJet services, including:

- files in the dropbox and your personal folder on the InterJet file server
- e-mail messages in your mailbox on the InterJet mail server
- Web pages on your intranet

You can also access files on other computers and all network resources that use TCP/IP, including printers and other devices.

To configure a PPTP client on computer running this operating system...	Follow the instructions in this section...
Windows 95 or 98	"Configuring the Microsoft VPN Adapter for Windows 95 or 98" on page 3-10
Windows 2000	"Configuring the Microsoft PPTP client for Windows 2000" on page 3-17
Windows NT	"Configuring the Microsoft PPTP client for Windows NT" on page 3-21
Mac OS	"Configuring TunnelBuilder for Mac OS" on page 3-29

Configuring the Microsoft VPN Adapter for Windows 95 or 98

To set up a remote Windows 95 or 98 computer for Secure Remote Access, first verify that the Microsoft VPN Adapter is installed on your computer, then create a new VPN dial-up connection.

Verifying that the Microsoft VPN Adapter is installed on your computer

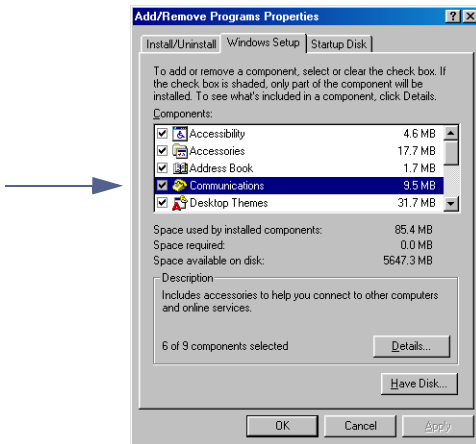
- 1 On your computer's desktop, double-click **My Computer**.
- 2 Double-click the Control Panel folder, then double-click **Add/Remove Programs**.

The Add/Remove Programs Properties dialog box appears.

- 3 Click the **Windows Setup** tab.

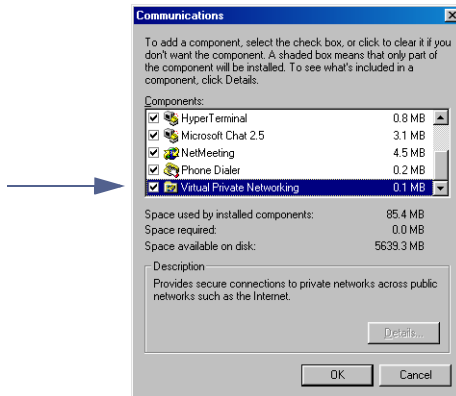
The Window Setup dialog box appears.

- 4 In the list of components, double-click **Communications**.



The Communications dialog box appears.

- 5 In the list of components, locate the **Virtual Private Networking** component and ensure that its check box is selected. If the check box is clear, select it.



- 6 Click **OK** to return to the Windows Setup dialog box.
- 7 Click **OK** to close the Windows Setup dialog box.



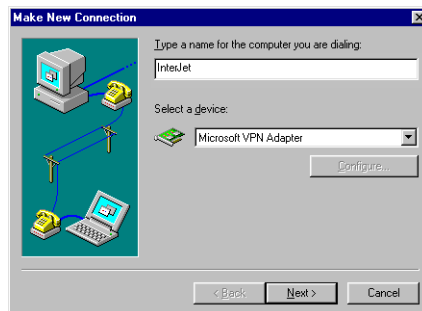
Important: If you selected the **Virtual Private Networking** check box, you must restart your computer to finish installing the component.

Creating a new VPN connection

- 1 On your computer's desktop, double-click **My Computer**.
- 2 Double-click **Dial-Up Networking**.

If you have *not* already created any dial-up networking connections for your computer, the Make New Connection Wizard starts automatically.

- 3 Double-click **Make New Connection** to start the Make New Connection Wizard.



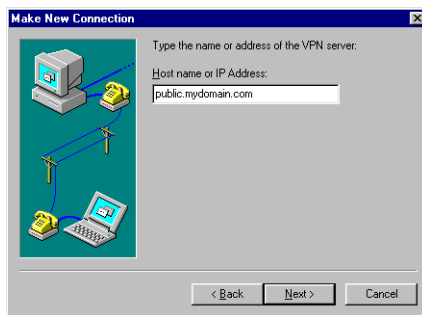
- 4 Type a description for your VPN connection in the **Type a name for the computer you are dialing** box.

For example, type InterJet, the name of your company, or a general description such as Office Connection.

- 5 In the **Select a device** drop-down list, select **Microsoft VPN Adapter**, then click **Next**.
- 6 Type the fully qualified domain name (FQDN) for the InterJet VPN server in the **Host name or IP Address** box.

For example, type `interjet.mycompany.com`.

Your InterJet administrator provides you with this server name. For more information about the VPN server name, see “Before you begin . . .” on page 3-1.



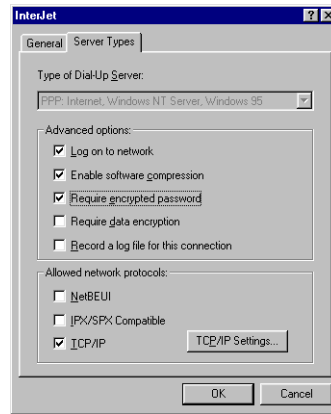
- 7 Click **Next**.
- 8 Click **Finish**.

A new icon for the VPN connection that you just created appears in the Dial-Up Networking folder. Depending on the name you chose for your connection, the icon might appear as follows:



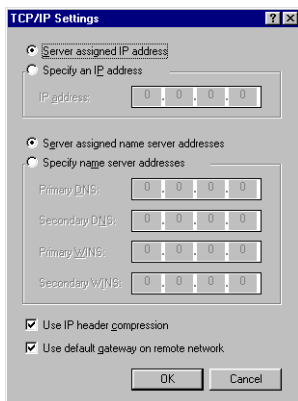
- 9 Right-click the icon for the VPN connection, then select **Properties**.
The dialog box for your VPN connection appears.
- 10 Click the **Server Types** tab.

The Server Types dialog box appears.



- 11 In the Server Types dialog box, select *only* the following check boxes:
 - **Log on to network**
 - **Enable software compression**
 - **Require encrypted password**
 - **Require data encryption** (the InterJet always encrypts your data, regardless of whether you select this option)
 - **TCP/IP**
- 12 Clear the **NetBEUI** and **IPX/SPX Compatible** check boxes. Secure Remote Access does not support NetBEUI or IPX/SPX over a PPTP connection.
- 13 Click **TCP/IP Settings**.

The TCP/IP Settings dialog box appears.
- 14 Ensure that *only* the following options are selected:
 - **Server assigned IP address**
 - **Server assigned name server addresses**
 - **Use IP header compression**
 - **Use default gateway on remote network**



- 15 Click **OK** to close the TCP/IP Settings dialog box.
- 16 Click **OK** to close the dialog box for your VPN connection.

Verifying that network components are installed on your computer.

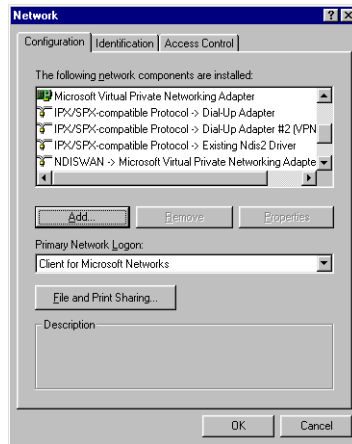
Once you have set up your VPN connection for Secure Remote Access, Whistle Communications recommends that you verify that all the required network components are installed on your Windows 95 or 98 computer.

Your remote computer must have all the components for the Microsoft VPN Adapter, Dial-Up Networking, and file sharing. If your remote computer requires an Ethernet connection—for example, if it uses a DSL or cable modem to connect to your ISP or it is connected to an Ethernet network at a remote office—your computer must also have an appropriate Ethernet adapter.

To verify that all the required network components are installed on your remote computer, follow these steps:

- 1 On your computer's desktop, double-click **My Computer**.
- 2 Double-click **Control Panel**.
- 3 Double-click **Network**.

The Network dialog box appears.



4 Under **The following network components are installed**, verify that the following components appear:

- Client for Microsoft Networks or another network client, as appropriate for your network

This component allows you to use Network Neighborhood for file sharing. If this component does not appear, click **Add** to install it. For complete instructions on installing a network client, refer to Windows Help.

- Dial-Up Adapter
- Dial-Up Adapter #2 (VPN Support)
- Microsoft Virtual Private Networking Adapter
- TCP/IP -> Dial-Up Adapter
- TCP/IP -> Dial-Up Adapter #2 (VPN Support)
- NDISWAN -> Microsoft Virtual Private Networking Adapter
- an Ethernet adapter, if your remote computer uses a DSL or cable modem to connect to your ISP or it is connected to an Ethernet network at a remote office



Note: If any of the VPN (virtual private networking) components do not appear, re-install the Microsoft VPN Adapter, as described in “Configuring the Microsoft VPN Adapter for Windows 95 or 98” on page 3-10.

- 5 If you did not make any changes to the network components, click **Cancel** to close the Network dialog box.

Once you have configured a VPN connection for Secure Remote Access and verified that all the required network components are installed on your computer, you can log in to the InterJet and access your private Office network. For instructions on logging in to the InterJet and accessing your network, see “Using the Microsoft PPTP Clients for Windows 95, 98, 2000, and NT” on page 4-2.

Configuring the Microsoft PPTP client for Windows 2000

Microsoft pre-installs the PPTP client for Windows 2000. Follow these steps to configure the client for a VPN connection:

- 1 On your computer's desktop, double-click **My Computer**.
- 2 Click **Network and Dial-up Connections** on the left.
- 3 In the Network and Dial-up Connections window, double-click **Make New Connection**.

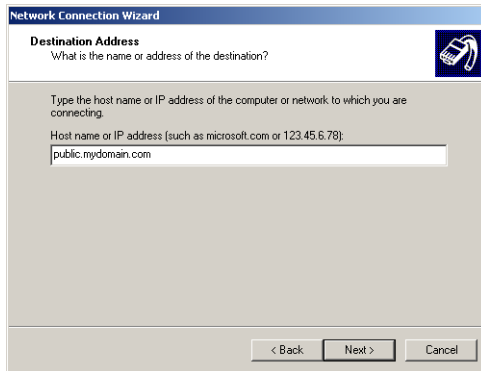
The Network Connection Wizard starts.



- 4 Click **Next**.
- 5 Click **Connect to private network through the Internet**, then click **Next**.
- 6 If you have already created a dial-up networking connection to an ISP, do one of the following:
 - If you want to use your dial-up networking connection to access the Internet when using Secure Remote Access, click **Automatically dial this initial connection**. Then, in the drop-down list, select the dial-up connection you use to access the Internet
 - If you do not want to use your dial-up networking connection to access the Internet when using Secure Remote Access, click **Do not dial this initial connection**.
- 7 Click **Next**.
- 8 Type the fully qualified domain name (FQDN) for the InterJet VPN server in the **Host name or IP Address** box.

For example, type `interjet.mycompany.com`.

Your InterJet administrator provides you with this server name. For more information about the VPN server name, see “Before you begin . . .” on page 3-1.



- 9 Click **Next**.
- 10 Click **Only for myself**, then click **Next**
- 11 Type a description for your VPN connection in the **Type the name you want to use for this connection** box.

For example, type InterJet, the name of your company, or a general description such as Office Connection.

- 12 Click **Finish**.

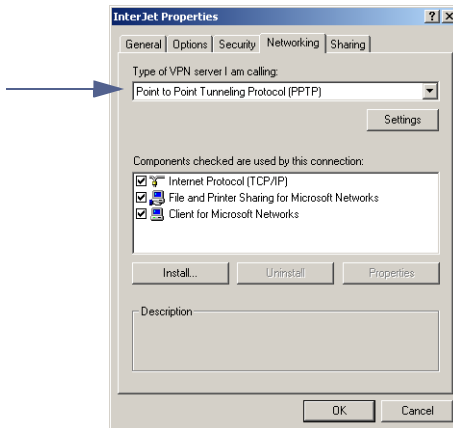
A new icon for the VPN connection that you just created appears in the Network and Dial-up Connections folder. Depending on the name you chose for your connection, the icon might appear as follows:



InterJet

- 13 Right-click the icon for the VPN connection, then select **Properties**.
The Properties dialog box for your VPN connection appears.
- 14 Click the **Networking** tab.

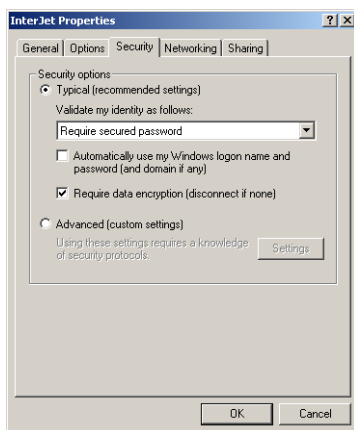
- 15** In the **Type of VPN server I am calling** drop-down list, select **Point-to-Point Tunneling Protocol (PPTP)**.



- 16** Under **Components checked are used by this connection**, ensure that the following components appear and that their check boxes are selected:
- **Internet Protocol (TCP/IP)**
 - **Client for Microsoft Networks** or another network client, as appropriate for your network
- This component allows you to use My Network Places for file sharing. If this component does not appear, click **Add** to install it. For complete instructions on installing a network client, refer to Windows Help.
- Option: **File and Printer Sharing for Microsoft Networks**
- 17** Click the **Security** tab.
- 18** Ensure that the following options are selected:
- **Typical (recommended settings)** is selected and that
 - **Required secured password**, in the **Validate my identity as follows** drop-down list



Note: Do not select **Automatically use my Windows logon name and password**, unless they are the same as your InterJet login name and password.



19 Click **OK**.

Configuring the Microsoft PPTP client for Windows NT

To create a VPN connection, you must first install the Microsoft PPTP client on your computer, then configure the client.



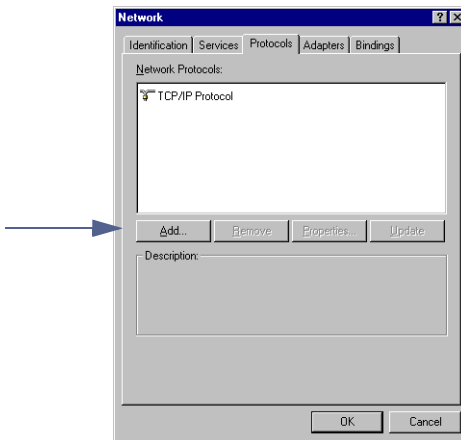
Note: Your computer must be running NT 4.0 with Service Pack 4 or a later version. During the installation process, you may need your Windows NT CD-ROM to install PPTP on your computer.

Installing the Microsoft PPTP client

- 1 On your computer's desktop, double-click **My Computer**.
- 2 Double-click Control Panel.
- 3 Double-click **Network**.

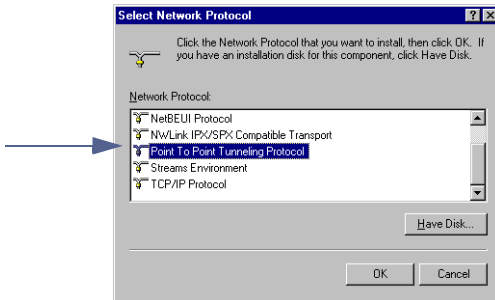
The Network dialog box appears.

- 4 Click the **Protocols** tab, then click **Add**.



The Select Network Protocol dialog box appears.

5 Select **Point-to-Point Tunneling Protocol**.



6 Click **OK**.

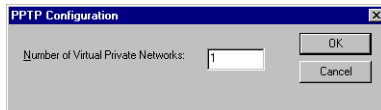
The Windows NT Setup dialog box appears.

7 Specify the location of your Windows NT installation files. You may need to insert your Windows NT CD-ROM into your computer's drive.

8 Click **Continue**.

The system installs the PPTP files on your computer, then the PPTP Configuration dialog box appears.

9 In the **Number of Virtual Private Networks** box, type 1, then click **OK**.

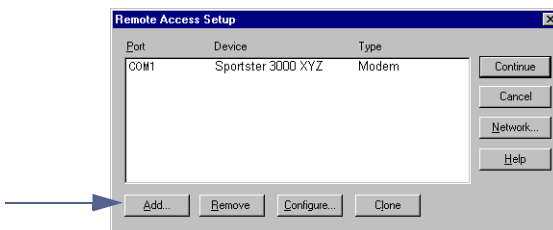


A dialog box appears, informing you that RAS set up will be invoked.

10 Click **OK**.

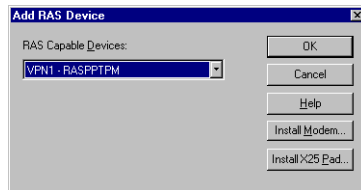
The Remote Access Setup dialog box appears.

11 Click **Add**.



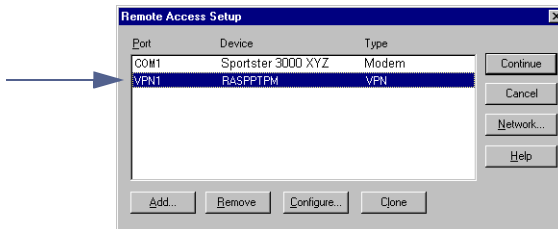
The Add RAS Device dialog box appears.

- 12 Select **VPN1-RASPPTPM**.



- 13 Click **OK** to return to the Remote Access Setup dialog box.

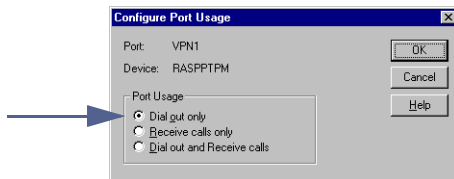
- 14 Under **Port**, select **VPN1**.



- 15 Click **Continue**.

The Configure Port Usage dialog box appears.

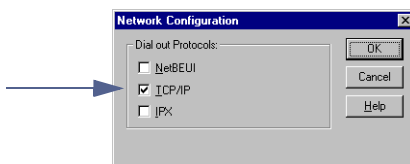
- 16 Ensure that the **Dial out only** button is selected and that no other options are selected, then click **OK** to return to the Remote Access Setup dialog box.



- 17 Click **Network**.

The Network Configuration dialog box appears.

- 18 Under **Dial-out Protocols**, select the **TCP/IP** check box. Ensure that all other check boxes are clear.



- 19 Click **OK** to return to the Remote Access Setup dialog box.

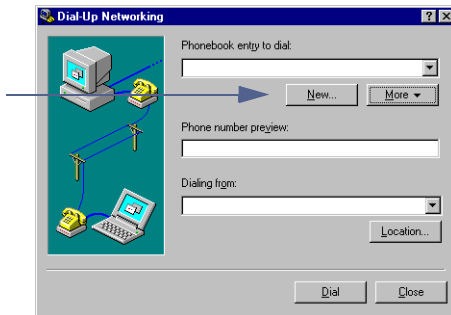
- 20 Click **Continue** to display the Network dialog box.
- 21 Click **Close**.
- 22 Restart your computer.

Creating a new phonebook entry for your VPN connection

- 1 Double-click **My Computer**.
- 2 Double-click **Dial-Up Networking**.

If this is your first phonebook entry, the Dial-Up Networking dialog box appears. Click **OK**.

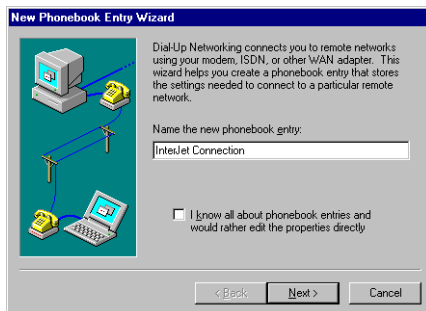
- 3 Click **New**.



The New Phonebook Entry Wizard starts.

- 4 Type a description for your VPN connection in the **Name the new phonebook entry** box.

For example, type **InterJet**, the name of your company, or a general description such as **Office Connection**.



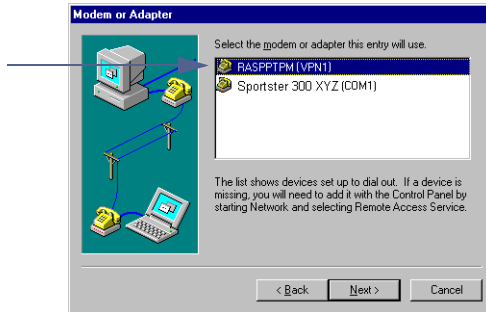
- 5 Click **Next**.

The Server dialog box appears.

- 6 Ensure that all option check boxes are clear, then click **Next**.

The Modem or Adapter dialog box appears.

- 7 In the **Select the modem or adapter this entry will use** drop-down list, select **RASPPTPM(VPN1)**.



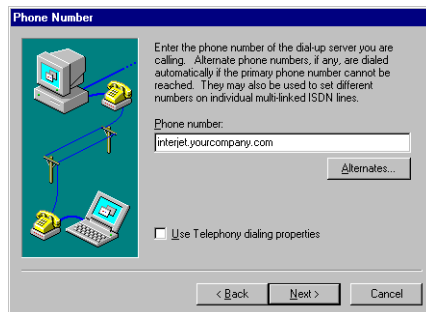
- 8 Click **Next**.

The Phone Number dialog box appears.

- 9 Type the fully qualified domain name (FQDN) for the InterJet in the **Phone number** box.

For example, type `interjet.mycompany.com`.

Your InterJet administrator provides you with this server name. For more information about the VPN server name, see “Before you begin . . .” on page 3-1.



- 10 Click **Next**.
- 11 Click **Finish** to return to the Dial-Up Networking dialog box.

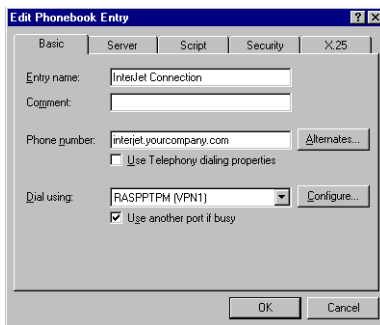
- 12 Under **Phonebook entry to dial**, select the PPTP phonebook connection that you just created, then click **More** to display a drop-down list.



- 13 Click the **Edit entry and modem properties**.

The Edit Phonebook Entry dialog box appears.

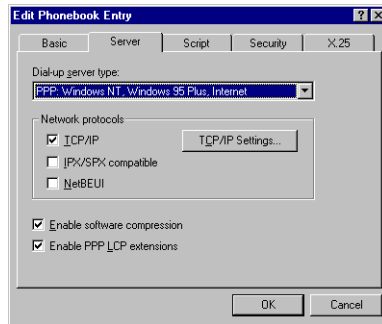
- 14 On the **Basic** tab, verify that
 - the FQDN for the InterJet VPN server is specified correctly in the **Phone number** box
 - **RASPPMP(VPN1)** is selected in the **Dial using** drop-down list



- 15 Click the **Server** tab.

- 16 In the Server Types dialog box, do the following
 - Verify that **PPP, Windows NT, Windows 95 Plus, Internet** appears in the **Dial-up server type** drop down list.
 - Under **Network protocols**, select **only TCP/IP**. If necessary, clear the **NetBEUI** and **IPX/SPX Compatible** check boxes. Secure Remote Access does not support NetBEUI or IPX/SPX over a PPTP connection.

- Ensure that the **Enable software compression** check box is selected.

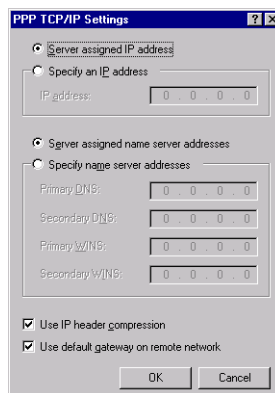


- 17 Click **TCP/IP Settings**.

The PPP TCP/IP Setting dialog box appears.

- 18 Ensure that *only* the following options are selected:

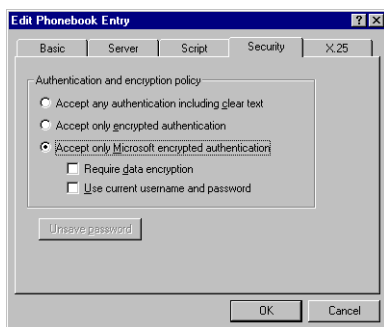
- **Server assigned IP address**
- **Server assigned name server addresses**
- **Use IP header compression**
- **Use default gateway on remote network**



- 19 Click **OK**.
- 20 Click the **Security** tab.
- 21 Select **Accept only Microsoft encrypted authentication**.

You can also select the **Require data encryption** check box; however, the InterJet always encrypts your data regardless of whether you select this option.

Ensure that the **Use current user name and password** check box is clear.



- 22** Click **OK** to close the dialog box for your PPTP phonebook entry.

Once you have configured the VPN connection for Secure Remote Access, you can access your InterJet and its Office network. For instructions on logging in to your InterJet and network, see “Using the Microsoft PPTP Clients for Windows 95, 98, 2000, and NT” on page 4-2.

Configuring TunnelBuilder for Mac OS

Install and configure TunnelBuilder for Mac OS by following the instructions that Network Telesystems provides. When configuring TunnelBuilder, follow the guidelines in the following sections to ensure that you can log in to the InterJet VPN server and access your Office network. If you have questions about configuring TunnelBuilder, please contact Network Telesystems technical support.

Remote TunnelBuilder

Configure the Remote TunnelBuilder component if you use an analog modem or ISDN connection to your ISP.

- **MacTCP or TCP/IP control panel:** Specify any required information about your own ISP dial-up account.
- **Network or AppleTalk control panel:** You need not configure this control panel because Secure Remote Access currently does not support AppleTalk over a PPTP connection.
- **NTS PPP Dialer:** On the **Account** tab, specify information about your own ISP dial-up account. On the **Modem** tab, specify information about your computer's modem. On the **DNS** tab, in the **Use DNS Addresses** pull-down menu, click **As determined by PPP negotiations**. On the **Misc.** tab, ensure that the **Attempt to negotiate for AppleTalk** check box is clear.
 - If your InterJet has a *static IP address*, do the following: In the VPN Settings dialog box, specify the IP address for the InterJet VPN server and your InterJet login name and password. Specify the *same* InterJet login name and password that you use at the office to access the InterJet. For the VPN protocol, specify **PPTP**.
 - If your InterJet uses a *dynamic IP address*, do the following: On the **Misc.** tab, clear the **Start virtual private network after connecting** check box. In the VPN Settings dialog box, type 1 . 1 . 1 . 1 for the VPN server IP address. This address is a placeholder, which you replace once you look up the actual IP address with a domain name lookup utility. In the VPN settings dialog box, specify your InterJet login name and password. Specify the *same* InterJet login name and password that you use at the office to access the InterJet. For the VPN protocol, specify **PPTP**.

LAN TunnelBuilder

Configure the LAN TunnelBuilder component if you use a DSL or cable modem connection to your ISP, or you are a guest on a remote network that has Internet access.

- **TCP/IP control panel:** Specify any required information about your own ISP dial-up account.
- **Network or AppleTalk control panel:** You need not configure this control panel because the Secure Remote Access currently does not support AppleTalk over a PPTP connection.
- **LAN TunnelBuilder Settings control panel:** For the VPN protocol, specify **PPTP**. For the VPN server address, specify the fully qualified domain name (FQDN) for the InterJet VPN server. For the VPN user name and password, specify your InterJet login name and password, respectively. Specify the *same* InterJet login name and password that you use at the office to access the InterJet.

3 Option: Set up a mail program on your remote computer.

You can use Secure Remote Access to retrieve your e-mail messages from your mailbox on the InterJet mail server. Depending on the remote computer that you are using, you may need to set up a mail program to retrieve your messages:

- If you are using Secure Remote Access to retrieve e-mail messages on the *same* portable computer that you also use at the office, you can use the same InterJet mail account as you use at the office. No further setup of your mail program is necessary.
- If you are using Secure Remote Access to retrieve e-mail messages on a *different* computer than the one you use at the office, you must create a *new* mail account for your InterJet mail using your remote computer's mail program. This new account tells your remote mail program where to retrieve your mail on the InterJet.

Alternatively, you can change the settings for an existing mail account. However, doing so would require you to change the settings back to their original values to retrieve mail sent to the existing account.

Creating a new mail account in your mail program

The following instructions explain how to create a new mail account on your remote computer using Netscape Messenger (Netscape Communicator 4.0 or later), Microsoft Outlook Express 5.0 or later, or Qualcomm Eudora Email 4.3 or later. For information about creating a new mail account using another mail program, refer to your mail program's manual or Help, and follow the guidelines in the section "Guidelines for setting up your new mail account" on page 3-33.

Creating a new mail account using Netscape Messenger (Communicator 4.0 or later) for Windows

- 1 On your computer's desktop, click **Start**, then point to **Programs**.
- 2 Point to **Netscape Communicator**, then point to **Utilities**.
- 3 Click **User Profile Manager**.

The Profile Manager program appears.

- 4 Click **New**.

- 5 Follow the instructions on the screen to set up a new profile for retrieving your remote mail. When specifying information, refer to the section “Guidelines for setting up your new mail account” on page 3-33.

Creating a new mail account using Netscape Messenger (Communicator 4.0 or later) for Mac OS

- 1 Run Netscape Communicator.
The Netscape Communicator Profiles dialog box appears.
- 2 Click **Manage Profiles**.
- 3 Click **New**.
The New Profile Setup program runs.
- 4 Follow the instructions on the screen to set up a new profile for retrieving your remote mail. When specifying information, refer to the section “Guidelines for setting up your new mail account” on page 3-33.

Creating a new mail account using Microsoft Outlook Express 5.0 or later for Windows and Mac OS

- 1 Run Outlook Express.
- 2 On the **Tools** menu, click **Accounts**.
The Internet Accounts dialog box appears.
- 3 Ensure that the **Mail** tab is selected, then click **New**.
 - **Windows:** The Internet Connection Wizard runs.
 - **Mac OS:** The Account Setup Assistant runs.
- 4 Follow the instructions on the screen to set up a new account for retrieving your remote mail. When specifying information, refer to the section “Guidelines for setting up your new mail account” on page 3-33.

Creating a new mail account using Qualcomm Eudora 4.3 or later for Windows

The following instructions apply to the Eudora Pro and Sponsored modes only. Eudora Light mode does not support multiple mail accounts.

- 1 Run Eudora.
- 2 On the **Tools** menu, click **Personalities**.
The Personalities window appears on the left.
- 3 Right-click anywhere in the Personalities window.

- 4 On the menu that appears, click **New**.
The New Account Wizard runs.
- 5 Follow the instructions on the screen to set up a new account for retrieving your remote mail. When specifying information, refer to the section “Guidelines for setting up your new mail account” on page 3-33.

Creating a new mail account using Qualcomm Eudora 4.3 or later for Mac OS

The following instructions apply to the Eudora Pro and Sponsored modes only. Eudora Light mode does not support multiple mail accounts.

- 1 Run Eudora.
- 2 On the **Windows** menu, click **Personalities**.
The Personalities window appears on the left.
- 3 Click **New**.
A new personality icon appears.
- 4 Type a name for the personality, then press **Enter**.
- 5 Ensure that the new personality icon is selected, then click **Edit**.
The Settings dialog box appears.
- 6 Specify information in the dialog box to set up a new account for retrieving your remote mail. When specifying information, refer to the section “Guidelines for setting up your new mail account” on page 3-33.

Guidelines for setting up your new mail account

When specifying options for your new mail account in your remote mail program, follow these guidelines:

- **Specifying your e-mail address:** Specify the same e-mail address that you use at the office. This address usually has the following form:
your_login_name@your_organization.com
- **Specifying whether to use POP or IMAP for the incoming mail server:** The InterJet mail server supports both POP (Post Office Protocol) and IMAP (Internet Mail Access Protocol). If you choose POP, your mail program downloads your e-mail messages from the server to your personal computer. If you choose IMAP, your mail program does not download messages to your computer, but instead allows you to access and manipulate e-mail messages on the mail server. If you are not sure which server protocol to use, choose

POP. You can change your selection at any time. For more information about choosing a server protocol and specifying protocol options, refer to your mail program's manual or Help.

- **Specifying your mail server:** Specify the InterJet mail server as *both* the outgoing mail (SMTP) server and the incoming mail (POP or IMAP) server. Your InterJet mail server name usually has the following form:

`interjet.your_organization_name.com`



Tip: If you do not know your InterJet mail server's name, check the settings for your mail account in the mail program that you use at the office.

- **Specifying your login name (user name) and password for the mail server:** Specify your InterJet login name and password to log in to the InterJet mail server. Specify the *same* InterJet login name and password that you use at the office to access your e-mail messages. Your login name is the first part of your e-mail address, which appears before the @ symbol.

If your mail program does not provide an option for specifying a password for your account on the mail server, the InterJet mail server will ask you to provide the password when you attempt to retrieve your mail.

- **Specifying authentication options:** For the new mail account, you do not need to specify any authentication options for the InterJet mail server. Because your remote computer is behind the InterJet firewall when you use Secure Remote Access, the InterJet mail server does not require any authentication methods other than your providing your InterJet password.
- **Specifying whether to leave your e-mail messages on the mail server:** If you selected POP rather than IMAP for the incoming mail server protocol, specify that your remote mail program leave, or store, copies of your messages on the InterJet mail server, rather than deleting messages when downloading them from the server. Otherwise, any messages that you retrieved remotely are not available on the server once you return to your office. Refer to your mail program's manual or Help for information about how to leave, or store, your messages on the mail server.



Important: If you have a separate, personal mail account with your ISP, you may use your remote mail program to retrieve e-mail messages sent to that account. If, when using Secure Remote Access, you attempt to reply to such a message, your mail program may display an error message. This message usually indicates that your mail server rejected the recipient's e-mail address and that relaying was denied. To avoid this problem, you can do *either* of the following:

- **Option 1:** Set up another mail account in your mail program, and use this account to reply to any e-mail messages sent to your personal mail account. When setting up the account, specify the following:
 - your ISP's mail server as the incoming (POP) mail server
 - the InterJet as the outgoing (SMTP) mail server
 - the e-mail address that you use with your personal mail account as the sender's e-mail address
 - **Option 2:** When you reply the message, use the account that you normally use to send and receive your InterJet mail. However, the recipient of your reply may see your InterJet e-mail address as the sender of the message—*not* the e-mail address that you use with your personal mail account.
-



Accessing Your Network Using Secure Remote Access

This chapter explains how to log in to the InterJet and access your private Office network using Secure Remote Access.

Before you begin . . .

Before you use Secure Remote Access to access your Office network, ensure that you have the following:

- **Internet access:** To use Secure Remote Access, you must have access to the Internet, using either an individual Internet service provider (ISP) account or Internet access provided on a remote network, such as a branch office.
- **One of the following PPTP client programs:**
 - Microsoft VPN Adapter for Windows 95 or 98
 - Microsoft PPTP client for Windows 2000
 - Microsoft PPTP client for Windows NT Workstation
 - Network Telesystems TunnelBuilder for Mac OS

For information about configuring these client programs, see Chapter 3, “Setting Up Your Remote Computer for Secure Remote Access.”

- **A safe password:** When you use your PPTP client program to access your network remotely, you must provide your InterJet password. Your password must be at least four characters and contain at least one character other than a letter, such as a number or symbol.

For information about changing your InterJet password, look up “password, changing” in the InterJet Help Index, or ask your InterJet administrator.

Using the Microsoft PPTP Clients for Windows 95, 98, 2000, and NT

If you use a *dial-up networking* connection to access the Internet through your own ISP account—for example, using a 56K modem—you must use two dial-up networking connections simultaneously to log in to the InterJet and access your Office network remotely, as follows:

- First, access the Internet using your own ISP dial-up networking connection. For example, if you have a personal ISP account that you use at home, you must *first* access the Internet using that account.
- Once you access the Internet, use your VPN connection—which you created using either the Microsoft VPN Adapter or PPTP client for Windows NT, as appropriate—to log in to the InterJet.



Note: If you configured a VPN connection using Windows 2000, the connection automatically dials your ISP before attempting to log in to the InterJet.

If you use a *full-time* connection to access the Internet through your own ISP account, you need to use *only* your VPN connection to log in to the InterJet and access your Office network remotely. You usually use a full-time connection to the Internet if your remote computer is connected to one of the following:

- a DSL modem
- a cable modem
- an “always on” ISDN line
- a local area network (LAN) that has access to the Internet—for example, a branch office

To log in to the InterJet and access your network, follow these steps:

- 1 Ensure that the InterJet is accessible.

If your InterJet uses a dial-on-demand connection to your organization’s ISP—for example, a 56K modem or ISDN connection—the InterJet may not be connected to the ISP when you attempt to access your network remotely. To ensure that the InterJet is accessible, you can use the remote dial-back feature on the InterJet. See “Using remote dial-back” on page 4-7.
- 2 If you are using a mobile computer that you also use at the office, clear any IP address information that your computer retains, as follows:
 - a Click **Start**, then click **Run**.

- b** In the **Open** box, do one of the following:
 - For Windows 95 or 98:** Type `winipcfg`. In the dialog box that appears, click **Release All**, then click **OK**.
 - For Windows NT or 2000:** Type `ipconfig /release`.
 - 3** If you use a dial-up networking connection to access the Internet, connect to your ISP using that connection, as follows:
 - For Windows 95 or 98:**
 - a** Double-click the Dial-up Networking icon for your ISP connection
 - b** In the Connect to dialog box, click **Connect**.
 - For Windows NT:**
 - a** Double-click the **Dial-up Networking** icon.
 - b** In the Dial-Up Networking dialog box, in the **Phonebook entry to dial** drop-down list, select the phonebook entry for your ISP connection.
 - c** Click **Dial**.
-  **Important:** Your computer must be connected to the Internet before you can run your PPTP client program to log in to the InterJet and access your private network.
- For Windows 2000:** If you configured your VPN connection to first dial your ISP before connecting to the InterJet, skip to the next step.
- 4** Run the VPN connection that you created using the Microsoft VPN Adapter for Windows 95 or 98, PPTP client for Windows 2000, or PPTP client for Windows NT, as follows:
 - For Windows 95 or 98:** Double-click the Dial-up Networking icon for your VPN connection. The Connect To dialog box appears.
 - For Windows 2000:** In the Network and Dial-up Connections window, double-click the icon for your VPN connection.
 - For Windows NT:** In the Dial-Up Networking dialog box, in the **Phonebook entry to dial** drop-down list, select the phonebook entry for your VPN connection.
- 5** Do one of the following, as appropriate for your computer's operating system:

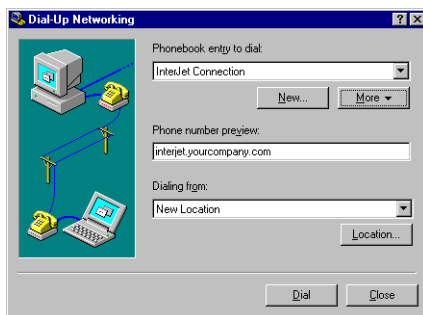
For Windows 95 or 98: Type your InterJet login name and password, then click **Connect**.



For Windows 2000: Type your InterJet login name and password, then click **Connect**.



For Windows NT: Click **Dial**, then type your InterJet login name and password.



Your computer logs in to the InterJet.



Note: If you are unable to log in to the InterJet, the maximum number of remote users may already be online. Secure Remote Access supports up to ten remote users at once.

Once you establish the Secure Remote Access connection, you can

- access files on the InterJet, such as files in the dropbox, using Windows Network Neighborhood (for Windows 95, 98, and NT) or My Network Places (for Windows 2000), a Web browser, or an FTP (File Transfer Protocol) client program
- access files on computers on your network that have file sharing enabled, using Windows Network Neighborhood/My Network Places
- access your e-mail messages using a mail program
- view Web pages on your intranet using a Web browser
- use network resources, such as printers and other devices that support TCP/IP

Using TunnelBuilder for Mac OS

If you are using NTS TunnelBuilder for Mac OS, please refer to the instructions that Network Telesystems provides. If you have questions about using TunnelBuilder, please contact Network Telesystems technical support.



Note: If your remote Macintosh computer uses a dial-up connection to your ISP— and your InterJet uses a dynamic IP address—you must first access the Internet using the NTS Dialer. Once you connect to the Internet, you must use a domain name lookup utility to determine the public IP address for the InterJet. A custom domain name lookup utility for Secure Remote Access users, called LookupName, is available at the following URL:

`ftp://ftp.whistle.com/pub/mac`

Once you determine the InterJet IP address, specify that address for the VPN server address in the NTS Dialer, then click **Connect**.

Once you establish the Secure Remote Access connection, you can do the following:

- Access files on the InterJet, such as files in the dropbox, using a Web browser or an FTP (File Transfer Protocol) client program.

To use a Web browser to access files on the InterJet, type `ftp://interjet.your_domain_name` in your browser's **Location** or **Address** box. If you use Netscape Communicator, you can use your browser's **Upload File** option in the **File** menu to upload files to the dropbox or your personal folder on the InterJet.



Important: You cannot use the Chooser on your remote Macintosh computer to access files on the InterJet.

- Access files on other computers running either Mac OS 9.0 or later that have the File Sharing option turned on or AppleShare IP server, using the Chooser.



Important: Secure Remote Access does not support AppleTalk over the remote connection. Therefore, computers and devices on your private network do not appear in the list of devices in the Chooser. To use the Chooser on your remote Macintosh computer to access files residing on a computer running either Mac OS 9.0 or later or AppleShare IP server, you must specify either the computer's IP address or its DNS (Domain Name

Service) name on the InterJet. If you do not know the IP address or DNS name of a computer on your network, ask your InterJet administrator.

- Access your e-mail messages using a mail program.
For information about setting up a remote mail program, see “Option: Set up a mail program on your remote computer.” on page 3-31.
- View Web pages on your intranet using a Web browser.
- Use network resources, such as printers and other devices that support TCP/IP.

Using remote dial-back

If your InterJet uses a dial-on-demand connection to IBM or another ISP and your InterJet administrator has turned on remote dial-back, you can use this option to ensure that the InterJet is accessible for remote access. Remote dial-back allows you to reliably establish a connection between the InterJet and the ISP at any time from a remote location.

To use remote dial-back, follow these steps:

- 1** From your InterJet administrator, obtain the telephone number for the line that your InterJet uses for its ISP connection.
- 2** Dial the InterJet telephone number.
- 3** After one ring, hang up.

The InterJet dials your organization's ISP and establishes a connection. You can now access the InterJet remotely.

Managing Secure Remote Access

If you have the System Administrator privilege, you can do the following to manage remote access to your Office network:

- **Change the times during which remote access is available:** You can allow or disallow remote access during your organization's work periods, using the InterJet Activity Schedule. For more information about scheduling Secure Remote Access, see "Specify when Secure Remote Access is available." on page 2-6.
- **View information about a remote connection:** You can view information such as a remote computer's IP address, a remote user's name, and the duration of a remote connection.
- **Disconnect a remote computer from your Office network:** At any time, you can use the System Agent to disconnect a remote computer from your Office network. Once you disconnect a remote computer, the remote user no longer has access to resources on your network.
- **View the Remote Users report:** The Remote Users report shows you which remote users accessed the InterJet the most. It also shows the average duration of remote access connections to the InterJet for each remote user per day, during the current or previous month. This information can help you to determine whether to restrict remote access during certain work periods for all users or individual users.

If you have the Personnel Administrator privilege, you can specify which users have remote access to your network by assigning the Secure Remote Access privilege to their InterJet accounts. For more information about assigning this privilege to a user's account, see "Specify who can use Secure Remote Access." on page 2-4.

Viewing information about a remote connection

To view information about a remote connection, follow these steps:

- 1 In the Agent Selector, click **System**.

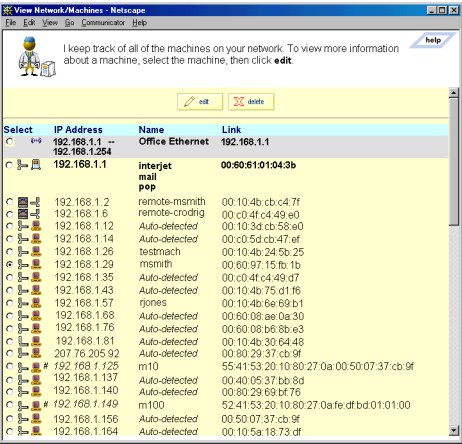
The System Agent View appears.

- 2 Point to the **Office Net** object.

The Office Network menu appears.

- 3 On the menu, click **Network/Machines List**.

The View Network/Machines page appears.



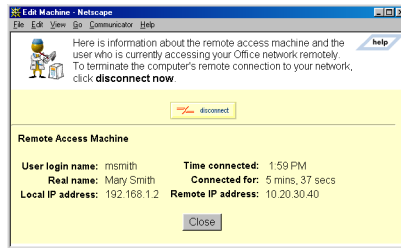
- 4 In the list of networks and machines, click the option button for the remote computer for which you want to view information.

The following icon identifies remote computers:



- 5 Click **edit**.

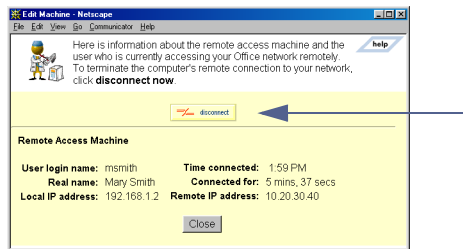
The Edit Remote Access Machine page appears, showing information about the remote connection.



Tip: For descriptions of the items on the page, click **help** at the top of the page.

Disconnecting a remote computer from your Office network

To disconnect a remote computer from your Office network at any time, follow the steps in “Viewing information about a remote connection” on page 5-2. On the Edit Remote Access Machine page, click **disconnect now**.



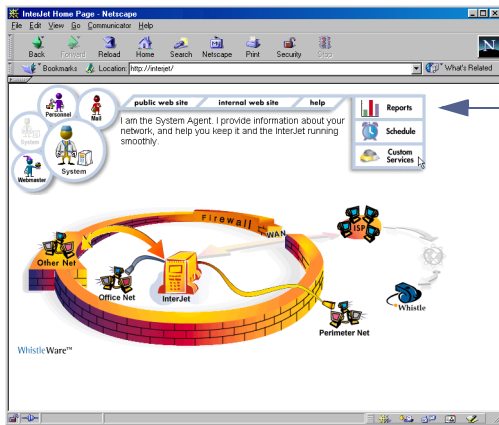
Viewing the Remote Users report

Data for the Remote Users Report is available only during work periods for which remote access is set to **Allow** in the InterJet Activity Schedule.

When viewing the report, you can export the report data to a text file as comma-separated values (CSVs), which you can then import into a spreadsheet or database program.

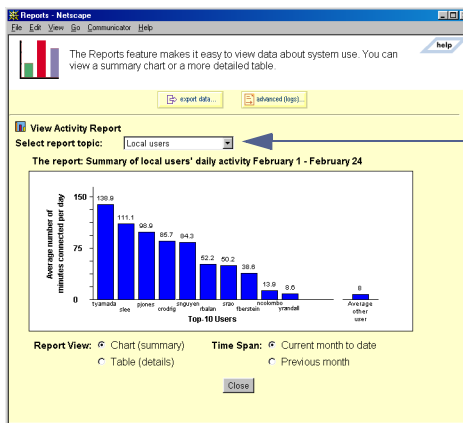
To view the Remote Users Report, follow these steps:

- 1 On the InterJet home page, click **Reports**.



The Reports page appears.

- 2 Under **Select report topic**, click **Remote users**.



The Remote Users Report appears, showing the chart view for the current month by default.

The chart view shows the ten remote users who spent the most time connected to the InterJet, and the average number of minutes that each of these users was connected to the InterJet per day. The chart also shows the average duration of remote access connections for all other users combined.

- 3 Option: To display the table view, under **Report view**, click **Table (details)**.

The more detailed table view shows the average number of minutes that each remote user was connected to the InterJet per day. The table displays the remote users' login names in alphabetical order.

- 4 Option: To display the report for the previous month, under **Time span**, click **Previous month**.

- 5 Option: To export report data to a text file that you can import into a database or spreadsheet program, follow these steps:

- a Click **export data**.

- b If your browser asks you what you want to do with the text file, specify that you want to save it to your computer's hard disk.

A dialog box appears, showing the default name for the file as `report.data`.

- c Specify the location at which to save the text file.

- d Click **OK** in the dialog box.

The InterJet formats the data in the text file as comma-separated values (CSVs). Most database and spreadsheet programs support this format.

- 6 When you have finished viewing the report, click **Close**.



Troubleshooting Secure Remote Access

The following table provides solutions to some common problems that you may encounter when attempting to

- access your Office network using Secure Remote Access
- use Windows Network Neighborhood (for Windows 95, 98, and NT) or My Network Places (for Windows 2000) to access machines on your network

Problems with accessing your network remotely

Possible Cause	Solution
Your remote PPTP (Point-to-Point Tunneling Protocol) client program is not configured properly.	Ensure that you follow the instructions in Chapter 3, "Setting Up Your Remote Computer for Secure Remote Access." Also refer to the configuration instructions that came with your PPTP program. Your PPTP client program must specify the fully qualified domain name (FQDN) for the InterJet.
The maximum number of remote users have already logged in to the InterJet. Secure Remote Access supports up to ten remote users at once.	Try logging in to the InterJet at a later time.
Your InterJet uses a dial-on-demand connection to your ISP, and the InterJet is not connected to your ISP when you attempted to log in to the InterJet remotely.	A System Administrator can allow users to establish a connection between the InterJet and the ISP from a remote location, at any time, using remote dial-back. For instructions on connecting the InterJet to the ISP remotely, see "Using remote dial-back" on page 4-7.

Problems with accessing your network remotely (continued)

Possible Cause	Solution
The password for your InterJet user account is not safe for remote access. You cannot log in to the InterJet remotely using an unsafe password.	Change the password for your user account on the InterJet to a safe password. Safe passwords consist of at least four characters, and have a combination of letters and at least one number or other character. The password cannot contain your InterJet login name. For instructions on changing your password, look up “password, changing” in the InterJet Help Index.
You are attempting to access your network from another, remote network—for example, a branch office—but the remote network’s firewall does not allow PPTP connections to pass through it.	Ask the administrator for the remote network to configure the network’s firewall to allow PPTP connections, which use IP protocol number 47, to pass through it.

Problems with using Network Neighborhood/My Network Places

Possible Cause	Solution
Your remote computer does not have a unique name.	Ensure that your remote computer does not have the same name as another computer on your network. To change the name of your remote computer, follow the instructions in “Changing your computer’s name or workgroup” on page 3-4.”
Your remote computer is not in the same workgroup as that of the InterJet and other machines on your network.	Ensure that your remote computer is in the same workgroup as that of the InterJet and other machines on your network. To change the workgroup in which your remote computer resides, follow the instructions in “Changing your computer’s name or workgroup” on page 3-4.”
Your remote computer does not have an appropriate network client installed on it.	Ensure that your remote computer has the appropriate networking client software—such as Client for Microsoft Networks—installed on it. For information about verifying whether your computer has a network client, see “Verifying that network components are installed on your computer.” on page 3-14.

Problems with using Network Neighborhood/My Network Places (continued)

Possible Cause	Solution
Other Windows computers on your network are not set up properly for file sharing.	Ensure that the appropriate client computers on your Office network are set up for file sharing on a network. To provide file-sharing services, a Windows computer must have the appropriate networking client software—such as Client for Microsoft Networks—installed on it.
Your remote Windows computer cannot communicate with other computers on your network.	To communicate with each other, your remote computer and the computers on your Office network must share the same network address and netmask. A netmask determines which part of a computer's IP address identifies the network address. The Microsoft implementation of PPTP—which Secure Remote Access uses—does not allow configuration of your network's netmask. Instead, PPTP on your remote computer assumes that your network is using one of the following standard, or "natural," netmasks, depending on the IP address it receives from the InterJet: ➤ IP address: 0 . x . x . x - 127 . x . x . x Standard netmask 255 . 0 . 0 . 0 (netmask width 8) ➤ IP address: 128 . 0 . x . x - 191 . 255 . x . x Standard netmask 255 . 255 . 0 . 0 (netmask width 16) ➤ IP address: 192 . 0 . 0 . x - 223 . 255 . 255 . x Standard netmask 255 . 255 . 255 . 0 (netmask width 24) To solve this problem, you must ensure that your Office network uses a standard netmask, as appropriate for your network's address. Refer to InterJet Help for instructions on viewing and changing the netmask for your Office network. In addition, you must ➤ change the range of IP addresses available for DHCP ➤ change the range of IP addresses available Secure Remote Access ➤ restart DHCP client machines on your network ➤ reconfigure any machines that use a static IP address with an appropriate IP address and netmask Whistle Communications recommends that only individuals who are familiar with network addressing perform these tasks.



110 Marsh Drive
Foster City, CA 94404
U.S.A.